IBM Security QRadar Risk Manager
Version 7.2.2

Benutzerhandbuch

SC12-5034-00

IBM Security QRadar Risk Manager
Version 7.2.2

Benutzerhandbuch

SC12-5034-00

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 145 gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security QRadar Risk Manager, Version 7.2.2, User's Guide,
IBM Form SC27-6247-00,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
März 2014

Inhaltsverzeichnis

Einführung in IBM Security QRadar Risk Manager

Diese Informationen richten sich an Benutzer von IBM® Security QRadar Risk Manager. QRadar Risk Manager ist eine Appliance zur Überwachung von Einheitenkonfigurationen, Simulation von Netzänderungen und Zuordnung von Prioritäten zu Risiken und Schwachstellen in Ihrem Netz.

Dieses Handbuch enthält Anweisungen zur Konfiguration und Verwendung von IBM Security QRadar Risk Manager auf einer IBM Security QRadar SIEM-Konsole.

Zielgruppe

Systemadministratoren, die für die Konfiguration und Verwendung von QRadar Risk Manager verantwortlich sind. Diese müssen einen Verwaltungszugriff auf IBM Security QRadar SIEM und Ihre Netzeinheiten und Firewalls besitzen. Der Systemadministrator muss Ihr Unternehmensnetz und Ihre Netztechnologien kennen.

Technische Dokumentation

Informationen zum Zugang zu weiteren technischen Dokumentationen, technischen Hinweisen und Releaseinformationen finden Sie auf der Webseite Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Kundenunterstützung anfordern

Informationen zur Anforderung der Kundenunterstützung finden Sie auf der Webseite Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Erklärung zu geeigneten Sicherheitsverfahren

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen durch Vorbeugung, Erkennung und Handhabung von unbefugten Zugriffen innerhalb des Unternehmens und von außen. Unbefugte Zugriffe können dazu führen, dass Informationen geändert, gelöscht, veruntreut oder unsachgemäß verwendet werden oder dass Ihre Systeme beschädigt oder missbraucht werden, z. B. für Attacken auf andere. Kein IT-System oder -Produkt sollte als vollständig sicher betrachtet werden und kein Endprodukt, kein Service und keine Sicherheitsmaßnahme kann einen unbefugten Gebrauch oder Zugriff mit absoluter Sicherheit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, was die Einbeziehung zusätzlicher Betriebsprozesse erforderlich macht und gegebenenfalls auch bei anderen Systemen, Produkten oder Services eine maximale Effektivität voraussetzt. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

Kapitel 1. Neuerungen für Benutzer in QRadar Risk Manager V7.2.2

In IBM Security QRadar Risk Manager V7.2.2 wurden Topologie- und Regelsuchvorgänge sowie Zugriffssteuerungslisten und Richtlinientests aktualisiert.

Pfadzusammenfassung für die Topologiesuche

Wenn Sie die Verbindungen zwischen Netzen oder Einheiten suchen, wird eine Pfadzusammenfassung angezeigt, in der die Portverbindungen zwischen Einheiten aufgezeigt werden. Falls keine Verbindung zwischen Einheiten verfügbar ist, wird die geblockte Verbindung im Topologiemodell mit einem roten Quadrat angezeigt.

Weitere Informationen...

Zugriffssteuerungslisten

Sie können die Zugriffssteuerungslisten überprüfen, mit denen der von einer Firewall in Ihrem Netz empfangene Datenverkehr gefiltert wird. Weitere Informationen...

Richtlinientests für das Windows-Betriebssystem

Es wurden zusätzliche Fragen für die Richtlinienüberwachung aufgenommen, die Informationen zur Konfiguration Ihrer Einheiten mit dem Windows-Betriebssystem bereitstellen. Weitere Informationen...

Kapitel 2. IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager ist eine separat installierte Appliance zur Überwachung von Einheitenkonfigurationen, Simulation von Änderungen in Ihrer Netzumgebung und Zuordnung von Prioritäten zu Risiken und Schwachstellen in Ihrem Netz.

QRadar Risk Manager wird über die Registerkarte **Risks** (Risiken) auf Ihrer IBM Security QRadar SIEM Console aufgerufen.

QRadar Risk Manager verwendet Daten, die durch QRadar erfasst werden. Dies können beispielsweise Konfigurationsdaten sein, die aus Firewalls, Routern, Switches oder Intrusion-Prevention-Systemen (IPSs), Schwachstellenfeeds und Sicherheitsquellen anderer Anbieter stammen können. Datenquellen ermöglichen QRadar Risk Manager die Ermittlung von Sicherheits-, Richtlinien- und Konformitätsrisiken in Ihrem Netz sowie die Einschätzung der Wahrscheinlichkeit einer Ausnutzung der Risiken.

QRadar Risk Manager warnt Sie vor den erkannten Risiken, indem entsprechende Angriffe auf der Registerkarte **Angriffe** angezeigt werden. Die Risikodaten werden analysiert und im Kontext von allen anderen Daten, die von QRadar verarbeitet werden, in Form von Berichten dokumentiert. Mithilfe von QRadar Risk Manager können Sie Risiken auf einer akzeptablen Ebene auf der Basis der Risikotoleranz in Ihrem Unternehmen bewerten und steuern.

Mit QRadar Risk Manager können Sie außerdem sämtliche Netzverbindungen abfragen, Einheitenkonfigurationen vergleichen, Ihre Netztopologie filtern und die möglichen Auswirkungen einer Aktualisierung von Einheitenkonfigurationen simulieren.

QRadar Risk Manager ermöglicht die Definition einer Gruppe von Richtlinien (oder Fragen) für Ihr Netz und deren Überwachung auf Änderungen. Wenn Sie zum Beispiel unverschlüsselte Protokolle in Ihrer Demilitarized Zone (DMZ) aus dem Internet zurückweisen möchten, können Sie eine Richtlinienüberwachungsfrage definieren, um unverschlüsselte Protokolle zu erkennen. Nach Übergabe der Frage wird eine Liste mit unverschlüsselten Protokollen, die aus dem Internet mit Ihrer DMZ kommunizieren, zurückgegeben und Sie können bestimmen, bei welchen unverschlüsselten Protokollen es sich um Sicherheitsrisiken handelt.

Verbindungen

Verwenden Sie die Seite **Verbindungen**, um Netzverbindungen von lokalen Hosts zu überwachen.

Sie können Abfragen und Berichte zu den Netzverbindungen lokaler Hosts ausführen, die auf Anwendungen, Ports, Protokollen und Websites basieren, mit denen lokale Hosts kommunizieren können.

Weitere Informationen zu Verbindungen finden Sie im Abschnitt Verbindungen untersuchen.

Konfigurationsüberwachung

Verwenden Sie die Konfigurationsüberwachung, um Einheitenkonfigurationen zu überprüfen und zu vergleichen. Dabei haben Sie die Möglichkeit, Sicherheitsrichtlinien durchzusetzen und Einheitenkonfigurationen innerhalb des Netzes zu überwachen.

Einheitenkonfigurationen können Switches, Router, Firewalls und Intrusion-Prevention-Systeme in einem Netz einschließen. Für jedes Gerät können das Einheitenkonfigurationsprotokoll, Schnittstellen und Regeln angezeigt werden. Sie können Konfigurationen innerhalb eines Geräts und über Geräte hinweg miteinander vergleichen.

Die Einheitenkonfigurationsinformationen werden auch verwendet, um die unternehmensweite Darstellung der Netztopologie zu erstellen, die es Ihnen ermöglicht, zulässige und verweigerte Aktivitäten für das gesamte Netz festzulegen. Mithilfe der Einheitenkonfiguration können Sie Inkonsistenzen und Konfigurationsänderungen ermitteln, die ein Risiko für das Netz darstellen.

Weitere Informationen zu Einheitenkonfigurationen finden Sie im Abschnitt Einheitenkonfigurationen anzeigen.

Topologie

Die Topologie ist eine grafische Darstellung zur Veranschaulichung der Vermittlungsschicht eines Netzes, die auf den über das Configuration Source Management hinzugefügten Einheiten basiert.

Die Vermittlungsschicht ist Schicht 3 des Open Systems Interconnection-(OSI-)Modells.

In der interaktiven Grafik in der Topologie können Verbindungen zwischen Einheiten, virtualisierte Netzsicherheitskomponenten mit mehreren Kontexten, Assets, Network Address Translation-(NAT-)Einheiten, NAT-Indikatoren und Informationen über NAT-Zuordnungen angezeigt werden.

Sie können nach Ereignissen, Einheiten und Pfaden suchen und Netzlayouts speichern.

In der Topologie können Sie die Transportschicht (Schicht 4) abfragen und Netzpfade abhängig von Ports und Protokollen filtern. Die Grafik- und Verbindungsinformationen werden aus detaillierten Konfigurationsinformationen erstellt, die von Netzeinheiten wie Firewalls, Routern und Intrusion-Prevention-Systemen abgerufen werden.

Weitere Informationen finden Sie im Abschnitt Topologie.

Richtlinienüberwachung

Verwenden Sie die Richtlinienüberwachung, um bestimmte Fragen zu Risiken in Ihrem Netz zu definieren und die Fragen an IBM Security QRadar Risk Manager zu übergeben.

QRadar Risk Manager wertet die Parameter aus, die Sie in Ihrer Frage definiert haben, und gibt Assets in Ihrem Netz zurück, um Ihnen bei der Bewertung des Risikos zu helfen. Die Fragen basieren auf einer Serie von Tests, die nach Bedarf kom-

biniert und konfiguriert werden können. QRadar Risk Manager stellt eine große Zahl von vordefinierten Richtlinienüberwachungsfragen bereit und ermöglicht die Erstellung von benutzerdefinierten Fragen. Richtlinienüberwachungsfragen können für folgende Situationen erstellt werden:

- Kommunikationen, die stattgefunden haben
- Mögliche Kommunikationen auf Basis der Konfiguration von Firewalls und Routern
- Tatsächliche Firewallregeln (Einheitentests)

Die Richtlinienüberwachung verwendet Daten, die aus Konfigurationsdaten, Netzaktivitätsdaten, Netz- und Sicherheitsereignissen sowie Schwachstellensuchen abgerufen werden, um die geeignete Antwort festzulegen. QRadar Risk Manager stellt Richtlinienvorlagen, die Sie bei der Bestimmung des Risikos hinsichtlich mehrerer gesetzlicher Vorschriften unterstützen, und bewährte Informationssicherheitsverfahren wie PCI, HIPPA und ISO 27001 bereit. Sie können die Vorlagen aktualisieren, um sie an den von Ihrem Unternehmen definierten Richtlinien zur Informationssicherheit auszurichten. Wenn die Antwort vollständig ist, können Sie die Antwort auf die Frage akzeptieren und angeben, wie das System auf nicht akzeptierte Ergebnisse reagieren soll.

Die Richtlinienüberwachung ermöglicht die aktive Überwachung einer unbegrenzten Anzahl von Fragen. Bei der Überwachung einer Frage überprüft QRadar Risk Manager die Frage kontinuierlich auf nicht genehmigte Ergebnisse. Wenn nicht genehmigte Ergebnisse auftreten, kann QRadar Risk Manager eine E-Mail senden, Benachrichtigungen anzeigen, ein syslog-Ereignis generieren oder einen Angriff in QRadar SIEM erstellen.

Weitere Informationen zur Richtlinienüberwachung finden Sie im Abschnitt Richtlinienüberwachung.

Simulationen

Verwenden Sie Simulationen, um Exploit-Simulationen zu definieren, zu planen und in Ihrem Netz durchzuführen.

Sie können eine simulierte Attacke auf eine Topologie auf der Basis einer Serie von Parametern erstellen, die auf ähnliche Weise wie für die Richtlinienüberwachung konfiguriert werden. Sie können eine simulierte Attacke auf die aktuelle Netztopologie oder ein Topologiemodell erstellen. Ein Topologiemodell ist eine virtuelle Topologie, die es Ihnen ermöglicht, Änderungen in der virtuellen Topologie vorzunehmen und eine Attacke zu simulieren. Auf diese Weise können Sie simulieren, wie sich Änderungen von Netzregeln, Ports, Protokollen und zulässigen oder verweigerten Verbindungen auf ein Netz auswirken können. Eine Simulation ist ein leistungsfähiges Tool, um die Risikoauswirkung von vorgeschlagenen Änderungen in einer Netzkonfiguration zu bestimmen, bevor die Änderungen implementiert werden.

Nach Abschluss einer Simulation können Sie die Ergebnisse prüfen. Wenn Sie die Ergebnisse akzeptieren möchten, können Sie den Simulationsmodus konfigurieren, in dem Sie definieren können, wie Sie auf nicht akzeptierte Ergebnisse antworten wollen.

QRadar Risk Manager ermöglicht die aktive Überwachung von bis zu zehn Simulationen. Bei der Überwachung einer Simulation analysiert QRadar Risk Manager die Topologie kontinuierlich auf nicht genehmigte Ergebnisse. Wenn nicht geneh-

migte Ergebnisse auftreten, kann QRadar Risk Manager eine E-Mail senden, Benachrichtigungen anzeigen, ein syslog-Ereignis generieren oder einen Angriff in QRadar SIEM erstellen.

Weitere Informationen zu Simulationen finden Sie im Abschnitt Simulationen verwenden.

QRadar Risk Manager-Berichte

Verwenden Sie die Registerkarte **Berichte**, um bestimmte Berichte auf der Basis von in QRadar Risk Manager verfügbaren Daten wie Verbindungen, Einheitenregeln und nicht verwendete Objekte auf Einheiten anzuzeigen.

Folgende zusätzliche detaillierte Berichte sind verfügbar:

- Verbindungen zwischen Einheiten
- Firewallregeln auf einer Einheit
- Nicht verwendete Objekte auf einer Einheit

Weitere Informationen zu Berichten finden Sie im Abschnitt IBM Security QRadar Risk Manager-Berichte verwalten.

Unterstützte Web-Browser

Damit die Funktionen in IBM Security QRadar-Produkten ordnungsgemäß ausgeführt werden können, müssen Sie einen unterstützen Web-Browser verwenden.

Wenn Sie auf das QRadar-System zugreifen, werden Sie aufgefordert, einen Benutzernamen und ein Kennwort einzugeben. Der Benutzername und das Kennwort müssen vorab vom Administrator konfiguriert werden.

In den folgenden Tabellen werden die unterstützten Web-Browser-Versionen aufgelistet.

Tabelle 1. Unterstützte Web-Browser für QRadar-Produkte

Web-Browser	Unterstützte Version
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32-Bit-Version von Microsoft Internet Explorer mit aktiviertem Dokument- und Browsermodus	9.0
Google Chrome	Die am Freigabedatum der Produkte aus IBM Security QRadar V7.2.2 aktuelle Version

Dokument- und Browsermodus in Internet Explorer aktivieren

Wenn Sie Microsoft Internet Explorer für den Zugriff auf die IBM Security QRadar-Produkte verwenden, müssen Sie den Browsermodus und den Dokumentmodus aktivieren.

Vorgehensweise

1. Drücken Sie in Ihrem Internet Explorer-Web-Browser die Taste F12, um das Fenster **Entwicklertools** zu öffnen.

2. Klicken Sie auf **Browsermodus** und wählen Sie die Version Ihres Web-Browsers aus.
3. Klicken Sie auf **Dokumentmodus**.
   - Wählen Sie für Internet Explorer V9.0 den Eintrag **Internet Explorer 9** aus.
   - Wählen Sie für Internet Explorer V8.0 den Eintrag **Internet Explorer 7.0-Standards** aus.

Zugriff auf die IBM Security QRadar Risk Manager-Benutzerschnittstelle

IBM Security QRadar Risk Manager verwendet Standardanmeldeinformationen für die URL, den Benutzernamen und das Kennwort.

Der Zugriff auf IBM Security QRadar Risk Manager erfolgt über die QRadar SIEM-Konsole. Verwenden Sie bei der Anmeldung an der IBM Security QRadar SIEM-Konsole die Informationen in der folgenden Tabelle.

Tabelle 2. Standardanmeldeinformationen für QRadar Risk Manager

Anmelde-informationen	**Standardwerte**
URL	https://<IP-Adresse>, wobei <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole steht.
Benutzername	admin
Kennwort	Das Kennwort, das QRadar Risk Manager während des Installationsprozesses zugewiesen wird.
Lizenzschlüssel	Ein Standardlizenzschlüssel ermöglicht fünf Wochen lang Zugriff auf das System.

Nicht unterstützte Funktionen in QRadar Risk Manager

Es ist wichtig zu wissen, welche Funktionen nicht von IBM Security QRadar Risk Manager unterstützt werden.

Die folgenden Funktionen werden nicht in QRadar Risk Manager unterstützt:

- Hochverfügbarkeit
- Dynamische Routing für Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) oder Routing Information Protocol (RIP)
- Internet Protocol Version 6 (IPv6)
- Nicht zusammenhängende Netzmasken
- Routen mit Lastausgleich
- Referenzzuordnungen
- Store-and-forward-Verfahren

Kapitel 3. IBM Security QRadar Risk Manager-Einstellungen konfigurieren

Sie können die Zugriffseinstellungen für IBM Security QRadar Risk Manager auf der Registerkarte **Verwaltung** von IBM Security QRadar SIEM konfigurieren.

Wenn Sie die geeigneten Berechtigungen besitzen, können Sie verschiedene Appliance-Einstellungen für QRadar Risk Manager konfigurieren.

Administratoren können folgende Aufgaben ausführen:

- Konfiguration von Einheiten, auf die QRadar Risk Manager über die lokale Firewall zugreifen kann. Weitere Informationen finden Sie im Abschnitt Firewallzugriff konfigurieren.
- Aktualisierung des E-Mail-Servers für QRadar Risk Manager. Weitere Informationen finden Sie im Abschnitt QRadar Risk Manager-Setup aktualisieren.
- Konfiguration der Schnittstellenrollen für einen Host. Weitere Informationen finden Sie im Abschnitt Benutzerschnittstellenrollen konfigurieren.
- Änderung des Kennworts für einen Host. Weitere Informationen finden Sie im Abschnitt Rootkennwort ändern.
- Aktualisierung der Systemzeit. Weitere Informationen finden Sie im Abschnitt Systemzeit aktualisieren.

Konfigurationsänderungen, die über die webbasierte Systemverwaltung erfolgen, werden sofort nach der Speicherung oder Anwendung der Änderungen wirksam.

Firewallzugriff konfigurieren

Sie können einen lokalen Firewallzugriff konfigurieren, um die Kommunikation zwischen QRadar Risk Manager und bestimmten IP-Adressen, Protokollen und Ports zu aktivieren oder zu deaktivieren.

Informationen zu diesem Vorgang

Sie können eine Liste von IP-Adressen definieren, die auf die webbasierte Systemverwaltung zugreifen dürfen. Diese Felder sind standardmäßig leer, wodurch es keine Einschränkung in der Kommunikation mit QRadar Risk Manager gibt. Wenn Sie jedoch eine IP-Adresse hinzufügen, wird nur dieser IP-Adresse Zugriff auf das System erteilt. Alle anderen IP-Adressen werden geblockt.

Sie müssen die IP-Adresse des Client-Desktops einschließen, den Sie für den Zugriff auf QRadar Risk Manager verwenden. Wenn Sie dies unterlassen, kann es Auswirkungen auf die Konnektivität haben.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie auf das Symbol für **Systemmanagement**.
4. Melden Sie sich als Rootbenutzer an, um auf die webbasierte Systemverwaltung zugreifen zu können. Bei Benutzername und Kennwort muss die Groß-/Kleinschreibung beachtet werden.

5. Wählen Sie im Menü **Managed Host Config** > **Local Firewall** (Konfiguration des verwalteten Host > Lokale Firewall) aus.
6. Konfigurieren Sie im Fenster 'Device Access' (Einheitenzugriff) die IP-Adressen, Ports und Protokolle, die Sie QRadar Risk Manager als lokale Firewallregel hinzufügen möchten.
7. Geben Sie im Feld **IP Address** (IP-Adresse) die IP-Adressen der Einheiten ein, auf die Sie zugreifen möchten.
8. Wählen Sie in der Liste **Protocol** (Protokoll) das Protokoll aus, für das Sie den Zugriff auf die angegebene IP-Adresse und den angegebenen Port aktivieren möchten.
9. Geben Sie im Feld **Port** den Port ein, auf dem Sie die Kommunikation aktivieren möchten, und klicken Sie auf **Allow** (Zulassen).
10. Geben Sie die IP-Adresse des verwalteten Hosts ein, für den Sie den Zugriff auf die webbasierte Systemverwaltung aktivieren möchten, und klicken Sie auf **Allow** (Zulassen). Nur aufgeführte IP-Adressen haben Zugriff auf die webbasierte Systemverwaltung. Wenn Sie das Feld leer lassen, haben alle IP-Adressen Zugriff.
11. Klicken Sie auf **Apply Access Controls** (Zugriffssteuerung anwenden).

QRadar Risk Manager-Einrichtung aktualisieren

Sie können den Mail-Server definieren, der für QRadar Risk Manager-Benachrichtigungen verwendet wird.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie auf das Symbol für **Systemmanagement**.
4. Melden Sie sich als Rootbenutzer an, um auf die webbasierte Systemverwaltung zugreifen zu können. Bei Benutzername und Kennwort muss die Groß-/Kleinschreibung werden.
5. Wählen Sie im Menü **Managed Host Config** > **QRM Setup** (Konfiguration des verwalteten Host > QRM-Einrichtung) aus.
6. Geben Sie im Feld **Mail Server** die IP-Adresse oder den Hostnamen für den Mail-Server ein, der von QRadar Risk Manager verwendet werden soll.

   QRadar Risk Manager verwendet diesen Mail-Server, um Alerts und Ereignisnachrichten weiterzugeben. Um den mit QRadar Risk Manager bereitgestellten Mail-Server zu verwenden, geben Sie **localhost** ein.
7. Klicken Sie auf **Apply Configuration** (Konfiguration anwenden).

Nächste Schritte

Warten Sie, bis die Anzeige aktualisiert wurde, bevor Sie weitere Änderungen vornehmen.

Rollen für die Benutzerschnittstelle konfigurieren

Wenn Ihr Gerät über mehrere Netzschnittstellen verfügt, können Sie den Netzschnittstellen auf jedem System bestimmte Rollen zuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie auf das Symbol für **Systemmanagement**.
4. Melden Sie sich als Rootbenutzer an, um auf die webbasierte Systemverwaltung zugreifen zu können. Bei Benutzername und Kennwort muss die Groß-/Kleinschreibung beachtet werden.
5. Wählen Sie im Menü **Managed Host Config** > **Network Interfaces** (Konfiguration des verwalteten Host > Netzschnittstellen) aus.
6. Wählen Sie mithilfe der Liste 'Role' (Rolle) für jede aufgeführte Schnittstelle die Rolle aus, die Sie der Schnittstelle zuweisen möchten.

   In den meisten Fällen kann die aktuell angezeigte Konfiguration nicht bearbeitet werden.
7. Klicken Sie auf **Konfiguration speichern**.
8. Warten Sie, bis die Anzeige aktualisiert wurde, bevor Sie weitere Änderungen vornehmen.

Rootkennwort ändern

Sie können das Rootkennwort ändern.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie auf das Symbol für **Systemmanagement**.
4. Melden Sie sich als Rootbenutzer an, um auf die Einstellungen der Systemverwaltung zugreifen zu können. Bei Benutzername und Kennwort muss die Groß-/Kleinschreibung beachtet werden.
5. Wählen Sie im Menü **Managed Host Config** > **Root Password** (Konfiguration des verwalteten Host > Rootkennwort) aus.
6. Geben Sie im Feld **New Root Password** (Neues Rootkennwort) das Rootkennwort für den Zugriff auf die webbasierte Systemverwaltung ein und geben Sie das Kennwort im Feld **Confirm New Root Password** (Neues Rootkennwort bestätigen) erneut ein.
7. Klicken Sie auf **Update Password** (Kennwort aktualisieren).

Systemzeit aktualisieren

Wenden Sie sich an die Kundenunterstützung, bevor Sie die Systemzeit für das QRadar Risk Manager-System aktualisieren.

Vorbereitende Schritte

Alle Änderungen an der Systemzeit müssen in der Konsole gespeichert werden. Anschließend werden die aktualisierten Zeiteinstellungen von der Konsole an alle verwalteten Host in Ihrer Implementierung weitergegeben.

Weitere Informationen zur Konfiguration der Systemzeit in Ihrer Konsole finden Sie im *IBM Security QRadar SIEM Administration Guide*.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie auf das Symbol für **Systemmanagement**.
4. Melden Sie sich als Rootbenutzer an, um auf die Einstellungen der Systemverwaltung zugreifen zu können. Bei Benutzername und Kennwort muss die Groß-/Kleinschreibung beachtet werden.
5. Wählen Sie im Menü **Managed Host Config** > **System Time** (Konfiguration des verwalteten Host > Systemzeit) aus. Das Fenster mit den Einstellungen für Datum und Uhrzeit ist in zwei Abschnitte unterteilt. Sie müssen jede Einstellung speicher, bevor Sie den Vorgang fortsetzen. Wenn Sie beispielsweise die Systemzeit konfigurieren, müssen Sie im Fenster 'Systemzeit' auf **Anwenden** klicken, bevor Sie fortfahren.
6. Klicken Sie auf **Set time** (Uhrzeit einstellen).
7. Wählen Sie unter **Systemzeit** das aktuelle Datum und die aktuelle Uhrzeit aus, die Sie dem verwalteten Host zuweisen möchten, und klicken Sie anschließend auf 'Anwenden'.
8. Wählen Sie im Fenster **Hardware Time** (Hardware-Zeit) das aktuelle Datum und die aktuelle Uhrzeit aus, die Sie dem verwalteten Host zuweisen möchten, und klicken Sie auf 'Speichern'.

Kapitel 4. Configuration Source Management

Verwenden Sie Configuration Source Management, um Berechtigungsnachweise zu konfigurieren, Einheiten hinzuzufügen oder zu erkennen, Einheitenkonfigurationen anzuzeigen und Einheitenkonfigurationen in QRadar Risk Manager zu sichern.

Die Daten, die von Einheiten in einem Netz abgerufen werden, werden zum Auffüllen der Topologie verwendet. Sie benötigen Administratorberechtigungen, um über die Registerkarte **Verwaltung** in QRadar SIEM auf die Configuration Source Management-Funktionen zugreifen zu können.

Um Konfigurationsquellen einzurichten, müssen Sie folgende Aufgaben ausführen:

1. Konfigurieren Sie die Einheitenberechtigungsnachweise.
2. Führen Sie eine Einheitenerkennung durch oder importieren Sie Einheiten. Es gibt zwei Möglichkeiten, Netzeinheiten zu QRadar Risk Manager hinzuzufügen: Erkennen von Einheiten über das Configuration Source Management oder Importieren einer Liste von Einheiten aus einer CSV-Datei über 'Geräteimport'.
3. Rufen Sie die Einheitenkonfiguration von jeder der Einheiten ab.
4. Verwalten Sie Sicherungsjobs, um sicherzustellen, dass alle Aktualisierungen von Einheitenkonfigurationen erfasst werden.
5. Legen Sie den Erkennungszeitplan fest, um sicherzustellen, dass neue Einheiten automatisch erkannt werden.

Verwenden Sie Configuration Source Management für folgende Aufgaben:

- Hinzufügen, Bearbeiten, Suchen und Löschen von Konfigurationsquellen. Weitere Informationen finden Sie im Abschnitt Einheiten verwalten.
- Konfigurieren oder Verwalten von Kommunikationsprotokollen für die Einheiten. Weitere Informationen finden Sie im Abschnitt Protokolle konfigurieren.

Wenn Sie die Juniper NSM-Einheit verwenden, müssen Sie ebenfalls Konfigurationsinformationen abrufen.

Ausführliche Informationen zu Adaptern für die Kommunikation mit Einheiten von bestimmten Herstellern finden Sie im *IBM Security QRadar Risk Manager Adapter Configuration Guide* .

Berechtigungsnachweise

In IBM Security QRadar Risk Manager werden Berechtigungsnachweise verwendet, um auf die Konfiguration von Einheiten wie Firewalls, Router, Switches oder Intrusion-Prevention-Systeme zuzugreifen und die Konfiguration herunterzuladen.

Administratoren verwenden Configuration Source Management, um Einheitenberechtigungsnachweise einzugeben. Dies ermöglicht QRadar Risk Manager den Zugriff auf eine bestimmte Einheit. Es können einzelne Einheitenberechtigungsnachweise für eine bestimmte Netzeinheit gespeichert werden. Wenn für mehrere Netzeinheiten dieselben Berechtigungsnachweise verwendet werden, können Sie Berechtigungsnachweise einer Gruppe zuweisen.

Wenn beispielsweise alle Firewalls im Unternehmen denselben Benutzernamen und dasselbe Kennwort haben, dann werden die Berechtigungsnachweise den Adress-

sätzen für alle Firewalls zugeordnet und zur Sicherung von Einheitenkonfigurationen für alle Firewalls im Unternehmen verwendet.

Wenn für eine bestimmte Einheit kein Netzberechtigungsnachweis erforderlich ist, kann der Parameter in Configuration Source Management leer bleiben. Eine Liste mit erforderlichen Adapterberechtigungsnachweisen finden Sie im *IBM Security QRadar Risk Manager Adapter Configuration Guide* .

Sie können unterschiedliche Einheiten im Netz zu Netzgruppen zuweisen und so Berechtigungsnachweis- und Adresssätze für die Einheiten zu Gruppen zusammenfassen.

Berechtigungsnachweissatz

Ein Berechtigungsnachweissatz enthält Informationen wie Benutzername und Kennwortwerte für eine Gruppe von Einheiten.

Netzgruppe

Jede Netzgruppe kann mehrere Berechtigungsnachweis- und Adresssätze einschließen. Sie können QRadar Risk Manager konfigurieren, um Prioritäten für die Bewertung der einzelnen Netzgruppen zu vergeben.

Die Netzgruppe am Anfang der Liste hat die höchste Priorität. Die erste Netzgruppe, die mit der konfigurierten IP-Adresse übereinstimmt, wird beim Speichern einer Einheit als Kandidat eingeschlossen. Es werden maximal drei Berechtigungsnachweissätze aus einer Netzgruppe berücksichtigt.

Angenommen, eine Konfiguration enthält die folgenden zwei Netzgruppen:

- Netzgruppe 1 schließt zwei Berechtigungsnachweissätze ein
- Netzgruppe 2 schließt zwei Berechtigungsnachweissätze ein

QRadar Risk Manager versucht, eine Liste mit maximal drei Berechtigungsnachweissätzen zusammenzustellen. Da Netzgruppe 1 in der Liste höher steht, werden beide Berechtigungsnachweissätze in Netzgruppe 1 zur Kandidatenliste hinzugefügt. Da drei Berechtigungsnachweissätze erforderlich sind, wird der erste Berechtigungsnachweissatz aus Netzgruppe 2 zur Liste hinzugefügt.

Wenn mit einem Berechtigungsnachweissatz erfolgreich auf eine Einheit zugegriffen wird, verwendet QRadar Risk Manager den Berechtigungsnachweissatz auch für nachfolgende Versuche, auf die Einheit zuzugreifen. Werden die Berechtigungsnachweise für die betreffende Einheit geändert, schlägt die Authentifizierung fehl, wenn versucht wird, auf die Einheit zuzugreifen. Beim nächsten Authentifizierungsversuch gleicht QRadar Risk Manager die Berechtigungsnachweise dann erneut ab, um einen erfolgreichen Zugriff sicherzustellen.

Adresssatz

Ein Adresssatz ist eine Liste mit IP-Adressen, die eine Gruppe von Einheiten definieren, für die derselbe Berechtigungsnachweissatz verwendet wird.

Berechtigungsnachweise für IBM Security QRadar Risk Manager konfigurieren

Administratoren müssen Berechtigungsnachweise konfigurieren, damit IBM Security QRadar Risk Manager eine Verbindung zu Einheiten im Netz herstellen kann.

Informationen zu diesem Vorgang

Sie können einen IP-Adressbereich mit einem Strich oder einem Platzhalterzeichen (*) zur Anzeige eines Bereichs eingeben, z. B. 10.100.20.0-10.100.20.240 oder 1.1.1*. Wenn Sie 1.1.1.* eingeben, werden alle IP-Adressen eingeschlossen, die diese Anforderung erfüllen.

Bei der Konfiguration der Adresse, die mit Juniper Networks NSM oder einem generischen XML-Adapter festgelegt wurde, müssen Sie den IP-Adressbereich oder den CIDR-Adressbereich für alle Einheiten eingeben, die von Juniper Networks NSM oder von Dateien für Einheiten im Repository verwaltet werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsfenster auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie im Navigationsmenü auf **Credentials** (Berechtigungsnachweise).
5. Klicken Sie im Fenster **Network Groups** (Netzgruppen) auf das Symbol **Hinzufügen (+)**.
6. Geben Sie einen Namen für eine Netzgruppe ein und klicken Sie anschließend auf 'OK'.
7. Verschieben Sie die Netzgruppe, die die erste Priorität erhalten soll, an den Anfang der Liste. Sie können die Priorität einer Netzgruppe mithilfe der Pfeilsymbole **Nach oben** und **Nach unten** zuordnen.
8. Geben Sie im Feld **Add Address** (Adresse hinzufügen) die IP-Adresse oder den CIDR-Bereich für die Netzgruppe ein und klicken Sie anschließend auf das Symbol **Hinzufügen (+)**.

   Wiederholen Sie diesen Vorgang für alle IP-Adressen, die Sie der für diese Netzgruppe festgelegten Adresse hinzufügen möchten.
9. Klicken Sie im Fenster **Credentials** (Berechtigungsnachweise) auf das Symbol **Hinzufügen (+)**.
10. Geben Sie einen Namen für die neue Berechtigungsnachweisgruppe ein und klicken Sie anschließend auf 'OK'.
11. Geben Sie Werte für die folgenden Parameter ein:

Option	Beschreibung
Benutzername	Geben Sie den Benutzernamen für die Berechtigungsnachweisgruppe ein. Wenn Sie Juniper Networks NSM oder einen generischen XML-Adapter verwenden, geben Sie einen Benutzernamen ein, mit dem Sie auf den Juniper NSM-Server bzw. auf das Dateirepository mit Ihren SED-Dateien zugreifen können.

Option	Beschreibung
Kennwort	Geben Sie das Kennwort für die Berechtigungsnachweisgruppe ein. Wenn Sie Juniper Networks NSM oder einen generischen XML-Adapter verwenden, geben Sie das Kennwort für die Anmeldung am Juniper NSM-Server bzw. für die Anmeldung am Dateirepository mit Ihren SED-Dateien ein.
Benutzername aktivieren	Geben Sie den Benutzernamen für die Authentifizierung der zweiten Stufe für die Berechtigungsnachweisgruppe ein.
Kennwort aktivieren	Geben Sie das Kennwort für die Authentifizierung der zweiten Stufe für die Berechtigungsnachweisgruppe ein.
SNMP Get Community	Geben Sie den Namen der SNMP-Get-Community ein.
Benutzername für SNMPv3-Authentifizierung	Geben Sie den Benutzernamen ein, der für die Authentifizierung von SNMPv3 verwendet werden soll.
Kennwort für SNMPv3-Authentifizierung	Geben Sie das Kennwort ein, das für die Authentifizierung von SNMPv3 verwendet werden soll.
Datenschutzkennwort für SNMPv3	Geben Sie das Protokoll ein, das für die Entschlüsselung von SNMPv3-Alarmnachrichten verwendet werden soll.

12. Verschieben Sie die Berechtigungsgruppe, die die erste Priorität erhalten soll, an den Anfang der Liste. Ordnen Sie die Priorität einer Berechtigungsgruppe mithilfe der Pfeilsymbole **Nach oben** und **Nach unten** zu.
13. Wiederholen Sie den Vorgang für jede Berechtigungsnachweisgruppe, die Sie hinzufügen möchten.
14. Klicken Sie auf **OK**.

Einheitenerkennung

Der Erkennungsprozess verwendet das Simple Networks Management Protocol (SNMP) und die Befehlszeilenschnittstelle (CLI), um Netzeinheiten zu erkennen.

Nachdem Sie eine IP-Adresse oder einen CIDR-Bereich konfiguriert haben, führt die Erkennungsengine einen TCP-Scan für die IP-Adresse durch, um festzustellen, ob Port 22, 23 oder 443 auf Verbindungen überwacht wird. Wenn der TCP-Scan erfolgreich ist und eine SNMP-Abfrage zur Bestimmung des Einheitentyps konfiguriert ist, wird der SNMP Get Community String auf Basis der IP-Adresse verwendet.

Mithilfe dieser Informationen wird bestimmt, welchem Adapter die Einheit bei ihrer Hinzufügung zugeordnet werden soll. QRadar Risk Manager stellt eine Verbindung mit der Einheit her und erstellt eine Liste mit Schnittstellen- und Nachbarstationsinformationen wie CDP-, NDP- oder ARP-Tabellen. Die Einheit wird dann zum Bestand hinzugefügt.

Die konfigurierte IP-Adresse, die zum Starten des Erkennungsprozesses verwendet wird, ist möglicherweise nicht die zugewiesene IP-Adresse für die neue Einheit. QRadar Risk Manager fügt eine Einheit unter Verwendung der Schnittstelle mit der niedrigsten Nummer an der Einheit (oder der niedrigsten Loopback-Adresse, falls vorhanden) hinzu.

Wenn Sie das Kontrollkästchen **Crawl the network from the addresses defined above** (Netz ab der oben angegebenen Adresse durchsuchen) aktivieren, werden die IP-Adressen der von der Einheit erfassten Nachbarn erneut in den Erkennungsprozess eingeführt und der Prozess für jede IP-Adresse wiederholt.

Einheiten erkennen

Administratoren verwenden die Erkennung von Einheiten, um den Typ der Einheit zu ermitteln.

Informationen zu diesem Vorgang

Beim Ausführen einer Einheitenerkennung wird jeder Einheit, die nicht unterstützt wird, aber auf SNMP antwortet, der generische SNMP-Adapter hinzugefügt. Wenn Sie eine Pfadfilterung für die Einheit mit simulierten Routen ausführen möchten, müssen Sie die Einheit manuell entfernen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie im Navigationsmenü auf **Discover Devices** (Einheiten erkennen).
5. Geben Sie eine IP-Adresse oder CIDR-Bereich ein.

   Diese IP-Adresse oder dieser CIDR-Bereich zeigt die Position der Einheit an, die Sie erkennen möchten.
6. Klicken Sie auf das Symbol **Hinzufügen (+)**.
7. Wenn auch nach Einheiten im Netz aus der definierten IP-Adresse oder dem definierten CIDR-Bereich gesucht werden soll, wählen Sie das Kontrollkästchen **Crawl the network from the addresses defined above** (Netz aus den oben definierten Adressen durchlaufen) aus.
8. Klicken Sie auf **Ausführen**.

Einheiten importieren

Fügen Sie mithilfe einer CSV-Datei über 'Geräteimport' eine Liste mit Adaptern und deren Netz-IP-Adressen zu Configuration Source Manager hinzu.

Die Einheitenimportliste kann bis zu 5000 Einheiten enthalten, wobei es jedoch für jeden Adapter und die zugehörige IP-Adresse eine einzelne Zeile in der Importdatei geben muss.

Beispiel:

```
<Adapter::Name 1>,<IP-Adresse>
<Adapter::Name 2>,<IP-Adresse>
<Adapter::Name 3>,<IP-Adresse>
```

Dabei gilt:

<Adapter::Name> gibt den Hersteller- und den Einheitennamen an, z. B. Cisco::IOS.

<IP-Adresse> gibt die IP-Adresse der Einheit an, z. B. 191.168.1.1.

Tabelle 3. Einheitenimportbeispiele

Hersteller	Name	Beispiel <Adapter::Name>,<IP-Adresse>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

CSV-Datei importieren

Sie können eine Liste mit Mastereinheiten in Configuration Source Management mithilfe einer CSV-Datei (Comma-separated Value) importieren.

Vorbereitende Schritte

Wenn Sie eine Liste der Einheiten importieren und anschließend eine IP-Adresse in der CSV-Datei ändern, kopieren Sie möglicherweise unbeabsichtigt eine Einheit in der Configuration Source Management-Liste. Löschen Sie deshalb eine Einheit aus Configuration Source Management, bevor Sie Ihre Mastereinheitenliste erneut importieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Plug-Ins** auf **Geräteimport**.
4. Klicken Sie auf **Durchsuchen**.
5. Suchen Sie die gewünschte CSV-Datei und klicken Sie auf **Öffnen**.
6. Klicken Sie auf **Import Devices** (Einheiten importieren).

Ergebnisse

Falls ein Fehler angezeigt wird, müssen Sie Ihre CSV-Datei überprüfen, die Fehler korrigieren und die Datei erneut importieren. Der Import der CSV-Datei schlägt möglicherweise fehl, wenn die Einheitenliste falsch strukturiert ist oder falsche Informationen enthält. In Ihrer CSV-Datei fehlen beispielsweise Spalten oder ein Befehl, mehrere Einheiten befinden sich in einer einzelnen Zeile oder ein Adaptername enthält einen Schreibfehler.

Wenn der Einheitenimport abgebrochen wird, werden Configuration Source Management keine Einheiten aus der CSV-Datei hinzugefügt.

Einheiten verwalten

Auf der Registerkarte 'Devices' (Einheiten) im Fenster 'Configuration Source Management' (Konfigurationsquellenverwaltung) können Sie die Einheiten im Netz verwalten.

Auf der Registerkarte 'Devices' (Einheiten) können Einheiten angezeigt, hinzugefügt, bearbeitet und gelöscht werden. Außerdem können die Einheitenliste gefiltert, Einheitenkonfigurationsinformationen abgerufen, Nachbarstationsdaten erfasst und in der Implementierung vorhandene Einheiten erkannt werden.

Einheiten anzeigen

Sie können alle Einheiten in Ihrer Implementierung in der Registerkarte 'Devices' (Einheiten) anzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Um ausführliche Informationen zu einer Einheitenkonfiguration anzuzeigen, wählen Sie die gewünschte Einheit aus und klicken auf **Öffnen**.

Einheit hinzufügen

Mithilfe von Configuration Source Management können Sie einzelne Netzeinheiten und Adapter hinzufügen.

Informationen zu diesem Vorgang

Sie können der Einheitenliste in Configuration Source Management eine einzelne Einheit hinzufügen oder mithilfe einer CSV-Datei mehrere Einheiten hinzufügen.

Weitere Informationen zum Hinzufügen mehrerer Einheiten finden Sie unter Einheiten importieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie im Navigationsfenster auf **Add Device** (Einheit hinzufügen).
5. Konfigurieren Sie Werte für die folgenden Parameter:

Option	Bezeichnung
IP-Adresse	Geben Sie die IP-Managementadresse der Einheit ein.
Adapter	Wählen Sie in der Dropdown-Liste **Adapter** den Adapter aus, den Sie dieser Einheit zuweisen möchten.

6. Klicken Sie auf **Hinzufügen**.
   Klicken Sie ggf. auf **Start**, um die Adapterliste zu aktualisieren.

Einheiten bearbeiten

Sie können eine Einheit bearbeiten, um die IP-Adresse oder den Adaptertyp zu korrigieren, falls ein Fehler vorliegt oder Ihr Netz geändert wurde und eine IP-Adresse erneut zugeordnet werden muss.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Wählen Sie die Einheit aus, die Sie bearbeiten möchten.
5. Klicken Sie auf **Bearbeiten**.
6. Konfigurieren Sie Werte für die folgenden Parameter:

Option	Bezeichnung
IP-Adresse	Geben Sie die IP-Managementadresse der Einheit ein.
Adapter	Wählen Sie in der Dropdown-Liste **Adapter** den Adapter aus, den Sie dieser Einheit zuweisen möchten.

7. Klicken Sie auf **Speichern**.

Einheit löschen

Sie können eine Einheit aus QRadar Risk Manager löschen. Eine gelöschte Einheit wird aus Configuration Source Management, Configuration Monitor und der Topologie entfernt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Wählen Sie die Einheit aus, die Sie löschen möchten.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **Ja**, um die Einheit zu löschen.

Ergebnisse

Nach dem Löschen einer Einheit kann der Prozess zum Entfernen der Einheit aus der Topologie einige Minuten dauern.

Einheitenliste filtern

Mithilfe von Filtern können Sie schnell Einheiten in der Einheitenliste finden.

Informationen zu diesem Vorgang

QRadar Risk Manager kann bis zu 5000 Netzeinheiten in Configuration Source Management verarbeiten. Durch eine große Anzahl von Netzeinheiten kann das Durchblättern der Einheitenliste langwierig werden.

In der folgenden Tabelle werden die Filtertypen beschrieben, die für die Einheitenliste angewendet werden können, damit Sie Einheiten schneller finden.

Tabelle 4. Filtertypen für die Einheitenliste

Suchoption	Beschreibung
Schnittstelle IP-Adresse	Filter mit Einheiten, deren Schnittstelle mit einer IP-Adresse oder einem CIDR-Bereich übereinstimmt. Geben Sie im Feld 'IP/CIDR' die IP-Adresse oder den CIDR-Bereich ein, in denen die Suche ausgeführt werden soll. Wenn Sie beispielsweise das Suchkriterium 10.100.22.6 eingeben, wird in den Suchergebnissen eine Einheit mit der IP-Adresse 10.100.22.6 zurückgegeben. Wenn Sie den CIDR-Bereich 10.100.22.0/24 eingeben, werden alle Einheiten im Bereich 10.100.22.* zurückgegeben.
IP-Adresse des Administrators	Filtert die Einheitenliste auf Basis der IP-Adresse der Verwaltungsschnittstellen. Bei einer administrativen IP-Adresse handelt es sich um die IP-Adresse, mit der eine Einheit eindeutig ermittelt wird. Geben Sie im Feld **IP/CIDR** die IP-Adresse oder den CIDR-Bereich ein, in denen die Suche ausgeführt werden soll.
Betriebssystemversion	Filtert die Einheitenliste auf Basis der Betriebssystemversion, auf der Einheiten ausgeführt werden. Wählen Sie Werte für die folgenden Parameter aus: • **Adapter** - Wählen Sie über die Dropdown-Liste den Adaptertyp aus, der gesucht werden soll. • **Version** - Wählen Sie über die Dropdown-Liste die Suchkriterien für die Version aus. Dies sind beispielsweise größer als, kleiner als oder gleich der angegebene Wert. Geben Sie in das Feld die Versionsnummer ein, nach der gesucht werden soll. Wenn Sie keine Suchoption für die Version auswählen, enthalten die Ergebnisse alle Einheiten, die mit dem ausgewählten Adapter konfiguriert wurden, unabhängig von der Version.

Tabelle 4. Filtertypen für die Einheitenliste (Forts.)

Suchoption	Beschreibung
Modell	Filtert die Einheitenliste auf Basis des Anbieters und der Modellnummer. Konfigurieren Sie Werte für die folgenden Parameter: • **Anbieter** - Wählen Sie in der Dropdown-Liste den Anbieter aus, der gesucht werden soll. • **Modell** - Geben Sie das Modell ein, das gesucht werden soll.
Hostname	Filtert die Einheitenliste auf Basis des Hostnamens. Geben Sie im Feld Hostname den Hostnamen ein, nach dem gesucht werden soll.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster 'Risk Manager' (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Wählen Sie in der Dropdown-Liste auf der linken Seite der Einheitenliste einen Filter aus:
6. Klicken Sie auf **Start**.

Ergebnisse

Alle Suchergebnisse, die mit Ihren Kriterien übereinstimmen, werden in der Tabelle angezeigt.

Nächste Schritte

Wenn Sie einen Filter zurücksetzen möchten, wählen Sie **Schnittstelle IP-Adresse** aus, löschen die **IP/CIDR**-Adresse und klicken anschließend auf **Start**.

Einheitenkonfiguration abrufen

Das Sichern einer Einheit für den Abruf einer Einheitenkonfiguration kann für eine einzelne Einheit in der Einheitenliste ausgeführt werden. Über die Registerkarte **Devices** (Einheiten) können Sie auch alle Einheiten sichern.

Informationen zu diesem Vorgang

Nach dem Konfigurieren von Berechtigungsnachweisgruppen und Adressgruppen für den Zugriff auf Netzeinheiten müssen Sie Ihre Einheiten für den Download der Einheitenkonfiguration sichern, damit die Einheitendaten in die Topologie integriert werden.

Weitere Informationen zum Planen automatisierter Sicherungen für Einheitenkonfigurationen aus der Registerkarte **Jobs** finden Sie unter Sicherungsjobs verwalten.

Weitere Informationen zu den Details der Sicherung von Netzeinheiten finden Sie im Abschnitt Einheitenkonfigurationen anzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Um die Konfiguration für alle Einheiten abzurufen, klicken Sie im Navigationsbereich auf **Backup All** (Alle sichern) und anschließend auf **Ja**, um den Vorgang fortzusetzen.
6. Um die Konfiguration für eine Einheit abzurufen, wählen Sie die entsprechende Einheit aus. Wenn Sie mehrere Einheiten auswählen möchten, halten Sie die Steuertaste gedrückt und wählen alle gewünschten Einheiten aus. Klicken Sie auf **Backup**.
7. Klicken Sie bei Bedarf auf **View Error** (Fehler anzeigen), um die Details eines Fehlers anzuzeigen. Nach dem Beheben des Fehlers klicken Sie im Navigationsbereich auf **Backup All** (Alle sichern).

Nachbardaten erfassen

Mit dem Erkennungsprozess können Sie benachbarte Daten aus einer Einheit mithilfe von SNMP und einer Befehlszeilenschnittstelle (Command Line Interface, CLI) abrufen.

Informationen zu diesem Vorgang

Mit benachbarten Daten werden die Verbindungslinien in einer Topologie gezogen, um die grafische Topologiemap Ihrer Netzeinheiten anzuzeigen. Über die Schaltfläche zum Ermitteln können Sie einzelne oder mehrere Einheiten auswählen und die Nachbardaten für eine Einheit aktualisieren Mit diesen Informationen werden die Verbindungslinien für eine oder viele Einheiten in der Topologie aktualisiert.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Wählen Sie die Einheit aus, für die Daten abgerufen werden sollen. Wenn Sie mehrere Einheiten auswählen möchten, halten Sie die Steuertaste gedrückt und wählen alle gewünschten Einheiten aus.
6. Klicken Sie auf **Discover** (Ermitteln).
7. Klicken Sie auf **Ja**, um fortzufahren.

Ergebnisse

Wenn Sie mehrere Einheiten auswählen, kann es einige Minuten dauern, bis der Erkennungsprozess abgeschlossen ist.

Nächste Schritte

Wählen Sie **Run in Background** (Im Hintergrund ausführen) aus, um andere Tasks zu bearbeiten.

Daten aus einem Dateirepository erfassen

Sie können XML-SED-Dateien für Einheiten oder Eingabedateien mit der Basiskonfiguration für eine Einheit aus einem Repository für die Netzdatei abrufen.

Informationen zu diesem Vorgang

Das Dateirepository, in dem die Dateien bereitgestellt werden, muss das FTP- oder SFTP-Protokoll unterstützen. QRadar Risk Manager ruft Einheiteninformationen aus allen SED-XML-Dateien ab, die sich im fernen Dateiverzeichnis des Dateirepositorys befinden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Wählen Sie **Discover from Repository** (Aus Repository erkennen) aus.
6. Konfigurieren Sie Werte für die folgenden Parameter:

Option	Beschreibung
Protokoll	Wählen Sie in der Dropdown-Liste **Protokoll** **FTP** oder **SFTP** als Kommunikationsprotokoll für den Zugriff auf Ihr Konfigurationsdateirepository aus.
IP-Adresse	Geben Sie die IP-Adresse des Konfigurationsdateirepositorys ein.
Ferner Pfad	Geben Sie den Pfad der fernen Datei zum Verzeichnis mit Ihren SED-XML-Dateien ein. Der Standarddateipfad für SED-Dateien lautet `<Installationsverzeichnis>/output`. Das <Installationsverzeichnis> ist die Position der extrahierten Datei `ziptie-adapter.<date>-<build>.zip`.
Benutzername	Geben Sie den Benutzernamen für die Anmeldung an dem System ein, in dem sich das Konfigurationsdateirepository befindet.
Kennwort	Geben Sie das Kennwort für die Anmeldung an dem System ein, in dem sich das Konfigurationsdateirepository befindet.

7. Klicken Sie auf **OK**, um eine Einheit aus einem Repository zu erkennen.
8. Klicken Sie auf **Start**, um die Einheitenliste zu aktualisieren.

Sicherungsjobs verwalten

Ein Job bezeichnet hier einen Sicherungsjob, der es Ihnen ermöglicht, Konfigurationsinformationen für alle Einheiten auf der Registerkarte **Devices** (Einheiten) nach einem Zeitplan automatisch zu sichern.

Auf der Registerkarte **Jobs** in Configuration Source Management können Sie Sicherungsjobs für alle Einheiten oder für einzelne Einheitengruppen in Configuration Source Management erstellen.

Sicherungsjobs, die Sie auf der Seite 'Configuration Source Management' (Konfigurationsquellenverwaltung) definieren, wirken sich nicht auf die QRadar SIEM-Sicherungskonfiguration über das Symbol **Sicherung und Wiederherstellung** auf der Registerkarte **Verwaltung** aus. Die Sicherungs- und Wiederherstellungsfunktion ruft Konfigurationsinformationen und Daten für QRadar SIEM ab. Ein Sicherungsjob ruft nur Informationen für externe Einheiten ab.

Sicherungsjobs anzeigen

Jobs und Jobdetails werden in der Registerkarte **Jobs** angezeigt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Jobs**.
5. Klicken Sie doppelt auf den Job, den Sie genauer betrachten möchten.

Sicherungsjob hinzufügen

Sie können Sicherungsjobs für alle Einheiten oder einzelne Einheitengruppen in Configuration Source Management erstellen.

Informationen zu diesem Vorgang

Legen Sie nach der Definition der Suchkriterien den Jobzeitplan fest. Die Zeitplankonfiguration wird in der Spalte 'Triggers' (Auslöser) angezeigt. Die Auslöser für einen Job stellen den Jobzeitplan dar. Es kann mehrere konfigurierte Zeitpläne geben. Sie können beispielsweise zwei Zeitplanoptionen konfigurieren, sodass ein Job jeden Montag und am ersten Tag jedes Monats ausgeführt wird.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Konfigurationsquellenverwaltung).
4. Klicken Sie auf die Registerkarte **Jobs**.
5. Wählen Sie **New Job** > **Backup** (Neuer Job > Sicherung) aus.
6. Konfigurieren Sie Werte für folgende Parameter:

Option	Beschreibung
Jobname	Geben Sie den Namen ein, den Sie dem Job geben möchten.
Gruppe	Wählen Sie in der Gruppenliste die Gruppe aus, der Sie diesen Job zuweisen möchten. Wenn keine Gruppen aufgelistet sind, können Sie einen Gruppennamen eingeben. Jobs können sortiert werden, nachdem sie einer Gruppe zugewiesen wurden.
Kommentar	Geben Sie einen Kommentar ein, den Sie diesem Sicherungsjob zuordnen möchten. Die Beschreibung des Sicherungsjobs kann maximal 255 Zeichen lang sein.

7. Klicken Sie auf **OK**.
8. Wählen Sie eine der folgenden Suchmethoden aus:

Option	Beschreibung
Statische Liste	Sie können eine statische Liste für die Suche nach Einheiten verwenden, wobei mehrere Optionen verfügbar sind. In der statischen Liste können Sie die Einheiten definieren, auf denen der Job ausgeführt werden soll.
Suche	Geben Sie eine IP-Adresse oder einen CIDR-Bereich ein, der in den Job eingeschlossen werden soll. Wenn Sie die Suchkriterien definieren, wird die Suche nach Einheiten nach der Ausführung des Jobs durchgeführt. Dies stellt sicher, dass neue Einheiten in den Job eingeschlossen werden.

9. Definieren Sie bei Auswahl der statischen Liste die Suchkriterien:
   a. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
   b. Wählen Sie in der Liste auf der Registerkarte **Devices** die Suchkriterien aus. Weitere Informationen finden Sie im Abschnitt Suchkriterien für eine statische Liste oder Suche.
   c. Klicken Sie auf **Start**.
   d. Wählen Sie auf der Registerkarte **Devices** die Einheiten aus, die in den Job eingeschlossen werden sollen.
   e. Klicken Sie im Fenster mit den Jobdetails auf **Add selected from device view search** (Auswahl aus Suche in Einheitenansicht hinzufügen).
10. Definieren Sie bei Auswahl der Suche die Suchkriterien:
   a. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
   b. Wählen Sie in der Liste auf der Registerkarte **Devices** die Suchkriterien aus. Weitere Informationen finden Sie im Abschnitt Suchkriterien für eine statische Liste oder Suche.
   c. Klicken Sie auf **Start**.
   d. Klicken Sie im Fenster mit den Jobdetails auf **Use search from devices view** (Suche aus Einheitenansicht verwenden). Diese Suchkriterien werden verwendet, um Einheiten festzulegen, die diesem Job zugeordnet sind.
11. Klicken Sie auf **Zeitplan** und konfigurieren Sie Werte für folgende Parameter:

Option	Beschreibung
Name	Geben Sie einen Namen für die Zeitplankonfiguration ein.
Startzeit	Wählen Sie Uhrzeit und Datum für den Start des Sicherungsprozesses aus. Die Zeit muss in Militärzeit angegeben werden.
Häufigkeit	Wählen Sie die Häufigkeit aus, die dem Zeitplan zugeordnet werden soll.
Cron	Geben Sie einen Cron-Ausdruck ein, der in Greenwich Mean Time (GMT) interpretiert wird. Wenden Sie sich zur Unterstützung an den Administrator.
Enddatum angeben	Optional: Wählen Sie ein Datum für die Beendigung des Jobzeitplans aus.

12. Klicken Sie im Fenster 'Trigger' (Auslöser) auf **Save** (Speichern).
13. Wiederholen Sie die Schritte 11 und 12, um mehrere Zeitpläne zu erstellen.
14. Wenn der Job sofort ausgeführt werden soll, klicken Sie auf **Run Now** (Jetzt ausführen).
15. Klicken Sie zur Fortsetzung auf **Yes** (Ja).

Sicherungsjob bearbeiten

Sie können Sicherungsjobs bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Jobs**.
5. Klicken Sie doppelt auf den Job, den Sie bearbeiten wollen.
6. Wählen Sie aus dem Parameter **Selection Type** (Auswahltyp) eine der folgenden Suchoptionen aus:

Option	Beschreibung
Statische Liste	Die Verwendung einer statischen Liste ermöglicht die Suche nach Einheiten über mehrere Optionen. Mithilfe der Option für die statische Liste können Sie die spezifischen Einheiten definieren, auf denen Sie den Job ausführen möchten.
Suche	Geben Sie eine IP-Adresse oder einen CIDR-Bereich für die Integration in den Job ein. Wenn Sie die Suchkriterien definieren, wird die Suche nach Einheiten nach der Ausführung des Jobs durchgeführt. Dadurch wird sichergestellt, dass alle neuen Einheiten in den Job integriert werden.

7. Wenn Sie 'Statische Liste' auswählen, definieren Sie die Suchkriterien:
   a. Klicken Sie auf die Registerkarte **Devices** (Einheiten).

b. Wählen Sie die Suchkriterien aus der Liste auf der Registerkarte **Devices** aus.
c. Klicken Sie auf **Start**.
d. Wählen Sie auf der Registerkarte **Devices** die Einheiten aus, die Sie in den Job integrieren möchten.
e. Klicken Sie im Fenster **Job Details** auf **Add selected from device view search** (Ausgewählte aus Suche in Einheitenansicht hinzufügen).

8. Wenn Sie 'Suche' auswählen, definieren Sie die Kriterien:
   a. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
   b. Wählen Sie die Suchkriterien in der Liste auf der Registerkarte **Devices** (Einheiten) aus.
   c. Klicken Sie auf **Start**.
   d. Klicken Sie im Fenster 'Job Details' auf **Use search from devices view** (Suche aus Einheitenansicht verwenden). Mit diesen Suchkriterien werden Einheiten ermittelt, die diesem Job zugeordnet sind.
9. Klicken Sie auf **Zeitplan** und konfigurieren Sie Werte für die folgenden Parameter:

Option	Beschreibung
Name	Geben Sie einen Namen für die Konfiguration des Zeitplans ein.
Startzeit	Wählen Sie eine Uhrzeit und ein Datum für den Start der Sicherungsverarbeitung aus. Die Uhrzeit muss in 24-Stunden-Zählung angegeben werden.
Häufigkeit	Wählen Sie die Häufigkeit dieses Zeitplans aus.
Cron	Geben Sie einen Cron-Ausdruck ein, der in Greenwich Mean Time (GMT) interpretiert wird. Wenden Sie sich an Ihren Administrator, wenn Sie Hilfe benötigen.
Enddatum angeben	Optional. Wählen Sie ein Datum aus, an dem der Jobzeitplan beendet werden soll.

10. Klicken Sie auf **Speichern**.
11. Klicken Sie auf **Jetzt ausführen**.
12. Wiederholen Sie ggf. die Schritte 9 und 10.
13. Klicken Sie auf **Ja**, um fortzufahren.

Sicherungsjob umbenennen

Sie können einen Sicherungsjob umbenennen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Jobs**.
5. Wählen Sie den Sicherungsjob aus, den Sie umbenennen möchten.
6. Klicken Sie auf **Rename** (Umbenennen).

7. Konfigurieren Sie Werte für die folgenden Parameter:

Option	Beschreibung
Jobname	Geben Sie den Namen ein, den Sie für diesen Job anwenden wollen.
Gruppe	Wählen Sie in der Liste **Gruppe** die Gruppe aus, der Sie diesen Job zuweisen möchten. Sie können auch einen neuen Gruppennamen angeben.
Kommentar	Optional. Geben Sie einen beliebigen Kommentar ein, den Sie diesem Sicherungsjob zuordnen wollen. Sie können für Ihre Beschreibung des Sicherungsjobs bis zu 255 Zeichen eingeben.

8. Klicken Sie auf **OK**.

Sicherungsjob löschen

Sie können einen Sicherungsjob löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie auf die Registerkarte **Jobs**.
5. Wählen Sie den Sicherungsjob aus, den Sie löschen möchten.
6. Klicken Sie auf **Löschen**.

Protokolle konfigurieren

Damit QRadar Risk Manager mit Einheiten kommuniziert, müssen Sie das für die Kommunikation zu Ihren Netzeinheiten benötigte Kommunikationsverfahren (Protokoll) definieren .

QRadar Risk Manager stellt die Standardprotokollkonfiguration für Ihr System zur Verfügung. Wenn Sie Protokolle definieren müssen, können Sie damit das Abrufen und Aktualisieren der Einheitenkonfiguration für QRadar Risk Manager ermöglichen. Viele Netzumgebungen verwenden unterschiedliche Kommunikationsprotokolle oder unterschiedliche Typen oder Funktionen für die Einheit. Beispielsweise kann ein Router ein anderes Protokoll als die Firewalls im Netz verwenden. Eine Liste der unterstützten Protokolle nach Gerätehersteller finden Sie im Handbuch *IBM Security QRadar Risk Manager Adapters Configuration Guide* .

QRadar Risk Manager verwendet Protokollgruppen, um Gruppen von Protokollen für eine Reine von Einheiten zu definieren, für die ein bestimmtes Kommunikationsprotokoll erforderlich ist. Sie können Einheiten zu Netzgruppen zuweisen, damit Protokollgruppen und Adressgruppen für Ihre Einheiten gemeinsam gruppiert werden.

Bei Protokollgruppen handelt es sich um eine benannte Gruppe von Protokollen für eine Gruppe von Einheiten, für die bestimmte Protokollberechtigungsnachweise erforderlich sind.

Bei Adressgruppen handelt es sich um IP-Adressen, mit denen die Netzgruppe definiert wird.

Protokolle konfigurieren

Sie können Protokolle definieren und Einheitenkonfigurationen abrufen und aktualisieren.

Informationen zu diesem Vorgang

Sie können die folgenden Werte für die Protokollparameter konfigurieren.

Tabelle 5. Protokollparameter

Protokoll	Parameter
SSH	Konfigurieren Sie die folgenden Parameter: • **Port** - Geben Sie den Port an, den das SSH-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der SSH-Standardprotokollport ist 22. • **Version** - Wählen Sie die SSH-Version aus, die diese Netzgruppe bei der Kommunikation mit Netzeinheiten verwenden soll. Folgende Optionen sind verfügbar: **Auto** - Mit dieser Option wird die SSH-Version für die Kommunikation mit Netzeinheiten automatisch ermittelt. **1** - Bei der Kommunikation mit Netzeinheiten wird SSH-1 verwendet. **2** - Bei der Kommunikation mit Netzeinheiten wird SSH-2 verwendet.
Telnet	Geben Sie den Port ein, den das Telnet-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der Telnet-Standardprotokollport ist 23.
HTTPS	Geben Sie den Port ein, den das HTTPS-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der HTTPS-Standardprotokollport ist 443.
HTTP	Geben Sie den Port ein, den das HTTP-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der HTTP-Standardprotokollport ist 80.
SCP	Geben Sie den Port ein, den das SCP-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der SCP-Standardprotokollport ist 22.

Tabelle 5. Protokollparameter (Forts.)

Protokoll	Parameter
SFTP	Geben Sie den Port ein, den das SFTP-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der SFTP-Standardprotokollport ist 22.
FTP	Geben Sie den Port ein, den das FTP-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. Der SFTP-Standardprotokollport ist 22.
TFTP	Das TFTP-Protokoll verfügt nicht über konfigurierbare Optionen.
SNMP	Konfigurieren Sie die folgenden Parameter: • **Port** - Geben Sie den Port an, den das SNMP-Protokoll bei der Kommunikation mit den Netzeinheiten sowie bei der Sicherung von Netzeinheiten verwenden soll. • **Timeout(ms)** (Zeitlimit (ms))- Wählen Sie die Dauer in Millisekunden aus, die zum Ermitteln eines Kommunikationszeitlimits verwendet werden soll. • **Retries** (Wiederholungen) - Wählen Sie die Häufigkeit aus, mit der die Kommunikation mit einer Einheit wiederholt werden soll. • **Version** - Wählen Sie die Version von SNMP aus, die für die Kommunikation verwendet werden soll. Mögliche Optionen sind v1, v2 oder v3. • **V3 Authentication** (V3-Authentifizierung) - Wählen Sie den Algorithmus aus, der zur Authentifizierung von SNMP-Alarmnachrichten verwendet werden soll. • **V3 Encryption** (V3-Verschlüsselung) - Wählen Sie das Protokoll aus, das zur Entschlüsselung von SNMP-Alarmnachrichten verwendet werden soll.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie im Navigationsmenü auf **Protocols** (Protokolle).
5. Konfigurieren Sie eine neue Netzgruppe:
   a. Klicken Sie im Fenster **Network Groups** (Netzgruppen) auf das Symbol **Hinzufügen (+)**.
   b. Geben Sie einen Namen für eine Netzgruppe ein.

c. Klicken Sie auf **OK**.

d. Ordnen Sie die Priorität der Netzgruppen mithilfe der Symbole **Nach oben** und **Nach unten** zu. Verschieben Sie die Netzgruppe, die die erste Priorität erhalten soll, an den Anfang der Liste.

6. Konfigurieren Sie die Adressgruppe:

a. Geben Sie im Feld **Add Address** (Adresse hinzufügen) die IP-Adresse oder den CIDR-Bereich für die Netzgruppe ein und klicken Sie anschließend auf das Symbol **Hinzufügen (+)**. Geben Sie beispielsweise einen IP-Adressbereich mit einem Strich oder einem Platzhalterzeichen (*) zur Anzeige eines Bereichs ein, z. B. 10.100.20.0-10.100.20.240 oder 1.1.1*. Wenn Sie 1.1.1.* eingeben, werden alle IP-Adressen eingeschlossen, die diese Anforderung erfüllen.

b. Wiederholen Sie diesen Vorgang für alle IP-Adressen, die Sie der für diese Netzgruppe festgelegten Adresse hinzufügen möchten.

7. Konfigurieren Sie die Protokollgruppe:

a. Stellen Sie im Fenster **Network Groups** (Netzgruppen) sicher, dass die Netzgruppe, für die Sie Protokolle konfigurieren möchten, ausgewählt ist.

b. Aktivieren Sie Kontrollkästchen, um ein Protokoll für den Bereich der IP-Adressen anzuwenden, die der von Ihnen erstellten Netzgruppe zugeordnet sind. Wenn Sie die Kontrollkästchen abwählen, wird beim Versuch, eine Netzeinheit zu sichern, die Kommunikationsoption für das Protokoll inaktiviert.

c. Konfigurieren Sie für jedes ausgewählte Protokoll Werte für die Parameter.

d. Ordnen Sie die Priorität der Protokolle mithilfe der Symbole **Nach oben** und **Nach unten** zu. Verschieben Sie das Protokoll, das die erste Priorität erhalten soll, an den Anfang der Liste.

8. Klicken Sie auf **OK**.

Erkennungszeitplan konfigurieren

Sie können einen Erkennungszeitplan konfigurieren, um ARP, MAC-Tabellen und benachbarte Informationen für Ihre Einheiten auszufüllen. Mit dem Erkennungszeitplan können außerdem neue Einheiten automatisch dem Inventar hinzugefügt werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Fenster **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung der Konfigurationsquelle).
4. Klicken Sie im Navigationsmenü auf **Schedule Discovery** (Erkennung planen).
5. Wählen Sie das Kontrollkästchen **Enable periodic discovery** (Regelmäßige Erkennung aktivieren) aus, um den Erkennungszeitplan zu aktivieren.

6. Konfigurieren Sie Werte für die folgenden Parameter:

Option	Beschreibung
Name	Geben Sie einen Namen für die Konfiguration des Zeitplans ein.
Startzeit	Wählen Sie eine Uhrzeit und ein Datum für den Start der Sicherungsverarbeitung aus. Die Uhrzeit muss in 24-Stunden-Zählung angegeben werden.
Häufigkeit	Wählen Sie die Häufigkeit dieses Zeitplans aus.
Cron	Geben Sie einen Cron-Ausdruck ein, der in Greenwich Mean Time (GMT) interpretiert wird. Wenden Sie sich an Ihren Administrator, wenn Sie Hilfe benötigen.
Enddatum angeben	Optional. Wählen Sie ein Datum aus, an dem der Jobzeitplan beendet werden soll.
Crawl and discover new devices (Neue Einheiten durchsuchen und ermitteln)	Aktivieren Sie dieses Kontrollkästchen, wenn der Erkennungsprozess neue Einheiten ermitteln soll. Heben Sie die Auswahl dieses Kontrollkästchens auf, wenn dem Inventar keine neuen Einheiten hinzugefügt werden sollen.

7. Klicken Sie auf **OK**.

Kapitel 5. Netztopologie

In IBM Security QRadar Risk Manager können Sie mithilfe der Topologiemodellgrafik die physische Konnektivität des Netzes anzeigen, filtern und überprüfen.

Die Netztopologiegrafik wird aus Konfigurationsinformationen erstellt, die von Einheiten wie Firewalls, Routern, Switches und Intrusion-Prevention-Systemen abgerufen werden. Durch Bewegen des Mauszeigers über Verbindungslinien können Netzverbindungsinformationen angezeigt werden. Sie können die Topologie filtern, indem Sie in zulässigen Protokollen und an Ports nach Pfaden für potenzielle Attacken oder nach Schwachstellen suchen, und den Datenfluss zwischen Einheiten oder Teilnetzen sowie Einheitenregeln anzeigen.

Sie können die Topologie für folgende Aktionen verwenden:

- Visualisierung bestimmter Netzpfade und der Datenverkehrsrichtung für eine erweiterte Bedrohungsanalyse
- Einfügung passiver Sicherheitszuordnungen von Intrusion-Prevention-Systemen in die Topologiegrafik
- Anpassung des Topologielayouts, einschließlich benutzerdefinierter Netzgruppen
- Erstellung von Suchfiltern für die Netztopologie auf der Basis von Protokollen, Ports oder Schwachstellen
- Anzeige detaillierter Verbindungsinformationen zwischen Einheiten und Teilnetzen
- Anzeige von Einheitenregeln für Topologieverbindungen mit den zulässigen Ports und Protokollen
- Anzeige von Network Address Translation-(NAT-)Einheiten, NAT-Indikatoren und Informationen über NAT-Zuordnungen
- Anzeige von virtualisierten Netzsicherheitseinheiten mit mehreren Kontexten

Bei der Anzeige der zulässigen Ports und Protokolle zwischen Einheiten sind TCP, UDP und ICMP die einzigen Protokolle, die im Topologiemodell dargestellt werden.

Grafikfunktionen des Topologiemodells

Sie können auf die Grafikfunktionen im Topologiemodell zugreifen.

Tabelle 6. Grafikfunktionen des Modells

Ziel	Vorgehensweise
Zusätzliche Details zu einem Teilnetz anzeigen	Bewegen Sie den Mauszeiger über das Teilnetz. Die Konfigurationsinformationen werden angezeigt.
Zusätzliche Details zu einer Einheit anzeigen	Bewegen Sie den Mauszeiger über die Einheit. Die Konfigurationsinformationen werden angezeigt.

Tabelle 6. Grafikfunktionen des Modells (Forts.)

Ziel	Vorgehensweise
Zusätzliche Details zu einer Verbindung anzeigen	Bewegen Sie den Mauszeiger über eine Verbindungslinie zwischen einer Einheit oder einem Teilnetz, um Verbindungsdetails anzuzeigen. Mehrere gekrümmte Kanten zwischen einer Einheit und einem Teilnetz zeigen an, dass eine Einheit oder eine Gruppe von Kontexten mehrere Schnittstellen im selben Teilnetz haben.
Zusätzliche Details zu einer Einheit mit mehreren Kontexten anzeigen	Bewegen Sie den Mauszeiger über die Einheit mit mehreren Kontexten. Die Konfigurationsinformationen werden angezeigt.
Knoten verteilen	Verteilen Sie Einheiten, Firewalls oder Teilnetze in der Grafik, indem Sie den Knoten mit dem Mauszeiger auf die gewünschte Position ziehen.
Vergrößern oder verkleinern	Skalieren Sie die Grafik mithilfe des Schiebereglers links oben in der Grafik. Sie können die Grafik auch mithilfe des Mausrads skalieren.
Nach links, rechts, oben oder unten verschieben	Klicken Sie mit der linken Maustaste auf den Leerraum des Topologiemodells und ziehen Sie den Cursor zum Verschieben in die gewünschte Richtung. Sie können auch den Zeichenrahmen in der rechten unteren Ecke verwenden, um das Topologiemodell in eine bestimmte Richtung zu verschieben.

Kontextmenüoptonen in der Topologie

Sie können in der Topologie mit der rechten Maustaste auf ein Ereignis klicken, um auf zusätzliche Ereignisfilterinformationen zuzugreifen.

Tabelle 7. Topologieoptionen im Kontextmenü

Ziel	Vorgehensweise
Verbindungen suchen	Klicken Sie mit der rechten Maustaste auf ein Teilnetz in der Topologie und wählen Sie **Verbindungen durchsuchen** aus. Es wird eine Suche erstellt, wobei die Quelle oder das Ziel die IP-Adresse des ausgewählten Teilnetzes ist. Sie können weitere Suchparameter hinzufügen und auf **Suchen** klicken, um die Ergebnisse anzuzeigen.
Konfigurationsinformationen für eine Einheit anzeigen	Bewegen Sie den Mauszeiger über die Einheit, klicken Sie mit der rechten Maustaste und wählen Sie **View Device Configuration** (Einheitenkonfiguration anzeigen) aus. Diese Informationen werden von der Einheit abgerufen.

Tabelle 7. Topologieoptionen im Kontextmenü (Forts.)

Ziel	Vorgehensweise
Konfigurationsinformationen für eine Einheit mit mehreren Kontexten anzeigen	Bewegen Sie den Mauszeiger über die Einheit, klicken Sie mit der rechten Maustaste und wählen Sie **View Device Configuration** (Einheitenkonfiguration anzeigen) aus. Es wird eine Liste der Kontexte angezeigt, die zu der Einheit mit mehreren Kontexten gehören, einschließlich grundlegender Einheitenkonfigurationsinformationen. Wenn Sie detaillierte Einheitenkonfigurationsinformationen zu einem Kontext sehen möchten, doppelklicken Sie in der Liste auf den betreffenden Kontext.
Nach Ereignissen suchen	Bewegen Sie den Mauszeiger über eine Einheit oder ein Teilnetz in der Topologie. Klicken Sie mit der rechten Maustaste und wählen Sie **Ereignisse suchen** aus. • Wenn Sie Ereignisse in einem Teilnetz suchen, werden die Suchparameter mit der Quellen- und Zieladresse im Suchfilter ausgefüllt. • Wenn Sie Ereignisse in einer Einheit suchen, die einer Protokollquelle zugeordnet ist, wird eine Ereignissuche mit dem Protokollquellennamen und der IP-Adresse im Suchfilter ausgefüllt. Dies ermöglicht eine Suche nach Ereignissen, die aus der Topologie an die Einheit gebunden sind. Wenn eine Einheit keiner Protokollquelle zugeordnet ist, ist die Option **Ereignisse suchen** nicht verfügbar.
Nach Flüssen suchen, die einem Teilnetz zugeordnet sind	Bewegen Sie den Mauszeiger über das Teilnetz. Klicken Sie mit der rechten Maustaste und wählen Sie **Flüsse durchsuchen** aus. Das Fenster 'Flusssuche' wird angezeigt. Weitere Informationen zur Suche nach Flüssen finden Sie im *IBM Security QRadar SIEM Users Guide*.
Assetprofilinformationen für ein Teilnetz anzeigen	Bewegen Sie den Mauszeiger über das Teilnetz, klicken Sie mit der rechten Maustaste und wählen Sie **Assets anzeigen** aus. Im Fenster 'Assetliste' wird die Liste der Assets für das Teilnetz angezeigt. Weitere Informationen zu Assets finden Sie im *IBM Security QRadar SIEM Users Guide*.

Tabelle 7. Topologieoptionen im Kontextmenü (Forts.)

Ziel	Vorgehensweise
IPS-Verbindung zwischen zwei Einheiten hinzufügen	Wenn die Topologie eine IPS-Einheit (Intrusion-Prevention-System) einschließt, bewegen Sie den Mauszeiger über eine Verbindungslinie zwischen einem Einheitenknoten und einem Teilnetzknoten. Klicken Sie mit der rechten Maustaste und wählen Sie **Add IPS** (Intrusion-Prevention-System hinzufügen) aus.
Intrusion-Prevention-System entfernen	Bewegen Sie den Mauszeiger über die Verbindungslinie zwischen einem Einheitenknoten und einem Teilnetzknoten, der das Intrusion-Prevention-System einschließt. Klicken Sie mit der rechten Maustaste und wählen Sie **Remove IPS** (Intrusion-Prevention-System entfernen) aus. Dieses Menü wird nur angezeigt, wenn es auf der Verbindung ein Intrusion-Prevention-System gibt.

Pfad und Assetsuchen über die Topologie

In IBM Security QRadar Risk Manager können Sie Ihre Topologie durchsuchen, um Netzassets, Teilnetze und die Pfade zwischen Netzen anzuzeigen.

Die Suche kann direkt über die Topologieansicht oder über das Menü **Suchen** erfolgen.

Bei einer Pfadsuche werden die Richtung des Datenverkehrs, vollständig oder teilweise zulässige Protokolle und Einheitenregeln angezeigt. Ein Indikator für die Netzadressumsetzung wird im Topologiediagramm angezeigt, wenn in Ihrer Suche ein Pfad gefunden wird, der Quellen- oder Zielumsetzungen enthält.

Wenn Sie nach einem Host suchen, werden alle Einheiten angezeigt, die mit dem Host kommunizieren. Wenn der Host nicht mit einer Schnittstelle in einer Einheit übereinstimmt, aber in das Teilnetz integriert ist, werden das Teilnetz und alle damit verbundenen Einheiten angezeigt.

Falls zwischen Netzen Portverbindungen bestehen, werden die zulässigen Ports in einer Pfadzusammenfassung angezeigt.

Eine geblockte Verbindung ist in der Topologie durch ein rotes Quadrat gekennzeichnet. Bewegen Sie Ihre Maus über das rote Quadrat, um die Firewallregeln zu überprüfen, die die geblockte Verbindung erzwingen.

NAT-Indikatoren in Suchergebnissen

Ein NAT-Indikator, der als ausgefüllter grüner Punkt dargestellt wird, wird im Topologiediagramm angezeigt, wenn in Ihrer Suche ein Pfad gefunden wird, der Quellen- oder Zielübersetzungen enthält.

Informationen zu diesem Vorgang

Ein NAT-Indikator zeigt an, dass die im Pfadfilter angegebene IP-Zieladresse möglicherweise nicht das endgültige Ziel ist. Sie können den Mauszeiger über den Indikator bewegen, um die folgenden Informationen zu den Übersetzungen anzuzeigen.

Tabelle 8. Verfügbare Informationen aus dem NAT-Indikator

Parameter	**Beschreibung**
Quelle	Die übersetzte Quellen-IP oder -CIDR.
Quellenport(s)	Die übersetzten Quellenports, falls zutreffend.
Übersetzte Quelle	Das Ergebnis der Übersetzung, die für die Quelle angewendet wurde.
Übersetzte Quellenport(s)	Das Ergebnis der Übersetzung, die für die Quellenport(s) angewendet wurde, falls zutreffend.
Ziel	Die übersetzte Ziel-IP oder -CIDR.
Zielport(s)	Die übersetzten Zielports, falls zutreffend.
Übersetztes Ziel	Das Ergebnis der Übersetzung, die für das Ziel angewendet wurde.
Übersetzte Zielport(s)	Das Ergebnis der Übersetzung, die für die Zielport(s) angewendet wurde, falls zutreffend.
Phase	Die Routing-Phase bei der Anwendung der Übersetzung. Übersetzungen werden vor oder nach dem Routing angewendet.

Intrusion-Prevention-System (IPS) hinzufügen

Wenn Ihre Configuration Source Management-Liste eine IPS-Einheit (Intrusion Prevention System) enthält, können Sie ein IPS einer Verbindung zwischen Knoten von Einheit zu Teilnetz und zwischen Knoten von Einheit zu Einheit hinzufügen.

Informationen zu diesem Vorgang

Das Hinzufügen einer IPS-Verbindung erleichtert die Ermittlung der Position von IPS, wenn die Einheit passiv ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Topologie**.
3. Bewegen Sie den Mauszeiger über die Verbindungslinie, die einen Einheitenknoten mit einem Teilnetzknoten verknüpft.
4. Klicken Sie mit der rechten Maustaste auf die Verbindungslinie und wählen Sie **Add IPS** (IPS hinzufügen) aus.

5. Wählen Sie in den folgenden Listen die Einheit und die Schnittstellen aus, die hinzugefügt werden sollen:

Option	Beschreibung
Place IPS (IPS anordnen)	Wählen Sie eine Position aus der Liste aus.
Connect IPS interface (IPS-Schnittstelle verbinden)	Wählen Sie eine Schnittstelle aus, die mit der Einheit verbunden werden soll. Wenn mehrere Einheiten zur Auswahl stehen, müssen Sie eine Einheit auswählen (siehe nächste Option).
to device (mit Einheit)	Wählen Sie die Einheit aus, die Sie mit IPS verbinden möchten. Diese Option ist verfügbar, wenn mehrere Einheiten vorhanden sind.
Connect IPS interface (IPS-Schnittstelle verbinden)	Wählen Sie eine Schnittstelle aus, die mit dem Teilnetz verbunden werden soll.

6. Wählen Sie mithilfe der Listen die Einheit und die Schnittstellen aus, um die IPS-Verbindung Ihrer Topologie hinzuzufügen.
7. Klicken Sie auf **OK**.

Intrusion-Prevention-System (IPS) entfernen

Sie können eine IPS-Verbindung entfernen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Topologie**.
3. Bewegen Sie den Mauszeiger über die Verbindungslinie, die einen Einheitenknoten mit einem Teilnetzknoten verknüpft.
4. Klicken Sie mit der rechten Maustaste auf die Verbindungslinie und wählen Sie die Option 'Remove IPS' (IPS entfernen) aus.
5. Klicken Sie auf **OK**.

Kapitel 6. Richtlinienüberwachung

Unternehmen verwenden die Richtlinienüberwachung, um bestimmte Risikofragen in Bezug auf das Netz zu definieren, um Risiken zu bewerten oder zu überwachen, die auf der Analyse von Risikoindikatoren basieren.

In der Richtlinienüberwachung können Sie Richtlinien definieren, die Einhaltung einer Richtlinie bewerten, Ergebnisse von Fragen auswerten und neue Risiken überwachen.

Es werden Standardfragevorlagen bereitgestellt, mit deren Hilfe Sie die Risiken für ein Netz bewerten und überwachen können. Sie können eine der Standardfragevorlagen als Grundlage für eigene Fragen verwenden oder eine neue Frage erstellen. Sie finden die Standardfragevorlagen im Menü **Gruppe** auf der Seite **Richtlinienüberwachung**.

Sie können die gewünschte Auswahl in der folgenden Liste der Risikoindikatoren treffen:

- Die Netzaktivität misst Risiken auf Basis der Netzkommunikation, die in der Vergangenheit stattfand.
- Konfiguration und Topologie messen Risiken, die auf möglichen Kommunikations- und Netzverbindungen basieren.
- Schwachstellen messen Risiken, die auf der Netzkonfiguration und den Schwachstellenscandaten basieren, die von Netzassets erfasst werden.
- Firewallregeln messen Risiken auf Basis der Durchsetzung oder des Fehlens von Firewallregeln, die im Netz angewendet werden.

Sie können Tests definieren, die auf den Risikoindikatoren basieren, und dann die Testergebnisse einschränken, um die Abfrage für bestimmte Ergebnisse oder Verstöße zu filtern.

Sicherheitsspezialisten erstellen Fragen für Assets oder Einheiten/Regeln, um Risiken in Netzen zu markieren. Die Risikostufe für ein Asset oder eine Einheit/Regel wird zurückgemeldet, nachdem eine Frage an die Richtlinienüberwachung übergeben wurde. Sie können Ergebnisse genehmigen, die von Assets zurückgegeben werden, oder festlegen, wie das System auf nicht genehmigte Ergebnissen antworten soll.

Sie können anhand der Ergebnisse Risikofälle für viele unterschiedliche Sicherheitsszenarien bewerten, z. B. können Sie

- bewerten, ob Benutzer verbotene Protokolle zur Kommunikation verwenden,
- bewerten, ob Benutzer in bestimmten Netzen mit verbotenen Netzen oder Assets kommunizieren können,
- bewerten, ob Firewallregeln der unternehmensinternen Richtlinie entsprechen,
- Prioritäten für Schwachstellen vergeben, indem Sie bewerten, welche Systeme aufgrund der Netzkonfiguration anfällig sind.

Fragen verwalten

Die Verwaltung von Fragen in der Richtlinienüberwachung umfasst das Erstellen, Übergeben, Genehmigen, Bearbeiten, Kopieren und Löschen von Fragen.

Bei der Übergabe einer Frage basiert die Topologiesuche auf dem ausgewählten Datentyp: Assets oder Einheiten/Regeln.

Wenn eine Frage auf Assets basiert, dann basiert die Suche auf den Assets im Netz, die gegen eine definierte Richtlinie verstoßen, oder auf Assets, die ein Risiko in die Umgebung eingeführt haben. Wenn eine Frage auf Einheiten/Regeln basiert, dann identifiziert die Suche entweder die Regeln in einer Einheit, die gegen eine definierte Richtlinie verstoßen oder das Risiko in die Umgebung eingeführt haben.

Fragen zu Einheiten/Regeln suchen nach Verstößen in Regeln und Richtlinien und besitzen keine einschränkenden Tests.

Es gibt zwei Kategorien von Assettests: beitragende Tests und einschränkende Tests.

Ein beitragender Test verwendet die Frageparameter, um die in der Frage angegebenen Risikoindikatoren zu untersuchen. Es werden Risikodatenergebnisse generiert, die durch einen einschränkenden Test weiter gefiltert werden können. Beitragende Tests werden standardmäßig im Fenster **Which tests do you want to include in your question** (Welche Tests sollen in die Frage eingeschlossen werden) angezeigt. Beitragende Tests geben Daten auf Basis erkannter Assets zurück, die mit der Testfrage übereinstimmen.

Ein einschränkender Test wird verwendet, um die Ergebnisse einzugrenzen, die von der Frage eines beitragenden Tests zurückgegeben werden. Einschränkende Tests werden nur im Fenster **Which tests do you want to include in your question** (Welche Tests sollen in die Frage eingeschlossen werden) angezeigt, nachdem ein beitragender Test hinzugefügt wurde. Einschränkende Tests können nur hinzugefügt werden, nachdem ein beitragender Test in die Frage eingeschlossen wurde. Wenn Sie die Frage eines beitragenden Tests entfernen oder löschen, kann die Frage des einschränkenden Tests nicht gespeichert werden.

Weitere Informationen zu beitragenden und einschränkenden Tests finden Sie im Abschnitt Frage übergeben.

Bedeutungsfaktor

Der Bedeutungsfaktor wird zur Berechnung der Risikobewertung und zur Festlegung der Anzahl der für eine Frage zurückgegebenen Ergebnisse verwendet.

Der Bereich umfasst die Werte 1 (geringe Bedeutung) bis 10 (große Bedeutung). Der Standardwert ist 5.

Tabelle 9. Ergebnismatrix des Bedeutungsfaktors

Bedeutungsfaktor	Zurückgegebene Ergebnisse für Assettests	Zurückgegebene Ergebnisse für Einheit/Regeln-Tests
1 (geringe Bedeutung)	10.000	1.000
10 (große Bedeutung)	1	1

Beispielsweise wäre für eine Richtlinienfrage, die **Kommunikation aus dem Internet akzeptieren und nur die folgenden Netze (DMZ) einschließen** angibt, ein hoher Bedeutungsfaktor von 10 erforderlich, weil aufgrund des hohen Risikos der Frage keine Ergebnisse der Frage akzeptabel sind. Für eine Richtlinienfrage, die "Kommunikation aus dem Internet akzeptieren und nur die folgenden Anwendun-

gen für ankommende Daten (P2P) einschließen" angibt, wäre dagegen ein niedriger Bedeutungsfaktor erforderlich, weil die Ergebnisse der Frage kein hohes Risiko anzeigen, aber Sie diese Kommunikation möglicherweise zu Informationszwecken überwachen.

Frageinformationen anzeigen

Informationen zu Richtlinienüberwachungsfragen und Parametern können auf der Seite **Richtlinienüberwachung** angezeigt werden.

Wenn Sie weitere Informationen zu einer Frage sehen möchten, können Sie die Frage auswählen, um die Beschreibung anzuzeigen.

Wenn sich eine Frage, die Sie auswählen, gerade im Überwachungsmodus befindet, können Sie die Ereignisse und Angriffe anzeigen, die als Ergebnis der ausgewählten Frage generiert werden.

Frage erstellen

Sie können in der Richtlinienüberwachung eine Frage erstellen.

Vorbereitende Schritte

Fragen zur Richtlinienüberwachung werden von oben nach unten ausgewertet. Bei der Erstellung von Fragen zur Richtlinienüberwachung hat die Reihenfolge der Fragen Auswirkung auf die Ergebnisse.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie im Menü **Aktionen** die Option **Neu** aus.
4. Geben Sie im Feld **What do you want to name this question** (Welche Bezeichnung soll diese Frage haben) einen Namen für die Frage ein.
5. Wählen Sie in der Liste **What type of data do you want to return** (Welchen Datentyp möchten Sie zurückgeben) den Datentyp aus, den Sie zurückgeben möchten.
6. Wenn Sie als Typ der zurückzugebenden Daten **Assets** ausgewählt haben, wählen Sie in der Liste **Evaluate On** (Auswerten auf) eine der folgenden Optionen aus:

Option	Beschreibung
Actual Communication (Tatsächliche Datenübertragung)	Enthält alle Assets, für die mithilfe von Verbindungen Datenübertragungen ermittelt wurden.
Possible Communication (Mögliche Datenübertragung)	Enthält alle Assets, auf denen Datenübertragungen über Ihre Netztopologie (z. B. Firewalls) zulässig sind. Mit Fragen zu möglichen Datenübertragungen können Sie überprüfen, ob bestimmte Datenübertragungen auf Assets möglich sind, unabhängig davon, ob eine Übertragung ermittelt wurde.

7. Wenn Sie in der Liste **Wichtigkeitsfaktor** den Datentyp **Einheiten/Regeln** für die Rückgabe ausgewählt haben, wählen Sie die Bewertungsstufe aus, die Sie

dieser Frage zuweisen möchten. Weitere Informationen finden Sie unter Matrix für die Ergebnisse der Zielgewichtung.

8. Geben Sie den Zeitbereich für die Frage ab.
9. Wählen Sie im Feld **Which tests do you want to include in your question** (Welche Tests sollen in Ihre Frage integriert werden) das Pluszeichen neben den Tests aus, die Sie integrieren möchten.
10. Konfigurieren Sie die Parameter für Ihre Tests.

    Konfigurierbare Parameter sind fett gedruckt und unterstrichen. Klicken Sie auf einen beliebigen Parameter, um die verfügbaren Optionen für Ihre Frage anzuzeigen.
11. Wählen Sie im Bereich 'Gruppen' die gewünschten Kontrollkästchen aus, um diese Frage einer Gruppe zuzuweisen. Weitere Informationen zum Gruppieren von Fragen finden Sie unter Fragen gruppieren.
12. Klicken Sie auf **Save Question** (Frage speichern).

Nächste Schritte

Sie können eine Frage übergeben, um den Risikofaktor zu bestimmen. Siehe Frage übergeben.

Frage übergeben

Durch das Übergeben einer Frage ermitteln Sie das zugehörige Risiko. Sie können außerdem die Dauer festlegen, die zum Ausführen einer Frage erforderlich ist, sowie das abgefragte Datenvolumen.

Informationen zu diesem Vorgang

Bei der Übergabe einer Frage hängen die daraus resultierenden Informationen von den abgefragten Daten ab: Assets oder Einheiten und Regeln.

Nach dem Übergeben einer Frage zur Richtlinienüberwachung können Sie anzeigen, wie lange die Ausführung der Frage dauert. Die Zeit, die zur Ausführung der Richtlinie erforderlich ist, zeigt auch an, wie viele Daten abgefragt werden. Wenn die Ausführungszeit beispielsweise 3 Stunden beträgt, dann sind 3 Stunden Daten vorhanden. Sie können die Zeit in der Spalte **Policy Execution Time** (Zeit für Richtlinienausführung) anzeigen, um eine effiziente Intervallfrequenz zu ermitteln, die Sie für die zu überwachenden Fragen festlegen. Wenn beispielsweise die Ausführungszeit der Richtlinie 3 Stunden beträgt, muss das Intervall für die Richtlinienauswertung größer als 3 Stunden sein.

Anmerkung: Wenn Sie eine Frage nach der Übergabe bearbeiten und die zugeordneten Tests von der Bearbeitung betroffen sind, kann es bis zu einer Stunde dauern, bis diese Änderungen angezeigt werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie die Frage aus, die Sie übergeben möchten.
4. Klicken Sie auf **Submit Question** (Frage übergeben).

Richtlinienüberwachungsfragen exportieren und importieren

Benutzer mit Administratorberechtigungen können Richtlinienüberwachungsfragen exportieren und importieren.

Der Export und Import von Fragen stellt eine Methode dar, um Fragen zu sichern und Fragen mit anderen Benutzern von IBM Security QRadar Risk Manager gemeinsam zu nutzen.

Einschränkungen für sensible Informationen

Sensible Unternehmens- oder Richtlinieninformationen können in Abhängigkeiten eingeschlossen sein. Beim Export oder Import von Richtlinienüberwachungsfragen sind die in den Abhängigkeiten enthaltenen sensiblen Daten nicht eingeschlossen.

Richtlinienüberwachungsfragen können folgende Typen von Abhängigkeiten enthalten:

- Assetbausteine
- Gespeicherte Assetsuchen
- Netze
- Ferne Netzadressen
- Geografische Netzadressen
- Referenzsets

Bevor Sie Fragen exportieren, die Abhängigkeiten enthalten, sollten Sie gegebenenfalls weiteren Kontext zum Typ der in der Abhängigkeit enthaltenen Informationen bereitstellen. Dank dieser Kontextinformationen wissen andere Benutzer, welchen Informationstyp sie beim Importieren der Frage in ihre Richtlinienüberwachung referenzieren müssen.

Fragen zur Richtlinienüberwachung exportieren

Sie können eine oder mehrere Ihrer Fragen zur Richtlinienüberwachung in eine XML-Datei exportieren. Der Export von Fragen zur Richtlinienüberwachung ist hilfreich beim Sichern Ihrer Fragen oder bei der gemeinsamen Nutzung von Fragen mit anderen Nutzern.

Informationen zu diesem Vorgang

Wenn Fragen zur Richtlinienüberwachung Abhängigkeiten enthalten, können Sie weiteren Kontext zum Typ der in der Abhängigkeit enthaltenen Informationen bereitstellen.

Der standardmäßige Name der XML-Datei für die exportierten Fragen lautet `policy_monitor_questions_export.xml`.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Risks** (Risiken) auf **Richtlinienüberwachung**.
2. Wählen Sie eine der folgenden Optionen aus:
   - Wenn Sie alle Fragen exportieren möchten, wählen Sie im Menü **Aktionen** die Option **Export All** (Alle exportieren) aus.

- Um ausgewählte Fragen zu exportieren, halten Sie die Steuertaste gedrückt und wählen alle Fragen aus, die Sie exportieren möchten. Wählen Sie anschließend im Menü **Aktionen** die Option **Export Selected** (Ausgewählte exportieren) aus.

3. Optional. Wenn eine Frage Abhängigkeiten enthält, klicken Sie auf den Parameterlink, um speziellere Informationen einzugeben. Die maximale Anzahl der Zeichen in diesem Feld beträgt 255.
4. Klicken Sie auf **Export Questions** (Fragen exportieren).

Ergebnisse

Es wird eine Standarddatei mit der Bezeichnung `policy_monitor_questions_export.xml` in Ihr Downloadverzeichnis exportiert.

Fragen zur Richtlinienüberwachung importieren

Sie können eine oder mehrere Fragen zur Richtlinienüberwachung in IBM Security QRadar Risk Manager importieren.

Informationen zu diesem Vorgang

Durch den Importprozess werden keine vorhandenen Fragen aktualisiert; jede Frage wird als neue Frage in der Richtlinienüberwachung angezeigt. Allen importierten Fragen wird eine Zeitmarke als Suffix hinzugefügt.

Nach dem Import einer Frage zur Richtlinienüberwachung wird in der Spalte **Status** eine Warnung angezeigt, falls eine importierte Frage eine Abhängigkeit enthält. Importierte Fragen mit Abhängigkeiten enthalten Parameter ohne Werte. Um sicherzustellen, dass die importierten Fragen zur Richtlinienüberwachung wie erwartet funktionieren, müssen Sie leeren Parametern Werte zuweisen.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Risks** (Risiken) auf **Richtlinienüberwachung**.
2. Wählen Sie im Menü **Aktionen** die Option **Importieren** aus.
3. Klicken Sie auf **Choose File** (Datei auswählen) und suchen Sie die XML-Datei, die Sie importieren möchten.
4. Klicken Sie auf **Öffnen**.
5. Wählen Sie mindestens eine Gruppe aus, der die Frage zugewiesen wird.
6. Klicken Sie auf **Import Question** (Frage importieren).
7. Überprüfen Sie die Spalte **Status** auf Warnungen. Wenn eine Frage eine Warnung enthält, öffnen Sie die Frage und bearbeiten die abhängigen Parameter. Sie können die Frage speichern, sobald die Bearbeitung der Parameter abgeschlossen ist.

Nächste Schritte

Die Überwachung ist für importierte Fragen inaktiviert. Sie können ein Ereignis erstellen, um die Ergebnisse von importierten Fragen zu überwachen.

Assetergebnisse

Assetergebnisse werden angezeigt, nachdem eine Richtlinienüberwachungsfrage übergeben wurde.

Die Parameter für Assetergebnisse werden in der folgenden Tabelle beschrieben.

Tabelle 10. Assetergebnisse

Parameter	Beschreibung
Risikobewertung	Die Risikobewertung wird auf Basis der Anzahl der Ergebnisse und des Bedeutungsfaktors, der einer Frage zugewiesen ist, berechnet. Die Risikobewertung zeigt die Risikostufe an, die der Frage zugeordnet ist.
IP	Die IP-Adresse des Assets.
Name	Der Name des Assets, wie aus dem Assetprofil abgerufen. Weitere Informationen zu Assetprofilen finden Sie im *IBM Security QRadar SIEM Users Guide*.
Gewichtung	Die Gewichtung des Assets, wie aus dem Assetprofil abgerufen.
Zielport(s)	Die Liste der dem Asset zugeordneten Zielports im Kontext der Fragetests. Wenn dem Asset und der Frage mehrere Ports zugeordnet sind, wird in diesem Feld 'Mehrere' und die Anzahl der Ports angezeigt. Die Liste der Ports wird erstellt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um alle eindeutigen Ports zu erhalten, wo das Asset entweder die Quelle, das Ziel oder die Verbindung war. Klicken Sie auf 'Mehrere (N)', um die Verbindungen anzuzeigen. Diese Anzeige enthält die nach Ports zusammengefassten Verbindungen, gefiltert nach der IP-Adresse des Assets und auf der Basis des in der Frage angegebenen Zeitintervalls.

Tabelle 10. Assetergebnisse (Forts.)

Parameter	Beschreibung
Protokoll(e)	Die Liste der dem Asset zugeordneten Protokolle im Kontext der Fragetests. Wenn dem Asset und der Frage mehrere Protokolle zugeordnet sind, wird in diesem Feld 'Mehrere' und die Anzahl der Protokolle angezeigt. Die Liste der Protokolle wird erstellt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um alle eindeutigen Protokolle zu erhalten, wo das Asset entweder die Quelle, das Ziel oder die Verbindung war. Klicken Sie auf 'Mehrere (N)', um die Verbindungen anzuzeigen. Diese Anzeige enthält die nach Protokollen zusammengefassten Verbindungen, gefiltert nach der IP-Adresse des Assets und auf der Basis des in der Frage angegebenen Zeitintervalls.
Flussanwendung(en)	Die Liste der dem Asset zugeordneten Anwendungen im Kontext der Fragetests. Wenn dem Asset und der Frage mehrere Anwendungen zugeordnet sind, wird in diesem Feld 'Mehrere' und die Anzahl der Anwendungen angezeigt. Die Liste der Anwendungen wird erstellt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um alle eindeutigen Anwendungen zu erhalten, wo das Asset entweder die Quelle, das Ziel oder die Verbindung war. Klicken Sie auf 'Mehrere (N)', um die Verbindungen anzuzeigen. Diese Anzeige enthält die nach Anwendungen zusammengefassten Verbindungen, gefiltert nach der IP-Adresse des Assets und auf der Basis des in der Frage angegebenen Zeitintervalls.

Tabelle 10. Assetergebnisse (Forts.)

Parameter	Beschreibung
Schwachstelle(n)	Die Liste der dem Asset zugeordneten Schwachstellen im Kontext der Fragetests. Wenn dem Asset und der Frage mehrere Schwachstellen zugeordnet sind, wird in diesem Feld 'Mehrere' und die Anzahl der Schwachstellen angezeigt. Die Liste der Schwachstellen wird erstellt, indem die auf dem Asset erkannten Schwachstellen anhand einer von relevanten Tests kompilierten Liste aller Schwachstellen gefiltert wird. Wenn für die Frage keine Schwachstellen angegeben sind, werden alle Schwachstellen des Assets verwendet, um diese Liste zu kompilieren. Klicken Sie auf 'Mehrere (N)', um die Assets anzuzeigen. Diese Anzeige enthält die nach Schwachstellen zusammengefassten Verbindungen, gefiltert nach der IP-Adresse des Assets und auf der Basis des in der Frage angegebenen Zeitintervalls.
Flusszähler	Die Gesamtzahl der dem Asset zugeordneten Flüsse im Kontext der Fragetests. Der Flusszähler wird ermittelt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um die Gesamtzahl der Flüsse zu erhalten, wo das Asset entweder die Quelle, das Ziel oder die Verbindung war.
Quelle(n)	Die Liste der dem Asset zugeordneten Quellen-IP-Adressen im Kontext der Fragetests. Wenn dem Asset und der Frage mehrere Quellen-IP-Adressen zugeordnet sind, wird in diesem Feld 'Mehrere' und die Anzahl der Quellen-IP-Adressen angezeigt. Die Liste der Quellen-IP-Adressen wird erstellt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um alle eindeutigen Quellen-IP-Adressen zu erhalten, wo das Asset das Ziel der Verbindung ist. Klicken Sie auf 'Mehrere (N)', um die Verbindungen anzuzeigen. Diese Anzeige enthält die nach Quellen-IP-Adressen zusammengefassten Verbindungen, gefiltert nach der IP-Adresse des Assets und auf der Basis des in der Frage angegebenen Zeitintervalls.

Tabelle 10. Assetergebnisse (Forts.)

Parameter	Beschreibung
Ziel(e)	Die Liste der dem Asset zugeordneten Ziel-IP-Adressen im Kontext der Fragetests. Wenn dem Asset und der Frage mehrere Ziel-IP-Adressen zugeordnet sind, wird in diesem Feld 'Mehrere' und die Anzahl der Fragetests angezeigt. Die Liste der Ziel-IP-Adressen wird erstellt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um alle eindeutigen Ziel-IP-Adressen zu erhalten, wo das Asset die Quelle der Verbindung ist. Klicken Sie auf 'Mehrere (N)', um die Verbindungen anzuzeigen. Diese Anzeige enthält die nach Ziel-IP-Adressen zusammengefassten Verbindungen, gefiltert nach der IP-Adresse des Assets und auf der Basis des in der Frage angegebenen Zeitintervalls.
Flussquellenbytes	Die Gesamtzahl der dem Asset zugeordneten Quellenbytes im Kontext des Fragetests. Die Quellenbytes werden ermittelt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um die Gesamtzahl der Quellenbytes zu erhalten, wo das Asset die Quelle der Verbindung ist.
Flusszielbytes	Die Gesamtzahl der dem Asset zugeordneten Zielbytes im Kontext des Fragetests. Die Zielbytes werden ermittelt, indem die der Frage zugeordneten Verbindungen gefiltert werden, um die Gesamtzahl der Zielbytes zu erhalten, wo das Asset das Ziel der Verbindung ist.

Einheitenergebnisse

Einheitenergebnisse werden angezeigt, nachdem eine Richtlinienüberwachungsfrage übergeben wurde.

Die Parameter für Einheitenergebnisse werden in der folgenden Tabelle beschrieben.

Tabelle 11. Einheiten- und Regelergebnisse

Parameter	Beschreibung
Risikobewertung	Die Risikostufe, die der Frage zugeordnet ist. Die Risikobewertung wird auf Basis der Anzahl der Ergebnisse und des Bedeutungsfaktors, der einer Frage zugewiesen ist, berechnet. Die Berechnung basiert auf folgenden Werten: • Der Assetgewichtung von Assets/ Einheiten, die in den Ergebnissen einer Frage zurückgegeben werden. • Dem Bedeutungsfaktor der Frage. • Die Anzahl der Ergebnisse, die für die Frage zurückgegeben werden.
Einheiten-IP	Die IP-Adresse der Einheit.
Einheitenname	Der Name der Einheit, wie aus der Konfigurationsüberwachung abgerufen.
Einheitentyp	Der Typ der Einheit, wie aus dem Assetprofil abgerufen. Weitere Informationen zu Assetprofilen finden Sie im *IBM Security QRadar SIEM Users Guide.*
Liste	Der Name der Regel aus der Einheit.
Eintrag	Die Eintragsnummer der Regel.
Aktion	Die Aktion, die der relevanten Regel aus der Einheit zugeordnet ist. Verfügbare Optionen: Zulassen, Verweigern, NA (Nicht zutreffend).

Tabelle 11. Einheiten- und Regelergebnisse (Forts.)

Parameter	Beschreibung

Quellenservice(s)	Die Quellenports und der Vergleich, die der relevanten Regel aus der Einheit zugeordnet sind, in folgendem Format:
	`<Vergleich>:<Port>`
	Wobei
	`<Vergleich>`
	eine der folgenden Optionen einschließen kann:
	• eq (equal) - gleich
	• ne (not equal) - ungleich
	• lt (less than) - kleiner als
	• gt (greater than) - größer als
	Wenn der Parameter beispielsweise ne:80 angibt, sind alle Ports außer 80 für diesen Quellenservice zulässig. Gibt der Parameter lt:80 an, sind die Ports von 0 bis 79 zulässig.
	Dieser Parameter zeigt den Quellenport für die Einheitenregel an. Wenn für diese Einheitenregel kein Port vorhanden ist, wird NA angezeigt.
	Quellenservices mit einem Hyperlink zeigen eine Objektgruppenreferenz an. Klicken Sie auf den Link, um detaillierte Informationen zu der Objektgruppenreferenz anzuzeigen.

Tabelle 11. Einheiten- und Regelergebnisse (Forts.)

Parameter	Beschreibung

Zielservice(s)	Die Zielports und der Vergleich, die der relevanten Regel aus der Einheit zugeordnet sind, werden in folgendem Format angezeigt:
	`<Vergleich>:<Port>`
	Wobei
	`<Vergleich>`
	eine der folgenden Optionen einschließen kann:
	• eq (equal) - gleich
	• ne (not equal) - ungleich
	• lt (less than) - kleiner als
	• gt (greater than) - größer als
	Wenn der Parameter beispielsweise ne:80 angibt, sind alle Ports außer 80 für diesen Zielservice zulässig. Gibt der Parameter lt:80 an, sind die Ports von 0 bis 79 zulässig.
	Dieser Parameter zeigt den Zielport für die Einheitenregel an. Wenn für diese Einheitenregel kein Port vorhanden ist, wird NA angezeigt.
	Zielservices mit einem Hyperlink zeigen eine Objektgruppenreferenz an. Klicken Sie auf den Link, um detaillierte Informationen zu der Objektgruppenreferenz anzuzeigen.

Quelle(n)	Das Quellennetz, das dem Asset zugeordnet ist. Quellen mit einem Hyperlink zeigen eine Objektgruppenreferenz an. Klicken Sie auf den Link, um detaillierte Informationen zu der Objektgruppenreferenz anzuzeigen.
Ziel(e)	Das Zielnetz, das der relevanten Regel aus der Einheit zugeordnet ist. Ziele mit einem Hyperlink zeigen eine Objektgruppenreferenz an. Klicken Sie auf den Link, um detaillierte Informationen zu der Objektgruppenreferenz anzuzeigen.
Protokoll(e)	Das Protokoll oder die Protokollgruppe, das bzw. die der relevanten Regel aus der Einheit zugeordnet ist.
Signatur(en)	Die Signatur für die Einheit, die nur für eine Einheitenregel in einer IP-Einheit angezeigt wird.

Ergebnisse von Richtlinienüberwachungsfragen bewerten

Sie können die von einer Richtlinienüberwachungsfrage zurückgegebenen Ergebnisse bewerten.

Ein Ergebnis einer Frage zu genehmigen ist nichts anderes, als das System dahingehend zu optimieren, dass es QRadar Risk Manager darüber informiert, dass das dem Frageergebnis zugeordnete Asset sicher ist oder in Zukunft ignoriert werden kann.

Wenn ein Benutzer ein Assetergebnis genehmigt, betrachtet die Richtlinienüberwachung das Assetergebnis als genehmigt, und wenn die Richtlinienüberwachungsfrage in Zukunft übergeben oder überwacht wird, ist das Asset nicht in den Frageergebnissen aufgelistet. Das genehmigte Asset wird nicht in der Ergebnisliste für die Frage angezeigt, außer wenn die Genehmigung widerrufen wird. Die Richtlinienüberwachung zeichnet die IP-Adresse der Einheit, die Begründung für die Genehmigung, die anwendbare Einheit/Regel sowie Datum und Uhrzeit für die Netzsicherheitsadministratoren auf.

Ergebnisse genehmigen

Sie können die zurückgegebene Liste der Assets oder Einheitenregeln auswerten, um die damit verbundenen Risiken zu ermitteln. Nach der Auswertung können Sie alle oder bestimmte Ergebnisse genehmigen.

Vorgehensweise

1. Aktivieren Sie in der Ergebnistabelle das Kontrollkästchen neben den Ergebnissen, die Sie akzeptieren möchten.
2. Wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Alle genehmigen	Wählen Sie diese Option aus, um alle Ergebnisse zu genehmigen.
Markierte genehmigen	Aktivieren Sie das Kontrollkästchen neben den Ergebnissen, die Sie genehmigen möchten, und klicken Sie anschließend auf 'Markierte genehmigen'.

3. Geben Sie den Grund für die Genehmigung ein.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf **OK**.
6. Um die genehmigten Ergebnisse für die Frage anzuzeigen, klicken Sie auf **View Approved** (Genehmigte anzeigen).

Ergebnisse

Im Fenster 'Approved Question Results' (Genehmigte Ergebnisse für die Frage) werden die folgenden Informationen bereitgestellt:

Tabelle 12. Parameter der genehmigten Ergebnisse für die Frage

Parameter	Beschreibung
Device/Rule	Für das Ergebnis einer Frage des Typs 'Device/Rule' (Einheit/Regel) wird die Einheit angezeigt, die diesem Ergebnis zugeordnet ist.
IP	Für das Ergebnis einer Asset-Frage wird die IP-Adresse angezeigt, die dem Asset zugeordnet ist.
Approved By	Der Benutzer, der die Ergebnisse genehmigt hat.
Approved On	Datum und Uhrzeit bei der Genehmigung der Ergebnisse.
Notes	Zeigt den Text der Hinweise, die diesem Ergebnis zugeordnet sind, sowie den Grund für die Genehmigung der Frage an.

Wenn Sie für beliebige Ergebnisse Genehmigungen entfernen möchten, aktivieren Sie die Kontrollkästchen der entsprechenden Ergebnissen und klicken auf **Revoke Selected** (Ausgewählte widerrufen). Klicken Sie auf **Revoke All** (Alle widerrufen), um alle Genehmigungen zu entfernen.

Fragen überwachen

Wenn bei einer Änderung der Ergebnisse einer Frage ein Ereignis generiert werden soll, können Sie eine zu überwachende Frage konfigurieren.

Wenn Sie eine Frage zur Überwachung auswählen, analysiert QRadar Risk Manager die Frage kontinuierlich, um zu erkennen, wenn sich die Ergebnisse einer Frage ändern. Wenn QRadar Risk Manager eine Ergebnisänderung erkennt, kann ein Angriff generiert werden, um Sie über eine Abweichung von der definierten Richtlinie zu benachrichtigen.

Für eine Frage im Überwachungsmodus gilt standardmäßig ein Zeitbereich von einer Stunde. Dieser Wert überschreibt den Zeitwert, der bei der Erstellung der Frage festgelegt wurde. Weitere Informationen zum Erstellen einer Frage finden Sie im Abschnitt Frage erstellen.

Ereignis zur Überwachung von Ergebnissen erstellen

Sie können ein Ereignis erstellen, um die Ergebnisse von Fragen zu überwachen, die in der Richtlinienüberwachung erstellt wurden.

Informationen zu diesem Vorgang

Die Parameter, die Sie für ein Ereignis konfigurieren, werden in der folgenden Tabelle beschrieben.

Tabelle 13. Ergebnisparameter von Fragen überwachen

Parameter	Beschreibung
Policy evaluation interval (Intervall für die Richtlinienauswertung)	Die Häufigkeit, mit der das Ereignis ausgeführt wird.

Tabelle 13. Ergebnisparameter von Fragen überwachen (Forts.)

Parameter	Beschreibung
Event Name (Ereignisname)	Der Name des Ereignisses, das in den Registerkarten **Protokollaktivität** und **Angriffe** angezeigt werden soll.
Event Description (Ereignisbeschreibung)	Die Beschreibung des Ereignisses. Die Beschreibung wird in den Anmerkungen zu den Ereignisdetails angezeigt.
High-Level Category (Übergeordnete Kategorie)	Die übergeordnete Ereigniskategorie, die diese Regel bei der Verarbeitung von Ereignissen verwenden soll.
Low-Level Category (Untergeordnete Kategorie)	Die untergeordnete Ereigniskategorie, die diese Regel bei der Verarbeitung von Ereignissen verwenden soll.
Ensure the dispatched event is part of an offense (Sicherstellen, dass das gesendete Ereignis Teil eines Angriffs ist)	Leitet das Ereignis an die Komponente 'Magistrat' weiter. Wenn kein Angriff generiert wurde, wird ein neuer Angriff erstellt. Falls ein Angriff vorhanden ist, wird das Ereignis hinzugefügt. Wenn Sie eine Korrelation nach Frage oder Simulation ausführen, werden alle Ereignisse aus einer Frage einem einzelnen Angriff zugeordnet. Wenn Sie eine Korrelation nach Asset ausführen, wird ein eindeutiger Angriff erstellt oder für jedes eindeutige Asset aktualisiert.
Dispatch question passed events (Frage weiterleiten, die Ereignisse übergeben hat)	Leitet Ereignisse weiter, die die Frage zur Richtlinienüberwachung an die Komponente 'Magistrat' übergibt.
Vulnerability Score Adjustments (Anpassungen von Schwachstellenbewertung)	Passt die Risikobewertung für Schwachstellen eines Assets abhängig davon ab, ob die Frage fehlschlägt oder übergeben wird. Die Risikobewertungen für Schwachstellen werden in IBM Security QRadar Vulnerability Manager angepasst.

Additional Actions (Weitere Aktionen)	Die weiteren Aktionen, die beim Empfang eines Ereignisses ausgeführt werden.
	
	Trennen Sie mehrere E-Mail-Adressen durch ein Komma.
	
	Wählen Sie **Benachrichtigen** aus, wenn Ereignisse, die als Ergebnis dieser überwachten Frage generiert werden, Ereignisse im Element 'Systembenachrichtigungen' im Dashboard anzeigen sollen.
	
	Die Ausgabe des Systemprotokolls kann folgendermaßen aussehen:
	`Sep 28 12:39:01 localhost.localdomain ECS:`
	`Rule 'Name of Rule'`
	`Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6,`
	`Event Name:SCAN SYN FIN, QID: 1000398, Category: 1011,`
	`Notes: Event description`

Enable Monitor (Überwachung aktivieren)	Frage überwachen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie die Frage aus, die Sie überwachen möchten.
4. Klicken Sie auf **Überwachen**.

5. Konfigurieren Sie Werte für die Parameter.
6. Klicken Sie auf **Save Monitor** (Überwachung speichern).

Fragen gruppieren

Sie können Fragen auf Basis der ausgewählten Kriterien gruppieren und anzeigen.

Die Kategorisierung Ihrer Fragen ermöglicht Ihnen eine effiziente Anzeige und Verfolgung der Fragen. Sie können beispielsweise alle Fragen anzeigen, die sich auf die Konformität beziehen.

Wenn Sie eine neue Frage erstellen, können Sie die Frage einer bestehenden Gruppe zuweisen.

Gruppen anzeigen

Sie können eine Gruppe Ihrer Fragen anzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie in der Liste **Gruppe** die Gruppe aus, die Sie anzeigen möchten.

Gruppe erstellen

Sie können eine neue Gruppe für Fragen erstellen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe aus, unter der Sie eine neue Gruppe erstellen wollen.
5. Klicken Sie auf **Neu**.
6. Geben Sie im **Namensfeld** den Namen an, den Sie der neuen Gruppe zuweisen möchten. Der Name kann bis zu 255 Zeichen lang sein.
7. Geben Sie im **Beschreibungsfeld** eine Beschreibung an, die Sie der Gruppe zuweisen möchten. Die Beschreibung kann bis zu 255 Zeichen lang sein.
8. Klicken Sie auf **OK**.
9. Wenn Sie die Position der neuen Gruppe ändern möchten, klicken Sie auf die neue Gruppe und ziehen den Ordner an die gewünschte Position in Ihrer Menübaumstruktur.

Gruppe bearbeiten

Sie können eine Gruppe von Fragen bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe aus, die Sie bearbeiten wollen.

5. Klicken Sie auf **Bearbeiten**.
6. Bearbeiten Sie gegebenenfalls den **Namen** und die **Beschreibung**.

   Die Felder für Name und Beschreibung können maximal 255 Zeichen enthalten.
7. Klicken Sie auf **OK**.
8. Wenn Sie die Position der Gruppe ändern möchten, wählen Sie die Gruppe aus und ziehen den Ordner an die gewünschte Position in der Menübaumstruktur.
9. Schließt das Fenster 'Gruppen'.

Element in eine andere Gruppe kopieren

Mit der Gruppenfunktion können Sie eine Simulation in eine oder mehrere Gruppen kopieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Frage aus, die Sie in eine andere Gruppe kopieren wollen.
5. Klicken Sie auf **Kopieren**.
6. Wählen Sie das Kontrollkästchen für die Gruppe aus, in die Sie die Simulation kopieren möchten.
7. Klicken Sie auf **Kopieren**.

Element aus einer Gruppe löschen

Sie können ein Element aus einer Gruppe löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe der höchsten Ebene aus.
5. Wählen Sie aus der Liste der Gruppen das Element oder die Gruppe aus, das bzw. die Sie löschen wollen.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **OK**.

Element einer Gruppe zuweisen

Eine Frage kann einer Gruppe zugeordnet werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie die Frage aus, die Sie einer Gruppe zuweisen wollen.
4. Wählen Sie im Menü **Aktionen** die Option **Gruppen zuweisen** aus.
5. Wählen Sie die Gruppe aus, der die Frage zugeordnet werden soll.
6. Klicken Sie auf **Gruppen zuweisen**.

Integration von IBM Security QRadar Risk Manager und IBM Security QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager kann mit QRadar Risk Manager integriert werden, um Sie bei der Vergabe von Prioritäten für die Risiken und Schwachstellen in einem Netz zu unterstützen.

Risikorichtlinien und Schwachstellenpriorisierung

Sie können QRadar Vulnerability Manager mit QRadar Risk Manager integrieren, indem Sie Risikorichtlinien für Assets oder Schwachstellen definieren und überwachen.

Immer wenn die von Ihnen in QRadar Risk Manager definierten Risikorichtlinien eingehalten oder nicht eingehalten werden, erfolgt eine entsprechende Anpassung der Risikobewertungen in QRadar Vulnerability Manager. Der Grad der Anpassung hängt von den Risikorichtlinien des Unternehmens ab.

Bei einer Anpassung der Schwachstellenrisikobewertungen in QRadar Vulnerability Manager können Administratoren folgende Aufgaben ausführen:

- Sofortige Sichtbarkeit der Schwachstellen, die eine Risikorichtlinie nicht eingehalten haben

  Zum Beispiel können neue Informationen am QRadar-Dashboard angezeigt oder als E-Mail gesendet werden.
- Neupriorisierung der Schwachstellen, die sofortige Aufmerksamkeit erfordern

  Zum Beispiel kann ein Administrator anhand der **Risikobewertung** schnell Schwachstellen mit hohem Risiko erkennen.

Wenn Sie Risikorichtlinien auf eine Assetebene in QRadar Risk Manager anwenden, werden die Risikobewertungen aller Schwachstellen des Assets angepasst.

Anwendungsfälle für Richtlinienüberwachung

Es sind viele Optionen verfügbar, wenn Sie Fragen zur Risikoanalyse eines Netzes erstellen.

Die folgenden Richtlinienüberwachungsbeispiele beschreiben allgemeine Anwendungsfälle, die Sie in einer Netzumgebung verwenden können.

Tatsächliche Kommunikation für in DMZ zulässige Protokolle

Dieser Anwendungsfall veranschaulicht, wie eine Richtlinienüberwachungsfrage auf Basis der bekannten Liste vertrauenswürdiger Protokolle für die DMZ (Demilitarized Zone) erstellt wird. In den meisten Unternehmen wird der Netzverkehr durch die DMZ auf wohlbekannte und vertrauenswürdige Protokolle eingeschränkt, z. B. HTTP oder HTTPS an festgelegten Ports.

Informationen zu diesem Vorgang

Aus Sicht der Risikoperspektive ist es wichtig, den Datenverkehr in der DMZ ständig zu überwachen, um sicherzustellen, dass nur vertrauenswürdige Protokolle vorhanden sind. QRadar Risk Manager erreicht dies, indem eine Richtlinienüberwachungsfrage auf Basis eines Assettests für tatsächliche Kommunikationen erstellt wird.

Es gibt mehrere Möglichkeiten, um eine Richtlinienüberwachungsfrage für dieses Anwendungsfallziel zu generieren. Da bekannt ist, dass die Netzrichtlinie nur wenige vertrauenswürdige Protokolle zulässt, wird eine Option ausgewählt, mit der die Richtlinienüberwachungsfrage auf Basis der bekannten Liste vertrauenswürdiger Protokolle für die DMZ erstellt wird.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Policy Monitor** (Richtlinienüberwachung).
3. Wählen Sie im Menü **Actions** (Aktionen) den Menüpunkt **New** (Neu) aus.
4. Geben Sie im Feld **What do you want to name this question** (Welchen Namen soll die Frage erhalten) einen Namen für die Frage ein.
5. Wählen Sie in der Dropdown-Liste **What type of data do you want to return** (Welcher Datentyp soll zurückgegeben werden) den Eintrag 'Assets' aus.
6. Wählen Sie in der Dropdown-Liste **Evaluate On** (Auswerten für) den Eintrag 'Actual Communication' (Tatsächliche Kommunikation) aus.
7. Wählen Sie in der Dropdown-Liste **Importance Factor** (Bewertungsfaktor) eine Bewertungsstufe aus, die der Frage zugeordnet werden soll.
8. Geben Sie im Abschnitt **Time Range** (Zeitbereich) einen Zeitbereich für die Frage ein.
9. Wählen Sie im Abschnitt **Which tests do you want to include in your question** (Welche Tests sollen in die Frage eingeschlossen werden) die Option **have accepted communication to destination networks** (Kommunikation mit Zielnetzen wurde akzeptiert) aus.
10. Klicken Sie im Abschnitt **Find Assets that** (Assets finden, die) auf **destination networks** (Zielnetze), um diesen Test weiter zu konfigurieren, und geben Sie ihre DMZ als Zielnetz an.
11. Wählen Sie die Option **and include the following inbound ports** (und die folgenden Ports für eingehende Daten einschließen) aus.
12. Klicken Sie im Abschnitt **Find Assets that** (Assets finden, die) auf den Parameter für 'Nur einschließen', sodass er in 'Ausschließen' geändert wird. Der Parameter zeigt jetzt 'and exclude the following inbound ports' (und die folgenden Ports für eingehende Daten ausschließen) an.
13. Klicken Sie auf **Ports**.
14. Fügen Sie die Ports 80 und 443 hinzu und klicken Sie dann auf **OK**.
15. Klicken Sie auf **Save Question** (Frage speichern).
16. Wählen Sie die DMZ-Richtlinienüberwachungsfrage aus, die Sie erstellt haben.
17. Klicken Sie auf **Submit Question** (Frage übergeben).
18. Prüfen Sie die Ergebnisse, um zu sehen, ob über andere Protokolle als Port 80 und Port 443 im Netz kommuniziert wird.
19. Optional: Nachdem die Ergebnisse auf geeignete Weise optimiert wurden, können Sie Ihre DMZ-Frage überwachen, indem Sie die Frage in den Überwachungsmodus versetzen.

Nächste Schritte

Sie können Ihre Fragen überwachen.

Asset-Test auf mögliche Datenübertragung in geschützten Assets

Dieser Anwendungsfall veranschaulicht die Erstellung einer Frage zur Richtlinienüberwachung auf Basis einer IP-Adresse. Jedes Unternehmen verfügt über Netze mit kritischen Servern, auf denen der Datenverkehr überwacht wird und auf die nur vertrauenswürdige Angestellte zugreifen können.

Informationen zu diesem Vorgang

Aus einer Risikoperspektive betrachtet ist es wichtig, dass Sie wissen, welche Benutzer in Ihrem Unternehmen mit kritischen Netzassets kommunizieren. QRadar Risk Manager erreicht diese Aufgabe, indem eine Frage zur Richtlinienüberwachung auf Basis eines Assettests auf mögliche Datenübertragungen erstellt wird.

Für das Ziel dieses Anwendungsfalls kann eine Frage zur Richtlinienüberwachung auf mehrere Arten generiert werden. Sie könnten alle Verbindungen zu dem kritischen Server über eine Zeitdauer betrachten, aber möglicherweise befürchten Sie auch, dass regionale Mitarbeiter nicht auf diese kritischen Server zugreifen. Hierzu können Sie eine Frage zur Richtlinienüberwachung erstellen, die die Topologie des Netzes nach IP-Adresse betrachtet.

Vorgehensweise

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie im Menü **Aktionen** die Option **Neu** aus.
4. Geben Sie im Feld **What do you want to name this question** (Welche Bezeichnung soll diese Frage haben) einen Namen für die Frage ein.
5. Wählen Sie in der Dropdown-Liste **What type of data do you want to return** (Welchen Datentyp möchten Sie zurückgeben) die Option 'Asset' aus.
6. Wählen Sie in der Dropdown-Liste **Evaluate On** (Auswerten auf) die Option 'Possible Communication' (Mögliche Kommunikation) aus.
7. Wählen Sie in der Dropdown-Liste **Wichtigkeitsfaktor** eine Bewertungsstufe aus, die Ihrer Frage zugeordnet werden soll.
8. Geben Sie im Abschnitt **Zeitraum** einen Zeitbereich für die Frage an.
9. Klicken Sie doppelt in den Abschnitt **Which tests do you want to include in your question** (Welche Tests sollen in Ihre Frage integriert werden) und wählen Sie die Option **have accepted communication to destination asset building blocks** (Kommunikation zu Assets-Bausteinen des Ziels akzeptieren) aus.
10. Klicken Sie im Abschnitt 'Find Assets that' (Assets suchen) auf **asset building blocks** (Asset-Bausteine), um diesen Test weiter zu konfigurieren, und geben Sie **Protected Assets** (Geschützte Assets) an.

    Anmerkung:

    Um Ihre fernen Netz-Assets zu definieren, müssen Sie zuvor die Bausteine für Ihre fernen Assets definiert haben.
11. Klicken Sie doppelt in den Abschnitt **Which tests do you want to include in your question**, um den restriktiven Test auszuwählen **und nur die folgenden IP-Adressen einzuschließen**.
12. Klicken Sie im Abschnitt 'Find Assets that' auf **IP-Adressen**.

13. Geben Sie den Bereich der IP-Adressen oder die CIDR-Adresse Ihres fernen Netzes an.
14. Klicken Sie auf **Save Question** (Frage speichern).
15. Wählen Sie die Frage zur Richtlinienüberwachung aus, die Sie für geschützte Assets erstellt haben.
16. Klicken Sie auf **Submit Question** (Frage übergeben).
17. Überprüfen Sie die Ergebnisse, um zu ermitteln, ob ein geschütztes Asset die Datenübertragung aus einer unbekannten IP-Adresse oder einem unbekannten CIDR-Bereich akzeptiert hat.
18. Optional. Nachdem die Ergebnisse korrekt optimiert wurden, können Sie Ihre geschützten Assets überwachen, indem Sie die Frage in den Überwachungsmodus einreihen. Wenn ein geschütztes Asset eine Verbindung zu einer nicht erkannten IP-Adresse herstellt, kann QRadar Risk Manager eine Benachrichtigung generieren.

Nächste Schritte

Sie können Ihre Fragen überwachen.

Test von Einheiten/Regeln auf Kommunikation über Internetzugriff

Mit diesem Anwendungsfall wird gezeigt, wie eine Frage zur Richtlinienüberwachung auf Basis von Einheiten/Regeln erstellt wird. Durch Einheitentests werden Regeln in einer Einheit ermittelt, die eine definierte Richtlinie nicht einhalten, oder Änderungen, die ein Risiko in die Umgebung einführen.

Informationen zu diesem Vorgang

Durch Einheitentests werden Regeln in einer Einheit ermittelt, die eine definierte Richtlinie nicht einhalten, oder Änderungen, die ein Risiko in die Umgebung einführen. Aus einer Netzperspektive ist es wichtig, zu wissen, welche Einheitenregeln möglicherweise geändert wurden, und eine Benachrichtigung zu der Regel zu erhalten, damit diese korrigiert werden kann. Dieses Verhalten tritt sehr häufig auf, wenn Server, die zuvor über keinen Internetzugang verfügten, aufgrund einer Firewall-Änderung im Netz Zugriff erteilt bekommen. QRadar Risk Manager kann Regeländerungen in Netzeinheiten überwachen, indem eine Frage zur Richtlinienüberwachung auf Basis der Einheitenregeln erstellt wird.

Für das Ziel dieses Anwendungsfalls kann eine Frage zur Richtlinienüberwachung auf mehrere Arten generiert werden. In diesem Beispiel erstellen Sie eine Frage zur Richtlinienüberwachung, mit der ermittelt wird, welche Einheiten auf das Internet zugreifen können.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie im Menü **Aktionen** die Option **Neu** aus.
4. Wählen Sie in der Dropdown-Liste **What type of data do you want to return** (Welchen Datentyp möchten Sie zurückgeben) die Option 'Devices/Rules' (Einheiten/Regeln) aus.
5. Wählen Sie in der Dropdown-Liste **Wichtigkeitsfaktor** eine Bewertungsstufe aus, die Ihrer Frage zugeordnet werden soll.

6. Klicken Sie doppelt in den Abschnitt **Which tests do you want to include in your question** (Welche Tests sollen in Ihre Frage integriert werden) und wählen Sie **allow connection to the internet** (Verbindung mit dem Internet ermöglichen) aus.
7. Klicken Sie auf **Save Question** (Frage speichern).
8. Wählen Sie die Frage zur Richtlinienüberwachung aus, die Sie zur Überwachung von Einheitenregeln erstellt haben.
9. Klicken Sie auf **Submit Question** (Frage übergeben).
10. Überprüfen Sie die Ergebnisse, um zu ermitteln, ob sie Regeln enthalten, die einen Internetzugriff ermöglichen.
11. Optional. Nachdem die Ergebnisse korrekt optimiert wurden, können Sie Ihre geschützten Assets überwachen, indem Sie die Frage in den Überwachungsmodus einreihen.

Nächste Schritte

Sie können Ihre Fragen überwachen.

Schwachstellen mit hohem Risiko durch das Anwenden von Risikorichtlinien priorisieren

In IBM Security QRadar Vulnerability Manager können Sie Administratoren auf Schwachstellen mit höherem Risiko benachrichtigen, indem Sie Risikorichtlinien für Ihre Schwachstellen anwenden.

Beim Anwenden einer Risikorichtlinie wird die Risikobewertung einer Schwachstelle angepasst, wodurch Administratoren die Schwachstellen, für die eine sofortige Aufmerksamkeit erforderlich ist, präziser priorisieren können.

In diesem Beispiel wird die Risikobewertung für eine Schwachstelle automatisch mit einem Prozentsatzfaktor für jede Schwachstelle erhöht, die in Ihrem Netz nach 40 Tagen noch aktiv ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Schwachstellen**.
2. Klicken Sie im Navigationsfenster auf **Schwachstellen verwalten**.
3. Klicken Sie in der Symbolleiste auf **Suchen** > **Neue Suche**.
4. Konfigurieren Sie im Fenster **Suchparameter** die folgenden Filter:
   a. **Risk Equals High** (Risiko gleich hoch)
   b. **Tage, seit Schwachstellen gefunden wurden größer-gleich 40**
5. Klicken Sie auf **Suchen** und klicken Sie anschließend in der Symbolleiste auf **Suchkriterien speichern**.

   Geben Sie einen Namen für die gespeicherte Suche ein, der in QRadar Risk Manager erkennbar ist.
6. Klicken Sie auf die Registerkarte **Risks** (Risiken).
7. Klicken Sie im Navigationsfenster auf **Richtlinienüberwachung**.
8. Klicken Sie in der Symbolleiste auf **Aktionen** > **Neu**.
9. Geben Sie im Feld **What do you want to name this question** (Welche Bezeichnung soll diese Frage haben) einen Namen ein.
10. Klicken Sie im Feld **Which tests do you want to include in your question** (Welche Tests sollen in Ihre Frage integriert werden) auf **are susceptible to**

vulnerabilities contained in vulnerability saved searches (sind anfällig für Schwachstellen in gespeicherten Suchvorgängen für Schwachstellen).

11. Klicken Sie im Feld **Find Assets that** (Assets suchen, die) auf den unterstrichenen Parameter in **are susceptible to vulnerabilities contained in vulnerability saved searches** (sind anfällig für Schwachstellen in gespeicherten Suchen für Schwachstellen).
12. Ermitteln Sie die gespeicherte Suche nach Schwachstellen mit hohem Risiko für QRadar Vulnerability Manager, klicken Sie auf **Hinzufügen** und anschließend auf **OK**.
13. Klicken Sie auf **Save Question** (Frage speichern).
14. Wählen Sie im Fenster **Questions** (Fragen) Ihre Frage aus der Liste aus und klicken Sie in der Symbolleiste auf **Monitor** (Überwachen).

    Einschränkung: Das Feld **Ereignisbeschreibung** ist verbindlich.
15. Klicken Sie auf **Dispatch question passed events** (Frage senden, die Ereignisse übergeben hat).
16. Geben Sie im Feld **Vulnerability Score Adjustments** (Anpassungen an Schwachstellenbewertung) einen Wert für den Prozentsatz der Risikoanpassung im Feld **Percentage vulnerability score adjustment on question fail** (Anpassung von Prozentsatz für Schwachstellenbewertung an Frage fehlgeschlagen) ein.
17. Klicken Sie auf **Apply adjustment to all vulnerabilities on an asset** (Anpassung für alle Schwachstellen in einem Asset anwenden) und anschließend auf **Save Monitor** (Überwachung speichern).

Nächste Schritte

In der Registerkarte **Schwachstellen** können Sie Schwachstellen mit hohem Risiko suchen und Ihre Schwachstellen priorisieren.

Richtlinienüberwachungsfragen

Sie können Testfragen definieren, um Risiken in Netzeinheiten oder Regeln in Netzeinheiten zu identifizieren.

Generische und testspezifische Parameter für Richtlinienüberwachungstests

Sie konfigurieren Parameter für jeden Richtlinienüberwachungstest. Konfigurierbare Parameter sind fett dargestellt und unterstrichen. Klicken Sie auf einen Parameter, um die verfügbaren Optionen für eine Frage anzuzeigen.

Für Richtlinienüberwachungstests werden zwei Typen von Parametern verwendet: generische und testspezifische. Generische Parameter stellen mindestens zwei Optionen zur Anpassung eines Tests bereit. Durch Klicken auf einen generischen Parameter wird zwischen den verfügbaren Auswahlmöglichkeiten umgeschaltet. Testspezifische Parameter erfordern eine Benutzereingabe. Klicken Sie auf testspezifische Parameter, um Informationen anzugeben.

Zum Beispiel enthält der Assettest **have accepted communication to destination remote network locations** (Kommunikation mit fernen Zielnetzadressen akzeptiert) zwei generische Parameter und einen testspezifischen Parameter. Klicken Sie auf den generischen Parameter **have accepted**, um entweder **have accepted** (akzeptiert) oder **have rejected** (abgelehnt) auszuwählen. Klicken Sie auf den generischen Para-

meter **to destination**, um entweder **to destination** (mit Ziel) oder **from source** (von Quelle) auszuwählen. Klicken Sie auf den testspezifischen Parameter **remote network locations**, um eine ferne Netzadresse für den Assettest hinzuzufügen oder zu entfernen.

Assettestfragen

Assetfragen werden verwendet, um Assets im Netz zu identifizieren, die gegen eine definierte Richtlinie verstoßen oder ein Risiko in die Umgebung einführen.

Für Assettestfragen gibt es zwei Kategorien von Kommunikationstypen: tatsächliche oder mögliche Kommunikation. Beide Kommunikationstypen verwenden beitragende und einschränkende Tests.

Tatsächliche Kommunikation schließt alle Assets ein, auf denen Kommunikationen über Verbindungen erkannt wurden. Mit Fragen zur möglichen Kommunikation können Sie prüfen, ob bestimmte Kommunikationen auf Assets möglich sind, unabhängig davon, ob eine Kommunikation erkannt wurde oder nicht.

Die Frage eines beitragenden Tests ist die Basistestfrage, die den Typ der tatsächlichen Kommunikation, die Sie zu testen versuchen, definiert.

Die Frage eines einschränkenden Tests schränkt die Testergebnisse des beitragenden Tests ein, um die tatsächliche Kommunikation auf bestimmte Verstöße hin weiter zu filtern.

Bei Verwendung eines einschränkenden Tests sollte die Richtung des einschränkenden Tests derselben Richtung folgen wie der beitragende Test. Einschränkende Tests, die eine Mischung aus Eingangs- und Ausgangsrichtungen verwenden, können in Situationen eingesetzt werden, in denen Sie versuchen, Assets zwischen zwei Punkten, z. B. zwei Netzen oder IP-Adressen, zu lokalisieren.

Eingangsrichtung bezieht sich auf einen Test, mit dem die Verbindungen gefiltert werden, für die das fragliche Asset ein Ziel darstellt. Ausgangsrichtung bezieht sich auf einen Test, mit dem Verbindungen gefiltert werden, für die das fragliche Asset eine Quelle darstellt.

Einheit/Regeln-Testfragen

Einheiten und Regeln werden verwendet, um Regeln in einer Einheit zu identifizieren, die gegen eine definierte Richtlinie verstoßen, was ein Risiko in die Umgebung einführen kann.

Eine detaillierte Liste der Einheitenregelfragen finden Sie im Abschnitt Einheit/ Regeln-Testfragen.

Beitragende Fragen für Tests der tatsächlichen Kommunikation

Die Tests der tatsächlichen Kommunikation für Assets schließen beitragende Fragen und Parameter ein, die Sie bei der Erstellung eines Richtlinienüberwachungstests auswählen.

Wenn Sie die Bedingung 'have not' auf einen Test anwenden, wird die Bedingung 'not' dem Parameter zugeordnet, den Sie testen.

Wenn Sie beispielsweise einen Test als **have not accepted communication to destination networks** (Kommunikation mit Zielnetzen nicht akzeptiert) konfigurieren, werden mit dem Test Assets erkannt, die Kommunikationen mit anderen Netzen als dem konfigurierten Netz akzeptiert haben. Ein anderes Beispiel: Wenn Sie einen Test als 'have not accepted communication to the Internet' (Kommunikation mit dem Internet nicht akzeptiert) konfigurieren, werden mit dem Test Assets erkannt, die Kommunikationen aus oder mit anderen Bereichen als dem Internet akzeptiert haben.

In der folgenden Tabelle werden die Parameter für beitragende Fragen für Tests der tatsächlichen Kommunikation aufgelistet und beschrieben.

Tabelle 14. Parameter für beitragende Fragen für Tests der tatsächlichen Kommunikation

Testname	Beschreibung
have accepted communication to any destination	Erkennt Assets, die mit einem konfigurierten Netz kommunizieren. Mit diesem Test können Sie einen Start- oder Endpunkt für eine Frage definieren. Konfigurieren Sie den Test beispielsweise wie folgt, um die Assets zu identifizieren, die eine Kommunikation aus der Demilitarized Zone (DMZ) akzeptiert haben: have accepted communication from any source Mit diesem Test können Sie nicht richtlinienkonforme Kommunikationen erkennen.
have accepted communication to destination networks	Erkennt Assets, die mit Netzen kommunizieren, die Sie angeben. Mit diesem Test können Sie einen Start- oder Endpunkt für eine Frage definieren. Konfigurieren Sie den Test beispielsweise wie folgt, um die Assets zu identifizieren, die mit der Demilitarized Zone (DMZ) kommuniziert haben: have accepted communication from source <networks> Mit diesem Test können Sie nicht richtlinienkonforme Kommunikationen erkennen.

Tabelle 14. Parameter für beitragende Fragen für Tests der tatsächlichen Kommunikation (Forts.)

Testname	Beschreibung
have accepted communication to destination IP addresses	Erkennt Assets, die mit der IP-Adresse kommunizieren, die Sie angeben. Bei diesem Test können Sie eine IP- oder CIDR-Adresse angeben. Konfigurieren Sie den Test beispielsweise wie folgt, um alle Assets zu identifizieren, die mit einem bestimmten Compliance-Server kommuniziert haben: have accepted communications to destination <compliance server IP address>
have accepted communication to destination asset building blocks	Erkennt Assets, die mit Assetbausteinen kommunizieren, die Sie angeben. Bei diesem Test können Sie Bausteine, die im QRadar-Regelassistenten definiert sind, in einer Abfrage wiederverwenden. Weitere Informationen zu Regeln, Assets und Bausteinen finden Sie im *IBM Security QRadar Administration Guide*.
have accepted communication to destination asset saved searches	Erkennt Assets, die mit den Assets kommunizieren, die von der gespeicherten Suche, die Sie angeben, zurückgegeben werden. Informationen zum Erstellen und Speichern einer Assetsuche finden Sie im *IBM Security QRadar SIEM Users Guide.*
have accepted communication to destination reference sets	Erkennt Assets, die mit den definierten Referenzsets kommuniziert haben.
have accepted communication to destination remote network locations	Erkennt Assets, die mit Netzen kommuniziert haben, die als fernes Netz definiert sind. Mit diesem Test können beispielsweise Hosts identifiziert werden, die mit Botnets oder anderen verdächtigen Internetadressräumen kommuniziert haben.
have accepted communication to destination geographic network locations	Erkennt Assets, die mit Netzen kommuniziert haben, die als geografische Netze definiert sind. Mit diesem Test können beispielsweise Assets erkannt werden, die versucht haben, mit Ländern zu kommunizieren, in denen Ihr Unternehmen nicht tätig ist.
have accepted communication to the Internet	Erkennt Quellen- oder Zielkommunikationen mit dem Internet.

Tabelle 14. Parameter für beitragende Fragen für Tests der tatsächlichen Kommunikation (Forts.)

Testname	Beschreibung
are susceptible to one of the following vulnerabilities	Erkennt bestimmte Schwachstellen. Wenn Sie Schwachstellen eines bestimmten Typs erkennen möchten, verwenden Sie den Test **are susceptible to vulnerabilities with one of the following classifications**. Sie können anhand der OSVDB-ID, CVE-ID, Bugtraq-ID oder des Titels nach Schwachstellen suchen.
are susceptible to vulnerabilities with one of the following classifications	Eine Schwachstelle kann einer oder mehreren Schwachstellenklassifikationen zugeordnet werden. Dieser Test filtert alle Assets, die Schwachstellen mit den angegebenen Klassifikationen einschließen. Konfigurieren Sie den Parameter **classifications**, um die Schwachstellenklassifikationen anzugeben, die dieser Test anwenden soll. Eine Schwachstellenklassifikation kann beispielsweise 'Eingabemanipulation' oder 'Denial of Service' sein.
are susceptible to vulnerabilities with CVSS score greater than 5	Ein CVSS-Wert (Common Vulnerability Scoring System) ist ein Branchenstandard für die Bewertung des Schweregrads von Schwachstellen. CVSS setzt sich aus drei Messwertgruppen zusammen: Base Score, Temporal Score und Environmental Score. Anhand dieser Messwerte kann CVSS grundlegende Merkmale einer Schwachstelle definieren und kommunizieren. Dieser Test filtert Assets im Netz, die Schwachstellen mit der CVSS-Bewertung einschließen, die Sie angeben.
are susceptible to vulnerabilities disclosed after specified date	Erkennt Assets im Netz, die eine Schwachstelle aufweisen, die nach, vor oder an dem konfigurierten Datum offengelegt wurde.
are susceptible to vulnerabilities on one of the following ports	Erkennt Assets im Netz, die eine Schwachstelle aufweisen, die den konfigurierten Ports zugeordnet ist. Konfigurieren Sie den Parameter **ports**, um Ports anzugeben, die dieser Test berücksichtigen soll.

Tabelle 14. Parameter für beitragende Fragen für Tests der tatsächlichen Kommunikation (Forts.)

Testname	Beschreibung
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Erkennt Assets im Netz, die eine Schwachstelle aufweisen, die auf Basis einer oder mehrerer Texteingaben mit dem Assetnamen, dem Hersteller, der Version oder dem Service übereinstimmt. Konfigurieren Sie den Parameter **text entries** (Texteingaben), um den Assetnamen, den Hersteller, die Version oder den Service anzugeben, die dieser Test berücksichtigen soll.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Erkennt Assets im Netz, die eine Schwachstelle aufweisen, die auf Basis eines oder mehrerer regulärer Ausdrücke mit dem Assetnamen, dem Hersteller, der Version oder dem Service übereinstimmt. Konfigurieren Sie den Parameter **regular expressions** (Reguläre Ausdrücke), um den Assetnamen, den Hersteller, die Version oder den Service anzugeben, die dieser Test berücksichtigen soll.
are susceptible to vulnerabilities contained in vulnerability saved searches	Erkennt Risiken, die gespeicherten Suchen zugeordnet sind, die in IBM Security QRadar Vulnerability Manager erstellt werden.

Veraltete beitragende Tests

Beitragende Tests, die durch einen anderen Test ersetzt werden, werden in der Richtlinienüberwachung ausgeblendet.

Folgende Tests sind in der Richtlinienüberwachung ausgeblendet:

- Assets, die für Schwachstellen anfällig sind
- Assets, die für Schwachstellen von folgenden Services anfällig sind

Diese beitragenden Tests wurden durch andere Tests ersetzt.

Einschränkende Fragen für Tests der tatsächlichen Kommunikation

Die Tests der tatsächlichen Kommunikation für Assets schließen einschränkende Fragen und Parameter ein, die Sie bei der Erstellung eines Richtlinienüberwachungstests auswählen können.

Wenn Sie die Ausschlussbedingung auf einen Test anwenden, gilt die Ausschlussbedingung für den Protokollparameter.

Wenn Sie einen Test beispielsweise als **exclude the following protocols** (Folgende Protokolle ausschließen) konfigurieren, schließt der Test alle zurückgegebenen Assetergebnisse aus, die diejenigen angegebenen Protokolle ausschließen, bei denen es sich nicht um die konfigurierten Protokolle handelt.

In der folgenden Tabelle werden die Parameter für einschränkende Fragen für Tests der tatsächlichen Kommunikation aufgelistet und beschrieben.

Tabelle 15. Parameter für einschränkende Fragen für Tests der tatsächlichen Kommunikation

Testname	Beschreibung
include only the following protocols	Filtert Assets aus dem beitragenden Test, die die angegebenen Protokolle einschließen oder ausschließen. Dieser Test ist nur auswählbar, wenn ein beitragender Assettest zur Frage hinzugefügt wird.
include only the following inbound ports	Filtert Assets aus dem beitragenden Test, die nur die angegebenen Ports einschließen oder diese ausschließen. Dieser Test ist nur auswählbar, wenn ein beitragender Assettest zur Frage hinzugefügt wird.
include only the following inbound applications	Filtert Assets aus der Frage des beitragenden Tests, die nur Anwendungen für eingehende oder abgehende Daten einschließen oder diese ausschließen. Dieser Test filtert Verbindungen, die nur Flussdaten einschließen.
include only if the source inbound and destination outbound bytes have a percentage difference less than 10	Filtert Assets aus der Frage des beitragenden Tests, die auf Kommunikationen mit einem bestimmten Verhältnis von eingehenden zu abgehenden (oder abgehenden zu eingehenden) Bytes basiert. Dieser Test ist zur Erkennung von Hosts hilfreich, die ein typisches Proxy-Verhalten zeigen (Eingang gleich Ausgang).

Tabelle 15. Parameter für einschränkende Fragen für Tests der tatsächlichen Kommunikation (Forts.)

Testname	Beschreibung
include only if the inbound and outbound flow count has a percentage difference less than 10	Filtert Assets aus der Frage des beitragenden Tests, die auf Kommunikationen mit einem bestimmten Verhältnis von eingehenden zu abgehenden (oder abgehenden zu eingehenden) Flüssen basiert. Dieser Test filtert Verbindungen, die Flussdaten einschließen, wenn Flussdaten ausgewählt sind. Für diesen einschränkenden Test sind zwei beitragende Tests erforderlich, die eine Quelle und ein Ziel angeben. Der folgende Test umfasst eine Gruppe von Fragen, mit denen festgestellt werden soll, welche Assets zwischen zwei Punkten eine prozentuale Differenz von mehr als 40% zwischen Eingang und Ausgang aufweisen. Beispiel: • **Beitragender Test** - have accepted communication to the internet. • **Beitragender Test** - and have accepted communication from the internet. • **Einschränkender Test** - and include only if the inbound and outbound flow count has a percentage difference greater than 40.
include only if the time is between start time and end time inclusive	Filtert Kommunikationen im Netz, die innerhalb eines bestimmten Zeitraums stattfanden. Auf diese Weise können nicht richtlinienkonforme Kommunikationen erkannt werden. Wenn die unternehmensinterne Richtlinie beispielsweise FTP-Kommunikationen zwischen 1 und 3 Uhr zulässt, können mit diesen Tests alle Versuche, außerhalb dieses Zeitraums über FTP zu kommunizieren, erkannt werden.
include only if the day of week is between start day and end day inclusive	Filtert Assets aus der Frage des beitragenden Tests auf Basis von Netzkommunikationen, die innerhalb eines bestimmten Zeitraums stattfanden. Auf diese Weise können nicht richtlinienkonforme Kommunikationen erkannt werden.

Tabelle 15. Parameter für einschränkende Fragen für Tests der tatsächlichen Kommunikation (Forts.)

Testname	Beschreibung
include only if susceptible to vulnerabilities that are exploitable.	Filtert Assets aus der Frage eines beitragenden Tests, indem nach bestimmten Schwachstellen gesucht wird, und schränkt Ergebnisse auf Assets mit ausnutzbaren Schwachstellen ein. Dieser einschränkende Test enthält keine konfigurierbaren Parameter, sondern wird in Verbindung mit dem beitragenden Test **are susceptible to one of the following vulnerabilities** (sind für eine der folgenden Schwachstellen anfällig) verwendet. Diese beitragende Regel, die einen Schwachstellenparameter enthält, ist erforderlich.
include only the following networks	Filtert Assets aus der Frage eines beitragenden Tests, die die konfigurierten Netze einschließt oder ausschließt.
include only the following asset building blocks	Filtert Assets aus der Frage eines beitragenden Tests, die den konfigurierten Assetbausteinen zugeordnet oder nicht zugeordnet sind.
include only the following asset saved searches	Filtert Assets aus der Frage eines beitragenden Tests, die der gespeicherten Assetsuche zugeordnet oder nicht zugeordnet sind.
include only the following reference sets	Filtert Assets aus der Frage eines beitragenden Tests, die die konfigurierten Referenzsets einschließt oder ausschließt.
include only the following IP addresses	Filtert Assets, die den konfigurierten IP-Adressen zugeordnet oder nicht zugeordnet sind.
include only if the Microsoft Windows service pack for operating systems is below 0	Filtert Assets, um festzustellen, ob eine Microsoft Windows-Service-Pack-Stufe für ein Betriebssystem unter der in der Unternehmensrichtlinie angegebenen Stufe liegt.
include only if the Microsoft Windows security setting is less than 0	Filtert Assets, um festzustellen, ob eine Microsoft Windows-Sicherheitseinstellung unter der in der Unternehmensrichtlinie angegebenen Stufe liegt.
include only if the Microsoft Windows service equals status	Filtert Assets, um festzustellen, ob ein Microsoft Windows-Dienst einen bestimmten Status hat (unknown, boot, kernel, auto, demand, disabled).
include only if the Microsoft Windows setting equals regular expressions	Filtert Assets, um festzustellen, ob es sich bei einer Microsoft Windows-Einstellung um den angegebenen regulären Ausdruck handelt.

Beitragende Fragen für Tests der möglichen Kommunikation

Die Tests der möglichen Kommunikation für Assets schließen beitragende Fragen und Parameter ein, die Sie bei der Erstellung eines Richtlinienüberwachungstests auswählen können.

In der folgenden Tabelle werden die Parameter für beitragende Fragen für Tests der möglichen Kommunikation aufgelistet und beschrieben.

Tabelle 16. Parameter für beitragende Fragen für Tests der möglichen Kommunikation

Testname	Beschreibung
have accepted communication to any destination	Erkennt Assets mit möglichen Kommunikationen mit einer angegebenen Quelle oder einem angegebenen Ziel. Konfigurieren Sie den Test beispielsweise wie folgt, um festzustellen, ob ein kritischer Server möglicherweise Kommunikationen von irgendeiner Quelle empfangen kann: have accepted communication from any source. Anschließend können Sie mithilfe eines einschränkenden Tests abfragen, ob der kritische Server Kommunikationen an Port 21 empfangen hat. Auf diese Weise können nicht richtlinienkonforme Kommunikationen für den kritischen Server erkannt werden.
have accepted communication to destination networks	Erkennt Assets mit möglichen Kommunikationen mit dem konfigurierten Netz. Mit diesem Test können Sie einen Start- oder Endpunkt für eine Frage definieren. Konfigurieren Sie den Test beispielsweise wie folgt, um die Assets zu identifizieren, denen es möglich ist, mit der Demilitarized Zone (DMZ) zu kommunizieren: have accepted communication from source <networks> Mit diesem Test können Sie nicht richtlinienkonforme Kommunikationen erkennen.
have accepted communication to destination IP addresses	Erkennt Assets mit möglichen Kommunikationen mit der konfigurierten IP-Adresse. Bei diesem Test können Sie eine einzelne IP-Adresse als Fokus für mögliche Kommunikationen angeben. Konfigurieren Sie den Test beispielsweise wie folgt, um alle Assets zu identifizieren, die mit einem bestimmten Compliance-Server kommunizieren können: have accepted communications to destination <compliance server IP address>

Tabelle 16. Parameter für beitragende Fragen für Tests der möglichen Kommunikation (Forts.)

Testname	Beschreibung
have accepted communication to destination asset building blocks	Erkennt Assets mit möglichen Kommunikationen mit dem konfigurierten Assetbaustein. Bei diesem Test können Sie Bausteine, die im QRadar-Regelassistenten definiert sind, in einer Abfrage wiederverwenden. Konfigurieren Sie den Test beispielsweise wie folgt, um alle Assets zu identifizieren, die mit geschützten Assets kommunizieren können: have accepted communications to destination <BB:HostDefinition:Protected Assets> Weitere Informationen zu Regeln und Bausteinen finden Sie im QRadar-Verwaltungshandbuch.
have accepted communication to destination asset saved searches	Erkennt Assets mit akzeptierten Kommunikationen mit den Assets, die von der gespeicherten Suche, die Sie angeben, zurückgegeben werden. Um diesen Test verwenden zu können, muss eine gespeicherte Assetsuche vorhanden sein. Informationen zum Erstellen und Speichern einer Assetsuche finden Sie im *IBM Security QRadar SIEM Users Guide.*
have accepted communication to destination reference sets	Erkennt, ob Quellen- oder Zielkommunikationen mit Referenzsets möglich sind.
have accepted communication to the Internet	Erkennt, ob Quellen- oder Zielkommunikationen mit dem Internet möglich sind. Geben Sie den Parameter **to** oder **from** an, sodass entweder der Kommunikationsdatenverkehr in das Internet oder aus dem Internet betrachtet wird.
are susceptible to one of the following vulnerabilities	Erkennt bestimmte mögliche Schwachstellen. Wenn Sie Schwachstellen eines bestimmten Typs erkennen möchten, verwenden Sie den Test **are susceptible to vulnerabilities with one of the following classifications**. Geben Sie die Schwachstellen an, auf die dieser Test angewendet werden soll. Sie können anhand der OSVDB-ID, CVE-ID, Bugtraq-ID oder des Titels nach Schwachstellen suchen.

Tabelle 16. Parameter für beitragende Fragen für Tests der möglichen Kommunikation (Forts.)

Testname	Beschreibung
are susceptible to vulnerabilities with one of the following classifications	Eine Schwachstelle kann einer oder mehreren Schwachstellenklassifikationen zugeordnet werden. Dieser Test filtert alle Assets, die mögliche Schwachstellen mit einer CVSS-Bewertung (Common Vulnerability Scoring System) wie angegeben aufweisen. Konfigurieren Sie den Klassifikationsparameter, um die Schwachstellenklassifikationen anzugeben, die dieser Test anwenden soll.
are susceptible to vulnerabilities with CVSS score greater than 5	Ein CVSS-Wert (Common Vulnerability Scoring System) ist ein Branchenstandard für die Bewertung des Schweregrads von möglichen Schwachstellen. CVSS setzt sich aus drei Messwertgruppen zusammen: Base Score, Temporal Score und Environmental Score. Anhand dieser Messwerte kann CVSS grundlegende Merkmale einer Schwachstelle definieren und kommunizieren. Dieser Test filtert Assets im Netz, die den konfigurierten CVSS-Wert einschließen.
are susceptible to vulnerabilities disclosed after specified date	Filtert Assets im Netz, die eine mögliche Schwachstelle aufweisen, die nach, vor oder an dem konfigurierten Datum offengelegt wurde.
are susceptible to vulnerabilities on one of the following ports	Filtert Assets im Netz, die eine mögliche Schwachstelle aufweisen, die den konfigurierten Ports zugeordnet ist. Konfigurieren Sie den Portparameter, um Assets, die mögliche Schwachstellen aufweisen, auf Basis der angegebenen Portnummer zu identifizieren.
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries	Erkennt Assets im Netz, die eine Schwachstelle aufweisen, die auf Basis einer oder mehrerer Texteingaben mit dem Assetnamen, dem Hersteller, der Version oder dem Service übereinstimmt. Konfigurieren Sie den Parameter **text entries** (Texteingaben), um den Assetnamen, den Hersteller, die Version oder den Service anzugeben, die dieser Test berücksichtigen soll.

Tabelle 16. Parameter für beitragende Fragen für Tests der möglichen Kommunikation (Forts.)

Testname	Beschreibung
are susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions	Erkennt Assets im Netz, die eine Schwachstelle aufweisen, die auf Basis eines oder mehrerer regulärer Ausdrücke mit dem Assetnamen, dem Hersteller, der Version oder dem Service übereinstimmt. Konfigurieren Sie den Parameter **regular expressions** (Reguläre Ausdrücke), um den Assetnamen, den Hersteller, die Version oder den Service anzugeben, die dieser Test berücksichtigen soll.
are susceptible to vulnerabilities contained in vulnerability saved searches	Erkennt Risiken, die gespeicherten Suchen zugeordnet sind, die in IBM Security QRadar Vulnerability Manager erstellt werden.

Veraltete beitragende Tests

Wenn ein Test durch einen anderen ersetzt wird, wird er in der Richtlinienüberwachung ausgeblendet.

Folgende Tests sind in der Richtlinienüberwachung ausgeblendet:

- Assets, die für Schwachstellen von folgenden Herstellern anfällig sind
- Assets, die für Schwachstellen von folgenden Services anfällig sind

Diese beitragenden Tests wurden durch andere Tests ersetzt.

Parameter für einschränkende Fragen für Tests der möglichen Kommunikation

Tests der möglichen Kommunikation für Assets schließen Parameter für einschränkende Fragen ein.

In der folgenden Tabelle werden die Parameter für einschränkende Fragen für Tests der möglichen Kommunikation aufgelistet und beschrieben.

Tabelle 17. Einschränkende Tests für Tests der möglichen Kommunikation

Testname	Beschreibung
include only the following protocols	Filtert Assets, die möglicherweise mit den konfigurierten Protokollen kommuniziert oder nicht kommuniziert haben, in Verbindung mit den anderen Tests, die zu dieser Frage hinzugefügt wurden.
include only the following inbound ports	Filtert Assets, die möglicherweise mit den konfigurierten Ports kommuniziert oder nicht kommuniziert haben, in Verbindung mit den anderen Tests, die zu dieser Frage hinzugefügt wurden.

Tabelle 17. Einschränkende Tests für Tests der möglichen Kommunikation (Forts.)

Testname	Beschreibung
include only ports other than the following inbound ports	Filtert Assets aus der Frage eines beitragenden Tests, die möglicherweise mit anderen als den konfigurierten Ports kommuniziert oder nicht kommuniziert haben, in Verbindung mit den anderen Tests, die zu dieser Frage hinzugefügt wurden.
include only if susceptible to vulnerabilities that are exploitable.	Filtert Assets aus der Frage eines beitragenden Tests, indem nach möglichen bestimmten Schwachstellen gesucht wird, und schränkt Ergebnisse auf Assets mit ausnutzbaren Schwachstellen ein. Dieser einschränkende Test enthält keine konfigurierbaren Parameter, sondern wird in Verbindung mit dem beitragenden Test **are susceptible to one of the following vulnerabilities** (sind für eine der folgenden Schwachstellen anfällig) verwendet. Diese beitragende Regel, die einen Schwachstellenparameter enthält, ist erforderlich.
include only the following networks	Filtert Assets aus der Frage eines beitragenden Tests, die nur die konfigurierten Netze einschließen oder diese ausschließen.
include only the following asset building blocks	Filtert Assets aus der Frage eines beitragenden Tests, die nur die konfigurierten Assetbausteine einschließen oder diese ausschließen.
include only the following asset saved searches	Filtert Assets aus der Frage eines beitragenden Tests, die nur die zugeordnete gespeicherte Assetsuche einschließen oder diese ausschließen.
include only the following reference sets	Filtert Assets aus der Frage eines beitragenden Tests, die nur die konfigurierten Referenzsets einschließen oder diese ausschließen.
include only the following IP addresses	Filtert Assets aus der Frage eines beitragenden Tests, die nur die konfigurierten IP-Adressen einschließen oder diese ausschließen.
include only if the Microsoft Windows service pack for operating systems is below 0	Filtert Assets, um festzustellen, ob eine Microsoft Windows-Service-Pack-Stufe für ein Betriebssystem unter der in der Unternehmensrichtlinie angegebenen Stufe liegt.
include only if the Microsoft Windows security setting is less than 0	Filtert Assets, um festzustellen, ob eine Microsoft Windows-Sicherheitseinstellung unter der in der Unternehmensrichtlinie angegebenen Stufe liegt.
include only if the Microsoft Windows service equals status	Filtert Assets, um festzustellen, ob ein Microsoft Windows-Dienst einen bestimmten Status hat (unknown, boot, kernel, auto, demand, disabled).

Tabelle 17. Einschränkende Tests für Tests der möglichen Kommunikation (Forts.)

Testname	Beschreibung
include only if the Microsoft Windows setting equals regular expressions	Filtert Assets, um festzustellen, ob es sich bei einer Microsoft Windows-Einstellung um den angegebenen regulären Ausdruck handelt.

Einheit/Regeln-Testfragen

Einheit/Regeln-Testfragen werden verwendet, um Regeln in einer Einheit zu identifizieren, die gegen eine definierte Richtlinie verstoßen, was ein Risiko in die Umgebung einführen kann.

Die Einheit/Regeln-Testfragen werden in der folgenden Tabelle beschrieben.

Tabelle 18. Einheit/Regeln-Tests

Testname	Beschreibung
allow connections to the following networks	Filtert Einheitenregeln und Verbindungen zu oder von den konfigurierten Netzen. Beispiel: Wenn Sie den Test konfigurieren, um Kommunikationen mit einem Netz zu ermöglichen, filtert der Test alle Regeln und Verbindungen, die Verbindungen zu dem konfigurierten Netz ermöglichen.
allow connections to the following IP addresses	Filtert Einheitenregeln und Verbindungen zu oder von den konfigurierten IP-Adressen. Beispiel: Wenn Sie den Test konfigurieren, um Kommunikationen mit einer IP-Adresse zu ermöglichen, filtert der Test alle Regeln und Verbindungen, die Verbindungen zu der konfigurierten IP-Adresse ermöglichen.
allow connections to the following asset building blocks	Filtert Einheitenregeln und Verbindungen zu oder von den konfigurierten Assetbausteinen.
allow connections to the following reference sets	Filtert Einheitenregeln und Verbindungen zu oder von den konfigurierten Referenzsets.
allow connections using the following destination ports and protocols	Filtert Einheitenregeln und Verbindungen zu oder von den konfigurierten Ports und Protokollen.
allow connections using the following protocols	Filtert Einheitenregeln und Verbindungen zu oder von den konfigurierten Protokollen.
allow connections to the Internet	Filtert Einheitenregeln und Verbindungen mit dem Internet.
?ßare one of the following devices	Filtert aus allen Netzeinheiten die konfigurierten Einheiten heraus. Dieser Test kann Filterungen auf Basis von Einheiten durchführen, die in der konfigurierten Liste enthalten oder nicht enthalten sind.
are one of the following reference sets	Filtert Einheitenregeln auf Basis der Referenzsets, die Sie angeben.

Tabelle 18. Einheit/Regeln-Tests (Forts.)

Testname	**Beschreibung**
are one of the following networks	Filtert Einheitenregeln auf Basis der Netze, die Sie angeben.
are using one of the following adapters	Filtert Einheitenregeln auf Basis der Adapter, die Sie angeben.

Kapitel 7. Verbindungen untersuchen

Eine Verbindung ist eine Aufzeichnung einer Kommunikation, einschließlich verweigerter Kommunikationen, zwischen zwei eindeutigen IP-Adressen über einen bestimmten Zielport, so wie für ein bestimmtes Zeitintervall erkannt.

Wenn zwei IP-Adressen viele Male in einem bestimmten Zeitintervall an einem Port miteinander kommunizieren, wird das nur als eine einzige Kommunikation aufgezeichnet, aber es werden alle übertragenen Bytes und die Gesamtzahl der Datenflüsse für die Verbindung erfasst. Am Ende des Intervalls werden die Verbindungsinformationen für das Intervall summiert und in der Datenbank gespeichert.

Über 'Connections' (Verbindungen) können Sie Netzeinheitenverbindungen überwachen und untersuchen oder erweiterte Suchen durchführen. Folgende Aktionen sind möglich:

- Verbindungen suchen
- Untergruppe von Verbindungen suchen
- Suchergebnisse als falschen Alarm markieren, um Fehlalarmereignisse aus erstellten Angriffen zu verhindern
- Verbindungsinformationen gruppiert nach verschiedenen Optionen anzeigen
- Verbindungen in XML- oder CSV-Format exportieren
- Verbindungen im Netz als interaktive Grafik anzeigen

Verbindungen anzeigen

Sie können Verbindungsinformationen anzeigen, die nach verschiedenen Optionen gruppiert sind.

Informationen zu diesem Vorgang

Wenn eine gespeicherte Suche die Standardeinstellung ist, werden die Ergebnisse für diese gespeicherte Suche angezeigt. Das Fenster 'Verbindungen' zeigt standardmäßig die folgenden Diagramme an:

- Datensätze, die mit Zeitdiagrammen abgeglichen wurden, stellen Zeitreiheninformationen bereit, in denen die Anzahl der Verbindungen auf Basis der Zeit angezeigt werden.
- Verbindungsdiagramme, die eine grafische Darstellung der abgerufenen Verbindungen bereitstellen.

Im Fenster 'Verbindungen' werden die folgenden Informationen angezeigt:

Tabelle 19. Fenster 'Verbindungen' - Standardeinstellung

Parameter	Beschreibung
Aktuelle Filter	Am Anfang der Tabelle werden die Details des Filters angezeigt, der für das Suchergebnis angewendet wird. Um diese Filterwerte zu löschen, klicken Sie auf 'Filter löschen'. Dieser Parameter wird nur nach dem Anwenden eines Filters angezeigt.

Tabelle 19. Fenster 'Verbindungen' - Standardeinstellung (Forts.)

Parameter	Beschreibung
Ansicht	Sie können den Zeitbereich für das Filtern angeben. Wählen Sie in der Dropdown-Liste den Zeitbereich aus, der gefiltert werden soll.
Aktuelle Statistik	Die aktuelle Statistik umfasst Folgendes: • Gesamtergebnisse - Die Gesamtzahl der Ergebnisse, die mit Ihren Suchkriterien übereinstimmen. • Durchsuchte Datendateien - Die Gesamtzahl der Datendateien, die innerhalb der angegebenen Zeitdauer durchsucht wurden. • Durchsuchte komprimierte Datendateien - Die Gesamtzahl der komprimierten Datendateien, die innerhalb der angegebenen Zeitdauer durchsucht wurden. • Anzahl indexierter Dateien - Die Gesamtzahl der Indexdateien, die innerhalb der angegebenen Zeitdauer durchsucht wurden. • Dauer - Die Dauer der Suche. • Bei der aktuellen Statistik handelt es sich um ein hilfreiches Fehlerbehebungstool. Wenn Sie sich an den Kundendienst wenden, um einen Fehler zu beheben, werden Sie möglicherweise nach den aktuellen statistischen Informationen gefragt. Klicken Sie auf den Pfeil neben 'Aktuelle Statistik', um die Statistik anzuzeigen oder auszublenden.
Diagramme	Die angezeigten Diagramme stellen die Datensätze dar, die mit dem Zeitintervall und/oder der Option zum Gruppieren übereinstimmen. Klicken Sie auf 'Diagramme ausblenden', wenn Sie das Diagramm aus Ihrer Anzeige entfernen möchten. Wenn Sie den Mozilla Firefox-Browser verwenden und die Browsererweiterung 'Adblock Plus' installiert ist, werden die Diagramme nicht angezeigt. Zur Anzeige der Diagramme müssen Sie die Browsererweiterung 'Adblock Plus' entfernen. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Browser.
Zeit des letzten Pakets	Bei der 'Zeit des letzten Pakets' handelt es sich um das Datum und die Uhrzeit des letzten verarbeiteten Pakets für diese Verbindung.
Quellentyp	Dies ist der Quellentyp für diese Verbindung. Mögliche Optionen sind 'Host' oder 'Fern'.

Tabelle 19. Fenster 'Verbindungen' - Standardeinstellung (Forts.)

Parameter	Beschreibung
Quelle	Die Quelle dieser Verbindung. Folgende Optionen sind verfügbar: • IP-Adresse - Die IP-Adresse für die Quelle dieser Verbindung. Die IP-Adresse wird angezeigt, wenn es sich bei dem Quellentyp um 'Host' handelt. • Country (Land) - Das Quellenland (mit dem Flag für das Land) für diese Verbindung. Das Flag für das Land wird nur angezeigt, wenn der Quellentyp fern ist.
Zieltyp	Der Zieltyp für diese Verbindung. Mögliche Optionen sind 'Host' oder 'Fern'.
Ziel	Die IP-Adresse für den Hosttyp einschließlich des Flags für das Land. Folgende Optionen sind verfügbar: • IP-Adresse - Die IP-Adresse für das Ziel dieser Verbindung. Die IP-Adresse wird angezeigt, wenn es sich bei dem Zieltyp um 'Host' handelt. • Country (Land) - Das Zielland (mit dem Flag für das Land) für diese Verbindung. Das Flag für das Land wird nur angezeigt, wenn der Zieltyp fern ist.
Protokoll	Das Protokoll, das für diese Verbindung verwendet wird.
Zielport	Der Zielport für diese Verbindung.
Flussanwendung	Die Flussanwendung, die die Verbindung generiert hat.
Flussquelle	Die Quelle der Datenflüsse, die dieser Verbindung zugeordnet sind. Dieser Parameter gilt nur für akzeptierte Verbindungen.
Flusszähler	Die Gesamtzahl der Datenflüsse, die dieser Verbindung zugeordnet sind.
Flussquellenbytes	Die Gesamtzahl der Flussquellenbytes, die dieser Verbindung zugeordnet sind.
Flusszielbytes	Die Gesamtzahl der Zielbytes, die dieser Verbindung zugeordnet sind.
Protokollquelle	Die Quelle der Ereignisse, die zu dieser Verbindung beigetragen haben.
Ereigniszähler	Die Gesamtzahl der Ereignisse, die für die Verbindung ermittelt wurden.
Verbindungstyp	Der Typ der Verbindung. Folgende Optionen sind verfügbar: • Zulassen - Ermöglicht die Verbindung. • Verweigern - Weist die Verbindung zurück.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Wählen Sie in der Liste **Ansicht** den Zeitrahmen aus, der angezeigt werden soll.

Verbindungsdaten als Grafiken anzeigen

Sie können Verbindungsdaten mithilfe verschiedener Grafikoptionen anzeigen. Daten können standardmäßig über die Optionen 'Im Lauf der Zeit abgeglichene Datensätze' und 'Verbindungsgrafik' angezeigt werden.

'Im Lauf der Zeit abgeglichene Datensätze' ist eine Option, mit der die Anzahl der Verbindungen abhängig von der Zeit angezeigt werden können.

Eine Verbindungsgrafik stellt eine visuelle Darstellung der abgerufenen Verbindung bereit. Wenn Sie Verbindungen mithilfe der Verbindungsgrafik weiter untersuchen möchten, lesen Sie den Abschnitt Verbindungsgrafik verwenden.

Als Grafikoptionen für gruppierte Verbindungen sind Tabellen-, Balken- und Kreisdiagramme verfügbar. Weitere Informationen zur Suche nach Verbindungen finden Sie im Abschnitt Nach Verbindungen suchen.

Wenn Sie im Mozilla Firefox-Web-Browser die Browsererweiterung Adblock Plus verwenden, werden die Diagramme möglicherweise nicht korrekt angezeigt. Damit die Diagramme angezeigt werden, müssen Sie die Browsererweiterung Adblock Plus entfernen. Weitere Informationen zum Entfernen von Add-ons finden Sie in der Web-Browser-Dokumentation.

Zeitreihengrafik verwenden

Zeitreihendiagramme sind grafische Darstellungen Ihrer Verbindungen im Zeitablauf; die angezeigten Werte für hohe und geringe Auslastung zeigen eine hohe und niedrige Verbindungsaktivität an.

Vorbereitende Schritte

Wenn Sie eine Suche zuvor als Standardsuche gespeichert haben, werden die Ergebnisse für diese gespeicherte Suche auf der Seite 'Verbindungen' angezeigt. Wenn Sie für diese Suche Optionen des Typs 'Gruppieren nach' im Fenster 'Erweiterte Ansichtsdefinitionen' ausgewählt haben, ist das Zeitreihendiagramm nicht verfügbar. Sie müssen die Suchkriterien löschen, bevor Sie den Vorgang fortsetzen.

Informationen zu diesem Vorgang

Zeitreihendiagramme sind bei der kurzfristigen und langfristigen Trendermittlung von Daten hilfreich. Mithilfe von Zeitreihendiagrammen können Sie aus verschiedenen Ansichten und Perspektiven auf Verbindungen zugreifen, zu diesen navigieren und sie überprüfen.

In der folgenden Tabelle werden Funktionen bereitgestellt, mit denen Sie Zeitreihendiagramme anzeigen können.

Tabelle 20. Funktionen des Zeitreihendiagramms

Gehen Sie gegebenenfalls wie folgt vor:	**Führen Sie dann folgende Schritte aus:**
Verbindungen ausführlicher anzeigen	Durch das Vergrößern der Daten im Zeitreihendiagramm können Sie kleinere Zeitsegmente der Verbindungen untersuchen. Sie können das Zeitreihendiagramm mit einer der folgenden Optionen vergrößern: • Drücken Sie die Umschalttaste und klicken Sie im Diagramm auf die Zeit, die Sie untersuchen möchten. • Halten Sie beim Klicken die Steuer- und Umschalttaste gedrückt und ziehen Sie den Mauszeiger auf den Zeitbereich, den Sie anzeigen möchten. • Bewegen Sie den Mauszeiger auf das Diagramm und drücken Sie den Aufwärtspfeil auf Ihrer Tastatur. • Bewegen Sie den Mauszeiger auf das Diagramm und vergrößern Sie den Bereich mithilfe des Mausrads (drehen Sie das Mausrad nach oben). Nach dem Vergrößern eines Zeitreihendiagramms wird das Diagramm aktualisiert und zeigt ein kleineres Zeitsegment an.
Größeren Zeitraum für Verbindungen anzeigen	Durch das Einfügen zusätzlicher Zeitbereiche in das Zeitreihendiagramm können Sie größere Zeitsegmente untersuchen oder zum maximalen Zeitbereich zurückkehren. Sie können einen Zeitbereich mit einer der folgenden Optionen anzeigen: • Klicken Sie in der linken oberen Ecke des Diagramms aus 'Max' oder drücken Sie die Taste für die erste Eingabeposition, um zum maximalen Zeitbereich zurückzukehren. • Bewegen Sie den Mauszeiger auf das Diagramm und drücken Sie den Abwärtspfeil auf Ihrer Tastatur. • Bewegen Sie den Mauszeiger auf das Kurvendiagramm und verkleinern Sie den Bereich mithilfe des Mausrads (drehen Sie das Mausrad nach unten).

Tabelle 20. Funktionen des Zeitreihendiagramms (Forts.)

Gehen Sie gegebenenfalls wie folgt vor:	Führen Sie dann folgende Schritte aus:
Diagramm durchsuchen	So zeigen Sie das Diagramm an, um Informationen an jedem Datenpunkt zu ermitteln: • Klicken und Ziehen Sie das Diagramm mit der Maus, um die Zeitachse zu durchsuchen. • Drücken Sie die Taste zum Zurückblättern, um die Zeitachse eine vollständige Seite nach links zu verschieben. • Drücken Sie die Linkspfeiltaste, um die Zeitachse eine halbe Seite nach links zu verschieben. • Drücken Sie die Taste zum Vorblättern, um die Zeitachse eine vollständige Seite nach rechts zu verschieben. • Drücken Sie die Rechtspfeiltaste, um die Zeitachse eine halbe Seite nach rechts zu verschieben.

Vorgehensweise

Vorgehensweise

1. Klicken Sie auf die Registerkarte 'Risks' (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Klicken Sie im Fenster 'Diagramme' auf das Symbol **Konfigurieren**.
4. Wählen Sie in der Dropdown-Liste **Diagrammtyp** die Option 'Zeitreihen' aus.
5. Mit den interaktiven Diagrammen zu Zeitreihen können Sie durch eine Zeitachse navigieren, um Verbindungen zu untersuchen.
6. Wenn Sie die Informationen im Diagramm aktualisieren möchten, klicken Sie auf 'Details aktualisieren'.

Netzverbindungen als Verbindungsgrafik anzeigen

Die Verbindungsgrafik stellt eine visuelle Darstellung der Verbindungen in einem Netz bereit.

Die im Fenster 'Verbindungen' angezeigte Grafik ist nicht interaktiv. Wenn Sie auf die Grafik klicken, wird das Fenster 'Radial Data Viewer' angezeigt. Im Fenster 'Radial Data Viewer' können Sie die Grafik nach Bedarf manipulieren.

Standardmäßig zeigt die Grafik die Netzverbindungen wie folgt an:

- Es werden nur zulässige Verbindungen angezeigt.
- Alle lokalen IP-Adressen werden ausgeblendet, um nur Endknotennetze anzuzeigen.
- Alle Länderknoten werden bis auf einen Knoten namens 'Remote Countries' (Ferne Länder) ausgeblendet.
- Alle fernen Netzknoten werden bis auf einen Knoten namens 'Remote Networks' (Ferne Netze) ausgeblendet.
- In einer Piktogrammansicht der Grafik wird ein Teil der Hauptgrafik als Vorschau angezeigt. Dies ist bei großen Grafiken hilfreich.

Der Radial Data Viewer enthält mehrere Menüoptionen, einschließlich:

Tabelle 21. Menüoptionen im Radial Data Viewer

Menüoption	**Beschreibung**
Verbindungstyp	Standardmäßig zeigt die sternförmige Grafik akzeptierte Verbindungen an. Wenn verweigerte Verbindungen angezeigt werden sollen, wählen Sie 'Verweigern' in der Dropdown-Liste **Verbindungstyp** aus.
Rückgängig machen	Die letzte Knotenerweiterung wird wieder ausgeblendet. Um mehrere Erweiterungen auszublenden, müssen Sie für jede Erweiterung auf diese Schaltfläche klicken.
Herunterladen	Klicken Sie auf **Herunterladen**, um die aktuelle Topologie als JPEG-Bilddatei oder Visio-Grafikdatei (VDX) zu speichern. Um die aktuelle Topologie herunterladen und als Visio-Grafikdatei (VDX) speichern zu können, ist mindestens die Softwareversion Microsoft Visio Standard 2010 erforderlich.

Die folgende Tabelle stellt zusätzliche Funktionen zum Anzeigen von Verbindungen bereit, einschließlich:

Tabelle 22. Funktionen im Radial Data Viewer

Ziel	**Vorgehensweise**
Vergrößern oder verkleinern	Verwenden Sie zum Ändern der Skalierung den Schieberegler rechts oben in der Grafik.
Knoten in der Grafik verteilen, um zusätzliche Details anzuzeigen	Ziehen Sie den Knoten an die gewünschte Position, um Knoten in der Grafik zu verteilen.
Netzknoten erweitern	Doppelklicken Sie auf den Knoten, um Assets für den Knoten zu erweitern und anzuzeigen. Der Knoten wird erweitert, um auch die Knoten einzublenden, mit denen der Knoten kommuniziert hat. Diese Erweiterung ist standardmäßig auf die ersten 100 Assets des Netzes begrenzt.
Zusätzliche Details zu einer Verbindung anzeigen	Setzen Sie den Mauszeiger auf die Verbindungslinie, um zusätzliche Details anzuzeigen. Wenn es sich um eine Verbindung zwischen einem Netzknoten und einem fernen Netz oder fernen Land handelt, klicken Sie mit der rechten Maustaste, um folgende Menüs für **Source** (Quelle) und **View Flows** (Flüsse anzeigen) anzuzeigen: Wenn es sich um eine Verbindung zwischen IP-Adressen handelt, werden die Quellen-, Ziel- und Portinformationen angezeigt, sobald Sie auf die Verbindungslinie klicken.

Tabelle 22. Funktionen im Radial Data Viewer (Forts.)

Ziel	Vorgehensweise
Datenvolumen auf der Verbindung bestimmten	Die Dicke der Linie in der Grafik weist auf das Datenvolumen auf der Verbindung hin. Je dicker die Linie, desto größer das Datenvolumen. Diese Information basiert auf der Menge der übertragenen Bytes.
Verbindungspfad hervorheben	Setzen Sie den Mauszeiger auf die Verbindungslinie. Wenn die Verbindung zulässig ist, wird der Pfad grün hervorgehoben. Wurde die Verbindung verweigert, wird der Pfad rot hervorgehoben.
Verbindungspfad für einen einzelnen Knoten bestimmen	Setzen Sie den Mauszeiger auf den Knoten. Wenn der Knoten zulässig ist, werden der Pfad zum Knoten und der Knoten grün hervorgehoben. Wurde der Knoten verweigert, werden der Pfad zum Knoten und der Knoten rot hervorgehoben.
Grafikansicht ändern	Verschieben Sie mithilfe des Vorschaupiktogramms das Piktogramm zu dem Teil der Grafik, der angezeigt werden soll.

Kreis-, Balken- und Tabellendiagramme verwenden

Sie können Verbindungsdaten mithilfe von Kreis-, Balken- oder Tabellendiagrammen anzeigen.

Informationen zu diesem Vorgang

Die Optionen für die Kreis-, Balken- und Tabellendiagramme werden nur angezeigt, wenn die Suche Optionen vom Typ 'Gruppieren nach' enthält, die unter 'Erweiterte Ansichtsdefinition' ausgewählt wurden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.

   Anmerkung: Die standardmäßig gespeicherten Suchergebnisse werden angezeigt.
3. Führen Sie eine Suchoperation durch.
4. Klicken Sie im Fenster 'Diagramme' auf das Symbol **Konfiguration**.
5. Konfigurieren Sie die Parameter:

Option	Beschreibung
Wert zu Diagramm	In der Liste **Wert zu Diagramm** können Sie den Objekttyp auswählen, mit dem Sie das Diagramm grafisch darstellen möchten. Die Optionen umfassen alle normalisierten und angepassten Flussparameter, die in Ihren Suchparametern enthalten sind.

Option	Beschreibung
Diagrammtyp	Mit der Option **Diagrammtyp** können Sie den Diagrammtyp auswählen, der angezeigt werden soll. Es gibt folgende Möglichkeiten: • **Tabelle** - Zeigt die Daten in einer Tabelle an. • **Balken** - Zeigt die Daten in einem Balkendiagramm an. • **Kreis** - Zeigt die Daten in einem Kreisdiagramm an.

6. Klicken Sie auf **Speichern**.

   Die Daten werden nur dann automatisch aktualisiert, wenn Sie Ihre Suchkriterien mit der Funktion zur automatischen Anzeige von Details anzeigen.
7. Zum Aktualisieren der Daten klicken Sie auf **Details aktualisieren**.

Verbindungen suchen

Sie können Verbindung mithilfe bestimmter Kriterien suchen und Verbindungen anzeigen, die mit den Suchkriterien in einer Ergebnisliste übereinstimmen. Sie können eine neue Suche erstellen oder eine zuvor gespeicherte Gruppe mit Suchkriterien laden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.

   Die standardmäßig gespeicherten Suchergebnisse werden ggf. angezeigt.
3. Wählen Sie in der Liste **Suchen** die Option **Neue Suche** aus.
4. Wenn Sie eine zuvor gespeicherte Suche laden möchten, verwenden Sie eine der folgenden Optionen:
   a. Wählen Sie in der Liste **Gruppe** die Gruppe aus, der die gespeicherte zugeordnet ist.
   b. Wählen Sie in der Liste **Verfügbare gespeicherte Suchvorgänge** die gespeicherte Suche aus, die Sie laden möchten.
   c. Geben Sie im Feld **Gespeicherten Suchvorgang eingeben oder aus Liste auswählen** den Namen der Suche ein, die geladen werden soll. Wählen Sie in der Liste 'Verfügbare gespeicherte Suchvorgänge' die gespeicherte Suche aus, die geladen werden soll.
   d. Klicken Sie auf **Laden**.
   e. Wählen Sie im Fenster **Suche bearbeiten** die Optionen aus, die Sie für diese Suche verwenden möchten.

Option	Beschreibung
In meine Schnellsuche aufnehmen	Diese Suche wird in die Elemente der Schnellsuche integriert.
In mein Dashboard aufnehmen	Die Daten Ihrer gespeicherten Suche werden in Ihr Dashboard integriert. Dieser Parameter ist nur verfügbar, wenn es sich um eine gruppierte Suche handelt.
Als Standardwert definieren	Diese Suche wird als Standardsuche festgelegt.

Option	Beschreibung
Freigeben für jeden	Sie können diese Suchanforderungen gemeinsam mit allen anderen QRadar Risk Manager-Benutzern verwenden.

5. Wählen Sie im Fenster 'Zeitraum' eine Option für den Zeitraum aus, den Sie für diese Suche erfassen möchten.

Option	Beschreibung
Aktuelle	Geben Sie mit dieser Liste den Zeitraum an, der gefiltert werden soll.
Bestimmtes Intervall	Geben Sie über den Kalender das Datum und den Zeitraum an, die gefiltert werden sollen.

6. Wenn Sie die Konfiguration der Suche abgeschlossen haben und die Ergebnisse anzeigen möchten, klicken Sie auf 'Suchen'.
7. Definieren Sie im Fenster 'Suchparameter' Ihre speziellen Suchkriterien:
   a. Wählen Sie mithilfe der ersten Liste ein Attribut aus, nach dem Sie suchen möchten. Beispiel: Verbindungstyp, Quellennetz oder Richtung.
   b. Wählen Sie mithilfe der zweiten Liste den Änderungswert, den Sie für die Suche verwenden möchten. Die Liste der angezeigten Änderungswerte ist von dem in der ersten Liste ausgewählten Attribut abhängig.
   c. Geben Sie im Textfeld bestimmte Informationen ein, die mit Ihrer Suche zusammenhängen.
   d. Klicken Sie auf **Filter hinzufügen**.
   e. Wiederholen Sie die Schritte a bis e für jeden Filter, der den Suchkriterien hinzugefügt werden soll.
   f. Wenn Sie die Konfiguration der Suche abgeschlossen haben und die Ergebnisse anzeigen möchten, klicken Sie auf **Suchen**. Fahren Sie andernfalls mit dem nächsten Schritt fort.
8. Wenn die Suchergebnisse nach Abschluss der Suche automatisch gespeichert werden sollen, wählen Sie das Kontrollkästchen 'Ergebnisse nach Abschluss des Suchvorgangs speichern' aus und geben einen Namen an.
9. Wenn Sie die Konfiguration der Suche abgeschlossen haben und die Ergebnisse anzeigen möchten, klicken Sie auf **Suchen**. Fahren Sie andernfalls mit dem nächsten Schritt fort.
10. Definieren Sie im Fenster 'Spaltendefinition' die Spalten und die Spaltenanordnung für die Anzeige der Ergebnisse:
    a. Wählen Sie in der Liste **Anzeige** die Anzeige aus, die Sie diesem Suchvorgang zuordnen möchten.
    b. Klicken Sie auf den Pfeil neben **Erweiterte Ansichtsdefinition**, um die erweiterten Suchparameter anzuzeigen. Klicken Sie erneut auf den Pfeil, um die Parameter auszublenden.
11. Klicken Sie auf **Suchen**.

Suchkriterien speichern

Durch die Angabe von Suchkriterien können Sie eine Suche erstellen und Sie können die Suche für die zukünftige Verwendung speichern.

Informationen zu diesem Vorgang

Sie können die Spalten anpassen, die in den Suchergebnissen angezeigt werden. Diese Optionen sind im Abschnitt 'Spaltendefinition' verfügbar und werden als 'Erweiterte Ansichtsdefinition' bezeichnet.

Tabelle 23. Option 'Erweitere Ansichtsdefinition'

Parameter	**Beschreibung**
Spalte eingeben oder aus Liste auswählen	Die Spalten in der Liste 'Verfügbare Spalten' werden gefiltert. Geben Sie den Namen der Spalte ein, die Sie suchen möchten, oder geben Sie ein Schlüsselwort ein, um eine Liste der Spaltennamen mit diesem Schlüsselwort anzuzeigen. Geben Sie beispielsweise **Quelle** ein, um eine Liste der Spalten anzuzeigen, in deren Spaltenname der Ausdruck 'Quelle' vorkommt.
Verfügbare Spalten	Es werden die verfügbaren Spalten aufgeführt, die der ausgewählten Ansicht zugeordnet sind. Spalten, die aktuell für diese gespeicherte Suche verwendet werden, werden hervorgehoben und in der Liste **Spalten** angezeigt.
Schaltflächen für Spalte hinzufügen und entfernen (obere Gruppe)	Mit der oberen Gruppe der Schaltflächen können Sie die Liste **Gruppieren nach** anpassen. • **Spalte hinzufügen** - Wählen Sie eine oder mehrere Spalten in der Liste **Verfügbare Spalten** aus und klicken Sie auf die Schaltfläche **Spalte hinzufügen**m • **Spalte entfernen** - Wählen Sie eine oder mehrere Spalten in der Liste **Gruppieren nach** aus und klicken Sie auf die Schaltfläche **Spalte entfernen**m
Schaltflächen für Spalte hinzufügen und entfernen (untere Gruppe)	Mit der unteren Gruppe der Schaltflächen können Sie die Liste **Spalten** anpassen. • **Spalte hinzufügen** - Wählen Sie eine oder mehrere Spalten in der Liste **Verfügbare Spalten** aus und klicken Sie auf die Schaltfläche **Spalte hinzufügen**m • **Spalte entfernen** - Wählen Sie eine oder mehrere Spalten in der Liste **Spalten** aus und klicken Sie auf die Schaltfläche **Spalte entfernen**m

Tabelle 23. Option 'Erweitere Ansichtsdefinition' (Forts.)

Parameter	Beschreibung
Gruppieren nach	Gibt die Spalten an, aus denen die gespeicherte Suche die Ergebnisse gruppiert. Sie können die Liste **Gruppieren nach** mit folgenden Optionen weiter anpassen: • **Nach oben** - Wählen Sie eine Spalte aus und verschieben Sie diese in der Prioritätenliste mithilfe des Symbols **Nach oben**. • **Nach unten** - Wählen Sie eine Spalte aus und verschieben Sie diese in der Prioritätenliste mithilfe des Symbols **Nach unten**. In der Prioritätenliste wird angegeben, in welcher Reihenfolge die Ergebnisse gruppiert werden. Die Suchergebnisse werden nach der ersten Spalte in der Liste **Gruppieren nach** und anschließend nach der nächsten Spalte in der Liste gruppiert.
Spalten	Es werden die Spalten angegeben, die für die Suche ausgewählt wurden. Die Spalten werden aus einer gespeicherten Suche geladen. Sie können die Liste **Spalten** anpassen, indem Sie Spalten aus der Liste **Verfügbare Spalten** auswählen. Sie können die Liste **Spalten** mit folgenden Optionen weiter anpassen: • **Nach oben** - Wählen Sie eine Spalte aus und verschieben Sie sie mit der Schaltfläche 'Nach oben' in der Prioritätenliste nach oben. • **Nach unten** - Wählen Sie eine Spalte aus und verschieben Sie sie mit der Schaltfläche 'Nach unten' in der Prioritätenliste nach unten. Wenn der Spaltentyp numerisch ist oder es sich dabei um eine Uhrzeit handelt und ein Eintrag in der Liste **Gruppieren nach** vorhanden ist, enthält die Spalte eine Dropdown-Liste, mit der Sie auswählen können, wie die Spalte gruppiert werden soll.
Sortieren nach	Geben Sie mithilfe der ersten Liste die Spalte an, nach der die Suchergebnisse sortiert werden sollen. Geben Sie anschließend mithilfe der zweiten Liste die Reihenfolge an, in der die Suchergebnisse angezeigt werden sollen: **Absteigend** oder **Aufsteigend**.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Führen Sie eine Suche durch.
4. Klicken Sie auf **Kriterien speichern**.
5. Konfigurieren Sie Werte für die folgenden Parameter:

Option	Beschreibung
Name suchen	Geben Sie einen Namen ein, den Sie diesen Suchkriterien zuweisen möchten.
Suche zu Gruppe(n) zuweisen	Dies ist die Gruppe, die Sie dieser gespeicherten Suche zuweisen möchten. Wenn Sie keine Gruppe auswählen, wird diese gespeicherte Suche standardmäßig der Gruppe 'Sonstige' zugewiesen.
Zeitdaueroptionen	Wählen Sie eine der folgenden Optionen aus: • Aktuell - Geben Sie über die Dropdown-Liste den Zeitbereich für das Filtern an. • Bestimmtes Intervall - Geben Sie über den Kalender den Bereich für Datum und Uhrzeit an, der gefiltert werden soll.
In meine Schnellsuche aufnehmen	Wählen Sie das Kontrollkästchen aus, wenn Sie diese Suche in die Elemente Ihrer Schnellsuche integrieren möchten, die in der Dropdown-Liste **Suchen** verfügbar ist.
In mein Dashboard aufnehmen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Daten aus Ihrer gespeicherten Suche in Ihr Dashboard integrieren möchten. Dieser Parameter wird nur angezeigt, wenn es sich um eine gruppierte Suche handelt.
Als Standardwert definieren	Wählen Sie das Kontrollkästchen aus, wenn Sie diese Suche als Ihre Standardsuche festlegen möchten.
Freigeben für jeden	Wählen Sie dieses Kontrollkästchen aus, wenn Sie diese Suchanforderungen gemeinsam mit allen anderen QRadar Risk Manager-Benutzern verwenden möchten.

6. Klicken Sie auf **OK**.

Untergeordnete Suche ausführen

Bei jeder Suche wird die gesamte Datenbank auf Verbindungen abgefragt, die mit Ihren Kriterien übereinstimmen. Dieser Prozess kann sich über einen längeren Zeitraum erstrecken, je nach der Größe Ihrer Datenbank.

Informationen zu diesem Vorgang

Mit einer untergeordneten Suche können Sie innerhalb einer Gruppe abgeschlossener Suchergebnisse suchen. Sie können Ihre Suchergebnisse eingrenzen, ohne die Datenbank erneut durchsuchen zu müssen. Eine untergeordnete Suche ist nicht für gruppierte Suchvorgänge oder für Suchvorgänge verfügbar, die gerade durchgeführt werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Führen Sie eine Suche durch. Die Suchergebnisse werden angezeigt. Weitere Suchvorgänge verwenden bei der Ausführung von untergeordneten Suchvorgängen das Dataset aus der vorherigen Suche.

4. Führen Sie die folgenden Schritte aus, um einen Filter hinzuzufügen:
   a. Klicken Sie auf **Filter hinzufügen**.
   b. Wählen Sie mithilfe der ersten Liste ein Attribut aus, nach dem Sie suchen möchten.
   c. Wählen Sie mithilfe der zweiten Liste den Änderungswert, den Sie für die Suche verwenden möchten. Die Liste der angezeigten Änderungswerte ist von dem in der ersten Liste ausgewählten Attribut abhängig.
   d. Geben Sie im Textfeld bestimmte Informationen ein, die mit Ihrer Suche zusammenhängen.
   e. Klicken Sie auf **Filter hinzufügen**.

      Anmerkung: Wenn die Suche weiterhin ausgeführt wird, werden Teilergebnisse angezeigt. Im Fenster 'Ursprünglicher Filter' wird der Filter angezeigt, auf dem die ursprüngliche Suche basiert. Im Fenster Aktueller Filter wird der Filter angezeigt, der für die untergeordnete Suche angewendet wird.

      Tipp: Sie können die Filter der untergeordneten Suche löschen, ohne die ursprüngliche Suche erneut starten zu müssen. Klicken Sie neben dem Filter, den Sie löschen möchten, auf 'Filter löschen'. Wenn Sie einen Filter aus dem Fenster 'Ursprünglicher Filter' löschen, wird die ursprüngliche Suche erneut gestartet.
5. Klicken Sie auf **Kriterien speichern**, um die untergeordnete Suche zu speichern.

Ergebnisse

Wenn Sie die ursprüngliche Suche löschen, können Sie auf die gespeicherte untergeordnete Suche zugreifen. Wenn Sie einen Filter hinzufügen, wird bei der untergeordneten Suche die gesamte Datenbank durchsucht, da die Suchfunktion die Suche nicht mehr auf ein zuvor durchsuchtes Dataset stützt.

Suchergebnisse verwalten

Sie können mehrere Suchvorgänge nach Verbindungen ausführen, während Sie zu anderen Schnittstellen navigieren.

Informationen zu diesem Vorgang

Sie können die Suchfunktion konfigurieren und eine E-Mail-Benachrichtigung senden, wenn eine Suche abgeschlossen ist. Sie können zu jedem Zeitpunkt während der Suche Teilergebnisse der Suche anzeigen, die gerade ausgeführt wird.

In der Symbolleiste für die Suchergebnissen werden die folgenden Optionen bereitgestellt:

Parameter	Beschreibung
Neue Suche	Klicken Sie auf **Neue Suche**, um eine neue Suche zu erstellen. Durch das Klicken auf diese Schaltfläche wird das Suchfenster angezeigt.
Ergebnisse speichern	Klicken Sie auf **Ergebnisse speichern**, um Suchergebnisse zu speichern. Diese Option ist nur aktiviert, wenn Sie eine Zeile in der Liste 'Suchergebnisse verwalten' ausgewählt haben.

Parameter	Beschreibung
Abbrechen	Klicken Sie auf **Abbrechen**, um Suchvorgänge abzubrechen, die gerade ausgeführt werden oder für den Start eingereiht sind.
Löschen	Klicken Sie auf **Löschen**, um ein Suchergebnis zu löschen.
Benachrichtigen	Wählen Sie die Suche(n) aus, für die Sie Benachrichtigungen empfangen möchten, und klicken Sie anschließend auf **Benachrichtigen**, um die E-Mail-Benachrichtigung nach Abschluss der Suche zu aktivieren.
Anzeigen	Geben Sie in der Dropdown-Liste an, welche Suchergebnisse im Fenster mit den Suchergebnissen aufgeführt werden sollen. Folgende Optionen sind verfügbar: • Ergebnisse des gespeicherten Suchvorgangs • Alle Suchergebnisse • Abgebrochene/fehlerhafte Suchvorgänge • Derzeit bearbeitete Suchvorgänge

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Wählen Sie im Menü **Suchen** > **Suchergebnisse verwalten** aus.

Suchergebnisse speichern

Sie können die Ergebnisse Ihrer Suche speichern.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Führen Sie eine Verbindungssuche oder eine untergeordnete Suche aus.
4. Wählen Sie im Fenster mit den Suchergebnissen **Suche** > **Suchergebnisse verwalten** aus und wählen Sie ein Suchergebnis aus.
5. Klicken Sie auf **Ergebnisse speichern**.
6. Geben Sie einen Namen für die Suchergebnisse ein.
7. Klicken Sie auf **OK**.

Suche abbrechen

Sie können eine oder mehrere Suchen abbrechen.

Informationen zu diesem Vorgang

Falls eine Suche während des Suchvorgangs abgebrochen wird, werden die bis zum Abbruch ermittelten Ergebnisse beibehalten.

Vorgehensweise

1. Wählen Sie im Fenster **Suchergebnisse verwalten** das Suchergebnis aus, welches sich in der Warteschlange befindet oder bearbeitet wird und das Sie abbrechen möchten. Sie können mehrere Suchen auswählen, die abgebrochen werden sollen.
2. Klicken Sie auf **Suchvorgang abbrechen**.
3. Klicken Sie auf **Ja**.

Suche löschen

Sie können eine Suche löschen.

Vorgehensweise

1. Wählen Sie im Fenster **Suchergebnisse verwalten** die Suchergebnisse aus, die Sie löschen möchten.
2. Klicken Sie auf **Löschen**.
3. Klicken Sie auf **Ja**.

Verbindungen exportieren

Sie können Verbindungen im XML-Format (Extensible Markup Language) oder im CSV-Format (Comma Separated Values) exportieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Verbindungen**.
3. Wenn Sie die Verbindung im XML-Format exportieren möchten, wählen Sie **Aktionen** > **In XML exportieren** aus.
4. Wenn Sie die Verbindung im CSV-Format exportieren möchten, wählen Sie **Aktionen > In CSV-Datei exportieren** aus.
5. Wenn Sie Ihre Aktivitäten fortsetzen möchten, klicken Sie auf **Bei Abschluss benachrichtigen**.

Kapitel 8. Netzeinheitenkonfigurationen

In IBM Security QRadar Risk Manager können Sie die Konfiguration Ihrer Router, Firewalls und Switches überprüfen.

Sie können Zugriffssteuerungslisten (Access Control Lists, ACLs) für den Einheitenzugriff und Regeln überprüfen, Netzeinheitenkonfigurationen vergleichen, den Zähler für ausgelöste Regeln überwachen und den Verlauf von Regeln in Ihrer Topologie überprüfen.

Sie können auch Regeln und Einheiten durchsuchen und Zuordnungen von Protokollquellen erstellen oder bearbeiten. Weitere Informationen hierzu finden Sie im Abschnitt „Protokollquellenzuordnung erstellen oder bearbeiten" auf Seite 99.

Einheitenregeln

Firewallregeln zeigen an, welcher Datenverkehr zwischen Ihren Netzeinheiten zulässig ist oder verweigert wird.

In QRadar Risk Manager wird eine Firewallregel ausgelöst, wenn alle Bedingungen der Regel erfüllt sind.

Falls alle Bedingungen einer Regel erfüllt sind, lässt die Regel den Netzverkehr je nach der **Aktion** der Regel entweder zu oder lehnt ihn ab. Als Aktion kann beispielsweise **Akzeptieren** oder **Verweigern** festgelegt sein.

Zugriffssteuerungslisten

Eine Zugriffssteuerungsliste (Access Control List, ACL) filtert den Datenverkehr, der von einer Firewall in Ihrem Netz empfangen wird, und enthält Regeln, die den Datenverkehr zwischen den Einheiten in Ihrem Netz entweder zulassen oder verweigern.

Eine Zugriffssteuerungsliste wird ausgelöst, sobald Einheiten in Ihrem Netz eine Kommunikation versuchen.

Zugehörige Tasks:

„Netzeinheitenkonfigurationen überprüfen" auf Seite 99
In IBM Security QRadar Risk Manager können Sie die Effizienz Ihrer Netzeinheiten steuern, Firewallregeln überprüfen und Sicherheitsrisiken ermitteln, die aufgrund von ungültigen Firewallregeln entstehen.

Netzeinheiten suchen

In IBM Security QRadar Risk Manager können Sie in Ihrer Liste der Netzrouter oder Firewalls nach der Einheit suchen, die Sie überprüfen möchten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsfenster auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Klicken Sie in der Symbolleiste auf **Suchen** > **Neue Suche**.

4. Klicken Sie im Teilfenster mit den Suchkriterien auf einen Zeitbereich.

   Die Suchoption für den Zeitbereich verwendet die Zeitmarke für die aktuellste Sicherung der Einheitenkonfiguration.Die Option **Intervall** umfasst ein Mindestzeitintervall von der letzten Stunde bis zu einem maximalen Intervall der letzten 30 Tage.
5. Wählen Sie eine der folgenden Optionen aus, um nach einer Einheit zu suchen, die Sie überprüfen möchten:
   - Wenn Sie nach einem Asset oder Assetbereich suchen möchten, geben Sie eine IP-Adresse oder einen CIDR-Bereich ein.
   - Wenn Sie nach einem Host suchen möchten, geben Sie den Hostnamen der Einheit ein.
   - Wenn Sie nach einem Modell suchen möchten, geben Sie das Modell der Einheit ein.

     Bei den Host- und Modelloptionen können Sie alphanumerische Zeichen, Gedankenstriche oder Punkte verwenden.
   - Wenn Sie nach einem Referenzset suchen möchten, geben Sie ein IP-basiertes Referenzset ein.

     Sie können auf alle Referenzsets zugreifen, die in Ihrem Benutzeraccount verfügbar sind.
6. Klicken Sie auf **Suchen**.

Protokollquellenzuordnung

Zur Überwachung der Auslöserhäufigkeit von Firewallregeln und für die Aktivierung von Ereignissuchen in der Topologie ermittelt IBM Security QRadar Risk Manager QRadar-Protokollquellen.

Durch eine gute Kenntnis der Firewallregeln können Sie die Firewalleffizienz aufrechterhalten und Sicherheitsrisiken verhindern.

Einer Protokollquelle in QRadar Risk Manager können maximal 255 Einheiten zugeordnet werden, aber Einheiten können mehrere Protokollquellen haben.

Anzeigeoptionen für die Protokollquellenzuordnung

Wenn Sie Ihre Netzeinheit als QRadar-Protokollquelle konfiguriert haben, wird auf der Seite **Configuration Monitor** (Konfigurationsüberwachung) einer der folgenden Einträge in der Spalte **Log Source** (Protokollquelle) angezeigt:

- **Auto-Mapped** (Automatisch zugeordnet) - Wenn QRadar Risk Manager die Protokollquelle automatisch ermittelt und der Einheit zuordnet.
- **Username** (Benutzername) - Wenn ein Administrator eine Protokollquelle manuell hinzugefügt oder bearbeitet hat.
- **Blank** (Leer) - Wenn QRadar Risk Manager nicht in der Lage ist, eine Protokollquelle für die Einheit zu ermitteln, wird in der Spalte **Log Source** (Protokollquelle) kein Wert angezeigt. Sie können eine Protokollquellenzuordnung manuell erstellen.

Weitere Informationen zur Konfiguration von Protokollquellen finden Sie im Handbuch *IBM Security QRadar Log Sources User Guide*.

Zugehörige Konzepte:

„Kontextmenüoptonen in der Topologie" auf Seite 36
Sie können in der Topologie mit der rechten Maustaste auf ein Ereignis klicken, um auf zusätzliche Ereignisfilterinformationen zuzugreifen.

Protokollquellenzuordnung erstellen oder bearbeiten

Wenn IBM Security QRadar Risk Manager keine Protokollquelle in QRadar ermitteln kann, können Sie eine Protokollquellenzuordnung konfigurieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsfenster auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Klicken Sie auf die Einheit ohne Protokollquellenzuordnung.
4. Klicken Sie in der Symbolleiste auf **Create/Edit Mapping** (Zuordnung erstellen/bearbeiten).
5. Wählen Sie in der Liste **Log Source** (Protokollquelle) eine Gruppe aus.
6. Wählen Sie eine Protokollquelle aus.
7. Klicken Sie auf **Hinzufügen**.
8. Klicken Sie auf **Speichern**.

Netzeinheitenkonfigurationen überprüfen

In IBM Security QRadar Risk Manager können Sie die Effizienz Ihrer Netzeinheiten steuern, Firewallregeln überprüfen und Sicherheitsrisiken ermitteln, die aufgrund von ungültigen Firewallregeln entstehen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsfenster auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Suchen Sie Ihre Netzeinheiten. Klicken Sie in der Symbolleiste auf **Suchen** > **Neue Suche**.
4. Doppelklicken Sie auf die Einheit, die Sie überprüfen möchten.

   In der Regelspalte **Ereignisanzahl** wird die Auslöserhäufigkeit für die Firewallregel angezeigt. Für die Regel wird die Ereignisanzahl null angezeigt, wenn einer der folgenden Gründe zutrifft:

   - Eine Regel wird nicht ausgelöst und kann zu einem Sicherheitsrisiko führen. Sie können Ihre Firewalleinheit überprüfen und alle Regeln entfernen, die nicht ausgelöst werden.
   - Eine QRadar-Protokollquellenzuordnung ist nicht konfiguriert.
5. Klicken Sie zum Durchsuchen der Regeln in der Symbolleiste **Regeln** auf **Suchen** > **Neue Suche**.

   Wenn in der Spalte **Status** ein Symbol angezeigt wird, können durch Bewegen des Mauszeigers über das Statussymbol weitere Informationen angezeigt werden.
6. Wenn Sie die Einheitenschnittstellen überprüfen möchten, klicken Sie in der Symbolleiste auf **Schnittstellen**.
7. Wenn Sie die Einheitenregeln für die Zugriffssteuerungsliste (Access Control List, ACL) überprüfen möchten, klicken Sie in der Symbolleiste auf **ACLs**.

   Jede Zugriffssteuerungsliste definiert die Schnittstellen, über die die Einheiten in Ihrem Netz kommunizieren. Sobald die Bedingungen einer Zugriffssteuerungsliste erfüllt werden, werden die Regeln ausgelöst, die einer Zugriffssteuerungsliste zugeordnet sind. Jede Regel wird getestet und lässt die Kommunikation zwischen Einheiten entweder zu oder lehnt diese ab.

8. Wenn Sie die Einheitenregeln für die Netzadressumsetzung (Network Address Translation, NAT) überprüfen möchten, klicken Sie in der Symbolleiste auf **NAT**.

   In der Spalte **Phase** ist angegeben, wann die Netzadressumsetzungsregel ausgelöst werden soll, zum Beispiel vor oder nach der Weiterleitung.

9. Wenn Sie das Protokoll überprüfen oder Einheitenkonfigurationen vergleichen möchten, klicken Sie in der Symbolleiste auf **Protokoll**.

   Sie können Einheitenregeln in einer normalisierten Vergleichsansicht oder in der Roheinheitenkonfiguration anzeigen. Die normalisierte Einheitenkonfiguration ist ein grafischer Vergleich mit Regeln, die zwischen Einheiten hinzugefügt, gelöscht oder geändert wurden. Die Roheinheitenkonfiguration ist eine XML- oder Klartextansicht der Einheitendatei.

Zugehörige Konzepte:

„Protokollquellenzuordnung” auf Seite 98
Zur Überwachung der Auslöserhäufigkeit von Firewallregeln und für die Aktivierung von Ereignissuchen in der Topologie ermittelt IBM Security QRadar Risk Manager QRadar-Protokollquellen.

Einheitenregeln suchen

In IBM Security QRadar Risk Manager können Sie nach Regeln suchen, die in den Einheiten Ihrer Topologie geändert wurden. Sie können auch Regeländerungen ermitteln, die zwischen den Sicherungen der Einheitenkonfiguration aufgetreten sind.

Die für eine Regelsuche zurückgegebenen Ergebnisse basieren auf der Sicherung der Verwaltung von Konfigurationsquellen Ihrer Einheit. Um sicherzustellen, dass die Regelsuche stets aktuelle Informationen bereitstellt, können Sie auf Ihrer Aktualisierungsseite für Firewallrichtlinien Einheitensicherungen planen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsfenster auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Doppelklicken Sie im Fenster **Configuration Monitor** (Konfigurationsüberwachung) auf eine Einheit.
4. Klicken Sie im Teilfenster **Regeln** auf **Suchen** > **Neue Suche**.
5. Klicken Sie im Teilfenster mit den Suchkriterien auf einen Zeitbereich.
6. Treffen Sie zur Suche nach Ihren Einheitenregeln eine Auswahl unter folgenden Optionen:
   - Klicken Sie auf eine der Statusoptionen **Shadowed** (Schatten), **Deleted** (Gelöscht) oder **Other** (Sonstige), um nach den entsprechenden Regeln zu suchen.

     Standardmäßig sind alle Statusoptionen aktiviert. Wenn Sie nur nach Schattenregeln suchen möchten, wählen Sie die Optionen **Deleted** (Gelöscht) und **Other** (Sonstige) ab.
   - Wenn Sie nach einer Zugriffssteuerungsliste (Access Control List, ACL) suchen möchten, geben Sie den entsprechenden Wert im Feld **List** (Liste) ein.
   - Wenn Sie nach der Folgenummer des Regeleintrags suchen möchten, geben Sie einen numerischen Wert im Feld **Entry** (Eintrag) ein.
   - Wenn Sie nach einer Quelle oder einem Ziel suchen möchten, geben Sie eine IP-Adresse, CIDR-Adresse, einen Hostnamen oder einen Objektgruppenverweis ein.

- Wenn Sie nach Ports oder Objektgruppenverweisen suchen möchten, geben Sie den entsprechenden Wert im Feld **Service** ein.

  Der Service kann Portbereiche (zum Beispiel 100-200) oder Portausdrücke wie 80(TCP) enthalten. Wenn der Port zurückgewiesen wird, enthalten die Portinformationen außerdem ein Ausrufezeichen und können von Klammern umschlossen sein (beispielsweise '!(100-200) oder '!80(TCP)).
- Wenn Sie nach Informationen einer Schwachstellenregel gemäß Definition durch die IPS-Einheit suchen möchten, geben Sie den entsprechenden Wert im Feld **Signature** (Signatur) ein.
- Wenn Sie Anwendungen nach Adaptern suchen möchten, klicken Sie auf **Select Applications** (Anwendungen auswählen) und geben Sie dann einen Adapter- oder Anwendungsnamen ein.

7. Klicken Sie auf **Suchen**.

Konfiguration Ihrer Netzeinheiten vergleichen

In IBM Security QRadar Risk Manager können Einheitenkonfigurationen miteinander verglichen werden, indem mehrere Sicherungen in einer einzelnen Einheit miteinander verglichen werden oder die Sicherung einer Netzeinheit mit derjenigen einer anderen verglichen wird.

Beispiele für allgemeine Konfigurationstypen:

- **Standard Element Document** - SED-Dateien (SED = Standard Element Document, Standardelementdokument) sind XML-Datendateien, die Informationen zu Ihrer Netzeinheit enthalten. Einzelne SED-Dateien werden in ihrem unaufbereiteten XML-Format angezeigt. Wird eine SED-Datei mit einer anderen SED-Datei verglichen, wird die Ansicht normalisiert, um die Regelunterschiede anzuzeigen.
- **Config** - Konfigurationsdateien werden von bestimmten Netzeinheiten abhängig vom Einheitenhersteller bereitgestellt. Sie können eine Konfigurationsdatei anzeigen, indem Sie auf sie doppelklicken.

Je nach den Informationen, die der Adapter für eine Einheit erfasst, können mehrere andere Konfigurationstypen angezeigt werden. Diese Dateien werden nach dem Doppelklicken in einer Klartextansicht angezeigt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Klicken Sie doppelt auf eine beliebige Einheit, um die ausführlichen Konfigurationsinformationen anzuzeigen.
4. Klicken Sie auf **Protokoll**, um das Protokoll für diese Einheit anzuzeigen.
5. So vergleichen Sie zwei Konfigurationen in einer einzelnen Einheit:
   a. Wählen Sie eine primäre Konfiguration aus.
   b. Drücken Sie die Steuertaste und wählen Sie eine weitere Konfiguration für den Vergleich aus.
   c. Klicken Sie im Teilfenster **History** (Protokoll) auf **Compare Selected** (Ausgewählte vergleichen).

      Wenn es sich bei den Vergleichsdateien um Standardelementdokumente (SEDs) handelt, werden im Fenster **Normalized Device Configuration Comparison** (Vergleich der normalisierten Einheitenkonfiguration) die Regelunterschiede zwischen den Sicherungen angezeigt.

Beim Vergleich von normalisierten Konfigurationen zeigt die Farbe des Textes die folgenden Einheitenaktualisierungen an:

- Eine grün gepunktete Umrandung eine Regel oder Konfiguration an, die der Einheit hinzugefügt wurde.
- Eine rot gestrichelte Umrandung zeigt eine Regel oder Konfiguration an, die aus der Einheit gelöscht wurde.
- Eine gelbe durchgehende Umrandung zeigt eine Regel oder Konfiguration an, die in der Einheit geändert wurde.

d. Wenn Sie die Unterschiede der unbearbeiteten Konfiguration anzeigen möchten, klicken Sie auf **View Raw Comparison** (Unbearbeiteten Vergleich anzeigen).

Wenn es sich beim Vergleich um eine Konfigurationsdatei oder um einen anderen Sicherungstyp handelt, wird der unbearbeitete Vergleich angezeigt.

6. So vergleichen Sie zwei Konfigurationen in verschiedenen Einheiten:
   a. Wählen Sie eine primäre Konfiguration in einer Einheit aus.
   b. Klicken Sie auf **Mark for Comparison** (Für Vergleich markieren).
   c. Wählen Sie im Navigationsmenü **All Devices** (Alle Einheiten) aus, um zur Einheitenliste zurückzukehren.
   d. Klicken Sie für den Vergleich doppelt auf die Einheit und klicken Sie anschließend auf **Protokoll**.
   e. Wählen Sie eine Konfiguration aus, die Sie mit der markierten Konfiguration vergleichen möchten.
   f. Klicken Sie auf **Compare with Marked** (Mit markierter vergleichen).
   g. Wenn Sie die Unterschiede der unbearbeiteten Konfiguration anzeigen möchten, klicken Sie auf **View Raw Comparison** (Unbearbeiteten Vergleich anzeigen).

Kapitel 9. IBM Security QRadar Risk Manager-Berichte verwalten

Sie können Berichte für die Netzeinheiten erstellen, bearbeiten, verteilen und verwalten. Oft sind detaillierte Berichte zu Firewallregeln und Verbindungen zwischen Einheiten erforderlich, um verschiedene gesetzliche Standards, z. B. PCI-Konformität, zu erfüllen.

Die folgenden Berichtsoptionen sind für QRadar Risk Manager spezifisch:

Tabelle 24. Berichtsoptionen für QRadar Risk Manager

Berichtsoption	Beschreibung
Verbindungen	Die Verbindungsdiagramme für Netzeinheiten, die während eines angegebenen Zeitrahmens auftraten.
Einheitenregeln	Die Regeln, die für eine Netzeinheit während eines angegebenen Zeitrahmens konfiguriert wurden. Mithilfe dieser Berichtsoption können folgende Regeltypen für eine oder viele Netzeinheiten angezeigt werden: • Am häufigsten angewendete Akzeptanzregeln • Am häufigsten angewendete Verweigerungsregeln • Am wenigsten angewendete Akzeptanzregeln • Am wenigsten angewendete Verweigerungsregeln • Schattenregeln • Nicht angewendete Objektregeln
Nicht genutzte Objekte einer Einheit	Es wird eine Tabelle mit dem Namen, Konfigurationsdatum/-uhrzeit und einer Definition für alle Objektreferenzgruppen erstellt, die in der Einheit nicht im Gebrauch sind. Eine Objektreferenzgruppe ist ein allgemeiner Begriff, der eine Zusammenstellung von IP-Adressen, CIDR-Adressen, Hostnamen, Ports oder anderen Einheitenparametern beschreibt, die zu Gruppen zusammengefasst und Regeln in der Einheit zugewiesen werden.

Bericht manuell erstellen

Berichte können manuell gestartet werden. Wenn Sie mehrere Berichte manuell starten, werden die Berichte zu einer Warteschlange hinzugefügt und mit ihrer Warteschlangenposition gekennzeichnet.

Informationen zu diesem Vorgang

Durch eine manuelle Berichterstellung wird der bestehende Berichtszeitplan nicht außer Kraft gesetzt. Wenn beispielsweise ein wöchentlicher Bericht für die aktivsten Firewallverweigerungen erstellt wird und Sie diesen Bericht dann manuell erstellen, wird der wöchentliche Bericht weiterhin nach dem ursprünglich konfigurierten Zeitplan erstellt.

Wird ein Bericht erstellt, wird in der Spalte **Nächste Ausführungszeit** eine der drei folgenden Nachrichten angezeigt:

- **Generating** - Der Bericht wird erstellt.
- **Queued (Position in Warteschlange)**- Der Bericht wird zur Erstellung in eine Warteschlange eingereiht. Die Nachricht gibt die Position des Berichts in der Warteschlange an. Beispiel: 1 von 3.
- **(x hour(s) x min(s)y sec(s))** - Die Ausführung des Berichts ist terminiert. Die Nachricht ist ein Countdown-Zähler, der angibt, wann der Bericht das nächste Mal ausgeführt wird.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie den Bericht aus, der erstellt werden soll.
3. Klicken Sie auf **Bericht ausführen**.
4. Optional: Klicken Sie auf **Aktualisieren**, um die Ansicht, einschließlich der Informationen in der Spalte **Nächste Ausführungszeit**, zu aktualisieren.

Nächste Schritte

Nachdem der Bericht erstellt wurde, kann der erstellte Bericht über die Spalte **Erstellte Berichte** angezeigt werden.

Berichtsassistenten verwenden

Sie können mit dem Berichtsassistenten einen neuen Bericht erstellen. Der Berichtsassistent bietet eine schrittweise Anleitung zum Entwerfen, Planen und Erstellen von Berichten.

Der Assistent verwendet die folgenden Schlüsselelemente, um Ihnen beim Erstellen eines Berichts zu helfen:

- **Layout** - Position und Größe der einzelnen Container
- **Container** - Platzhalter und Position für Inhalte im Bericht
- **Content** - Definiert die Berichtsdaten, die QRadar Risk Manager in das Diagramm für den Container einschließt

Berücksichtigen Sie bei der Auswahl des Layouts eines Berichts den Typ des Berichts, den Sie erstellen möchten. Wählen Sie beispielsweise keinen zu kleinen Diagrammkcontainer für grafische Inhalte, die eine große Zahl von Objekten anzeigen. Jede Grafik beinhaltet eine Legende und eine Liste der Netze, aus denen die Inhalte abgeleitet werden. Wählen Sie einen Container, der groß genug für die Aufnahme der Daten ist.

Für Berichte, die wöchentlich oder monatlich erstellt werden, gibt der erstellte Bericht erst nach Ablauf der terminierten Zeit Ergebnisse zurück. Bei einem geplanten Bericht müssen Sie die terminierte Zeit bis zur Erstellung der Ergebnisse war-

ten. Für eine wöchentliche Suche sind beispielsweise sieben Tage zum Erstellen der Daten erforderlich. Eine solche Suche gibt Ergebnisse nach Ablauf von sieben Tagen zurück.

Bericht erstellen

Sie können Berichte für ein bestimmtes Intervall erstellen und einen Diagrammtyp auswählen.

Informationen zu diesem Vorgang

Ein Bericht kann aus mehreren Datenelementen bestehen und Netz- und Sicherheitsdaten in einer Reihe von Stilen darstellen, beispielsweise als Tabellen, Liniendiagramme, Kreisdiagramme und Balkendiagramme.

Als Verteilungsoptionen können Sie 'Berichtskonsole' oder 'E-Mail' angeben. In der folgenden Tabelle werden die Parameter für diese Verteilungsoptionen beschrieben.

Tabelle 25. Generierte Berichtsverteilungsoptionen

Option	Beschreibung
Berichtskonsole	Wählen Sie dieses Kontrollkästchen aus, um den generierten Bericht an die Registerkate **Berichte** zu senden. Dies ist der Standardverteilungskanal.
Benutzer auswählen, die den generierten Bericht anzeigen können.	Diese Option wird nur angezeigt, wenn Sie das Kontrollkästchen **Berichtskonsole** aktiviert haben. Wählen Sie aus der Liste der Benutzer die QRadar Risk Manager-Benutzer aus, die die Berechtigung zum Anzeigen der generierten Berichte erhalten sollen. Sie müssen über die entsprechenden Netzberechtigungen verfügen, um den generierten Bericht gemeinsam mit anderen Benutzern nutzen zu können. Weitere Informationen zu Berechtigungen finden Sie im Handbuch 'IBM Security QRadar SIEM Administration Guide'.
Alle Benutzer auswählen	Diese Option wird nur angezeigt, wenn sie das Kontrollkästchen **Berichtskonsole** auswählen. Aktivieren Sie dieses Kontrollkästchen, wenn Sie allen QRadar Risk Manager-Benutzern die Berechtigung zum Anzeigen der generierten Berichte erteilen möchten. Sie müssen über die entsprechenden Netzberechtigungen verfügen, um den generierten Bericht gemeinsam mit anderen Benutzern nutzen zu können. Weitere Informationen zu Berechtigungen finden Sie im Handbuch 'IBM Security QRadar SIEM Administration Guide'.

Tabelle 25. Generierte Berichtsverteilungsoptionen (Forts.)

Option	Beschreibung
E-Mail	Wählen Sie dieses Kontrollkästchen aus, wenn Sie den generierten Bericht als E-Mail verteilen möchten.
E-Mail-Adresse(n) für die Verteilung des Berichts eingeben.	Diese Option wird nur angezeigt, wenn Sie das Kontrollkästchen **E-Mail** aktiviert haben. Geben Sie die E-Mail-Adresse für jeden Empfänger des generierten Berichts ein; eine Liste von E-Mail-Adresse wird durch Kommas getrennt. Die maximale Anzahl der Zeichen für diesen Parameter ist 255. E-Mail-Empfänger erhalten diese E-Mail vom Absender 'no_reply_reports@qradar'.
Bericht als Anhang einschließen (nur Nicht-HTML)	Diese Option wird nur angezeigt, wenn Sie das Kontrollkästchen **E-Mail** aktiviert haben. Wählen Sie dieses Kontrollkästchen aus, um den generierten Bericht als Anhang zu senden.
Link zur Berichtskonsole einschließen	Diese Option wird nur angezeigt, wenn Sie das Kontrollkästchen **E-Mail** aktiviert haben. Wählen Sie dieses Kontrollkästchen aus, um in der E-Mail einen Link zur Berichtskonsole einzuschließen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie aus der Liste **Aktionen** den Eintrag **Erstellen** aus.
3. Klicken Sie auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.
4. Wählen Sie die Häufigkeit des Berichtszeitplans aus.
5. Wählen Sie im Fenster 'Darf dieser Bericht manuell erstellt werden?' die Option **Ja** aus, um die manuelle Erstellung zu aktivieren, oder wählen Sie **Nein** aus, um die manuelle Generierung dieses Berichts zu sperren. Diese Option ist für manuell generierte Berichte nicht verfügbar.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie ein Layout für Ihren Bericht aus und klicken Sie anschließend auf 'Weiter'.
8. Geben Sie einen Titel für den Bericht ein. Der Titel kann bis zu 100 Zeichen lang sein. Verwenden Sie keine Sonderzeichen.
9. Wählen Sie ein Logo aus. Das QRadar-Logo ist das Standardlogo. Weitere Informationen zur Markenkennzeichnung Ihres Berichts finden Sie im Handbuch *IBM Security QRadar SIEM Administrator Guide*.
10. Wählen Sie in der Liste **Diagrammtyp** einen der spezifischen QRadar Risk Manager-Berichte aus.
11. Konfigurieren Sie die Berichtsdaten für Ihr Diagramm.
12. Klicken Sie auf **Containerdetails speichern**.

13. Klicken Sie auf **Weiter**.
14. Klicken Sie auf **Weiter**, um zum nächsten Schritt des Berichtsassistenten zu wechseln.
15. Wählen Sie Berichtsformate aus. Sie können mehrere Optionen auswählen.

    Anmerkung: Die Berichte 'Einheitenregeln' und 'Nicht verwendete Objektregeln' unterstützten nur die Berichtsformate PDF, HTML und RTF.
16. Klicken Sie auf **Weiter**.
17. Wählen Sie die Verteilungskanäle für Ihren Bericht aus.
18. Klicken Sie auf **Weiter**.
19. Geben Sie eine Beschreibung für diesen Bericht ein. Die Beschreibung wird auf der Seite 'Berichtszusammenfassung' und in der E-Mail zur Verteilung des generierten Berichts angezeigt.
20. Wählen Sie die Gruppen aus, denen Sie diesen Bericht zuweisen wollen. Weitere Informationen zu Gruppen finden Sie im Handbuch *IBM Security QRadar SIEM Administration Guide* unter 'Managing Reports' (Berichte verwalten).
21. Optional. Wählen Sie 'Ja' aus, um diesen Bericht auszuführen, sobald die Installation des Assistenten abgeschlossen ist. Klicken Sie auf **Weiter**, um die Berichtszusammenfassung anzuzeigen. Sie können die in der Berichtszusammenfassung verfügbaren Registerkarten auswählen, um eine Voranzeige der Berichtsauswahl aufzurufen.
22. Klicken Sie auf **Beenden**.

Ergebnisse

Der Bericht wird sofort erstellt. Wenn Sie das Kontrollkästchen **Soll der Bericht jetzt ausgeführt werden?** auf der letzten Seite des Assistenten nicht ausgewählt haben, wird der Bericht gespeichert und als geplanter Bericht generiert.

Beim Berichtstitel handelt es sich um den Standardtitel für den generierten Bericht. Wenn Sie einen Bericht erneut konfigurieren, um einen neuen Berichtstitel einzugeben, wird der Bericht als neuer Bericht unter dem neuen Namen gespeichert. Der ursprüngliche Bericht bleibt aber unverändert erhalten.

Bericht bearbeiten

Sie können einen Bericht bearbeiten, um Berichtszeitplan, Layout, Konfiguration, Titel, Format und Liefermethode anzupassen. Sie können vorhandene Berichte oder einen Standardbericht bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie den Bericht aus, den Sie bearbeiten möchten.
3. Wählen Sie in der Liste **Aktionen** die Option **Bearbeiten** aus.
4. Wählen Sie die Häufigkeit des neuen Berichtszeitplans aus.
5. Wählen Sie im Fenster 'Darf dieser Bericht manuell erstellt werden?' eine der folgenden Optionen aus:
   - **Ja** - Die manuelle Generierung dieses Berichts ist aktiviert.
   - **Nein** - Die manuelle Generierung dieses Berichts ist nicht aktiviert.
6. Klicken Sie auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.

7. Konfigurieren Sie das Layout Ihres Berichts:
   a. Wählen Sie in der Liste **Ausrichtung** die Seitenausrichtung aus.
   b. Wählen Sie eine Layout-Option für Ihren QRadar Risk Manager-Bericht.
   c. Klicken Sie auf **Weiter**.
8. Geben Sie Werte für die folgenden Parameter an:
   - **Berichtstitel** - Geben Sie einen Berichtstitel ein. Der Titel kann bis zu 100 Zeichen lang sein. Verwenden Sie keine Sonderzeichen.
   - **Logo** - Wählen Sie ein Logo aus der Liste aus. Das QRadar-Logo ist das Standardlogo. Weitere Informationen zur Markenkennzeichnung Ihres Berichts finden Sie im Handbuch *IBM Security QRadar SIEM Administrator Guide*.
9. Konfigurieren Sie den Container für Ihre Berichtsdaten:
   a. Klicken Sie auf **Definieren**.
   b. Konfigurieren Sie die Berichtsdaten für Ihr Diagramm.
   c. Klicken Sie auf **Containerdetails speichern**.
   d. Wiederholen Sie diese Schritte gegebenenfalls, um zusätzliche Container zu bearbeiten.
   e. Klicken Sie auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.
10. Klicken Sie auf **Weiter**, um zum nächsten Schritt des Berichtsassistenten zu wechseln.
11. Aktivieren Sie die Kontrollkästchen für die Berichtsformate. Sie können mehrere Optionen auswählen.

    Anmerkung: Die für QRadar Risk Manager spezifischen Berichte (z. B. die Berichte 'Device Rule' und 'Device Unused Object') unterstützen nur PDF-, HTML und RTF-Formate.
12. Klicken Sie auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.
13. Wählen Sie die Verteilungskanäle für Ihren Bericht aus.
14. Klicken Sie auf **Weiter**, um den letzten Schritt des Berichtsassistenten auszuführen.
15. Geben Sie eine Beschreibung für diesen Bericht ein. Die Beschreibung wird auf der Seite **Berichtszusammenfassung** und in der E-Mail zur Verteilung des generierten Berichts angezeigt.
16. Wählen Sie die Gruppen aus, denen Sie diesen Bericht zuweisen wollen. Weitere Informationen zu Gruppen finden Sie im Handbuch *IBM Security QRadar SIEM Administration Guide* unter 'Managing Reports' (Berichte verwalten).
17. Optional. Wählen Sie 'Ja' aus, um diesen Bericht auszuführen, sobald die Installation des Assistenten abgeschlossen ist.
18. Klicken Sie auf **Weiter**, um die Berichtszusammenfassung anzuzeigen. Die Seite **Berichtszusammenfassung** mit den Details zum Bericht wird angezeigt. Sie können die in der Berichtszusammenfassung verfügbaren Registerkarten auswählen, um eine Voranzeige der Berichtsauswahl aufzurufen.
19. Klicken Sie auf **Beenden**.

Bericht duplizieren

Sie können jeden Bericht duplizieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie den zu duplizierenden Bericht aus.
3. Klicken Sie in der Liste **Aktionen** auf **Duplikat**.
4. Geben Sie einen neuen Namen für den Bericht ohne Leerzeichen ein.

Bericht gemeinsam nutzen

Sie können Berichte gemeinsam mit anderen Benutzern nutzen. Beim gemeinsamen Nutzen eines Berichts stellen Sie anderen Benutzern eine Kopie des ausgewählten Berichts zur Bearbeitung oder Planung bereit.

Vorbereitende Schritte

Zur gemeinsamen Nutzung von Berichten müssen Sie Administratorberechtigung haben. Damit ein neuer Benutzer Berichte anzeigen und auf diese zugreifen kann, muss ein Benutzer mit Verwaltungsaufgaben außerdem alle erforderlichen Berichte für den neuen Benutzer freigeben

Informationen zu diesem Vorgang

Die Aktualisierungen, die der Benutzer an einem freigegebenen Bericht vornimmt, haben keine Auswirkung auf die ursprüngliche Version des Berichts.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie die Berichte aus, die Sie gemeinsam nutzen möchten.
3. Klicken Sie in der Liste **Aktionen** auf **Freigeben**.
4. Wählen Sie aus der Liste der Benutzer die Benutzer aus, mit denen Sie diesen Bericht gemeinsam nutzen möchten.

   Falls keine Benutzer mit ausreichenden Zugriffsberechtigungen verfügbar sind, wird eine Nachricht angezeigt.
5. Schritt 5: Klicken Sie auf **Freigeben**.

   Weitere Informationen zu Berichten finden Sie im Handbuch *IBM Security QRadar SIEM Users Guide*.

Diagramme konfigurieren

Der Diagrammtyp legt die Daten fest, die im Diagramm konfiguriert und angezeigt werden. Sie können mehrere Diagramme für bestimmte Daten, die von Einheiten in QRadar Risk Manager erfasst werden, erstellen.

Die folgenden Diagrammtypen sind für QRadar Risk Manager spezifisch:

- Verbindung
- Einheitenregeln
- Nicht genutzte Objekte einer Einheit

Verbindungsdiagramme

Sie können das Diagramm 'Verbindungen' verwenden, um Netzverbindungsinformationen anzuzeigen. Dabei können die Diagramme auf Daten aus gespeicherten Suchen nach Verbindungen auf der Registerkarte 'Risiken' basieren.

Sie können die Daten anpassen, die im erstellten Bericht angezeigt werden sollen. Sie können das Diagramm so konfigurieren, dass Daten über einen konfigurierbaren Zeitraum dargestellt werden. Mithilfe dieser Funktion können Sie Verbindungstrends erkennen.

Die folgende Tabelle stellt Konfigurationsinformationen für den Verbindungsdiagrammcontainer bereit.

Tabelle 26. Verbindungsdiagrammparameter

Parameter	Beschreibung
Containerdetails - Verbindungen	
Diagrammtitel	Geben Sie einen Diagrammtitel aus maximal 100 Zeichen ein.
Diagrammuntertitel	Inaktivieren Sie das Kontrollkästchen, um den automatisch erstellten Untertitel zu ändern. Geben Sie einen Titel aus maximal 100 Zeichen ein.
Grafiktyp	Wählen Sie in der Liste den Typ der Grafik aus, die im erstellten Bericht angezeigt werden soll. Verfügbare Typen: • **Balken** - Zeigt die Daten als Balkendiagramm an. Dies ist der Standardgrafiktyp. Für diesen Grafiktyp muss die gespeicherte Suche eine gruppierte Suche sein. • **Linie** - Zeigt die Daten als Liniendiagramm an. • **Kreis** - Zeigt die Daten als Kreisdiagramm an. Für diesen Grafiktyp muss die gespeicherte Suche eine gruppierte Suche sein. • **Gestapelter Balken** - Zeigt die Daten als gestapeltes Balkendiagramm an. • **Gestapelte Linie** - Zeigt die Daten als gestapeltes Liniendiagramm an. • **Tabelle** - Zeigt die Daten im Tabellenformat an. Der Typ **Tabelle** ist nur für den Container mit voller Seitenbreite verfügbar.
Grafik	Wählen Sie in der Liste die Anzahl der Verbindungen aus, die im erstellten Bericht angezeigt werden sollen.

Tabelle 26. Verbindungsdiagrammparameter (Forts.)

Parameter	Beschreibung
Manuelle Planung	Das Teilfenster 'Manuelle Planung' wird nur angezeigt, wenn Sie im Berichtsassistenten die Planungsoption **Manuell** ausgewählt haben. So erstellen Sie einen manuellen Zeitplan: 1. Geben Sie im Listenfeld **Von** das gewünschte Startdatum für den Bericht ein oder wählen Sie das Datum über das Symbol **Kalender** aus. Der Standardwert ist das aktuelle Datum. 2. Wählen Sie in den Listenfeldern die gewünschte Startzeit für den Bericht aus. Die Zeit kann in Halbstundenschritten angegeben werden. Der Standardwert ist 1:00 Uhr. 3. Geben Sie im Listenfeld **Bis** das gewünschte Enddatum für den Bericht ein oder wählen Sie das Datum über das Symbol **Kalender** aus. Der Standardwert ist das aktuelle Datum. 4. Wählen Sie in den Listenfeldern die gewünschte Endzeit für den Bericht aus. Die Zeit kann in Halbstundenschritten angegeben werden. Der Standardwert ist 1:00 Uhr.
Stündliche Planung	Das Teilfenster 'Stündliche Planung' wird nur angezeigt, wenn Sie im Berichtsassistenten die Planungsoption **Stündlich** ausgewählt haben. Bei der stündlichen Planung werden automatisch alle Daten aus der vorherigen Stunde grafisch dargestellt.
Tägliche Planung	Das Teilfenster 'Tägliche Planung' wird nur angezeigt, wenn Sie im Berichtsassistenten die Planungsoption **Täglich** ausgewählt haben. Wählen Sie eine der folgenden Optionen aus: • **Alle Daten vom vorherigen Tag (24 Stunden)** • **Daten des vorherigen Tages von** - Wählen Sie in den Listen den gewünschten Zeitraum für den erstellten Bericht aus. Die Zeit kann in Halbstundenschritten angegeben werden. Der Standardwert ist 1:00 Uhr.

Tabelle 26. Verbindungsdiagrammparameter (Forts.)

Parameter	Beschreibung
Wöchentliche Planung	Das Teilfenster 'Wöchentliche Planung' wird nur angezeigt, wenn Sie im Berichtsassistenten die Planungsoption **Wöchentlich** ausgewählt haben. Wählen Sie eine der folgenden Optionen aus: • **Alle Daten aus vorheriger Woche** • **Alle Daten aus vorheriger Woche von** - Wählen Sie in den Listen den gewünschten Zeitraum für den erstellten Bericht aus. Die Standardeinstellung ist Sonntag.
Monatliche Planung	Das Teilfenster 'Monatliche Planung' wird nur angezeigt, wenn Sie im Berichtsassistenten die Planungsoption **Monatlich** ausgewählt haben. Wählen Sie eine der folgenden Optionen aus: • **Alle Daten aus vorherigem Monat** • **Daten des vorherige Monats von** - Wählen Sie in den Listen den gewünschten Zeitraum für den erstellten Bericht aus. Der Standardwert ist der 31. des Monats.
Grafikinhalt	
Gruppe	Wählen Sie in der Liste eine Gruppe für gespeicherte Suchvorgänge aus, um die gespeicherten Suchvorgänge anzuzeigen, die zu der Gruppe in der Liste **Verfügbare gespeicherte Suchvorgänge** gehören.
Gespeicherten Suchvorgang eingeben oder aus Liste auswählen	Sie können die Liste **Verfügbare gespeicherte Suchvorgänge** eingrenzen, indem Sie den Namen der gewünschten Suche im Feld **Gespeicherten Suchvorgang eingeben oder aus Liste auswählen** eingeben. Sie können auch ein Schlüsselwort eingeben, um eine Liste mit Suchvorgängen anzuzeigen, die das Schlüsselwort enthalten. Geben Sie beispielsweise `DMZ` ein, um eine Liste aller Suchvorgänge anzuzeigen, die DMZ im Suchnamen enthalten.
Verfügbare gespeicherte Suchvorgänge	Stellt eine Liste der verfügbaren gespeicherten Suchvorgänge bereit. Standardmäßig werden alle verfügbaren gespeicherten Suchvorgänge angezeigt. Sie können die Liste jedoch filtern, indem Sie eine Gruppe in der Liste **Gruppe** auswählen oder den Namen einer bekannten gespeicherten Suche im Feld **Gespeicherten Suchvorgang eingeben oder aus Liste auswählen** eingeben.
Neue Verbindungssuche erstellen	Klicken Sie auf **Neue Verbindungssuche erstellen**, um eine neue Suche zu erstellen.

Einheitenregeldiagramme

Sie können das Einheitenregeldiagramm verwenden, um Firewallregeln und den Ereigniszähler für in einem Netz ausgelöste Firewallregeln anzuzeigen.

Mithilfe von Einheitenregelberichten können Sie einen Bericht für folgende Firewallregeln erstellen:

- Aktivste Akzeptanzeinheitenregeln
- Aktivste Verweigerungseinheitenregeln
- Am wenigsten aktive Akzeptanzeinheitenregeln
- Am wenigsten aktive Verweigerungseinheitenregeln
- Nicht verwendete Einheitenregeln
- Schatteneinheitenregeln

Anhand der Berichte, die Sie erstellen, können Sie erkennen, welche Regeln für eine einzelne Einheit, einen bestimmten Adapter oder mehrere Einheiten akzeptiert, verweigert, nicht verwendet oder nicht ausgelöst werden. Berichte ermöglichen es QRadar Risk Manager, die Erstellung von Berichten über den Status der Einheitenregeln zu automatisieren und die Berichte an der QRadar SIEM-Konsole anzuzeigen.

Mithilfe dieser Funktionalität können Sie ermitteln, welche Regeln in den Netzeinheiten verwendet werden.

Um einen Container für ein Einheitenregeldiagramm zu erstellen, müssen Sie Werte für folgende Parameter konfigurieren:

Tabelle 27. Parameter für Einheitenregeldiagramm

Parameter	Beschreibung
Containerdetails - Einheitenregeln	
Regeln begrenzen auf wichtigste	Wählen Sie in der Liste die Anzahl der Regeln aus, die im erstellten Bericht angezeigt werden sollen. Wenn Sie den Bericht beispielsweise auf die zehn wichtigsten Regeln begrenzen, erstellen Sie einen Bericht für die am häufigsten verwendeten Akzeptanzregeln für alle Einheiten; der Bericht gibt zehn Ergebnisse zurück. Die Ergebnisse enthalten eine Liste der zehn am häufigsten verwendeten Akzeptanzregeln auf der Basis des Ereigniszählers für alle Einheiten, die für QRadar Risk Manager sichtbar sind.

Tabelle 27. Parameter für Einheitenregeldiagramm (Forts.)

Parameter	Beschreibung
Typ	Wählen Sie den Typ der Einheitenregeln aus, die im Bericht angezeigt werden sollen. Verfügbare Typen: • **Am häufigsten angewendete Akzeptanzregeln** - Zeigt die laut Ereigniszähler am häufigsten verwendeten Akzeptanzregeln für eine einzelne Einheit oder eine Gruppe von Einheiten an. Dieser Bericht listet in absteigender Reihenfolge die Regeln mit den höchsten Akzeptanzereigniszählern für den Zeitrahmen auf, den Sie im Bericht angegeben haben. • **Am häufigsten angewendete Verweigerungsregeln** - Zeigt die laut Ereigniszähler am häufigsten verwendeten Verweigerungsregeln für eine einzelne Einheit oder eine Gruppe von Einheiten an. Dieser Bericht listet in absteigender Reihenfolge die Regeln mit den höchsten Verweigerungsereigniszählern für den Zeitrahmen auf, den Sie im Bericht angegeben haben. • **Nicht angewendete Regeln** - Zeigt alle Regeln für eine einzelne Einheit oder eine Gruppe von Einheiten an, die nicht verwendet werden. Nicht verwendete Regeln haben Nullwert-Ereigniszähler für den Zeitrahmen, den Sie für den Bericht angegeben haben. • **Am wenigsten angewendete Akzeptanzregeln** - Zeigt die am wenigsten verwendeten Akzeptanzregeln für eine einzelne Einheit oder eine Gruppe von Einheiten an. Dieser Bericht listet in aufsteigender Reihenfolge die Regeln mit den niedrigsten Akzeptanzereigniszählern für den Zeitrahmen auf, den Sie im Bericht angegeben haben. • **Am wenigsten angewendete Verweigerungsregeln** - Zeigt die am wenigsten verwendeten Verweigerungsregeln für eine einzelne Einheit oder eine Gruppe von Einheiten an. Dieser Bericht listet in aufsteigender Reihenfolge die Regeln mit den niedrigsten Verweigerungsereigniszählern für den Zeitrahmen auf, den Sie im Bericht angegeben haben. • **Schattenregeln** - Zeigt alle Regeln für eine einzelne Einheit an, die niemals ausgelöst werden können, weil sie durch eine vorhergehende Regel blockiert werden. Die Ergebnisse zeigen eine Tabelle mit der Regel, die den Schatten bildet, und allen Regeln, die niemals in der Einheit ausgelöst werden können, weil sie von einer vorhergehenden Regel in der Einheit blockiert werden. **Anmerkung:** Berichte über Schattenregeln können nur für eine einzelne Einheit ausgeführt werden. Diese Regeln haben Nullwert-Ereigniszähler für den Zeitrahmen, den Sie für den Bericht angegeben haben, und sind in der Statusspalte durch ein Symbol gekennzeichnet.

Tabelle 27. Parameter für Einheitenregeldiagramm (Forts.)

Parameter	Beschreibung
Datum/Uhrzeit-Bereich	Wählen Sie den Zeitrahmen für den Bericht aus. Folgende Optionen sind verfügbar: • **Aktuelle Konfiguration** - Die Ergebnisse des Einheitenregelberichts basieren auf den Regeln, die in der aktuellen Einheitenkonfiguration vorhanden sind. Dieser Bericht zeigt Regeln und Ereigniszähler für die bestehende Einheitenkonfiguration an. Die aktuelle Konfiguration für eine Einheit basiert auf dem Zeitpunkt, an dem die Netzeinheit zum letzten Mal vom Configuration Source Management gesichert wurde. • **Intervall** - Die Ergebnisse des Einheitenregelberichts basieren auf den Regeln, die während des Zeitrahmens des Intervalls bestanden. Dieser Bericht zeigt Regeln und Ereigniszähler für das angegebene Intervall von der letzten Stunde bis zu 30 Tagen an. • **Bestimmter Bereich** - Die Ergebnisse des Einheitenregelberichts basieren auf den Regeln, die zwischen der Startzeit und der Endzeit des Zeitbereichs bestanden. Dieser Bericht zeigt Regeln und Ereigniszähler für den angegebenen Zeitrahmen an.
Zeitzone	Wählen Sie die Zeitzone aus, die als Basis für den Bericht verwenden werden soll. Die Standardzeitzone basiert auf der Konfiguration der QRadar SIEM-Konsole. Berücksichtigen Sie bei der Konfiguration der Zeitzonenparameter für den Bericht den Standort der Einheiten, die den Berichtsdaten zugeordnet sind. Wenn die Daten des Berichts mehrere Zeitzonen umfassen, basieren die für den Bericht verwendeten Daten auf dem spezifischen Zeitbereich der Zeitzone. Wenn die QRadar SIEM-Konsole beispielsweise für die Eastern Standard Time (EST) konfiguriert ist und Sie einen täglichen Bericht zwischen 13 und 15 Uhr planen und als Zeitzone die Central Standard Time (CST) festlegen, enthalten die Ergebnisse im Bericht Informationen aus der Zeit zwischen 14 und 16 Uhr EST.
Zieldatenauswahl	Die Zieldatenauswahl dient zur Filterung des Datum/Uhrzeit-Bereichs nach einem bestimmten Wert. Mithilfe der Zieldatenauswahloptionen können Sie einen Bericht erstellen, der Einheitenregeln für einen benutzerdefinierten Zeitraum anzeigt und in den optional nur Daten aus den Stunden und Tagen eingeschlossen sind, die Sie auswählen. Sie können beispielsweise einen Bericht planen, der vom 1. bis 31. Oktober ausgeführt werden soll und die aktivsten, am wenigsten aktiven oder nicht verwendeten Regeln, die während der Geschäftszeiten (z. B. Montag bis Freitag von 8 bis 21 Uhr) auftreten, und die zugehörigen Regelzähler anzeigt. **Anmerkung:** Die Filterdetails werden nur angezeigt, wenn Sie im Berichtsassistenten das Kontrollkästchen **Zieldatenauswahl** aktivieren.

Tabelle 27. Parameter für Einheitenregeldiagramm (Forts.)

Parameter	Beschreibung
Format	Wählen Sie das Format für den Einheitenregelbericht aus. Folgende Optionen sind verfügbar: • **Ein einziger Bericht für alle angegebenen Einheiten** - Dieses Berichtsformat fasst die Berichtsdaten für mehrere Einheiten zusammen. Wenn Sie beispielsweise einen Bericht erstellen, der die zehn am häufigsten verweigerten Regeln anzeigen soll, dann enthält ein Bericht dieses Formats die zehn am häufigsten verweigerten Regeln für alle Einheiten, die Sie für den Bericht ausgewählt haben. Dieser Bericht gibt insgesamt zehn Ergebnisse für den Bericht zurück. • **Ein Bericht pro Einheit** - Dieses Berichtsformat zeigt die Berichtsdaten für eine einzige Einheit an. Wenn Sie beispielsweise einen Bericht erstellen, der die zehn am häufigsten verweigerten Regeln anzeigen soll, dann enthält ein Bericht dieses Formats die zehn am häufigsten verweigerten Regeln für jede einzelne Einheit, die Sie für den Bericht ausgewählt haben. Dieser Bericht gibt die zehn wichtigsten Ergebnisse für jede für den Bericht ausgewählte Einheit zurück. Wenn Sie fünf Einheiten ausgewählt haben, enthält der Bericht fünfzig Ergebnisse. **Anmerkung:** In Schattenregelberichten kann nur ein Bericht pro Einheit angezeigt werden.

Tabelle 27. Parameter für Einheitenregeldiagramm (Forts.)

Parameter	Beschreibung
Einheiten	Wählen Sie die Einheiten aus, die in den Bericht eingeschlossen werden sollen. Folgende Optionen sind verfügbar: • **Alle Einheiten** - Wählen Sie diese Option aus, um alle Einheiten in QRadar Risk Manager in den Bericht einzuschließen. • **Adapter** - Wählen Sie in der Liste einen Adaptertyp aus, der in den Bericht eingeschlossen werden soll. Es kann für einen Bericht nur ein einziger Adaptertyp in der Liste ausgewählt werden. • **Bestimmte Einheiten** - Wählen Sie diese Option aus, um nur bestimmte Einheiten in den Bericht einzuschließen. Sie können im Einheitenauswahlfenster Einheiten auswählen und zum Bericht hinzufügen. So fügen Sie einzelne Einheiten zum Bericht hinzu: 1. Klicken Sie auf **Durchsuchen**, um das Einheitenauswahlfenster zu öffnen. 2. Wählen Sie Einheiten aus und klicken Sie auf **Ausgewählte hinzufügen**. So fügen Sie alle Einheiten zum Bericht hinzu: 1. Klicken Sie auf **Durchsuchen**, um das Einheitenauswahlfenster zu öffnen. 2. Klicken Sie auf **Alle hinzufügen**. So suchen Sie nach Einheiten, um sie in den Bericht einzuschließen: 1. Klicken Sie auf **Durchsuchen**, um das Einheitenauswahlfenster zu öffnen. 2. Klicken Sie auf **Suchen**. 3. Wählen Sie die Suchoptionen aus, um die vollständige Einheitenliste nach abgerufener Konfiguration, IP- oder CIDR-Adresse, Hostname, Typ, Adapter, Hersteller oder Modell zu filtern. 4. Klicken Sie auf **Suchen**. 5. Wählen Sie Einheiten aus und klicken Sie auf **Ausgewählte hinzufügen**.

Diagramme für nicht verwendete Objekte einer Einheit

Ein Bericht über nicht verwendete Objekte einer Einheit zeigt Objektreferenzgruppen an, die von einer Netzeinheit nicht verwendet werden.

Dieser Bericht zeigt Objektreferenzen an, z. B. eine Zusammenstellung von IP-Adressen, CIDR-Adressbereichen oder Hostnamen, die von einer Netzeinheit nicht verwendet werden.

Wenn Sie einen Container für nicht verwendete Objekte einer Einheit konfigurieren, müssen Sie Werte für folgende Parameter konfigurieren:

Tabelle 28. Parameter für Bericht über nicht verwendete Objekte einer Einheit

Parameter	Beschreibung
Containerdetails - Nicht verwendete Objekte einer Einheit	
Objekte begrenzen auf wichtigste	Wählen Sie in der Liste die Anzahl der Objekte aus, die im erstellten Bericht angezeigt werden sollen.
Einheiten	Wählen Sie die Einheiten aus, die in den Bericht eingeschlossen werden sollen. Folgende Optionen sind verfügbar: • **Alle Einheiten** - Wählen Sie diese Option aus, um alle Einheiten in QRadar Risk Manager in den Bericht einzuschließen. • **Adapter** - Wählen Sie in der Liste einen Adaptertyp aus, der in den Bericht eingeschlossen werden soll. Es kann für einen Bericht nur ein einziger Adaptertyp in der Liste ausgewählt werden. • **Bestimmte Einheiten** - Wählen Sie diese Option aus, um nur bestimmte Einheiten in den Bericht einzuschließen. Sie können im Einheitenauswahlfenster Einheiten auswählen und zum Bericht hinzufügen. So fügen Sie einzelne Einheiten zum Bericht hinzu: 1. Klicken Sie auf **Durchsuchen**, um das Einheitenauswahlfenster zu öffnen. 2. Wählen Sie Einheiten aus und klicken Sie auf **Ausgewählte hinzufügen**. So fügen Sie alle Einheiten zum Bericht hinzu: 1. Klicken Sie auf **Durchsuchen**, um das Einheitenauswahlfenster zu öffnen. 2. Klicken Sie auf **Alle hinzufügen**. So suchen Sie nach Einheiten, um sie in den Bericht einzuschließen: 1. Klicken Sie auf **Durchsuchen**, um das Einheitenauswahlfenster zu öffnen. 2. Klicken Sie auf **Suchen**. 3. Wählen Sie die Suchoptionen aus, um die vollständige Einheitenliste nach abgerufener Konfiguration, IP- oder CIDR-Adresse, Hostname, Typ, Adapter, Hersteller oder Modell zu filtern. 4. Klicken Sie auf **Suchen**. 5. Wählen Sie Einheiten aus und klicken Sie auf **Ausgewählte hinzufügen**.

Kapitel 10. Simulationen in QRadar Risk Manager verwenden

Verwenden Sie Simulationen, um Exploit-Simulationen zu definieren, zu planen und im Netz durchzuführen. Sie können Simulationen erstellen, anzeigen, bearbeiten, duplizieren, und löschen.

Sie können Simulationen erstellen, die auf einer Folge von Regeln basieren, die kombiniert und konfiguriert werden können. Die Simulation kann für eine regelmäßige Ausführung geplant oder manuell ausgeführt werden. Nach Abschluss einer Simulation können Sie die Ergebnisse der Simulation prüfen und jedes Ergebnis mit annehmbarem oder geringem Risiko, das auf Ihrer Netzrichtlinie basiert, genehmigen. Bei der Prüfung von Ergebnissen können Sie annehmbare Aktionen oder Datenverkehr abhängig von den Ergebnissen genehmigen. Nachdem Sie die Simulation optimiert haben, können Sie die Simulation für eine Überwachung der Ergebnisse konfigurieren.

Bei der Überwachung einer Simulation können Sie festlegen, wie das System antworten soll, wenn nicht genehmigte Ergebnisse zurückgegeben werden. Eine Systemantwort kann eine E-Mail, die Erstellung eines Ereignisses oder das Senden der Antwort an das Systemprotokoll (syslog) sein.

Simulationen können aus einer aktuellen Topologie oder einem Topologiemodell modelliert werden.

Die Seite **Simulation** enthält eine Zusammenfassung aller Informationen zu Simulationen und Simulationsergebnissen.

Simulationsergebnisse werden nur nach erfolgreicher Ausführung einer Simulation angezeigt. Nach Abschluss einer Simulation werden in der Spalte **Ergebnisse** die Termine und die jeweiligen Ergebnisse der Simulation angezeigt.

Simulationen

Von Benutzern erstellte Simulationen und Simulationsergebnisse können auf der Simulationsseite angezeigt werden.

Das Simulationsfenster stellt folgende Informationen bereit:

Tabelle 29. Parameter für Simulationsdefinitionen

Parameter	Beschreibung
Simulationsname	Der Name der Simulation, wie vom Ersteller der Simulation definiert.
Modell	Der Modelltyp. Simulationen können aus einer aktuellen Topologie oder einem Topologiemodell modelliert werden. Verfügbare Optionen: • Aktuelle Topologie • Der Name des Topologiemodells.
Gruppen	Die Gruppen, denen die Simulation zugeordnet ist.
Erstellt von	Der Benutzer, der die Simulation erstellt hat.

Tabelle 29. Parameter für Simulationsdefinitionen (Forts.)

Parameter	Beschreibung
Erstellungsdatum	Der Zeitpunkt (Datum und Uhrzeit), an dem die Simulation erstellt wurde.
Letzte Änderung	Der Zeitpunkt (Datum und Uhrzeit), an dem die Simulation zuletzt geändert wurde.
Zeitplan	Gibt an, wie oft die Simulation ausgeführt werden soll. Folgende Optionen sind verfügbar: • **Manuell** - Die Simulation muss manuell ausgeführt werden. • **Einmal** - Geben Sie Datum und Uhrzeit der geplanten Ausführung der Simulation an. • **Täglich** - Geben Sie die Tageszeit für die geplante Ausführung der Simulation an. • **Wöchentlich** - Geben Sie den Wochentag und die Uhrzeit für die geplante Ausführung der Simulation an. • **Monatlich** - Geben Sie den Tag des Monats und die Uhrzeit für die geplante Ausführung der Simulation an.
Letzte Ausführung	Datum und Uhrzeit der letzten Ausführung der Simulation.
Nächste Ausführung	Datum und Uhrzeit der nächsten Ausführung der Simulation.
Ergebnisse	Nachdem die Simulation ausgeführt wurde, schließt dieser Parameter eine Liste ein, die eine Liste der Termine mit den Ergebnissen der Simulation enthält. Wenn die Simulation nicht ausgeführt wurde, wird in der Spalte für Ergebnisse 'Keine Ergebnisse' angezeigt.

Simulation erstellen

Sie können Simulationen erstellen, die auf eine Reihe von Regeln basiert werden, welche verbunden und konfiguriert werden können.

Informationen zu diesem Vorgang

Parameter, die für Simulationstests konfiguriert werden können, sind unterstrichen. In der folgenden Tabelle sind die Simulationstests beschrieben, die Sie konfigurieren können.

Tabelle 30. Simulationstests

Testname	Beschreibung	Parameter
Attack targets one of the following IP addresses (Attacke zielt auf eine der folgenden IP-Adressen)	Simuliert Attacken auf bestimmte IP-Adressen oder CIDR-Bereiche.	Konfigurieren Sie den Parameter für die IP-Adressen, um die IP-Adresse oder den CIDR-Bereich anzugeben, für den Sie diese Simulation anwenden möchten.

Tabelle 30. Simulationstests (Forts.)

Testname	Beschreibung	Parameter
Attack targets one of the following networks (Attacke zielt auf eines der folgenden Netze)	Simuliert Attacken auf Netze, die Mitglied bei mindestens einer definierten Netzadresse sind.	Konfigurieren Sie die Netzparameter, um Netze anzugeben, für die Sie diese Simulation anwenden möchten.
Attack targets one of the following asset building blocks (Attacke zielt auf die folgenden Asset-Bausteine)	Simuliert Attacken auf mindestens einen definierten Asset-Baustein.	Konfigurieren Sie die Parameter für die Asset-Bausteine, um die Asset-Bausteine anzugeben, für die Sie diese Simulation anwenden möchten.
Attack targets one of the following reference sets (Attacke zielt auf eines der folgenden Referenzsets)	Simuliert Attacken, die auf mindestens ein definiertes Referenzset zielen.	Konfigurieren Sie Parameter für die Referenzsets, um die Referenzsets anzugeben, für die Sie diese Simulation anwenden möchten.
Attack targets a vulnerability on one of the following ports using protocols (Attacke zielt auf eine Schwachstelle auf einem der folgenden Ports mithilfe von Protokollen)	Simuliert Attacken, die auf eine Schwachstelle in mindestens einem definierten Port zielen.	Konfigurieren Sie die folgenden Parameter: • Offene Ports - Geben Sie die Ports an, die in dieser Simulation berücksichtigt werden sollen. • Protokolle - Geben Sie das Protokoll an, das in dieser Simulation berücksichtigt werden soll.
Attack targets assets susceptible to one of the following vulnerabilities (Attacke zielt auf Assets, die in einer der folgenden Schwachstellen anfällig sind)	Simuliert Attacken, die auf Assets zielen, die in mindestens einer definierten Schwachstelle anfällig sind.	Konfigurieren Sie den Parameter **Schwachstellen**, um die Schwachstellen zu ermitteln, die für diesen Test angewendet werden sollen. Sie können in OSVDB-ID, Bugtraq-ID, CVE-ID oder im Titel nach Schwachstellen suchen.
Attack targets assets susceptible to vulnerabilities with one of the following classifications (Attacke zielt auf Assets, die in Schwachstellen mit einer der folgenden Klassifizierungen anfällig sind)	Ermöglicht das Simulieren von Attacken, die auf ein Asset zielen, das in Schwachstellen für mindestens eine definierte Klassifizierung anfällig ist.	Konfigurieren Sie den Parameter **classifications** (Klassifizierungen), um die Klassifizierungen von Schwachstellen zu ermitteln. Die Klassifizierung einer Schwachstelle kann beispielsweise 'Input Manipulation' (Manipulation bei der Eingabe) oder 'Denial of Service' (Verweigerung eines Service) sein.

Tabelle 30. Simulationstests (Forts.)

Testname	Beschreibung	Parameter
Attack targets assets susceptible to vulnerabilities with CVSS score greater than 5 (Attacke zielt auf Assets, die anfällig für Schwachstellen mit einer CVSS-Bewertung größer als 5 sind)	Bei einem CVSS-Wert (Common Vulnerability Scoring System) handelt es sich um einen Industriestandard zur Bewertung des Schweregrads von Schwachstellen. Diese Simulation filtert Assets in Ihrem Netz, die den konfigurierten CVSS-Wert enthalten. Ermöglicht Ihnen das Simulieren von Attacken, die auf ein Asset zielen, das für Schwachstellen mit einer CVSS-Bewertung größer als 5 anfällig ist.	Konfigurieren Sie die folgenden Parameter: • **Größer als** - Geben Sie an, ob die CVSS-Bewertung in Bezug auf den konfigurierten Wert größer als, größer-gleich, kleiner als, kleiner-gleich, gleich oder ungleich ist. Der Standardwert ist 'größer als'. • **5** - Geben Sie die CVSS-Bewertung an, die von diesem Test berücksichtigt werden soll. Der Standardwert ist 5.
Attack targets assets susceptible to vulnerabilities disclosed after this date (Attacke zielt auf Assets, die für Schwachstellen anfällig sind, die nach diesem Datum bekanntgegeben wurden)	Ermöglicht Ihnen das Simulieren von Attacken, die auf ein Asset zielen, das für Schwachstellen anfällig ist, die vor, nach oder an dem Datum der Konfiguration ermittelt wurden.	Konfigurieren Sie die folgenden Parameter: • **vor** | **nach** | **am** - Geben Sie an, ob die Simulation die bekanntgegebenen Schwachstellen auf Assets nach, vor oder an dem Datum der Konfiguration berücksichtigen soll. Die Standardeinstellung ist 'vor'. • **this date** (dieses Datum) - Geben Sie das Datum an, das von dieser Simulation berücksichtigt werden soll.
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following text entries (Attacke zielt auf Assets, die für Schwachstellen anfällig sind, in denen der Name, Anbieter, die Version oder der Service einen der folgenden Texteinträge enthält)	Ermöglicht Ihnen das Simulieren von Attacken, die auf ein Asset zielen, das für Schwachstellen anfällig ist, die mit dem Namen, Anbieter, der Version oder dem Service des Assets in mindestens einem Texteintrag übereinstimmen.	Konfigurieren Sie den Parameter **text entries** (Texteinträge), um den Namen, Anbieter, die Version oder den Service des Assets zu ermitteln, die von dieser Simulation berücksichtigt werden sollen.

Tabelle 30. Simulationstests (Forts.)

Testname	Beschreibung	Parameter
Attack targets assets susceptible to vulnerabilities where the name, vendor, version or service contains one of the following regular expressions (Attacke zielt auf Assets, die für Schwachstellen anfällig sind, in denen der Name, Anbieter, die Version oder der Service einen der folgenden regulären Ausdrücke enthält)	Ermöglicht Ihnen das Simulieren von Attacken, die auf ein Asset zielen, das für Schwachstellen anfällig ist, die mit dem Namen, Anbieter, der Version oder dem Service des Assets in mindestens einem regulären Ausdruck übereinstimmen.	Konfigurieren Sie den Parameter **regular expressions** (reguläre Ausdrücke), um den Namen, Anbieter, die Version oder den Service des Assets zu ermitteln, die von dieser Simulation berücksichtigt werden sollen.

Die folgenden beitragenden Tests sind veraltet und werden in der Richtlinienüberwachung ausgeblendet:

- **attack targets a vulnerability on one of the following operating systems** (Attacke zielt auf eine Schwachstelle in einem der folgenden Betriebssysteme)
- **attack targets assets susceptible to vulnerabilities from one of the following vendors** (Attacke zielt auf Assets, die für Schwachstellen von einem der folgenden Anbieter anfällig sind)
- **attack targets assets susceptible to vulnerabilities from one of the following products** (Attacke zielt auf Assets, die für Schwachstellen in einem der folgenden Produkte anfällig sind)

Die veralteten beitragenden Tests wurden durch andere Tests ersetzt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie im Menü **Aktionen** die Option **Neu** aus.
4. Geben Sie im Parameter **What do you want to name this simulation** (Welche Bezeichnung soll diese Simulation haben) einen Namen für die Simulation ein.
5. Wählen Sie in der Dropdown-Liste **Which model do you want to base this on** (Welches Modell soll als Basis dienen) den Datentyp aus, der zurückgegeben werden soll. Es werden alle vorhandenen Topologiemodelle aufgelistet. Wenn Sie Aktuelle Topologie auswählen, verwendet die Simulation das aktuelle Topologiemodell.
6. Wählen Sie eine der folgenden Optionen aus:

Option	Bezeichnung
Select Use Connection Data ('Verbindungsdaten verwenden' auswählen)	Die Simulation basiert auf Verbindungs- und Topologiedaten.
Clear Use Connection Data ('Verbindungsdaten verwenden' abwählen)	Die Simulation basiert ausschließlich auf Topologiedaten. Wenn Ihr Topologiemodell keine Daten einschließt und Sie die Auswahl des Kontrollkästchens **Use Connection Data** aufheben, gibt die Simulation keine Ergebnisse zurück.

7. Wählen Sie in der Liste **Wichtigkeitsfaktor** die Bewertungsstufe aus, die dieser Simulation zugeordnet werden soll.

   Mit dem Wichtigkeitsfaktor wird die Risikobewertung berechnet. Der Wert liegt zwischen 1 (geringe Wichtigkeit) und 10 (hohe Wichtigkeit). Der Standardwert ist 5.
8. Wählen Sie in der Liste **Where do you want the simulation to begin** (Wo soll die Simulation beginnen) einen Ursprung für die Simulation aus.

   Der ausgewählte Wert ermittelt den Ausgangspunkt der Simulation. Beispielsweise entsteht die Attacke in einem bestimmten Netz. Die ausgewählten Simulationsparameter werden im Fenster **Generate a simulation where** (Simulation an welcher Stelle generieren) angezeigt.
9. Fügen Sie dem Simulationstest Ziele für die Attacke der Simulation hinzu.
10. Wählen Sie im Feld 'Which simulations do you want to include in the attack' (Welche Simulationen sollen in der Attacke enthalten sein) das Pluszeichen (+) neben der Simulation ein, die Sie einschließen möchten.

    Die Simulationsoptionen werden im Fenster **Generate a simulation where** angezeigt.
11. Klicken Sie im Fenster **Generate a simulation where** auf einen beliebigen unterstrichenen Parameter, um die Simulationsparameter weiter zu konfigurieren.
12. Wählen Sie in der Dropdown-Liste **Run this simulation for** (Diese Simulation ausführen für) die Anzahl der Schritte aus, die diese Simulation durchlaufen soll (1 bis 5).
13. Wählen Sie in der Dropdown-Liste mit den Schritten den Zeitplan für die Ausführung der Simulation aus.
14. Wählen Sie im Gruppenbereich ein Kontrollkästchen für jede Gruppe aus, der Sie diese Simulation zuweisen möchten.
15. Klicken Sie auf **Save Simulation** (Simulation speichern).

Simulation bearbeiten

Sie können Simulationen bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie die Simulationsdefinition aus, die Sie bearbeiten möchten.
4. Wählen Sie im Menü **Aktionen** die Option **Bearbeiten** aus.
5. Aktualisieren Sie bei Bedarf die Parameter.

   Weitere Informationen zu den Simulationsparametern finden Sie im Abschnitt Simulationstests.
6. Klicken Sie auf **Save Simulation** (Simulation speichern).

Simulation duplizieren

Sie können Simulationen duplizieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie die Simulation aus, die Sie duplizieren möchten.

4. Wählen Sie im Menü **Aktionen** die Option **Duplikat** aus.
5. Geben Sie den Namen für die Simulation ein.
6. Klicken Sie auf **OK**.

Simulation löschen

Sie können Simulationen löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie die Simulation aus, die Sie löschen möchten.
4. Wählen Sie im Menü **Aktionen** die Option **Löschen** aus.
5. Klicken Sie auf **OK**.

Simulation manuell ausführen

Mit dem Simulationseditor können Sie eine Simulation manuell ausführen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Menü **Aktionen** die Option **Run Simulation** (Simulation ausführen) aus.
3. Klicken Sie auf **OK**.

Ergebnisse

Der Simulationsprozess kann einige Zeit in Anspruch nehmen. Während der Ausführung der Simulation wird in der Spalte 'Next Run' (Nächste Ausführung) der Prozentsatz angezeigt, der bereits abgeschlossen ist. Wenn die Ausführung beendet wurde, werden in der Spalte 'Ergebnisse' das Datum und die Uhrzeit der Simulation angezeigt.

Wenn Sie eine Simulation ausführen und anschließend Änderungen vornehmen, die sich auf die dieser Simulation zugeordneten Tests auswirken, werden diese Änderungen möglicherweise erst nach einer Stunde angezeigt.

Simulationsergebnisse verwalten

Nach der Ausführung der Simulation wird in der Spalte 'Ergebnisse' eine Dropdown-Liste angezeigt, in der das Datum angegeben ist, an dem die Simulation generiert wurde.

Simulationsergebnisse werden 30 Tage gespeichert. Die Ergebnisse werden in der Spalte 'Ergebnisse' nur nach dem Ausführen einer Simulation angezeigt.

Simulationsergebnisse anzeigen

Sie können Simulationsergebnisse auf der Seite 'Simulationen' in der Spalte 'Ergebnisse' anzeigen.

Informationen zu diesem Vorgang

Die Ergebnisse werden in der Spalte 'Ergebnisse' nur nach der Ausführung einer Simulation angezeigt. Simulationsergebnisse stellen Informationen zu jedem Schritt der Simulation bereit.

Beispielsweise wird durch den ersten Schritt einer Simulation eine Liste der direkt verbundenen Assets bereitgestellt, die von der Simulation betroffen sind. Im zweiten Schritt werden Assets in Ihrem Netz aufgeführt, die mit den Assets der ersten Stufe in Ihrer Simulation kommunizieren können.

Wenn Sie auf 'Ergebnis anzeigen' klicken, werden die folgenden Informationen bereitgestellt:

Tabelle 31. Informationen zum Simulationsergebnis

Parameter	Beschreibung
Simulation Definition (Simulationsdefinition)	Die Beschreibung der Simulation.
Using Model (Modell verwenden)	Der Name des Modells, auf dem die Simulation ausgeführt wurde.
Simulation Result (Simulationsergebnis)	Das Datum, an dem die Simulation ausgeführt wurde.
Step Results (Schrittergebnis)	Die Anzahl der Schritte für das Ergebnis, einschließlich des Schritts, der aktuell angezeigt wird.
Assets Compromised (Beeinträchtigte Assets)	Die Anzahl aller Assets, die in diesem Schritt und in allen Simulationsschritten beeinträchtigt sind. Wenn das Topologiemodell Daten aus dem IP-Bereich /32 enthält, die als erreichbar definiert sind, prüft QRadar Risk Manager diese Assets nicht für die Datenbank. Deshalb werden diese Assets im Gesamtergebnis der beeinträchtigten Assets nicht berücksichtigt. QRadar Risk Manager prüft nur Assets in umfassenderen IP-Bereichen (z. B. /24), um zu ermitteln, welche Assets vorhanden sind.
Risk Score (Risikobewertung)	Bei der Risikobewertung handelt es sich um einen Wert, der auf Basis der Anzahl der Ergebnisse und Schritte, der Anzahl der beeinträchtigten Assets und des der Simulation zugeordneten Wichtigkeitsfaktors berechnet wird. Dieser Wert zeigt die Bewertungsstufe an, die der Simulation für den angezeigten Schritt zugeordnet wird.

Sie können Ihren Mauszeiger auf eine Verbindung bewegen, um die an dieser Simulation beteiligten Assets zu ermitteln.

Die 10 häufigsten Assets werden angezeigt, wenn Sie Ihren Mauszeiger über die Verbindung bewegen.

Bewegen Sie Ihren Mauszeiger über die Verbindung, um den Pfad im Netz wie vom Teilnetz definiert anzuzeigen.

Auf der Seite mit den Simulationsergebnissen wird eine Tabelle mit der Bezeichnung 'Results for this step' (Ergebnisse in diesem Schritt) bereitgestellt. Diese Tabelle enthält die folgenden Informationen:

Tabelle 32. Informationen in der Tabelle 'Results for this step'

Parameter	Beschreibung
Genehmigen	Ermöglicht Ihnen das Freigeben der Simulationsergebnisse. Siehe Simulationsergebnisse genehmigen.
Übergeordnet	Die ursprüngliche IP-Adresse für den angezeigten Schritt der Simulation.
IP	Die IP-Adresse des beteiligten Assets.
Netz	Das Netz der Ziel-IP-Adresse gemäß der Definition in der Netzhierarchie.
Assetname	Der Name des beteiligten Assets gemäß der Definition im Assetprofil.
Assetgewichtung	Die Gewichtung des beteiligten Assets gemäß der Definition im Assetprofil.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie in der Spalte 'Ergebnisse' das Datum und die Uhrzeit der Simulation aus, die mithilfe der Liste angezeigt werden soll.
4. Klicken Sie auf **View Result** (Ergebnis anzeigen). Sie können Informationen zu den Simulationsergebnissen anzeigen und dabei in Schritt 1 der Simulation beginnen.
5. Zeigen Sie die Tabelle 'Results for this Step' an, um die beteiligten Assets zu ermitteln.
6. Um den nächsten Schritt der Simulationsergebnisse anzuzeigen, klicken Sie auf **Next Step** (Nächster Schritt).

Simulationsergebnisse genehmigen

Sie können Simulationsergebnisse genehmigen.

Informationen zu diesem Vorgang

Sie können im Asset Netzverkehr, der mit niedrigem Risiko eingestuft wird, oder normale Kommunikation genehmigen. Beim Genehmigen von Ergebnissen filtern Sie das Ergebnis so, dass zukünftige Simulationen die normale oder genehmigte Kommunikation ignorieren.

Die Ergebnisse werden in der Spalte 'Ergebnisse' nur nach der Ausführung einer Simulation angezeigt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie in der Spalte 'Ergebnisse' das Datum und die Uhrzeit der Simulation aus, die mithilfe der Liste angezeigt werden soll.
4. Klicken Sie auf **View Result** (Ergebnis anzeigen).

5. Genehmigen Sie Assets in der Tabelle 'Ergebnisse' mit einer der folgenden Methoden:

Option	Beschreibung
Markierte genehmigen	Aktivieren Sie das Kontrollkästchen für jedes Asset, das Sie genehmigen möchten, und klicken Sie anschließend auf **Markierte genehmigen**.
Alle genehmigen	Klicken Sie hier, um alle aufgeführten Assets zu genehmigen.

6. Optional. Klicken Sie auf **View Approved** (Genehmigte anzeigen), um alle genehmigten Assets anzuzeigen.

Genehmigung einer Simulation widerrufen

Sie können eine genehmigte Verbindung oder Datenübertragung aus der genehmigten Liste entfernen. Nachdem ein genehmigtes Ergebnis für die Simulation entfernt wurde, werden in künftigen Simulationen nicht genehmigte Datenübertragungen in den Simulationsergebnissen angezeigt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie in der Spalte 'Ergebnisse' das Datum und die Uhrzeit der Simulation aus, die mithilfe der Liste angezeigt werden soll.
4. **View Result** (Ergebnis anzeigen).
5. Klicken Sie auf **View Approved** (Genehmigte anzeigen), um alle genehmigten Assets anzuzeigen.
6. Wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Revoke Selected (Ausgewählte widerrufen)	Aktivieren Sie das Kontrollkästchen für jedes Asset, das Sie widerrufen möchten, und klicken Sie anschließend auf **Revoke Selected** (Ausgewählte widerrufen).
Revoke All (Alle widerrufen)	Klicken Sie hier, um alle aufgeführten Assets zu widerrufen.

Simulationen überwachen

Sie können eine Simulation überwachen, um zu ermitteln, ob sich die Ergebnisse der Simulation geändert haben. Beim Auftreten einer Änderung wird ein Ereignis generiert. Es können sich maximal 10 Simulationen im Überwachungsmodus befinden.

Informationen zu diesem Vorgang

Bei einer Simulation im Überwachungsmodus liegt der standardmäßige Zeitbereich bei 1 Stunde. Dieser Wert überschreibt den konfigurierten Zeitwert, wenn die Simulation erstellt wird.

Weitere Informationen zu Ereigniskategorien finden Sie im Handbuch *IBM Security QRadar SIEM Users Guide*.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie die Simulation aus, die Sie überwachen möchten.
4. Klicken Sie auf **Überwachen**.
5. Geben Sie im Feld **Ereignisname** den Namen des Ereignisses ein, das in den Registerkarten **Protokollaktivität** und **Angriffe** angezeigt werden soll.
6. Geben Sie im Feld **Ereignisbeschreibung** eine Beschreibung für das Ereignis ein. Die Beschreibung wird in den Anmerkungen zu den Ereignisdetails angezeigt.
7. Wählen Sie in der Liste **Übergeordnete Kategorie** die übergeordnete Ereigniskategorie aus, die in dieser Simulation bei der Verarbeitung von Ereignissen verwendet werden soll.
8. Wählen Sie in der Liste **Untergeordnete Kategorie** die untergeordnete Ereigniskategorie aus, die in dieser Simulation bei der Verarbeitung von Ereignissen verwendet werden soll.
9. Aktivieren Sie das Kontrollkästchen **Stellen Sie sicher, dass das gesendete Ereignis Teil eines Angriffs ist**, wenn die Ereignisse als Ergebnis dieser überwachten Simulation an die Komponente 'Magistrat' weitergeleitet werden sollen. Falls kein Angriff generiert wurde, wird ein neuer Angriff erstellt. Wenn ein Angriff vorhanden ist, wird dieses Ereignis dem vorhandenen Angriff hinzugefügt. Wenn Sie das Kontrollkästchen aktivieren, wählen Sie eine der folgenden Optionen aus:

Option	Beschreibung
Question/Simulation (Frage/Simulation)	Alle Ereignisse aus einer Frage werden einem einzelnen Angriff zugeordnet.
Asset	Für jedes eindeutige Asset wird ein eindeutiger Angriff erstellt (oder aktualisiert).

10. Wählen Sie im Abschnitt **Weitere Aktionen** mindestens eine der folgenden Optionen aus:

Option	Beschreibung
E-Mail	Wählen Sie dieses Kontrollkästchen aus und geben Sie die E-Mail-Adresse an, an die beim Generieren des Ereignisses Benachrichtigungen gesendet werden sollen. Trennen Sie mehrere E-Mail-Adressen mit einem Komma.
An Systemprotokoll senden	Aktivieren Sie dieses Kontrollkästchen, wenn das Ereignis protokolliert werden soll. Die Ausgabe des Systemprotokoll kann beispielsweise folgendermaßen aussehen: `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule'Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name:SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Eventdescription`
Benachrichtigen	Aktivieren Sie dieses Kontrollkästchen, wenn Ereignisse, die als Ergebnis dieser überwachten Frage generiert werden, im Element 'Systembenachrichtigungen' im Dashboard angezeigt werden sollen.

11. Wählen Sie im Abschnitt **Enable Monitor** (Überwachung aktivieren) das Kontrollkästchen aus, um die Simulation zu überwachen.
12. Klicken Sie auf **Save Monitor** (Überwachung speichern).

Simulationen gruppieren

Das Zuweisen von Simulationen zu Gruppen ist eine effiziente Möglichkeit, alle Simulationen anzuzeigen und zu überwachen. Sie können beispielsweise alle Simulationen anzeigen, die sich auf die Konformität beziehen.

Informationen zu diesem Vorgang

Beim Erstellen neuer Simulationen können Sie die Simulationen einer vorhandenen Gruppe zuweisen.

Nach dem Erstellen einer Gruppe können Sie Gruppen in die Menübaumstruktur ziehen, um die Organisation zu ändern.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe aus, unter der Sie eine neue Gruppe erstellen wollen.
5. Klicken Sie auf **Neu**.
6. Geben Sie im Feld **Name** einen Namen für die neue Gruppe ein. Der Gruppenname kann bis zu 255 Zeichen lang sein.
7. Geben Sie im Feld **Beschreibung** eine Beschreibung für die Gruppe ein. Die Beschreibung kann bis zu 255 Zeichen lang sein.
8. Klicken Sie auf **OK**.

Gruppe bearbeiten

Sie können eine Gruppe bearbeiten.

Informationen zu diesem Vorgang

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe aus, die Sie bearbeiten wollen.
5. Klicken Sie auf **Bearbeiten**.
6. Bearbeiten Sie gegebenenfalls die Felder für Namen und Beschreibung.
7. Klicken Sie auf **OK**.

Element in eine andere Gruppe kopieren

Mit der Gruppenfunktion können Sie eine Simulation in eine oder mehrere Gruppen kopieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Frage aus, die Sie in eine andere Gruppe kopieren wollen.
5. Klicken Sie auf **Kopieren**.
6. Wählen Sie das Kontrollkästchen für die Gruppe aus, in die Sie die Simulation kopieren möchten.
7. Klicken Sie auf **Kopieren**.

Element aus einer Gruppe löschen

Sie können ein Element aus einer Gruppe löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe der höchsten Ebene aus.
5. Wählen Sie aus der Liste der Gruppen das Element oder die Gruppe aus, das bzw. die Sie löschen wollen.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **OK**.

Element einer Gruppe zuweisen

Sie können eine Simulation einer Gruppe zuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie die Simulation aus, die Sie einer Gruppe zuweisen wollen.
4. Wählen Sie im Menü **Aktionen** die Option **Gruppen zuweisen** aus.
5. Wählen Sie die Gruppe aus, der die Frage zugeordnet werden soll.
6. Klicken Sie auf **Gruppen zuweisen**.

Kapitel 11. Topologiemodelle

Mithilfe eines Topologiemodells können virtuelle Netzmodelle auf Basis des vorhandenen Netzes definiert werden.

Sie können ein Netzmodell auf Basis einer Folge von Änderungen erstellen, die kombiniert und konfiguriert werden können. Dies gibt Ihnen die Möglichkeit, mithilfe einer Simulation die Auswirkungen von Konfigurationsänderungen auf das Netz festzustellen. Weitere Informationen zu Simulationen finden Sie im Abschnitt Simulationen verwenden.

Topologiemodelle können auf der Simulationsseite angezeigt werden. Die Topologiemodelle stellen folgende Informationen bereit:

Tabelle 33. Parameter für Modelldefinitionen

Parameter	Beschreibung
Modellname	Der Name des Topologiemodells, wie bei der Erstellung vom Benutzer definiert.
Gruppe(n)	Die Gruppen, denen diese Topologie zugeordnet ist.
Erstellt von	Der Benutzer, der die Modelldefinition erstellt hat.
Erstellt am	Der Zeitpunkt (Datum und Uhrzeit), an dem die Modelldefinition erstellt wurde.
Letzte Änderung	Die Anzahl Tage, die seit der Erstellung der Modelldefinition vergangen sind.

Topologiemodell erstellen

Sie können ein oder mehrere Topologiemodelle erstellen.

Informationen zu diesem Vorgang

In der folgenden Tabelle werden die Testnamen und Parameter beschrieben, die Sie konfigurieren können.

Tabelle 34. Topologietests

Testname	Parameter
A rule is added to the selected devices that allows connections from source CIDRs to destination CIDRs on protocols, ports (Den ausgewählten Einheiten wird eine Regel hinzugefügt, mit der Verbindungen aus Quellen-CIDRs zu Ziel-CIDRs auf Protokollen, Ports möglich sind)	Konfigurieren Sie die folgenden Parameter: • **Einheiten** - Geben Sie die Einheiten an, denen diese Regel hinzugefügt werden soll. Wählen Sie im Fenster 'Customize Parameter' (Parameter anpassen) das Kontrollkästchen 'All' aus, um alle Einheiten einzuschließen, oder suchen Sie mit einem der folgenden Suchkriterien nach Einheiten: – **IP/CIDR** - Wählen Sie die Option 'IP/CIDR' aus und geben Sie die IP-Adresse oder die CIDR-Adresse für das Hinzufügen zu dieser Regel an. – **Hostname** - Wählen Sie die Option 'Hostname' aus und geben Sie den Hostnamen an, den Sie filtern möchten. Für die Suche nach mehreren Hostnamen verwenden Sie am Anfang oder Ende der Zeichenfolge ein Platzhalterzeichen (*). – **Adapter** - Wählen Sie die Option 'Adapter' aus und verwenden Sie die Dropdown-Liste, um die Einheitenliste nach Adapter zu filtern. – **Anbieter** - Wählen Sie die Option 'Anbieter' aus und verwenden Sie die Dropdown-Liste, um die Einheitenliste nach Anbieter zu filtern. Sie können auch ein Modell für den Anbieter auswählen. Für die Suche nach mehreren Modellen verwenden Sie am Anfang oder Ende der Zeichenfolge ein Platzhalterzeichen (*). • **zulassen | verweigern** - Wählen Sie die Bedingung (akzeptiert oder verweigert) für Verbindungen an, die dieser Test anwenden soll. • **CIDRs** - Wählen Sie Ausgangs-IP-Adressen oder CIDR-Bereiche für das Hinzufügen zu dieser Regel aus. • **CIDRs** - Wählen Sie Ziel-IP-Adresse oder CIDR-Bereiche für das Hinzufügen zu dieser Regel aus. • **Protokolle** - Geben Sie die Protokolle für das Hinzufügen zu dieser Regel an. Wählen Sie das Kontrollkästchen 'Alle' aus, um alle Protokolle einzuschließen. • **Ports** - Geben Sie die Ports für das Hinzufügen zu dieser Regel an. Wählen Sie das Kontrollkästchen 'Alle' aus, um alle Ports einzuschließen.

Tabelle 34. Topologietests (Forts.)

Testname	Parameter
A rule is added to the selected IPS devices that allows connections from source CIDRs to destination CIDRs with vulnerabilities (Den ausgewählten IPS-Einheiten wird eine Regel hinzugefügt, mit der Verbindungen aus Quellen-CIDRs zu Ziel-CIDRs mit Schwachstellen möglich sind)	Konfigurieren Sie die folgenden Parameter: • **IPS-Einheiten** - Geben Sie die IPS-Einheiten an, die dieses Topologiemodell einschließen soll. Wählen Sie das Kontrollkästchen 'Alle' aus, um alle IPS-Einheiten einzuschließen. • zulassen | verweigern - Geben Sie die Bedingung (akzeptiert oder verweigert) für Verbindungen an, die dieser Test anwenden soll. • **CIDRs** - Geben Sie alle Quellen-IP-Adressen oder CIDR-Bereiche an, die dieses Topologiemodell einschließen soll. • **CIDRs** - Geben Sie alle Ziel-IP-Adressen oder CIDR-Bereiche an, die dieses Topologiemodell einschließen soll. • **Schwachstellen** - Geben Sie die Schwachstellen an, die Sie für das Topologiemodell anwenden möchten. Sie können die Schwachstellen nach Bugtraq-ID, OSVDB-ID, CVE-ID oder Titel suchen.
Für die folgenden Assets sind Verbindungen zu den ausgewählten Ports zulässig	Konfigurieren Sie die folgenden Parameter: • Assets - Geben Sie die Assets an, die dieses Topologiemodell einschließen soll. • **Zulassen** | Verweigern - Geben Sie die Bedingung ('Zulassen' oder 'Verweigern') für Verbindungen an, die dieses Topologiemodell anwenden soll. Die Standardeinstellung ist 'Zulassen'. • Ports - Geben Sie die Ports an, die dieses Topologiemodell einschließen soll. Wählen Sie das Kontrollkästchen 'Alle' aus, um alle Ports einzuschließen.
Assets in the following asset building blocks allow connections to ports (Assets in den folgenden Asset-Bausteinen ermöglichen Verbindungen zu Ports)	Konfigurieren Sie die folgenden Parameter: • assets building blocks (Asset-Bausteine) - Geben Sie die Bausteine an, die dieses Topologiemodell einschließen soll. • **Zulassen** | Verweigern - Geben Sie die Bedingung ('Zulassen' oder 'Verweigern') an, die dieses Topologiemodell anwenden soll. Die Standardeinstellung ist 'Zulassen'. • **Ports** - Geben Sie die Ports an, die dieses Topologiemodell einschließen soll. Wählen Sie das Kontrollkästchen 'Alle' aus, um alle Ports einzuschließen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.

3. Wählen Sie im Menü **Aktionen** die Option 'Neu' aus.
4. Geben Sie im Feld **What do you want to name this model** (Welchen Namen soll dieses Modell haben) einen Namen für die Modelldefinition ein.
5. Wählen Sie im Fenster **Which modifications do you want to apply to your model** (Welche Änderungen sollen für Ihr Modell angewendet werden) die Änderungen aus, die Sie in der Topologie zur Erstellung Ihres Modells anwenden möchten.
6. Konfigurieren Sie die Tests, die dem Fenster **Configure model as follows** (Modell folgendermaßen konfigurieren) hinzugefügt wurden.
7. Wenn der Test im Fenster angezeigt wird, sind die konfigurierbaren Parameter unterstrichen. Klicken Sie auf jeden Parameter, um diese Änderung für Ihr Modell weiter zu konfigurieren. Wählen Sie im Bereich 'Gruppen' das Kontrollkästchen aus, um dieser Frage Gruppen zuzuweisen.
8. Klicken Sie auf **Save Model** (Modell speichern).

Topologiemodell bearbeiten

Sie können ein Topologiemodell bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.
3. Wählen Sie die Modelldefinition aus, die Sie bearbeiten möchten.
4. Wählen Sie im Menü **Aktionen** die Option 'Bearbeiten' aus.
5. Aktualisieren Sie bei Bedarf die Parameter.

   Weitere Informationen zu den Parametern zum Bearbeiten von Modellen finden Sie im Abschnitt Topologiemodell erstellen.
6. Klicken Sie auf **Save Model** (Modell speichern).

Topologiemodell duplizieren

Sie können ein Topologiemodell duplizieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.
3. Wählen Sie die Modelldefinition aus, die Sie duplizieren möchten.
4. Wählen Sie im Menü **Aktionen** die Option **Duplikat** aus.
5. Geben Sie einen Namen ein, den Sie dem kopierten Topologiemodell zuweisen möchten.
6. Klicken Sie auf **OK**.
7. Bearbeiten Sie das Modell.

Topologiemodell löschen

Sie können ein Topologiemodell löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).

2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.
3. Wählen Sie die Modelldefinition aus, die Sie löschen möchten.
4. Wählen Sie im Menü **Aktionen** die Option **Löschen** aus.
5. Klicken Sie auf **OK**.

Topologiemodelle gruppieren

Topologiemodelle können nach ausgewählten Kriterien gruppiert und angezeigt werden.

Die Kategorisierung eines Topologiemodells ist eine effiziente Möglichkeit, Modelle anzuzeigen und zu überwachen. Sie können beispielsweise alle Topologiemodelle anzeigen, die sich auf die Konformität beziehen.

Wenn Sie neue Topologiemodelle erstellen, können Sie die Topologiemodelle einer bestehenden Gruppe zuweisen. Informationen zum Zuweisen einer Gruppe finden Sie im Abschnitt Topologiemodell erstellen.

Gruppen anzeigen

Sie können Topologiemodelle mithilfe von Gruppen anzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.
3. Wählen Sie über die Liste **Gruppe** die Gruppe aus, die Sie anzeigen möchten.

Gruppe erstellen

Sie können eine Gruppe erstellen, um Topologiemodelle effizient anzuzeigen und aufzuzeichnen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe aus, unter der Sie eine neue Gruppe erstellen wollen.

   Nach dem Erstellen der Gruppe können Sie Gruppen in die Elemente der Menübaumstruktur ziehen und dort ablegen, um die Organisation zu ändern.
5. Klicken Sie auf **Neu**.
6. Geben Sie den Namen ein, den Sie der neuen Gruppe zuweisen wollen. Der Name kann bis zu 255 Zeichen lang sein.
7. Geben Sie eine Beschreibung für die Gruppe ein. Die Beschreibung kann bis zu 255 Zeichen lang sein.
8. Klicken Sie auf **OK**.
9. Wenn Sie die Position der neuen Gruppe ändern möchten, klicken Sie auf die neue Gruppe und ziehen den Ordner an die gewünschte Position in Ihrer Menübaumstruktur.

Gruppe bearbeiten

Sie können eine Gruppe bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Topology Models** (Simulation > Topologiemodelle) aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe aus, die Sie bearbeiten wollen.
5. Klicken Sie auf **Bearbeiten**.
6. Aktualisieren Sie die Werte für die Parameter.
7. Klicken Sie auf **OK**.
8. Wenn Sie die Position der Gruppe ändern möchten, klicken Sie auf die neue Gruppe und ziehen den Ordner an die gewünschte Position in Ihrer Menübaumstruktur.

Element in eine andere Gruppe kopieren

Mit der Gruppenfunktion können Sie ein Topologiemodell in eine oder mehrere Gruppen kopieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulations** > **Topology Models** (Simulationen > Topologiemodelle) aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Frage aus, die Sie in eine andere Gruppe kopieren wollen.
5. Klicken Sie auf **Kopieren**.
6. Wählen Sie das Kontrollkästchen für die Gruppe aus, in die Sie die Simulation kopieren möchten.
7. Klicken Sie auf **Kopieren**.

Element aus einer Gruppe löschen

Sie können ein Element aus einer Gruppe löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Menübaumstruktur die Gruppe der höchsten Ebene aus.
5. Wählen Sie aus der Liste der Gruppen das Element oder die Gruppe aus, das bzw. die Sie löschen wollen.
6. Klicken Sie auf **Entfernen**.
7. Klicken Sie auf **OK**.

Topologie einer Gruppe zuweisen

Ein Topologiemodell kann einer Gruppe zugewiesen werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie das Topologiemodell aus, das Sie einer Gruppe zuweisen möchten.
4. Wählen Sie im Menü **Aktionen** die Option **Gruppe zuweisen** aus.
5. Wählen Sie die Gruppe aus, der die Frage zugewiesen werden soll.
6. Klicken Sie auf **Gruppe zuweisen**.

Kapitel 12. Prüfprotokolldaten

Von IBM Security QRadar Risk Manager-Benutzern durchgeführte Änderungen werden auf der Registerkarte **Protokollaktivität** von IBM Security QRadar SIEM aufgezeichnet.

Alle Protokolle werden in der Kategorie 'Risikomanager-Audit' angezeigt. Weitere Informationen zur Verwendung der Registerkarte **Protokollaktivität** in QRadar SIEM finden Sie im *IBM Security QRadar SIEM Users Guide*.

Protokollierte Aktionen

Aktionen werden für Komponenten protokolliert.

In der folgenden Tabelle werden die Kategorien und die entsprechenden Aktionen, die protokolliert werden, aufgelistet.

Tabelle 35. Protokollierte Aktionen

Kategorie	Aktion
Richtlinienüberwachung	Frage erstellen
	Frage bearbeiten
	Frage löschen
	Frage manuell übergeben
	Frage automatisch übergeben
	Ergebnisse genehmigen
	Genehmigung von Ergebnissen widerrufen
Topologiemodell	Topologiemodell erstellen
	Topologiemodell bearbeiten
	Topologiemodell löschen
Topologie	Layout speichern
	Gespeicherte Suche für Topologie erstellen
	Gespeicherte Suche für Topologie bearbeiten
	Gespeicherte Suche für Topologie löschen
	Intrusion-Prevention-System platzieren
Konfigurationsüberwachung	Protokollquellenzuordnung erstellen
	Protokollquellenzuordnung bearbeiten
	Protokollquellenzuordnung löschen
Simulationen	Simulation erstellen
	Simulation bearbeiten
	Simulation löschen
	Simulation manuell ausführen
	Simulation automatisch ausführen
	Simulationsergebnisse genehmigen
	Simulationsergebnisse widerrufen

Tabelle 35. Protokollierte Aktionen (Forts.)

Kategorie	Aktion
Configuration Source Management	Zum ersten Mal erfolgreich für eine Sitzung authentifizieren
	Einheit hinzufügen
	Einheit entfernen
	IP-Adresse oder Adapter für eine Einheit bearbeiten
	Berechtigungsnachweiskonfiguration speichern
	Berechtigungsnachweiskonfiguration löschen
	Protokollkonfiguration speichern
	Protokollkonfiguration entfernen
	Zeitplan für einen Sicherungsjob erstellen
	Zeitplan für einen Sicherungsjob löschen
	Sicherungsjob bearbeiten
	Sicherungsjob hinzufügen
	Sicherungsjob löschen
	Geplanten Sicherungsjob ausführen
	Geplanten Job abschließen, egal ob er erfolgreich war oder fehlgeschlagen ist
	Nachdem ein Sicherungsjob verarbeitet und die Konfiguration beibehalten wurde, wurden keine Änderungen erkannt.
	Nachdem ein Sicherungsjob verarbeitet und die Konfiguration beibehalten wurde, wurden Änderungen erkannt.
	Nachdem ein Sicherungsjob verarbeitet und die Konfiguration beibehalten wurde, wurden nicht persistente Änderungen erkannt.
	Nachdem ein Sicherungsjob verarbeitet wurde und sich die Konfiguration, die zuvor beibehalten wurde, nicht mehr auf der Einheit befindet.
	Es hat ein Versuch einer Adapteroperation begonnen, der Protokolle und Berechtigungsnachweise einschließt.
	Der Versuch einer Adapteroperation war erfolgreich, einschließlich der Protokolle und Berechtigungsnachweise.

Benutzeraktivität anzeigen

Sie können die Benutzeraktivität für QRadar Risk Manager-Benutzer anzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**. Wenn Sie zuvor eine Suche als Standardsuche gespeichert haben, werden die Ergebnisse für diese gespeicherte Suche angezeigt.

2. Klicken Sie auf **Suchen** > **Neue Suche**, um eine Suche zu erstellen.
3. Wählen Sie im Fenster **Zeitraum** eine Option für den Zeitraum aus, den Sie für diese Suche erfassen möchten.
4. Definieren Sie im Fenster **Suchparameter** Ihre Suchkriterien:
   a. Wählen Sie in der ersten Liste **Kategorie** aus.
   b. Wählen Sie in der Dropdown-Liste **Übergeordnete Kategorie** die Option **Risikomanager-Audit** aus.
   c. Optional. Wählen Sie in der Dropdown-Liste **Untergeordnete Kategorie** eine Kategorie aus, um Ihre Suche einzugrenzen.
5. Klicken Sie auf **Filter hinzufügen**.
6. Klicken Sie auf **Filter**, um nach QRadar Risk Manager-Ereignissen zu suchen.

Protokolldatei anzeigen

Prüfprotokolle werden in einer Textdatei gespeichert. Sie werden archiviert und komprimiert, wenn die Prüfprotokolldatei eine Größe von 200 MB erreicht.

Informationen zu diesem Vorgang

Die aktuelle Protokolldatei hat die Bezeichnung 'audit.log'. Wenn die Prüfprotokolldatei ein zweites Mal eine Größe von 200 MB erreicht, wird die Datei komprimiert und das alte Auditprotokoll wird in 'audit.1.gz' umbenannt. Die Dateinummer wird bei jedem Archivieren einer Protokolldatei erhöht. QRadar Risk Manager kann bis zu 50 archivierte Protokolldateien speichern.

Die maximale Größe einer Prüfnachricht (außer Datum, Uhrzeit und Hostname) beträgt 1024 Zeichen.

Jeder Eintrag in der Protokolldatei wird in folgendem Format angezeigt:

```
<Datum_Uhrzeit> <Hostname> <Benutzer>@<IP-Adresse>
(Thread-ID) [<Kategorie>] [<Unterkategorie>]
[<Aktion>] <Nutzdaten>
```

In der folgenden Tabelle werden die Parameter beschrieben, die in der Protokolldatei verwendet werden.

Tabelle 36. Informationen zur Prüfprotokolldatei

Parameter	Beschreibung
<Datum_Uhrzeit>	Das Datum und die Uhrzeit der Aktivität im Format: Monat Datum HH:MM:SS.
<Hostname>	Der Hostname der Konsole, auf der diese Aktivität protokolliert wurde.
<Benutzer>	Der Name des Benutzers, der die Aktion ausgeführt hat.
<IP-Adresse>	Die IP-Adresse des Benutzers, der die Aktion ausgeführt hat.
(Thread-ID)	Die ID des Java™-Threads, durch den diese Aktivität protokolliert wurde.
<Kategorie>	Die übergeordnete Kategorie dieser Aktivität.
<Unterkategorie>	Die untergeordnete Kategorie dieser Aktivität.

Tabelle 36. Informationen zur Prüfprotokolldatei (Forts.)

Parameter	Beschreibung
<Aktion>	Die Aktivität, die auftrat.
<Nutzdaten>	Der vollständige Datensatz, der geändert wurde (falls zutreffend).

Vorgehensweise

1. Melden Sie sich über SSH in der QRadar SIEM-Konsole als Rootbenutzer an.
2. Melden Sie sich über SSH aus der QRadar SIEM-Konsole in der QRadar Risk Manager-Appliance als Rootbenutzer an.
3. Wechseln Sie in folgendes Verzeichnis: `/var/log/audit`
4. Öffnen Sie Ihre Prüfprotokolldatei.

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 in diesem Handbuch beschriebene 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 Defense
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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

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 unter Umständen 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 Namen und Adressen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

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

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

Hinweise zur Datenschutzrichtlinie

IBM Software-Produkte, einschließlich "Software as a Service"-Lösungen (Softwareangebote) verwenden möglicherweise Cookies oder andere Technologien, um Nutzungsinformationen zum Produkt zu erfassen, die Erfahrung der Endbenutzer zu verbessern, Interaktionen mit dem Endbenutzer zu optimieren usw. 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, dadurch geht aber auch die von diesen bereitgestellte Funktionalität verloren.

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, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

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

Glossar

Dieses Glossar enthält Begriffe und Definitionen für die IBM Security QRadar Risk Manager-Software und die zugehörigen Produkte.

In diesem Glossar werden die folgenden Querverweise verwendet:

- *Siehe* verweist von einem nicht bevorzugten Begriff auf den den bevorzugten Begriff oder von einer Abkürzung auf die vollständige Form.
- *Siehe auch* verweist auf einen verwandten oder gegensätzlichen Begriff.

Informationen zu anderen Begriffen und Definitionen finden Sie auf der IBM Terminologiewebsite (wird in einem neuen Fenster geöffnet).

„A" „B" „E" „G" „N" „R" auf Seite 150 „S" auf Seite 150 „T" auf Seite 150 „U" auf Seite 150 „V" auf Seite 150 „Z" auf Seite 150

A

Adapter
Eine zwischengeschaltete Softwarekomponente, mit der die Kommunikation zwischen zwei anderen Softwarekomponenten ermöglicht wird.

Angriff
Jegliche Versuche eines Unbefugten, den Betrieb eines Softwareprogramms oder vernetzten Systems zu beeinträchtigen.

Angriffspfad
Quelle, Ziel und Geräte, die mit einem Angriff verknüpft sind.

Asset Ein einfach zu verwaltendes Objekt, das in einer Betriebsumgebung implementiert wird oder implementiert werden soll.

Asset-Test
Mit diesem Test werden mögliche Risikoindikatoren ermittelt, durch die angezeigt wird, wenn Assets in einem Netz eine definierte Richtlinie nicht einhalten oder ein Risiko für die Umgebung darstellen.

Attribut
Daten, die einer Komponente zugeordnet sind, wie beispielsweise ein Hostname, eine IP-Adresse oder die Anzahl der Festplatten, die einer Serverkomponente zugeordnet werden können.

B

Beitragender Test
Mit diesem Test werden die Risikoindikatoren untersucht, die in einer Frage angegeben sind.

E

Einheit mit mehreren Kontexten
Ein einzelnes Gerät, das in mehrere virtuelle Einheiten partitioniert ist. Bei jeder virtuellen Einheit handelt es sich um eine unabhängige Einheit mit eigener Sicherheitsrichtlinie.

Einschränkender Test
Dieser Test filtert die Ergebnisse, die von einer beitragenden Testfrage zurückgegeben werden.

G

Gefährliches Protokoll
Ein gefährliches Protokoll ist Services zugeordnet, die in einem offenen Port in einer eingehenden Kommunikation zwischen dem Internet und DMZ ausgeführt werden.

N

Nachbardaten
Mit den von Adaptern erfassten Daten werden Informationen zu Einheiten ermittelt, die mit den von QRadar Quality Manager verwalteten Hosts verbunden sind.

NAT Siehe Netzadressumsetzung.

NAT-Indikator
Dieser Indikator im Topologiediagramm zeigt an, dass der Pfad zwischen zwei Netzverbindungen Quellen- oder Zieladressenumsetzungen enthält.

Netzadressumsetzung (Network Address Translation, NAT)
In einer Firewall die Konvertierung von

sicheren IP-Adressen in extern registrierte Adressen. Dadurch ist die Kommunikation mit externen Netzen möglich, aber die IP-Adressen, die innerhalb der Firewall benutzt werden, werden maskiert.

R

Regel Eine Gruppe bedingter Anweisungen, die Computersystemen ermöglichen, Beziehungen zu identifizieren und entsprechend automatisierte Antworten auszuführen.

Risikoindikator
Eine Kennzahl für die mögliche Gefährdung eines System durch eine Sicherheitsverletzung.

S

Schwachstelle
Ein Sicherheitsrisiko in einer Komponente des Betriebssystems, der Systemsoftware oder der Anwendungssoftware.

T

Topologiediagramm
Dieses Diagramm beschreibt Teilnetze, Einheiten und Firewalls.

Topologiemodell
Eine virtuelle Darstellung der Anordnung von Netzassets, mit der ein Angriff simuliert wird.

U

Untergeordnete Suche
Diese Funktion ermöglicht, dass eine Suchabfrage innerhalb einer Gruppe abgeschlossener Suchergebnisse ausgeführt wird.

V

Verbindungsgrafik
Diese Grafik zeigt Verbindungen aus fernen Netzknoten mit lokalen IP-Adressen und lokalen Netzknoten.

Verbindungslinie
Eine Linie in der Verbindungsgrafik zwischen einem fernen Netzknoten und einem lokalen Netzknoten oder zwischen zwei lokalen Netzknoten.

Verstoß
Eine unternehmensinterne Richtlinie wird übergangen oder es wird dagegen verstoßen.

Z

Zeitreihendiagramm
Eine grafische Darstellung von Netzverbindungen im Ablauf der Zeit.

Index

S

T

U

V

W

Z

SC12-5034-00