IBM Security QRadar

Adapterkonfigurationshandbuch

September 2016

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen unter „Bemerkungen" auf Seite 57 lesen.

Produktinformation

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security QRadar, Adapter Configuration Guide September 2016,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
TSC Germany
Kst. 2877
November 2016

Inhaltsverzeichnis

Einführung in die Konfiguration von Adaptern für QRadar Risk Manager

IBM® Security QRadar Risk Manager ist eine Appliance für die Überwachung der Einheitenkonfiguration, die Simulation von Änderungen an Netzumgebungen und die Priorisierung von Risiken und Schwachstellen. QRadar Risk Manager verwendet zur Integration mit Ihren Netzeinheiten Adapter.

Zielgruppe

Netzadministratoren, die für die Installation und Konfiguration von Adaptern zuständig sind, müssen mit den Konzepten der Netzsicherheit und der Einheitenkonfiguration vertraut sein.

Technische Dokumentation

Wenn Sie im Web nach der Produktdokumentation zu IBM Security QRadar einschließlich der gesamten übersetzten Dokumentation suchen möchten, rufen Sie das IBM Knowledge Center auf (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Informationen zum Zugriff auf weitere technische Dokumentationen in der QRadar-Produktbibliothek finden Sie unter Accessing IBM Security QRadar Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Kontaktierung der Kundenunterstützung

Informationen zur Kontaktierung der Kundenunterstützung finden Sie im Dokument Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden gesetzlichen Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter schützen.

Bitte beachten:

Bei der Nutzung dieses Programms muss ggf. eine Reihe von Gesetzen und Bestimmungen beachtet werden, einschließlich solcher, die sich auf den Datenschutz, die Datensicherheit, arbeitsrechtliche Angelegenheiten sowie die elektronische Kommunikation und die Speicherung beziehen. IBM Security QRadar darf nur für legale Zwecke eingesetzt und nur auf legale Weise verwendet werden. Der Kunde verpflichtet sich, dieses Programm gemäß geltendem Recht, geltenden Regelungen und Richtlinien zu verwenden und übernimmt die gesamte Verantwortung für die Einhaltung dieser Bestimmungen. Der Lizenznehmer gewährleistet, dass er alle für eine rechtmäßige Verwendung von IBM Security QRadar erforderlichen Einwilligungen, Berechtigungen oder Lizenzen eingeholt bzw. erworben hat oder einholen bzw. erwerben wird.

Kapitel 1. Übersicht über Adapter

Über Adapter wird IBM Security QRadar Risk Manager mit Ihren Netzeinheiten integriert. Über die passenden Adapter kann QRadar Risk Manager die Konfigurationsparameter von Netzeinheiten (z. B. Firewalls, Router und Switches) abfragen und importieren.

Netztopologie und Konfiguration

QRadar Risk Manager verwendet zur Erfassung von Netzkonfigurationen Adapter. Diese Adapter konvertieren die Konfigurationsdaten in ein für die unterstützten Einheitenmodelle, Hersteller und Typen einheitliches Format. Die Daten benötigt QRadar Risk Manager zum Verständnis Ihrer Netztopologie und der Konfiguration Ihrer Netzeinheiten.

Zum Verbinden externer Einheiten mit dem Netz muss QRadar Risk Manager auf die Einheiten zugreifen können. QRadar Risk Manager verwendet die in QRadar konfigurierten Benutzerberechtigungsnachweise für den Zugriff auf die Einheiten und zum Herunterladen der Konfigurationen.

Integration von Netzeinheiten

Führen Sie zur Integration von Netzeinheiten mit QRadar Risk Manager die folgenden Schritte aus:

1. Konfigurieren Sie die Netzeinheit für die Kommunikation mit QRadar Risk Manager.
2. Installieren Sie den Adapter für Ihre Netzeinheit auf Ihrer QRadar Risk Manager-Appliance.
3. Fügen Sie Ihre Netzeinheiten in Configuration Source Management zu QRadar Risk Manager hinzu.
4. Definieren Sie das Netzprotokoll für die Kommunikation mit Ihren Netzeinheiten.

   Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Adaptertypen

IBM Security QRadar Risk Manager unterstützt verschiedene Adaptertypen.

Die folgenden Adapter werden unterstützt:

- F5 BIG-IP
- Check Point SecurePlatform Appliances
- Check Point Security Management Server
- Cisco Catalyst (CatOS)
- Cisco Internet Operating System (IOS)
- Cisco Nexus
- Cisco Security Appliances
- Fortinet FortiOS
- HP Networking ProVision

- Juniper Networks ScreenOS
- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto
- Sourcefire 3D-Sensor
- Generisches SNMP
- TippingPoint IPS
- McAfee Sidewinder

Kapitel 2. Adapter installieren

Sie müssen die Adapterdateien in Ihre IBM Security QRadar SIEM-Konsole laden und sie anschließend nach IBM Security QRadar Risk Manager kopieren.

Vorbereitende Schritte

Nach der Einrichtung einer einleitenden Verbindung ist die QRadar SIEM-Konsole die einzige Einheit, die direkt mit QRadar Risk Manager kommunizieren kann.

Vorgehensweise

1. Melden Sie sich über SSH als Rootbenutzer auf Ihrer QRadar SIEM-Konsole an.
2. Laden Sie die komprimierte Datei für QRadar Risk Manager-Adapter von Fix Central (www.ibm.com/support/fixcentral/) auf Ihre QRadar SIEM-Konsole herunter.
3. Um die komprimierte Datei aus Ihrer QRadar SIEM-Konsole in QRadar Risk Manager zu kopieren, geben Sie den folgenden Befehl ein:

   `scp` *`Adapter`*`.zip root@`*`IP-Adresse`*`:`

   Die Option *IP-Adresse* ist die IP-Adresse oder der Hostname von QRadar Risk Manager.

   Beispiel:

   ```
   scp adapters.bundle-2014-10-972165.zip root@100.100.100.100:
   ```
4. Geben Sie auf Ihrer QRadar Risk Manager-Appliance das Kennwort für den Rootbenutzer ein.
5. Melden Sie sich von Ihrer QRadar SIEM-Konsole über SSH als Rootbenutzer auf Ihrer QRadar Risk Manager-Appliance an.
6. Um die Adapter zu entpacken und zu installieren, geben Sie folgende Befehle aus dem Stammverzeichnis ein, das die komprimierte Datei enthält:

   `unzip` *`Adapter`*`.zip`

   ```
   yum install -y adapters*.rpm
   ```

   Beispiel:

   ```
   unzip adapters.bundle-2014-10-972165.zip
   yum install -y adapters*.rpm
   ```

   Anmerkung:

   Bei älteren QRadar Risk Manager-Versionen als V.7.2.8 wird der Befehl **`rpm`** verwendet.

   Beispiel:

   ```
   rpm -Uvh adapters*.rpm
   ```
7. Geben Sie für den Neustart der Services für den ziptie-Server und zum Abschluss der Installation folgenden Befehl ein:

   ```
   service ziptie-server restart
   ```

   Wichtig: Durch den Neustart der Services für den ziptie-Server werden zurzeit aktive Einheitenbackups in Configuration Source Management unterbrochen.

Adapter deinstallieren

Verwenden Sie zum Entfernen eines Adapters aus IBM Security QRadar Risk Manager den Befehl **yum**.

Vorgehensweise

1. Melden Sie sich über SSH als Rootbenutzer auf der IBM Security QRadar SIEM-Konsole an.
2. Geben Sie zum Deinstallieren eines Adapters folgenden Befehl ein:

   `yum remove -y` *`Adapterpaket`*

   Beispiel: `yum remove -y adapters.cisco.ios-2011_05-205181.noarch`

   Anmerkung:

   Bei älteren QRadar Risk Manager-Versionen als V.7.2.8 wird der Befehl **rpm** verwendet.

   Beispiel:

   `rpm -e` *`Adapterdatei`*

   `rpm -e adapters.cisco.ios-2011_05-205181.noarch.rpm`

Kapitel 3. Methoden zum Hinzufügen von Netzeinheiten

Fügen Sie Netzeinheiten in Configuration Source Management zu IBM Security QRadar Risk Manager hinzu.

In der folgenden Tabelle werden die Methoden zum Hinzufügen von Netzeinheiten beschrieben.

Tabelle 1. Methoden zum Hinzufügen einer Netzeinheit zu QRadar Risk Manager

Methode	Beschreibung
Add Device (Einheit hinzufügen)	Fügt eine Einheit hinzu.
Discover Devices (Einheiten erkennen)	Fügt mehrere Einheiten hinzu.
Discover From NSM (Von NSM erkennen)	Fügt von der Juniper Networks NSM-Konsole verwaltete Einheiten hinzu.
Discover Check Point SMS (Von Check Point SMS erkennen)	Fügt von einem Check Point Security Manager Server (CPSMS) verwaltete Einheiten hinzu.
Discover From SiteProtector (Von SiteProtector erkennen)	Fügt Einheiten von SiteProtector hinzu.
Discover From Defense Center (Von Defense Center erkennen)	Fügt Einheiten von Sourcefire Defense Center hinzu.

Netzeinheit hinzufügen

Zum Hinzufügen einer Netzeinheit zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

Vorbereitende Schritte

Lesen Sie zunächst, welche Softwareversionen unterstützt, welche Berechtigungsnachweise benötigt und welche Befehle für Ihre Netzeinheiten verwendet werden. Weitere Informationen finden Sie in Kapitel 5, „Unterstützte Adapter", auf Seite 17.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer Einheit ein und klicken Sie auf **Hinzufügen**.

      Sie können eine IP-Adresse, einen IP-Adressbereich, ein CIDR-Teilnetz oder einen Platzhalter eingeben.

      Wenn Sie einen Platzhalter verwenden möchten, geben Sie ein Format wie das Folgende ein: `10.1.*.*`

Wenn Sie eine CIDR verwenden möchten, geben Sie ein Format wie das Folgende ein: `10.2.1.0/24`.

Einschränkung: Geben Sie Einheitenadressen, die bereits in anderen Netzgruppen vorkommen, nicht ein zweites Mal in Configuration Source Management ein.

c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.

d. Wiederholen Sie die vorangegangenen zwei Schritte für jede IP-Adresse, die Sie hinzufügen möchten.

6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).

   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.

   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie die angefragten Parameterwerte ein.

   In der folgenden Tabelle werden die Parameter beschrieben.

Tabelle 2. Parameter für die Berechtigungsnachweise

Parameter	Beschreibung

Benutzername	Ein gültiger Benutzername für die Anmeldung beim Adapter.
	
	Für Adapter ist für den Benutzernamen und das Kennwort Zugriff auf verschiedene Dateien, wie die folgenden, erforderlich:
	
	`rule.C`
	
	`objects.C`
	
	`implied_rules.C`
	
	`Standard.PF`

Kennwort	Das Kennwort für die Einheit.
Kennwort aktivieren	Das Kennwort für die Authentifizierung auf zweiter Ebene. Dieses Kennwort ist nur erforderlich, wenn bei der Authentifizierung nach den Benutzerberechtigungsnachweisen für den Zugriff im Expertenmodus gefragt wird.
SNMP Get Community	Optional
SNMPv3 Authentication Username (Benutzername für die SNMPv3-Authentifizierung)	Optional
SNMPv3 Authentication Password (Kennwort für die SNMPv3-Authentifizierung)	Optional
SNMPv3 Privacy Password (Datenschutzkennwort für SNMPv3)	Optional Das Protokoll für die Entschlüsselung von SNMPv3-Alarmnachrichten.

Einschränkung: Wenn Ihre Netzeinheit eine der folgenden Voraussetzungen erfüllt, müssen Sie in Configuration Source Management Protokolle konfigurieren:

- Ihre Einheit verwendet für das Kommunikationsprotokoll keinen Standardport.
- Sie möchten, dass das von IBM Security QRadar Risk Manager verwendete Protokoll mit bestimmten IP-Adressen kommuniziert.

Weitere Informationen zur Konfiguration von Quellen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

7. Fügen Sie über das Navigationsmenü eine oder mehrere Einheiten hinzu.
   - Klicken Sie zum Hinzufügen einer Netzeinheit auf **Add Device** (Einheit hinzufügen).
   - Klicken Sie zum Hinzufügen mehrerer IP-Adressen für Netzeinheiten auf **Discover Devices** (Einheiten erkennen).
8. Geben Sie die IP-Adresse der Einheit ein, wählen Sie den Adaptertyp aus und klicken Sie auf **Hinzufügen**.

   Wenn die Einheit nicht gesichert ist, wird neben dem Adapter ein blaues Fragezeichen angezeigt.
9. Zum Sichern der Einheit, die Sie der Einheitenliste hinzufügen, wählen Sie die Einheit aus und klicken Sie auf **Backup** (Sichern).
10. Wiederholen Sie diese Schritte für jede CPSMS-Einheit, die Sie der Einheitenliste hinzufügen möchten.

Nächste Schritte

Nachdem Sie die erforderlichen Einheiten hinzugefügt haben, können Sie die Protokolle konfigurieren. Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Von einer NSM-Konsole verwaltete Einheiten hinzufügen

Zum Hinzufügen aller Einheiten von einer Juniper Networks NSM-Konsole (Network and Security Manager) zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

Vorbereitende Schritte

Lesen Sie zunächst, welche Softwareversionen unterstützt, welche Berechtigungsnachweise benötigt und welche Befehle für Ihre Netzeinheiten verwendet werden. Weitere Informationen finden Sie in Kapitel 5, „Unterstützte Adapter", auf Seite 17.

Vorgehensweise

1. Klicken Sie in IBM Security QRadar SIEM auf die Registerkarte **Admin**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer Einheit ein und klicken Sie auf **Hinzufügen**.

Sie können eine IP-Adresse, einen IP-Adressbereich, ein CIDR-Teilnetz oder einen Platzhalter eingeben.

Einschränkung: Geben Sie Einheitenadressen, die bereits in anderen Netzgruppen vorkommen, nicht ein zweites Mal in Configuration Source Management ein.

c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.

d. Wiederholen Sie die vorangegangenen zwei Schritte für jede IP-Adresse, die Sie hinzufügen möchten.

6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).

a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.

b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie die angefragten Parameterwerte ein.

In der folgenden Tabelle werden die Parameter beschrieben.

Tabelle 3. Parameter für die Berechtigungsnachweise der Juniper NSM-Web-Services

Parameter	Beschreibung
Benutzername	Ein gültiger Benutzername für die Anmeldung bei den Juniper NSM (Network and Security Manager)-Web-Services. Der Benutzer muss auf den Juniper NSM-Server zugreifen können.
Kennwort	Das Kennwort für die Einheit.
Kennwort aktivieren	Nicht erforderlich.

Einschränkung: Juniper Networks NSM (Network and Security Manager) unterstützt kein SNMP.

7. Klicken Sie im Navigationsmenü auf **Discover from NSM** (Erkennen aus NSM).
8. Geben Sie die Werte für die IP-Adresse und die Benutzerberechtigungsnachweise ein und klicken Sie dann auf **OK** und auf **GO** (Los).
9. Wählen Sie die Einheit aus, die Sie der Einheitenliste hinzugefügt haben, und klicken Sie dann auf **Backup** (Sichern) und auf **Yes** (Ja).

Nächste Schritte

Nachdem Sie die erforderlichen Einheiten hinzugefügt haben, können Sie die Protokolle konfigurieren. Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Einheiten zu QRadar Risk Manager hinzufügen, die über eine CPSMS-Konsole verwaltet werden

Zum Hinzufügen von Einheiten von einem Check Point Security Manager Server (CPSMS) zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

Abhängig von Ihrer Version von Check Point Security Manager Server müssen Sie eine der folgenden Erkennungsmethoden wählen, mit denen Ihre Einheiten zu QRadar Risk Manager hinzugefügt werden.

Einheiten, die von CPSMS verwaltet werden, über OPSEC hinzufügen

Einheiten, die von den Check Point Security Manager Server-Versionen NGX R60 bis R77 verwaltet werden, werden in IBM Security QRadar Risk Manager hinzugefügt, indem sie mithilfe von OPSEC erkannt und hinzugefügt werden.

Vorbereitende Schritte

Lesen Sie zunächst, welche Softwareversionen unterstützt, welche Berechtigungsnachweise benötigt und welche Befehle für Ihre Netzeinheiten verwendet werden. Weitere Informationen finden Sie in Kapitel 5, „Unterstützte Adapter", auf Seite 17.

Für dieses Verfahren benötigen Sie den PSEC Entity SIC-Namen, den OPSEC Application Object SIC-Namen und das einmalig verwendbare *Pull Certificate*-Kennwort. Weitere Informationen hierzu finden Sie in Ihrer CPSMS-Dokumentation.

Anmerkung: Die Funktion "Device Import" (Geräteimport) ist mit CPSMS-Adaptern nicht kompatibel.

Informationen zu diesem Vorgang

Wiederholen Sie dieses Verfahren für jeden CPSMS, zu dem Sie eine Verbindung herstellen möchten, um die Erkennung der von ihm verwalteten Firewalls zu aktivieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer CPSMS-Einheit ein und klicken Sie auf **Hinzufügen**.

      Einschränkung: Geben Sie Einheitenadressen, die bereits in anderen Netzgruppen vorkommen, nicht ein zweites Mal in Configuration Source Management ein.
   c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.
6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).
   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.

b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Einheit ein.

7. Geben Sie den OPSEC Entity SIC-Namen des CPSMS ein, der die zu erkennenden Firewalleinheiten verwaltet. Dieser Wert muss präzise sein, da das Format vom Typ der Einheit abhängig ist, von der die Erkennung durchgeführt wurde. Verwenden Sie die folgende Tabelle als Referenz für OPSEC Entity SIC-Namensformate.

Typ	Name
Management-Server	`CN=cp_mgmt,O=<take O value from DN field>`
Gateway zu Management-Server	`CN=cp_mgmt_<gateway hostname>,O=<take O value from DN field>`

Wenn Sie die Erkennung z. B. vom Management-Server aus durchführen:

- Definierter Name der OPSEC-Anwendung: `CN=cpsms226,O=vm226-CPSMS..bs7ocx`
- Host der OPSEC-Anwendung: `vm226-CPSMS`

Der SIC-Name der Entität ist `CN=cp_mgmt,O=vm226-CPSMS..bs7ocx`

Wenn Sie die Erkennung z. B. vom Gateway zum Management-Server aus durchführen:

- Definierter Name der OPSEC-Anwendung: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
- Host der OPSEC-Anwendung: `vm230-CPSMS2-GW3`

Der SIC-Name der Entität ist `CN=cp_mgmt_vm230-CPSMS2-GW3,O=vm226-CPSMS..bs7ocx`

8. Verwenden Sie die Check Point SmartDashboard-Anwendung, um den SIC-Namen der OPSEC-Anwendung einzugeben, der auf dem CPSMS erstellt wurde.

   Beispiel: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`

9. Rufen Sie ein OPSEC-SSL-Zertifikat ab:
   a. Klicken Sie auf **Get Certificate** (Zertifikat abrufen).
   b. Geben Sie im Feld **Certificate Authority IP** (IP der Zertifizierungsstelle) die IP-Adresse der Zertifizierungsstelle ein.
   c. Geben Sie im Feld **Pull Certificate Password** (Pull Certificate-Kennwort) das einmalig verwendbare Kennwort für die OPSEC-Anwendung ein.
   d. Klicken Sie auf **OK**.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf **Protocols** (Protokolle) und stellen Sie sicher, dass das Protokoll **CPSMS** ausgewählt ist.

    Der Standardport für das CPSMS-Protokoll ist 18190.

12. Klicken Sie auf **Discover From Check Point OPSEC** (Über Check Point-OPSEC erkennen) und geben Sie die IP-Adresse von CPSMS ein.
13. Klicken Sie auf **OK**.
14. Wiederholen Sie diese Schritte für jede CPSMS-Einheit, die Sie hinzufügen möchten.

Nächste Schritte

Nachdem alle erforderlichen Einheiten hinzugefügt wurden, sichern Sie diese Einheiten und zeigen Sie sie in der Topologie an.

Einheiten, die von CPSMS verwaltet werden, über HTTPS hinzufügen

Einheiten, die von der Check Point Security Manager Server-Version R80 verwaltet werden, werden in IBM Security QRadar Risk Manager hinzugefügt, indem sie über das HTTPS-Protokoll erkannt und hinzugefügt werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse der Check Point-Einheit ein und klicken Sie auf **Hinzufügen**.
   c. Stellen Sie sicher, dass die Adresse im Feld **Network address** (Netzadresse) angezeigt wird.
6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).
   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.
   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Einheit ein.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Protocols** (Protokolle) und stellen Sie sicher, dass das **HTTPS**-Protokoll ausgewählt ist.
9. Klicken Sie auf **Discover From Check Point HTTPS** (Über Check Point-HTTPS erkennen) und geben Sie die Check Point-IP-Adresse ein.
10. Klicken Sie auf **OK**.

Nächste Schritte

Nachdem alle erforderlichen Einheiten hinzugefügt wurden, sichern Sie diese Einheiten und zeigen Sie sie in der Topologie an.

Von SiteProtector verwaltete Einheiten hinzufügen

Fügen Sie in Configuration Source Management Einheiten aus SiteProtector zu IBM Security QRadar Risk Manager hinzu.

Vorbereitende Schritte

Die IBM Internet Security Systems GX- und IBM Security SiteProtector System-Adapter müssen installiert sein, bevor Sie Einheiten hinzufügen können.

Das Microsoft SQL-Protokoll muss für Microsoft SQL Server-Port 1433 konfiguriert sein.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer SiteProtector-Einheit ein und klicken Sie auf **Hinzufügen**.
   c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.
6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).
   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.
   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Einheit ein.

      Einschränkung: Als Benutzername und Kennwort werden die gleichen Berechtigungsnachweise verwendet wie für die von SiteProtector verwendete Microsoft SQL Server-Datenbank.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Discover From SiteProtector** (Aus SiteProtector erkennen) und geben Sie die IP-Adresse von SiteProtector ein.
9. Klicken Sie auf **OK**.

Nächste Schritte

Nachdem Sie alle erforderlichen Einheiten hinzugefügt haben, sichern Sie diese und zeigen Sie dann in der Topologie an.

Kapitel 4. Fehlerbehebung bei der Erkennung und Sicherung von Einheiten

Behebung von Problemen bei der Erkennung und Sicherung von Einheiten. Als Hilfe bei der Fehlerbehebung können Sie sich ausführliche Informationen zu Protokollen sowie die Fehlernachrichten und Warnmeldungen anzeigen lassen.

Fehler bei Einheitensicherung

Berechtigungsnachweise zur Einheitenanmeldung prüfen.

1. Klicken Sie auf der Registerkarte **Verwaltung** auf **Configuration Source Management** (Konfigurationsquellenverwaltung).
2. Überprüfen Sie, ob die Berechtigungsnachweise für den Zugriff auf die Zieleinheit korrekt sind.
3. Testen Sie die Berechtigungsnachweise auf der Zieleinheit.

Anzeigen von Fehlern bei der Einheitensicherung

Gehen Sie wie folgt vor, um die Sicherungsfehler anzuzeigen:

1. Klicken Sie auf der Registerkarte **Verwaltung** auf **Configuration Source Management** (Konfigurationsquellenverwaltung).
2. Klicken Sie auf eine Einheit und klicken Sie dann auf **Fehler anzeigen**.

In dieser Tabelle werden die Kennungen der Fehlernachrichten, die Beschreibung der jeweiligen Nachricht sowie die vorgeschlagene Fehlerbehebungsmaßnahme aufgeführt.

Tabelle 4. Fehler bei Einheitensicherung

Sicherungsfehler	**Fehlerbeschreibung**	**Vorgeschlagene Fehlerbehebungsmaßnahme**
`UNEXPECTED_RESPONSE`	Verbindungsversuch hat zulässiges Zeitlimit überschritten.	Überprüfen Sie, ob Sie den richtigen Adapter verwenden.
`INVALID_CREDENTIALS`	Falsche Berechtigungsnachweise	Überprüfen Sie die Berechtigungsnachweise unter **Configuration Source Management** (Konfigurationsquellenverwaltung).
`SSH_ERROR`	Verbindungsfehler	Stellen Sie sicher, dass die Einheit funktioniert und mit dem Netz verbunden ist. Verwenden Sie andere Netzprotokolle und Fehlerbehebungstools, um zu prüfen, ob das Geräte aufgerufen werden kann. Stellen Sie sicher, dass das SSH-Verbindungsprotokoll zulässig ist und ordnungsgemäß konfiguriert wurde.

Tabelle 4. Fehler bei Einheitensicherung (Forts.)

Sicherungsfehler	Fehlerbeschreibung	Vorgeschlagene Fehlerbehebungsmaßnahme
TELNET_ERROR	Verbindungsfehler	Stellen Sie sicher, dass die Einheit funktioniert und mit dem Netz verbunden ist. Verwenden Sie andere Netzprotokolle und Fehlerbehebungstools, um zu prüfen, ob das Geräte aufgerufen werden kann. Stellen Sie sicher, dass das Telnet-Verbindungsprotokoll zulässig ist und ordnungsgemäß konfiguriert wurde.
SNMP_ERROR	Verbindungsfehler	Stellen Sie sicher, dass die Einheit funktioniert und mit dem Netz verbunden ist. Verwenden Sie andere Netzprotokolle und Fehlerbehebungstools, um zu prüfen, ob das Geräte aufgerufen werden kann. Stellen Sie sicher, dass das SNMP-Protokoll zulässig ist und ordnungsgemäß konfiguriert wurde.
TOO_MANY_USERS	Die Anzahl der Benutzer, die gemäß Konfiguration auf diese Einheit zugreifen dürfen, wurde überschritten.	Prüfen Sie die maximale Anzahl der Benutzer, die auf die Einheit zugreifen dürfen, indem Sie sich an der Einheit anmelden und die Konfiguration auf die maximale Anzahl der Benutzer prüfen, die gleichzeitig Zugriff auf die Einheit zugreifen können.
DEVICE_MEMORY_ERROR	Fehler bei Einheitenkonfiguration	Überprüfen Sie, ob die Einheit ordnungsgemäß funktioniert. Rufen Sie die Einheit auf, verifizieren Sie die Konfiguration und überprüfen Sie die Protokolle auf Fehler. Ziehen Sie zur Fehlerbehebung die Einheitendokumentation zu Rate.
NVRAM_CORRUPTION_ERROR	Probleme beim Zugriff auf Einheiten	Prüfen Sie unter **Configuration Source Management** (Konfigurationsquellenverwaltung) die Zugriffsebenen des Benutzernamens, der für den Zugriff auf die Einheit konfiguriert wurde.
INSUFFICIENT_PRIVILEGE	Benutzer, der für den Zugriff auf die Einheit konfiguriert wurde, verfügt nicht über ausreichende Berechtigungen.	Prüfen Sie unter **Configuration Source Management** (Konfigurationsquellenverwaltung) die Zugriffsebenen des Benutzernamens, der für den Zugriff auf die Einheit konfiguriert wurde.

Tabelle 4. Fehler bei Einheitensicherung (Forts.)

Sicherungsfehler	Fehlerbeschreibung	Vorgeschlagene Fehlerbehebungsmaßnahme
DEVICE_ISSUE	Fehler in der Einheit	Wählen Sie unter **Configuration Source Management** (Konfigurationsquellenverwaltung) die Einheit aus und klicken Sie auf **Fehler anzeigen**, um ausführlichere Informationen anzuzeigen.

Sicherungsabschluss mit Warnung zur Syntaxanalyse

Gehen Sie wie folgt vor, um ausführlichere Informationen zur Warnung anzuzeigen:

1. Klicken Sie auf die Registerkarte **Risiken**.
2. Klicken Sie im Navigationsmenü auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Klicken Sie für die ausgewählte Einheit in der Tabelle **Device List** (Einheitenliste) auf **See Log** (Protokoll anzeigen).

Arbeiten Sie mit den aktuellsten Adapterversionen?

Zur Überprüfung der Adapterversionen melden Sie sich als Rootbenutzer an der QRadar Risk Manager-Appliance an und geben Sie dann folgenden Befehl ein:

```
yum list adapter\*
```

Die jeweiligen Freigabedaten erkennen Sie an den Datumsinformationen in den Adapternamen.

So laden Sie das aktuellste Adapter-Bundle herunter:

1. Gehen Sie zu IBM Fix Central (https://www.ibm.com/support/fixcentral/).
2. Geben Sie im Feld **Product selector** (Produktauswahl) das Produkt `Risk Manager` ein, um Ihre Auswahl zu filtern.
3. Klicken Sie auf IBM Security QRadar Risk Manager.
4. Wählen Sie in der Liste **Installed Version** (Installierte Version) die auf Ihrem System installierte Version aus.
5. Wählen Sie in der Liste **Platform** (Plattform) das auf Ihrem System installierte Betriebssystem aus und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Browse for fixes** (Nach Fixes suchen) und klicken Sie dann auf **Weiter**.
7. Klicken Sie zum Herunterladen des aktuellsten Adapter-Bundle auf oben in der Liste **Adapter** auf den Adpater-Bundle-Link.

Verfügen Sie über das aktuellste Einheiten-Backup?

So prüfen Sie, ob Sie über ein aktuelles Backup verfügen:

1. Klicken Sie auf die Registerkarte **Risiken**.
2. Klicken Sie im Navigationsmenü auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Doppelklicken Sie in der Tabelle **Device List** (Einheitenliste) auf die Einheit.

4. Klicken Sie in der Symbolleiste auf **Protokoll**. Die aktuellste importierte Konfiguration wird angezeigt.

Wenn Sie der Meinung sind, nicht mit der aktuellsten Konfiguration zu arbeiten, führen Sie erneut ein Backup durch.

Fehler beim Importieren von Konfigurationen von Ihrer Einheit

Eine nicht ordnungsgemäß formatierte CSV-Datei kann Fehler beim Einheiten-Backup verursachen. So überprüfen Sie die CSV-Datei:

1. Prüfen Sie die CSV-Datei auf Fehler und beheben Sie diese.
2. Importieren Sie die Einheitenkonfigurationen mit der aktualisierten CSV-Datei erneut.

Einheiten können nicht über Check Point SMS (OPSEC) erkannt werden

Führen Sie sämtliche in Abschnitt "Von einer CPSMS-Konsole verwaltete Einheiten hinzufügen", Handbuch *IBM Security QRadar Risk Manager-Adapterkonfigurationshandbuch*, aufgeführten Schritte aus. Achten Sie insbesondere bei den Schritten 7 und 8 auf korrekt ausgefüllte OPSEC-Felder.

Zugehörige Tasks:

„Einheiten, die von CPSMS verwaltet werden, über OPSEC hinzufügen" auf Seite 9
Einheiten, die von den Check Point Security Manager Server-Versionen NGX R60 bis R77 verwaltet werden, werden in IBM Security QRadar Risk Manager hinzugefügt, indem sie mithilfe von OPSEC erkannt und hinzugefügt werden.

Kapitel 5. Unterstützte Adapter

IBM Security QRadar Risk Manager lässt sich mit Sicherheitsprodukten der verschiedensten Hersteller und Anbieter integrieren.

Für jeden unterstützten Adapter werden folgende Informationen bereitgestellt:

Unterstützte Versionen

Hier werden der Produktname und die unterstützten Versionen angegeben.

Neighbor-Datenunterstützung

Hier wird angegeben, ob für diesen Adapter Neighbor-Daten unterstützt werden. Wenn Ihre Einheit Neighbor-Daten unterstützt, erhalten Sie diese über das Simple Network Management Protocol (SNMP) und eine Befehlszeilenschnittstelle (CLI) von der Einheit.

SNMP-Erkennung

Hier wird angegeben, ob die Einheit die Erkennung mittels SNMP zulässt.

Für die Erkennung mittels SNMP müssen die Einheiten Standard-MIB-2 unterstützen und die SNMP-Konfiguration der Einheit muss unterstützt werden und korrekt konfiguriert sein.

Erforderliche Parameter für Berechtigungsnachweise

Hier werden die Zugriffsanforderungen für die Verbindung zwischen QRadar Risk Manager und der Einheit angegeben.

Die in QRadar Risk Manager konfigurierten Berechtigungsnachweise und die Berechtigungsnachweise auf der Einheit müssen identisch sein.

Die Felder für nicht erforderliche Parameter lassen Sie einfach leer.

Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.

Verbindungsprotokolle

Hier werden die für die Netzeinheit unterstützten Protokolle angegeben.

Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.

Erforderliche Befehle

Hier werden die Befehle aufgelistet, die der Adapter zur Anmeldung und Erfassung der Daten benötigt.

Zur Ausführung dieser Befehle auf dem Adapter müssen die in QRadar Risk Manager bereitgestellten Berechtigungsnachweise über die entsprechenden Berechtigungen verfügen.

Erfasste Dateien

Hier werden die Dateien aufgelistet, auf die der Adapter Zugriff benötigt. Der Adapter muss über die entsprechenden Berechtigungsnachweise für den Zugriff auf diese Dateien verfügen.

Check Point SecurePlatform Appliances

IBM Security QRadar Risk Manager unterstützt den Check Point SecurePlatform Appliances-Adapter.

Mit dem Check Point SecurePlatform Appliances-Adapter sind folgende Funktionen verfügbar:

- Dynamische Netzadressumsetzung
- Statische Netzadressumsetzung
- SNMP-Erkennung
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für den Check Point SecurePlatform Appliances-Adapter beschrieben.

Tabelle 5. Integrationsanforderungen für den Check Point SecurePlatform Appliances-Adapter

Integrationsanforderungen	Beschreibung
Versionen	R65 bis R77.30 **Einschränkung:** Nokia IPSO-Appliances werden für Backups nicht unterstützt.
SNMP-Erkennung	Gleicht in der SNMP sysDescr NGX ab
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort** **Kennwort aktivieren** (Expertenmodus)
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH**

Tabelle 5. Integrationsanforderungen für den Check Point SecurePlatform Appliances-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`hostname`
	`dmidecode`
	`ver`
	`uptime`
	`dmesg`
	`route -n`
	`show users`
	`ifconfig -a`
	`echo $FWDIR`

Erfasste Dateien	`rules.C`
	`objects.C`
	`implied_rules.C`
	`Standard.pf`
	`snmpd.com`

Check Point Security Management Server-Adapter

Mit dem Check Point-Adapter können Sie Endknoten erkennen und sichern, die von CPSMS (Check Point Security Management Server) verwaltet werden.

Wählen Sie einen der folgenden Adapter zum Erkennen und Sichern von Endknoten, die von CPSMS verwaltet werden, aus:

CPSMS-Adapter (Check Point Security Management Server) für OPSEC

Mit dem CPSMS-Adapter (Check Point Security Management Server) für OPSEC können Sie Endknoten erkennen und sichern, die von den CPSMS-Versionen NGX R60 bis R77 verwaltet werden.

Der CPSMS-Adapter (Check Point Security Management Server) für OPSEC stellt die folgenden Funktionen zur Verfügung:

- OPSEC-Protokoll
- Dynamische Netzadressumsetzung
- Statische Netzadressumsetzung
- Statisches Routing

Der CPSMS-Adapter basiert auf OPSEC SDK 6.0, das Check Point-Produkte unterstützt, die gemäß Konfiguration Zertifikate verwenden, welche nur mit SHA-1 signiert sind.

In der folgenden Tabelle werden die Integrationsanforderungen für den CPSMS-Adapter beschrieben.

Tabelle 6. Integrationsanforderungen für den CPSMS-Adapter

Integrationsanforderungen	Beschreibung
Versionen	NGX R60 bis R77
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie die Berechtigungsnachweise, die Sie in 'Von einer CPSMS-Konsole verwaltete Einheiten hinzufügen' festgelegt haben.
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**CPSMS**
Konfigurationsanforderungen	Damit `cpsms_client` mit Check Point Management Server kommunizieren kann, muss die Datei `$CPDIR/conf/sic_policy.conf` auf dem CPSMS die folgende Zeile enthalten: `# OPSEC applications defaultANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp# sam proxyANY ; Modules, DN_Mgmt ; ANY; sam ; sslcaANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_compANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_compANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp`
Erforderliche Ports	Folgende Ports werden von QRadar Risk Manager verwendet und müssen auf CPSMS offen sein: Port 18190 für den Check Point Management Interface-Service (CPMI) Port 18210 für den Check Point Internal CA Pull Certificate-Service (FW1_ica_pull) Falls Sie Port 18190 nicht als Empfangsport für die CPMI verwenden können, muss die Portnummer des CPSMS-Adapters dem zugehörigen Wert in der Datei `$FWDIR/conf/fwopsec.conf` für die CPMI auf dem CPSMS entsprechen. Beispiel: `cpmi_server auth_port 18190`.

CPSMS-Adapter (Check Point Security Management Server) für HTTPS

Mit dem CPSMS-Adapter (Check Point Security Management Server) für HTTPS können Sie Endknoten erkennen und sichern, die mit Firewall-Blades verbunden sind, die von Security Management Server Version R80 verwaltet werden.

Der CPSMS-Adapter (Check Point Security Management Server) für HTTPS stellt die folgenden Funktionen zur Verfügung:

- Statische Netzadressumsetzung
- Statisches Routing
- HTTPS-Verbindungsprotokoll

Die folgenden Funktionen werden vom CPSMS-Adapter nicht unterstützt:

- Dynamische Objekte (Netzobjekte)
- Sicherheitszonen (Netzobjekte)
- RPC-Objekte (Services)
- DCE-RPC-Objekte (Services)
- ICMP-Services (Services)
- GTP-Objekte (Services)
- Zusammengesetzte TCP-Objekte (Services)
- Citrix-TCP-Objekte (Services)
- Andere Services (Services)
- Benutzerobjekte
- Zeitobjekte
- Negation von Kriterien der Zugriffssteuerungsrichtlinien

Anmerkung:

Bei einer Aktualisierung von einer älteren CPSMS-Version auf Check Point Security Management Server R80 müssen Sie Ihre Einheiten mithilfe der Erkennungsmethode **Discover From Check Point HTTPS** (Über Check Point-HTTPS erkennen) erneut erkennen, auch wenn die Einheiten über **Configuration Source Management** erfasst werden.

Die folgende Tabelle enthält eine Beschreibung der Integrationsanforderungen für den CPSMS-Adapter (Check Point Security Management Server).

Tabelle 7. Integrationsanforderungen für den CPSMS-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	R80
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**. **Anmerkung:** Vor der Konfiguration der Einheitenerkennung müssen Sie zunächst die Berechtigungsnachweise für Check Point Security Management Server hinzufügen.	**Benutzername** **Kennwort**

Tabelle 7. Integrationsanforderungen für den CPSMS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung
Konfiguration der Einheitenerkennung Um die Einheitenerkennung in QRadar zu konfigurieren, melden Sie sich als Administrator an und wählen Sie **Configuration Source Management** auf der Registerkarte **Verwaltung** aus. Um die Erkennungsmethode zu konfigurieren, klicken Sie auf **Discover From Check Point HTTPS** (Über Check Point-HTTPS erkennen), geben Sie die IP-Adresse von Check Point Security Management Server ein und klicken Sie anschließend auf **OK**.	Erkennung über Check Point-HTTPS
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	HTTPS
Voraussetzungen für Zugriff auf Benutzerebene	Schreib-/Lesezugriff 'all'

Tabelle 7. Integrationsanforderungen für den CPSMS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung
Angeforderte API-Endpunkte	Geben Sie die aufgeführten Befehle im folgenden Format an Einheiten aus: https://*<Management-Server>*:*<Port>*/*Web-API*/*<Befehl>* show-simple-gateways show-hosts show-networks show-address-ranges show-groups show-groups-with-exclusion show-services-tcp show-services-udp show-service-groups show-packages show-access-rulebase show-nat-rulebase run-script show-task

Cisco CatOS

IBM Security QRadar Risk Manager unterstützt den Cisco Catalyst (CatOS)-Adapter.

Der Cisco CatOS-Adapter erfasst Einheitenkonfigurationen, indem er CatOS-Netzeinheiten sichert, auf die QRadar Risk Manager Zugriff hat.

Mit dem Cisco CatOS-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- SNMP-Erkennung
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für den Cisco CatOS-Adapter beschrieben.

Tabelle 8. Integrationsanforderungen für den Cisco CatOS-Adapter

Integrationsanforderungen	Beschreibung
Versionen	Catalyst 6500 Series-Chassiseinheiten. 4.2 6.4 **Einschränkung:** Der CatOS-Adapter sichert nur den essenziellen Teil der Switch-Port-Struktur. CatOS-Adapter für Multilayer Switch Feature Card (MSFC) werden durch Cisco IOS-Adapter gesichert. CatOS-Adapter für das Firewall Services Module (FWSM) werden durch Cisco ASA-Adapter gesichert.
SNMP-Erkennung	Gleicht in der SNMP sysDescr CATOS oder Catalyst Operating System ab
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort** **Kennwort aktivieren**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH**

Tabelle 8. Integrationsanforderungen für den Cisco CatOS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show version`
	`whichboot`
	`show module`
	`show mod ver`
	`show system`
	`show flash devices`
	`show flash`
	`show snmp ifalias`
	`show port ifindex`
	`show interface`
	`show port`
	`show spantree`
	`show ip route`
	`show vlan`
	`show vtp domain`
	`show arp`
	`show cdp`
	`show cam dynamic`
	`show port status`
	`show counters`

Cisco IOS

IBM Security QRadar Risk Manager unterstützt den Cisco Internet Operating System (IOS)-Adapter.

Der Cisco IOS-Adapter erfasst Einheitenkonfigurationen, indem er IOS-basierte Netzswitches und -router sichert.

Mit dem Cisco IOS-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- Dynamische Netzadressumsetzung
- Statische Netzadressumsetzung
- SNMP-Erkennung
- Statisches Routing
- Dynamisches EIGRP- und OSPF-Routing
- P2P-Tunnelung/VPN
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für Cisco IOS beschrieben.

Tabelle 9. Integrationsanforderungen für Cisco IOS

Integrationsanforderungen	Beschreibung
Versionen	IOS 12.0 bis 15.1 für Router und Switches Cisco Catalyst 6500-Switches mit MSFC. Verwenden Sie den Cisco IOS-Adapter zum Sichern der Konfiguration und des Status von MSFC Card Services. Wenn ein Cisco IOS 7600 Series-Router einen FWSM hat, verwenden Sie zu dessen Sicherung den Cisco ASA-Adapter.
Benutzerzugriffsebene	Ein Benutzer mit der Berechtigungsstufe zur Befehlsausführung für jeden Befehl, den der Adapter zur Anmeldung und Erfassung der Daten benötigt. Sie können zum Beispiel einen Benutzer mit benutzerdefinierten Berechtigungen und Berechtigungsstufe 10 und lokaler Datenbankauthentifizierung konfigurieren. Das folgende Beispiel setzt alle `show ip`-Befehle auf die privilegierte Berechtigungsstufe 10. `privilege exec level 10 show ip`
SNMP-Erkennung	Gleicht in der SNMP sysDescr ISO oder Cisco Internet Operation System ab
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort** **Benutzername aktivieren** (optional) Verwenden Sie dieses Feld, wenn der Benutzer bei der Anmeldung an der Einheit eine bestimmte Berechtigungsstufe eingeben muss. Verwenden Sie das Format `level-<n>`, wobei *n* eine Berechtigungsstufe ist [0-15]. Um beispielsweise die Berechtigungsstufe 10 einzugeben, verwenden Sie folgenden Befehl: `level-10` Daraufhin wird der Befehl **`enable 10`** an die Cisco-Einheit gesendet. **Kennwort aktivieren** (optional)
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH**

Tabelle 9. Integrationsanforderungen für Cisco IOS (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show access-lists`
	`show cdp neighbors detail`
	`show diag`
	`show diagbus`
	`show file systems`
	`show glbp`
	`show install running`
	`show interfaces`
	`show inventory`
	`show ip route ospf`
	`show mac address-table dynamic`
	`show module`
	`show mod version`
	`show object-group`
	`show power`
	`show snmp`
	`show spanning-tree`
	`show standby`
	`show startup-config`
	`show version`
	`show vlan`
	`show vrrp`
	`show vtp status`

Tabelle 9. Integrationsanforderungen für Cisco IOS (Forts.)

Integrationsanforderungen	Beschreibung

`show ip`-Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show ip arp`
	`show ip bgp neighbors`
	`show ip eigrp interface`
	`show ip eigrp neighbors`
	`show ip eigrp topology`
	`show ip ospf`
	`show ip ospf interface`
	`show ip ospf neighbor`
	`show ip protocols`
	`show ip route eigrp`
	`terminal length 0`

Cisco Nexus

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Cisco Nexus-Adapter erfüllt sein.

Mit dem Cisco Nexus-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- SNMP-Erkennung
- Dynamisches EIGRP- und OSPF-Routing
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für den Cisco Nexus-Adapter beschrieben.

Tabelle 10. Integrationsanforderungen für den Cisco Nexus-Adapter

Integrationsanforderungen	Beschreibung
Versionen und unterstützte Betriebssystemebenen	Nexus 5548: BS-Ebene 6.0 Nexus 7000 Series: BS-Ebene 6.2 Nexus 9000 Series: BS-Ebene 6.1
SNMP-Erkennung	Gleicht in der SNMP sysDescr *Cisco NX-OS* und eine optionale Qualifizierungszeichenfolge ab, die auf *Software* endet. **Beispiel:** *(Cisco NX\-OS.* Software)*

Tabelle 10. Integrationsanforderungen für den Cisco Nexus-Adapter (Forts.)

Integrationsanforderungen	**Beschreibung**
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort** **Kennwort aktivieren** **Wenn Sie virtuelle Gerätekontexte (VDCs = Virtual Device Contexts) als separate Einheiten hinzufügen, müssen Sie sicherstellen, dass mit den erforderlichen Berechtigungsnachweisen folgende Aktionen ausgeführt werden können:** Zugriff auf das für die VDCs aktivierte Konto Verwendung der erforderlichen Befehle im virtuellen Kontext
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH**

Tabelle 10. Integrationsanforderungen für den Cisco Nexus-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show hostname`
	
	`show version`
	
	`show vdc`
	
	`show vdc current-vdc`
	
	`switchto vdc <vdc>`, wobei *vdc* ein aktiver `vdc` ist, der aufgelistet wird, wenn Sie den Befehl `show vdc` eingeben.
	
	`show snmp`
	
	`dir <Dateisystem>` , wobei *Dateisystem* `bootflash`, `slot0`, `volatile`, `log`, `logflash` oder `system` ist.
	
	`show running-config`
	
	`show startup-config`
	
	`show module`
	
	`show interface brief`
	
	`show interface snmp-ifindex`
	
	`show ip access-lists`
	
	`show vlan`
	
	`show vtp status`
	
	`show spanning-tree summary`
	
	`show object-group`
	
	`show interface <Schnittstelle>`, wobei *Schnittstelle* eine der Schnittstellen ist, die aufgelistet werden, wenn Sie den Befehl `show running-config` eingeben.
	
	`show hsrp`
	
	`show vrrp`
	
	`show vtp`
	
	`show glbp`
	
	`show ip eigrp`
	
	`show ip route eigrp`
	
	`show ip ospf`
	
	`show ip route ospf`
	
	`show ip rip`
	
	`show ip route rip`

Tabelle 10. Integrationsanforderungen für den Cisco Nexus-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Telemetrie-Befehle	`terminal length 0`
	
	`show hostname`
	
	`show vdc`
	
	`switchto vdc <vdc>`, wobei *vdc* ein aktiver `vdc` ist, der aufgelistet wird, wenn Sie den Befehl `show vdc` eingeben.
	
	`show cdp entry all`
	
	`show interface brief`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`

Methoden zum Hinzufügen von VDCs für Cisco Nexus-Einheiten

Zum Hinzufügen von Nexus-Netzeinheiten und virtuellen Gerätekontexten (VDCs = Virtual Device Contexts) zu IBM Security QRadar SIEM verwenden Sie Configuration Source Management. Es gibt zwei Methoden zum Hinzufügen mehrerer VDCs zu IBM Security QRadar Risk Manager.

VDCs können als untergeordnete Einheiten der Nexus-Einheit oder als separate Einheiten hinzugefügt werden.

Virtuelle Gerätekontexte anzeigen

Als separate Einheiten hinzugefügte VDCs werden in der Topologie als eigene Einheiten angezeigt.

Als untergeordnete Einheiten hinzugefügte VDCs werden in der Topologie nicht angezeigt. Diese VDCs können Sie im Fenster **Configuration Monitor** (Konfigurationsüberwachung) anzeigen.

VDCs als untergeordnete Einheiten einer Cisco Nexus-Einheit hinzufügen

Zum Hinzufügen von VDCs als untergeordnete Einheiten einer Cisco Nexus-Einheit verwenden Sie Configuration Source Management.

Vorgehensweise

1. Aktivieren Sie für den in den Berechtigungsnachweisen angegebenen Benutzer die folgenden Befehle:
   - `show vdc` (Verwaltungskontext)
   - `switchto vdc` *x*; dabei ist *x* die unterstützte VDC.

   In **Configuration Monitor** können Sie die Nexus-Einheit sowie die untergeordneten VDC-Einheiten anzeigen. Die übergeordnete Einheit wird in der Topolo-

gie angezeigt. Weitere Informationen zum Anzeigen von Einheiten finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

2. Verwenden Sie Configuration Source Management, um die *Verwaltungskontext*-IP-Adresse der Nexus-Einheit hinzuzufügen.

   Weitere Informationen finden Sie im Abschnitt „Netzeinheit hinzufügen" auf Seite 5.

VDCs als separate Einheiten hinzufügen

Mit Configuration Source Manager können Sie jeden VDC (virtuellen Gerätekontext) als separate Einheiten hinzufügen. Wenn Sie diese Methode verwenden, werden die Nexus-Einheit sowie die VDCs in der Topologie angezeigt.

In der Topologie wird das Chassis getrennt von der Cisco Nexus-Einheit und den VDCs dargestellt.

Vorgehensweise

1. Fügen Sie die IP-Verwaltungsadresse jedes VDC in Configuration Source Manager hinzu.

   Weitere Informationen finden Sie im Abschnitt „Netzeinheit hinzufügen" auf Seite 5.

2. Rufen Sie die Konfigurationsdaten Ihrer VDCs über Configuration Source Manager ab.
3. Inaktivieren Sie auf der Cisco Nexus-Einheit in der Cisco Nexus-CLI den Befehl **switchto vdc** für den Benutzernamen, der dem Adapter zugeordnet ist.

   Beispiel: Der Benutzername für eine Cisco Nexus-Einheit ist *qrmuser*. In diesem Fall geben Sie folgende Befehle ein:

```
NexusDevice(config)# role name qrmuser
NexusDevice(config-role)# rule 1 deny command switchto vdc
NexusDevice(config-role)# rule 2 permit command show *
NexusDevice(config-role)# rule 3 permit command terminal
NexusDevice(config-role)# rule 4 permit command dir
```

Cisco Security Appliances

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Cisco Security Appliances-Adapter erfüllt sein.

Mit dem Cisco Security Appliances-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- Statische Netzadressumsetzung
- SNMP-Erkennung
- Dynamisches EIGRP- und OSPF-Routing
- Statisches Routing
- IPSec-Tunnelung
- Telnet- und SSH-Verbindungsprotokolle

Der Cisco Security Appliances-Adapter erfasst Einheitenkonfigurationen, indem er Einheiten der Cisco-Produktfamilie sichert. Der Cisco Security Appliances-Adapter unterstützt die folgenden Firewalls:

- Cisco Adaptive Security Appliances (ASA) 5500-Serie

- Firewall Service Module (FWSM)
- Modul in einem Catalyst-Chassis
- Established Private Internet Exchange-Einheiten (PIX)

Anmerkung: Transparenter Cisco ASA-Kontext kann nicht in die QRadar Risk Manager-Topologie eingefügt werden. Zudem können Sie in diesen transparenten Kontexten keine Pfadsuchen durchführen.

In der folgenden Tabelle werden die Integrationsanforderungen für den Cisco Security Appliances-Adapter beschrieben.

Tabelle 11. Integrationsanforderungen für den Cisco Security Appliances-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	ASA: 8.2, 8.4 bis 9.1.7 PIX: 6.1, 6.3 FWSM: 3.1, 3.2

Minimale Benutzerzugriffsebene	Berechtigungsstufe 5
	
	Mit Berechtigungsstufe 5 können Einheiten gesichert werden. Mit den folgenden Befehlen können Sie beispielsweise einen Benutzer mit Berechtigungsstufe 5 mit lokaler Datenbankauthentifizierung konfigurieren:
	
	`aaa authorization command LOCAL`
	
	`aaa authentication enable console LOCAL`
	
	`privilege cmd level 5 mode exec command terminal`
	
	`privilege cmd level 5 mode exec command changeto` (nur *mehrere Kontexte*)
	
	`privilege show level 5 mode exec command running-config`
	
	`privilege show level 5 mode exec command startup-config`
	
	`privilege show level 5 mode exec command version`
	
	`privilege show level 5 mode exec command shun`
	
	`privilege show level 5 mode exec command names`
	
	`privilege show level 5 mode exec command interface`
	
	`privilege show level 5 mode exec command pager`
	
	`privilege show level 5 mode exec command arp`
	
	`privilege show level 5 mode exec command route`
	
	`privilege show level 5 mode exec command context`
	
	`privilege show level 5 mode exec command mac-address-table`

SNMP-Erkennung	Gleicht in der SNMP sysDescr PIX oder Adaptive Security Appliance oder Firewall Service Module ab.

Tabelle 11. Integrationsanforderungen für den Cisco Security Appliances-Adapter (Forts.)

Integrationsanforderungen	Beschreibung
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort** **Kennwort aktivieren**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH** **SCP**

Tabelle 11. Integrationsanforderungen für den Cisco Security Appliances-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`changeto context <context>`
	
	`changeto system`
	
	`show running-config`
	
	`show startup-config`
	
	`show arp`
	
	`show context`
	
	`show interface`
	
	`show mac-address-table`
	
	`show names`
	
	`show ospf neighbor`
	
	`show route`
	
	`show shun`
	
	`show version`
	
	`terminal pager 0`
	
	`show interface detail`
	
	`show crypto ipsec sa`
	
	`show eigrp topology`
	
	`show eigrp neighbors`
	
	`show firewall`
	
	Der Befehl `changeto context <context>` wird für jeden Kontext auf der ASA-Einheit verwendet.
	
	Der Befehl `changeto system` ermittelt, ob das System Konfigurationen mit *mehreren Kontexten* aufweist. Außerdem ermittelt er den *Administratorkontext*.
	
	Der Befehl `changeto context` wird benötigt, wenn der Befehl `changeto system` eine Konfiguration mit *mehreren Kontexten* oder eine *Administratorkonfiguration* aufweist.
	
	Mit dem Befehl `terminal pager` wird das Auslagerungsverhalten inaktiviert.

F5 BIG-IP

IBM Security QRadar Risk Manager unterstützt den Adapter F5 BIG-IP.

Mit dem Adapter F5 BIG-IP sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- Dynamische Netzadressumsetzung

- Statische Netzadressumsetzung
- SNMP-Erkennung
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

F5 BIG-IP-Appliances für den Lastausgleich, auf denen LTM (Local Traffic Manager) ausgeführt wird, werden unterstützt.

Sie müssen auf der F5 BIG-IP-Einheit die Rolle **Admin** für den Benutzernamen konfigurieren, den QRadar Risk Manager für Sicherungen verwendet, und Sie müssen **Advanced Shell** (Erweiterte Shell) für **Terminal Access** (Terminalzugriff) konfigurieren.

In der folgenden Tabelle werden die Integrationsanforderungen für den F5 BIG-IP-Adapter beschrieben.

Tabelle 12. Integrationsanforderungen für den F5 BIG-IP-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	10.1.1 11.4.1
SNMP-Erkennung	Gleicht F5 BIG-IP in SNMP sysDescr ab
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**SSH**

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`cat filename`
	
	`dmesg`
	
	`uptime`
	
	`route -n`
	
	`ip addr list`
	
	`snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.1`
	
	`snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.2`

Tabelle 12. Integrationsanforderungen für den F5 BIG-IP-Adapter (Forts.)

Integrationsanforderungen	**Beschreibung**

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Bigpipe-Daten benötigt	`bigpipe global`
	`bigpipe system hostname`
	`bigpipe platform`
	`bigpipe version show`
	`bigpipe db packetfilter`
	`bigpipe db packetfilter.defaultaction`
	`bigpipe packet filter list`
	`bigpipe nat list all`
	`bigpipe vlan show all`
	`bigpipe vlangroup list all`
	`bigpipe vlangroup`
	`bigpipe interface show all`
	`bigpipe interface all media speed`
	`bigpipe trunk all interfaces`
	`bigpipe stp show all`
	`bigpipe route all list all`
	`bigpipe mgmt show all`
	`bigpipe mgmt route show all`
	`bigpipe pool`
	`bigpipe self`
	`bigpipe virtual list all`
	`bigpipe snat list all`
	`bigpipe snatpool list all`

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`b db snat.anyipprotocol`

Tabelle 12. Integrationsanforderungen für den F5 BIG-IP-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der TMSH-Daten benötigt	`tmsh -q list sys global-settings hostname`
	`tmsh -q show sys version`
	`tmsh -q show sys hardware`
	`tmsh -q list sys snmp sys-contact`
	`tmsh -q show sys memory`
	`tmsh -q list /net interface all-properties`
	`tmsh -q list net trunk`
	`tmsh -q list /sys db packetfilter`
	`tmsh -q list /sys db packetfilter.defaultaction`
	`tmsh -q list /net packet-filter`
	`tmsh -q list /net vlan all-properties`
	`tmsh -q show /net vlan`
	`tmsh -q list /net vlan-group all all-properties`
	`tmsh -q list net tunnels`

Befehle, die der Adapter zur Anmeldung und zum Abrufen der TMSH-Daten benötigt (Fortsetzung)	`tmsh -q show /net vlan-group`
	`tmsh -q list ltm virtual`
	`tmsh -q list ltm nat`
	`tmsh -q list ltm snatpool`
	`tmsh -q list ltm snat`
	`tmsh -q list sys db snat.anyipprotocol`
	`tmsh -q list net stp-globals all-properties`
	`tmsh -q list net stp priority`
	`tmsh -q list net stp all-properties`
	`tmsh -q list net route`
	`tmsh -q list sys management-ip`
	`tmsh -q list sys management-route`
	`tmsh -q list ltm pool`
	`tmsh -q list net self`
	`tmsh -q list net ipsec`

Erfasste Dateien	`/config/bigip.license`
	`/config/snmp/snmpd.conf`
	`/etc/passwd`

Fortinet FortiOS

IBM Security QRadar Risk Manager-Adapter für Fortinet FortiOS unterstützt Fortinet FortiGate-Appliances, die das Fortinet-Betriebssystem (FortiOS) ausführen.

Mit dem Fortinet FortiOS-Adapter sind folgende Funktionen verfügbar:

- Statische Netzadressumsetzung
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

Der Fortinet FortiOS-Adapter interagiert mit FortiOS über Telnet oder SSH. In der folgenden Liste werden Einschränkungen von QRadar Risk Manager und dem Fortinet FortiOS-Adapter beschrieben:

- Geographiebasierte Adressen und referenzierte Richtlinien werden nicht von QRadar Risk Manager unterstützt.
- Identitätsbasierte, VPN- und Internet Protocol Security-Richtlinien werden nicht von QRadar Risk Manager unterstützt.
- Richtlinien, bei denen es sich um Unified Threat Management-Profile (UTM) handelt, werden nicht vom Fortinet FortiOS-Adapter unterstützt. Es werden nur Layer 3-Firewallrichtlinien unterstützt.
- Richtlinienrouten werden nicht unterstützt.
- Virtuelle Domänen mit virtuellen Verbindungen, die über IP-Teiladressen oder über keine IP-Adressen verfügen, werden nicht unterstützt.

Die Integrationsanforderungen für den Fortinet FortiOS-Adapter werden in der folgenden Tabelle beschrieben:

Tabelle 13. Integrationsanforderungen für den Fortinet FortiOS-Adapter

Integrationsanforderung	**Beschreibung**
Version	4.0 MR3 bis 5.2.4
SNMP-Erkennung	Nein
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH**
Voraussetzungen für Zugriff auf Benutzerebene	Schreib-/Lesezugriff für Fortinet-Firewalls mit aktivierten VDOMs Lesezugriff für Fortinet-Firewalls ohne aktivierte VDOMs

Tabelle 13. Integrationsanforderungen für den Fortinet FortiOS-Adapter (Forts.)

Integrationsanforderung	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`config system console`
	
	`set output standard`
	Anmerkung: Die Befehle `config system console` und `set output standard` setzen einen Benutzer mit Schreib-/Lesezugriff auf die Systemkonfiguration voraus. Verfügt der Benutzer beim Backup einer Fortigate-Einheit nur über Leseberechtigung mit aktiviertem Seitenumbruch, beeinträchtigt dies die Leistung signifikant.
	
	`show system interface`
	
	`get hardware nic <Variable>`
	
	`get system status`
	
	`get system performance status`
	
	`get router info routing-table static`
	
	`get test dnsproxy 6`
	
	`show firewall addrgrp`
	
	`show firewall address`
	
	`show full-configuration`
	
	`get firewall service predefined <Variable>`
	
	`show firewall service custom`
	
	`show firewall service group`
	
	`show firewall policy`
	
	`show system zone`
	
	`show firewall vip`
	
	`show firewall vipgrp`
	
	`show firewall ippool`

Befehle, die für VDOMs verwendet werden	`config global`: Globalen Konfigurationsmodus eingeben `config vdom; edit <VDOM-Name>`: Umschalten zwischen VDOMs

Generischer SNMP-Adapter

Mit dem generischen SNMP-Adapter unterstützt IBM Security QRadar Risk Manager auch Appliances mit einem SNMP-Agenten.

Dieser Adapter interagiert mittels SNMP-Abfragen mit dem SNMP-Agenten.

Die Objektkennungen (OIDs) sind in SNMP MIB-2 enthalten und werden von allen SNMP-Agenten bereitgestellt.

Für den Adapter gelten folgende Einschränkungen:

- Erfasst nur die grundlegenden Schnittstellen- und Systeminformationen. Regel- und Routing-Informationen werden nicht erfasst.
- Auch wenn in **Configuration Source Management** angezeigt, unterstützt der Adapter bei Verwendung von SNMPv3 keine AES-Verschlüsselung.
- Der Adapter unterstützt bei Verwendung von SNMPv3 keine AES-Verschlüsselung, selbst wenn im Fenster **Configuration Source Management** angegeben ist, dass diese Verschlüsselung unterstützt wird.

Die Integrationsanforderungen für den generischen SNMP-Adapter sind in der folgenden Tabelle beschrieben:

Integrationsanforderung	**Beschreibung**
Version	SNMPv1, SNMPv2c, SNMPv3
Neighbor-Datenunterstützung	Nein
SNMP-Erkennung	Nein
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Für SNMPv1 und SNMPv2c ist Folgendes erforderlich: **SNMP Get Community** Für SNMPv3 ist Folgendes erforderlich: **SNMPv3 Authentication Username (Benutzername für die SNMPv3-Authentifizierung)** SNMPv3 unterstützt folgende Berechtigungsnachweise: **SNMPv3 Authentication Password (Kennwort für die SNMPv3-Authentifizierung)** **SNMPv3 Privacy Password (Datenschutzkennwort für SNMPv3)**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **SNMPv1** **SNMPv2c** **SNMPv3 using MD5** **SHA with DES**

Integrationsanforderung	Beschreibung
Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	SNMP Get-Befehle .1.3.6.1.2.1.1.1.0 .1.3.6.1.2.1.1.2.0 .1.3.6.1.2.1.1.3.0 .1.3.6.1.2.1.1.4.0 .1.3.6.1.2.1.1.5.0 .1.3.6.1.2.1.1.6.0 SNMP Walk-Befehle .1.3.6.1.2.1.2.2.1.2 .1.3.6.1.2.1.2.2.1.3 .1.3.6.1.2.1.2.2.1.4 .1.3.6.1.2.1.2.2.1.5 .1.3.6.1.2.1.2.2.1.6 .1.3.6.1.2.1.2.2.1.7 .1.3.6.1.2.1.4.20

HP Networking ProVision

IBM Security QRadar Risk Manager unterstützt den HP Networking ProVision-Adapter.

Mit dem HP Networking ProVision-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- SNMP-Erkennung
- Dynamisches RIP-Routing
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für den HP Networking ProVision-Adapter beschrieben.

Tabelle 14. Integrationsanforderungen für den HP Networking ProVision-Adapter

Integrationsanforderungen	Beschreibung
Versionen	HP Networking ProVision Switches K/KA.15.X **Einschränkung:** HP-Switches mit Comware-Betriebssystem werden nicht unterstützt.
SNMP-Erkennung	Gleicht in der sysDescr Versionsnummern mit dem Format `HP(.*)Switch(.*)(revision [A-Z]{1,2}\.(\d+)\.(\d+))` ab.

Tabelle 14. Integrationsanforderungen für den HP Networking ProVision-Adapter (Forts.)

Integrationsanforderungen	**Beschreibung**
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort** **Kennwort aktivieren**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**SSH**

Tabelle 14. Integrationsanforderungen für den HP Networking ProVision-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Vom Adapter an die Einheit ausgegebene Backup-Befehle	`dmesgshow system power-supply`
	
	`getmib`
	
	`show access-list vlan <VLAN-ID>`
	
	`show access-list`
	
	`show access-list <Name oder Zahl>`
	
	`show access-list ports <Portnummer>`
	
	`show config`
	
	`show filter`
	
	`show filter <ID>`
	
	`show running-config`
	
	`show interfaces brief`
	
	`show interfaces <Schnittstellen-ID>` (für jede Schnittstelle)
	
	`show jumbos`
	
	`show trunks`
	
	`show lacp`
	
	`show module`
	
	`show snmp-server`
	
	`show spanning-tree`
	
	`show spanning-tree config`
	
	`show spanning-tree instance <ID oder Liste>` (für jeden auf der Einheit konfigurierten Spanning Tree)
	
	`show spanning-tree mst-config`
	
	`show system information`
	
	`show version`
	
	`show vlans`
	
	`show vlans <ID>` (für jedes VLAN)
	
	`show vrrp`
	
	`walkmib`

Tabelle 14. Integrationsanforderungen für den HP Networking ProVision-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

`show ip` Vom Adapter an die Einheit ausgegebene Backup-Befehle	`show ip`
	`show ip route`
	`show ip odpf`
	`show ip odpf redistribute`
	`show ip rip`
	`show ip rip redistribute`

Telemetry- und Neighbor-Datenbefehle	`getmib`
	`show arp`
	`show cdp neighbors`
	`show cdp neighbors detail <Portnummer>`
	`show interfaces brief`
	`show interface`
	`show ip route`
	`show lldp info remote-device`
	`show lldp info remote-device <Portnummer>`
	`show mac-address oder show mac address`
	`show system information`
	`show vlans`
	`show vlans custom id state ipaddr ipmask`
	`walkmib`

Juniper Networks JUNOS

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Juniper Networks JUNOS-Adapter erfüllt sein.

Mit dem Juniper Networks JUNOS-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- SNMP-Erkennung
- Dynamisches OSPF-Routing
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für den Juniper Networks JUNOS-Adapter beschrieben.

Tabelle 15. Integrationsanforderungen für den Juniper Networks JUNOS-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	10.4 11.2 bis 12.3 13.2
SNMP-Erkennung	Gleicht SNMP sysOID 1.3.6.1.4.1.2636 ab
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH** **SCP**

Tabelle 15. Integrationsanforderungen für den Juniper Networks JUNOS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show version`
	`show system uptime`
	`show chassis hardware`
	`show chassis firmware`
	`show chassis mac-address`
	`show chassis routing-engine`
	`show configuration snmp`
	`show snmp mib walk system configure`
	`show configuration firewall`
	`show configuration firewall family inet6`
	`show configuration security`
	`show configuration security zones`
	`show interfaces`
	`show interfaces filters`
	`show ospf interface detail`
	`show bgp neighbor`
	`show configuration routing-option`
	`show arp no-resolve`
	`show ospf neighbor`
	`show rip neighbor`

Juniper Networks NSM

Der IBM Security QRadar Risk Manager-Adapter unterstützt Juniper Networks NSM (Network and Security Manager).

Mit QRadar Risk Manager können Sie eine einzelne Juniper Networks-Einheit verwenden oder Einheitendaten von einer Juniper Networks NSM-Konsole abrufen.

Die Juniper Networks NSM-Konsole (Network and Security Manager) enthält die Konfigurations- und Einheitendaten der von der Konsole verwalteten Juniper Networks-Router und -Switches.

Sie können HTTPS- und SOAP-Verbindungsprotokolle mit Juniper Networks NSM verwenden.

In der folgenden Tabelle werden die für Juniper Networks NSM unterstützten Umgebungen beschrieben.

Tabelle 16. Adapterunterstützte QRadar Risk Manager Umgebungen für Juniper Networks NSM

Unterstützte Umgebung	Beschreibung
Versionen	Von NSM verwaltete IDP-Appliances
SNMP-Erkennung	Nicht unterstützt
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **SOAP** **HTTP**

Juniper Networks ScreenOS

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Juniper Networks ScreenOS-Adapter erfüllt sein.

Mit dem Juniper Networks ScreenOS-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- Dynamische Netzadressumsetzung
- Statische Netzadressumsetzung
- SNMP-Erkennung
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

In der folgenden Tabelle werden die Integrationsanforderungen für den Juniper Networks ScreenOS-Adapter beschrieben.

Tabelle 17. Integrationsanforderungen für den Juniper Networks ScreenOS-Adapter

Integrationsanforderungen	Beschreibung
Versionen	5.4 6.2
SNMP-Erkennung	Gleicht in der SNMP sysDescr netscreen oder SSG ab
Erforderliche Parameter für Berechtigungsnachweise	**Benutzername** **Kennwort**

Tabelle 17. Integrationsanforderungen für den Juniper Networks ScreenOS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung
Unterstützte Verbindungsprotokolle	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** **SSH**

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`set console page 0`
	`get system`
	`get config`
	`get snmp`
	`get memory`
	`get file info`
	`get file`
	`get service`
	`get group address`*`Zone Gruppe`*
	`get address`

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt (Fortsetzung)	`get service group`
	`get service group` *`Variable`*
	`get interface`
	`get interface`*`Variable`*
	`get policy all`
	`get policy id`*`Variable`*
	`get admin user`
	`get route`
	`get arp`
	`get mac-learn`
	`get counter statistics interface` *`Variable`*
	Dabei gilt: *Zone* sind die vom Befehl `get config` zurückgegebenen Zonendaten.
	Gruppe sind die vom Befehl `get config` zurückgegebenen Gruppendaten.
	Variable ist eine Liste der vom Befehl `get service group`, `get interface` oder `get policy id` zurückgegebenen Daten.

Palo Alto

IBM Security QRadar Risk Manager unterstützt den Palo Alto-Adapter. Die Kommunikation zwischen dem Palo Alto-Adapter und Palo Alto-Firewalleinheiten erfolgt über die XML-basierte REST-API von PAN-OS.

Mit dem Palo Alto-Adapter sind folgende Funktionen verfügbar:

- Neighbor-Datenunterstützung
- Dynamische Netzadressumsetzung
- Statische Netzadressumsetzung
- SNMP-Erkennung
- IPSec-Tunnelung/VPN
- Anwendungen
- Benutzer/Gruppen
- HTTPS-Verbindungsprotokoll

Anmerkung:

Gemeinsam genutzte Richtlinien, die von Panorama, dem Palo Alto-Managementsystem für Netzsicherheit, an Einheiten weitergeleitet werden, werden vom Palo Alto-Adapter nicht unterstützt.

In der folgenden Tabelle werden die Integrationsanforderungen für den Palo Alto-Adapter beschrieben.

Tabelle 18. Integrationsanforderungen für den Palo Alto-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	PAN-OS Versionen 5.0 bis 7.0
Minimale Benutzerzugriffsebene	Superuser (uneingeschränkter Zugriff) für PA-Einheiten, die für die Ausführung von Befehlen auf Systemebene dynamische Blockiert-Listen verwenden. Superuser (nur Lesen) für alle anderen PA-Einheiten.
SNMP-Erkennung	Gleicht in der SysDescr 'Palo Alto Networks(.*)series firewall' ab und in der sysOid 'panPA'.
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**HTTPS**

Tabelle 18. Integrationsanforderungen für den Palo Alto-Adapter (Forts.)

Integrationsanforderungen	Beschreibung
Erforderliche Befehle für die Backup-Operation.	/api/?type=op&cmd=<show><system><info></info></system>/show> /api/?type=op&cmd=<show><config><running></running></config></show> /api/?type=op&cmd=<show><interface>all</interface></show>
Optionale Befehle für die Back-up-Operation.	/api/?type=op&cmd=<show><system><resources></resources></system></show> /api/?type=op&cmd=/config/predefined/service /api/?type=op&cmd=<request><system><external-list><show><name>$listName</name>< /show></external-list></system></request>, wobei *$listName* eine Variable in diesem Befehl ist, die mehrfach ausgeführt wird. /api/?type=op&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show> /api/?type=config&action=get&xpath=/config/predefined/application
Erforderliche Befehle für Telemetrie- und benachbarte Daten.	/api/?type=op&cmd=<show><system><info></info></system></show> /api/?type=op&cmd=<show><interface>all</interface></show> /api/?type=op&cmd=<show><routing><interface></interface></routing></show>
Optionale Befehle für Telemetrie- und benachbarte Daten.	/api/?type=op&cmd=<show><counter><interface>all</interface></counter></show> /api/?type=op&cmd=<show><arp>all</arp></show> <show><mac>all</mac></show> /api/?type=op&cmd=<show><arp>all</arp></show> /api/?type=op&cmd=<show><routing><route></route></routing></show>
Erforderliche Befehle für die Get-Anwendung.	/api/?type=config&action=get&xpath=/config/predefined/application

Sidewinder

IBM Security QRadar Risk Manager unterstützt McAfee Enterprise Firewall (Sidewinder)-Appliances mit SecureOS.

Mit dem Sidewinder-Adapter sind folgende Funktionen verfügbar:

- Statische Netzadressumsetzung
- Statisches Routing
- Telnet- und SSH-Verbindungsprotokolle

Der Sidewinder-Adapter interagiert mit dem CLI-basierten McAfee-Betriebssystem (SecureOS) über Telnet oder SSH.

Für den Sidewinder-Adapter gelten folgende Einschränkungen:

- Es werden nur Firewallrichtlinien der Stufe 3 unterstützt, da die Richtlinien der Stufe 7, die Sidewinder-Anwendungsabwehrmechanismen verwenden, nicht unterstützt werden.
- Identitätsbasierte, geografiebasierte und IPv6-Richtlinien werden ignoriert, da diese Richtlinien von QRadar Risk Manager nicht unterstützt werden.

Die Integrationsanforderungen für den Sidewinder-Adapter sind in der folgenden Tabelle beschrieben:

Tabelle 19. Sidewinder-Adapter

Integrationsanforderung	**Beschreibung**
Unterstützte Versionen	8.3.2
Minimale Benutzerzugriffsebene	admin Die Benutzerzugriffsebene "Admin" ist zum Abrufen vordefinierter Serviceinformationen aus der Datenbank mit dem Befehl **`cf appdb list verbose=on`** erforderlich.
SNMP-Erkennung	Nein
Erforderliche Parameter für Berechtigungsnachweise	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **SSH** **Telnet**

Tabelle 19. Sidewinder-Adapter (Forts.)

Integrationsanforderung	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`hostname`
	
	`uname -r`
	
	`uptime`
	
	`cf license q`
	
	`cf route status`
	
	`cf ipaddr q`
	
	`cf iprange q`
	
	`cf subnet q`
	
	`cf domain q`
	
	Verwenden Sie `"dig $address +noall +answer"` für jede Domänenausgabe aus: `cf domain q`
	
	`cf host q`
	
	`cf netmap q`
	
	`cf netgroup q`
	
	`cf appdb list verbose=on`
	
	`cf application q`
	
	`cf appgroup q`
	
	`cf policy q`
	
	`cf interface q`
	
	`cf zone q`

Sourcefire 3D Sensor

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Sourcefire 3D Sensor-Adapter erfüllt sein.

Mit dem Sourcefire 3D Sensor-Adapter sind folgende Funktionen verfügbar:

- IPS
- SSH-Verbindungsprotokoll

Einschränkungen:

- Von QRadar Risk Manager werden keine Richtlinien zum Angriff von außen für einzelne Regeln zur Zugriffssteuerung verwendet. Es wird nur die standardmäßige Richtlinie zum Angriff von außen unterstützt.
- Netzadressumsetzung und virtuelles privates Netz werden nicht unterstützt.

In der folgenden Tabelle werden die Integrationsanforderungen für den Sourcefire 3D Sensor-Adapter beschrieben.

Tabelle 20. Integrationsanforderungen für den Sourcefire 3D Sensor-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	5.2
Unterstützung für 3D-Sensoren (Series 2-Einheiten)	3D500 3D1000 3D2000 3D2100 3D2500 3D3500 3D4500 3D6500 3D9900
SNMP-Erkennung	Nein
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**Benutzername** **Kennwort**
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	**SSH**

Tabelle 20. Integrationsanforderungen für den Sourcefire 3D Sensor-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show version`
	`show memory`
	`show network`
	`show interfaces`
	`expert`
	`sudo`
	`su`
	`df`
	`hostname`
	`ip addr`
	`route`
	`cat`
	`find`
	`head`
	`mysql`

TippingPoint IPS-Adapter

IBM Security QRadar Risk Manager unterstützt TippingPoint IPS (Intrusion Prevention System)-Appliances mit TOS, die unter der Kontrolle von SMS stehen.

Mit dem TippingPoint IPS-Adapter sind folgende Funktionen verfügbar:

- IPS
- Telnet-, SSH+HTTPS-Verbindungsprotokolle

Für diesen Adapter ist eine Interaktion mit den folgenden Einheiten erforderlich:

- IPS (direkt) über das Betriebssystem TippingPoint (TOS) über Telnet oder SSH
- TippingPoint Secure Management Server (SMS) über die Web-Service-API über HTTPS

Zum Abrufen der aktuellen, von SMS verwalteten Digital Vaccines-Signaturen ist eine Verbindung mit TippingPoint SMS erforderlich.

Dieser Adapter funktioniert nur, wenn die IPS-Einheiten unter SMS-Kontrolle stehen. Für eine erfolgreiche Sicherung müssen die SMS-Web-Services aktiviert sein.

Es folgt eine Liste mit Einschränkungen des TippingPoint-Adapters:

- QRadar Risk Manager verarbeitet keine Quell- oder Ziel-IP-Adressen in IPS-Regeln oder -Filtern. Die folgenden Funktionen von TippingPoint werden nicht unterstützt:
  - Verwaltungsfilter für Datenverkehr
  - Profil- oder Filterausnahmen und -einschränkungen

– Benutzerdefinierte Filter
- IPS-Filter ohne zugeordnete CVE werden nicht modelliert, da IPS in diesem Fall keinen QRadar-Schwachstellen zugeordnet werden kann.

Die Integrationsanforderungen für den TippingPoint-Adapter sind in der folgenden Tabelle beschrieben:

Tabelle 21. TippingPoint IPS-Adapter

Integrationsanforderung	**Beschreibung**
Unterstützte Versionen	TOS 3.6 und SMS 4.2
Minimale Benutzerzugriffsebene	IPS: Operator SMS: Operator (benutzerdefiniert) Ein Benutzer, der einer Gruppe mit einer *benutzerdefinierten Operatorrolle* angehört, für die `Access SMS Web Services` (Auf SMS-Web-Services zugreifen) aktiviert ist.
SNMP-Erkennung	Nein
Erforderliche Parameter für Berechtigungsnachweise Zum Hinzufügen von Berechtigungsnachweisen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Geben Sie die folgenden Berechtigungsnachweise ein: **Username**: *<IPS-CLI-Benutzername>* **Password**: *<IPS CLI Kennwort>* **Enable Username**: *<SMS-Benutzername>* **Enable Password**: *<SMS-Kennwort>*
Unterstützte Verbindungsprotokolle Zum Hinzufügen von Protokollen in QRadar melden Sie sich als Administrator an und gehen dann auf der Registerkarte **Verwaltung** zu **Configuration Source Management**.	Verwenden Sie eines der folgenden unterstützten Verbindungsprotokolle: **Telnet** für IPS CLI **SSH** für IPS CLI **HTTPS** für SMS

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show config`
	
	`show version`
	
	`show interface`
	
	`show host`
	
	`show sms`
	
	`show filter $filterNumber` (für jede Signatur in Digital Vaccine)

API-Befehle an das SMS zum Abrufen der aktuellen Signaturen	`https://<SMS-Server>/dbAccess/tptDBServlet?method=DataDictionary&table=SIGNATURE&format=xml`

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Défense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Director of Licensing
IBM Corporation

North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die angeführten Leistungsdaten und Kundenbeispiele dienen lediglich zu Zwecken der Information und Erläuterung. Die tatsächlichen Leistungsergebnisse können daher je nach Konfigurationen und Betriebsbedingungen anders ausfallen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Personen oder Unternehmen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Bedingungen für die Produktdokumentation

Die Rechte zur Nutzung dieser Veröffentlichungen werden zu den nachstehenden Bedingungen erteilt.

Anwendbarkeit

Die vorliegenden Bedingungen gelten zusätzlich zu den Nutzungsbedingungen für die IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens nicht vervielfältigen, weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Rechte

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Informationen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

IBM Online-Datenschutzerklärung

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Je nachdem, welche Konfigurationen bereitgestellt sind, kann dieses Softwareangebot Sitzungscookies verwenden, die für das Sitzungsmanagement und die Authentifizierung die Sitzungs-ID jedes Benutzers erfassen. Diese Cookies können inaktiviert werden, damit wird aber zugleich die dadurch ermöglichte Funktionalität inaktiviert.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung rechtlich beraten lassen, insbesondere Meldepflichten sowie die Einforderung von Einwilligungen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Datenschutzerklärung unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und unter "IBM Software Products and Software-as-a-Service Privacy Statement" (http://www.ibm.com/software/info/product-privacy).