IBM Security QRadar Log Manager
Version 7.2.4

Benutzerhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 159 gelesen werden.

Produktinformation

Dieses Dokument bezieht sich auf IBM QRadar Security Intelligence Platform V7.2.4 sowie auf nachfolgende Releases, sofern es nicht durch eine aktuellere Version ersetzt wurde.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security QRadar Log Manager, Version 7.2.4, User's Guide,
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
TSC Germany
Kst. 2877
November 2014

Inhaltsverzeichnis

Informationen zum QRadar Log Manager Benutzerhandbuch

Im IBM® Security QRadar Log Manager Benutzerhandbuch finden Sie Informationen zur Verwaltung von IBM Security QRadar SIEM einschließlich der Registerkarten 'Dashboard', 'Protokollaktivität' und 'Berichte'.

Zielgruppe

Dieses Handbuch richtet sich an alle QRadar SIEM-Benutzer, die für die Überprüfung und Verwaltung der Netzsicherheit zuständig sind. In dem Handbuch wird vorausgesetzt, dass Sie über QRadar SIEM-Zugriff verfügen und Ihr Unternehmensnetz und die Netztechnologien kennen.

Technische Dokumentation

Wie Sie auf weitere technische Dokumentation, technische Hinweise und Releaseinformationen zugreifen können, erfahren Sie im technischen Hinweis zum Zugriff auf die IBM Security-Dokumentation (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Kontaktaufnahme mit der Kundenunterstützung

Informationen zur Kontaktaufnahme mit der Kundenunterstützung finden Sie im technischen Hinweis zu Support und Downloads (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Erklärung zu geeigneten Sicherheitsvorkehrungen

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

Hinweis:

Bei Verwendung dieses Programms können unter Umständen verschiedene Gesetze oder Verordnungen zum Tragen kommen. Dazu gehören unter anderem Gesetze oder Verordnungen in Bezug auf die Privatsphäre, den Datenschutz, die Nutzung sowie die elektronische Datenübertragung und die Datenspeicherung. IBM Security QRadar darf nur für legale Zwecke eingesetzt und nur auf legale Weise verwendet

werden. Der Kunde erklärt sich damit einverstanden, dieses Programm gemäß geltenden Rechten, Regelungen und Richtlinien zu verwenden, und übernimmt die vollständige Verantwortung für die Einhaltung dieser Rechte, Regelungen und Richtlinien. Der Lizenznehmer gewährleistet, dass er alle für eine rechtmäßige Verwendung von IBM Security QRadar erforderlichen Einwilligungen, Berechtigungen oder Lizenzen eingeholt bzw. erworten hat oder einholen bzw. erwerben wird.

Kapitel 1. Neuerungen für Benutzer in QRadar Log Manager V7.2.4

In IBM Security QRadar Log Manager V7.2.4 ist jetzt eine erweiterte Integration von IBM Security X-Force Threat Intelligence möglich.

Mit dem IBM Security X-Force Threat Intelligence-Feed eine Echtzeitliste potenziell zerstörerischer IP-Adressen bereitstellen

Für den Inhalt des X-Force-Feeds wird eine relative Risikobewertung vergeben. QRadar-Benutzer können Vorfällen bzw. Verstößen, die durch diesen Inhalt entstehen, anhand dieser Risikobewertung Prioritäten zuweisen. Die Daten aus diesen Informationsquellen werden automatisch in die Korrelations- und Analysefunktionen von QRadar übernommen; die Funktionen des Produkts zur Erkennung von Sicherheitsbedrohungen werden somit durch aktuellste Daten zu Bedrohungen aus dem Internet erweitert. Alle Daten zu sicherheitsrelevanten Ereignissen oder Netzaktivitäten in Zusammenhang mit diesen Adressen werden automatisch markiert; dadurch erhält man wertvolle Kontextinformationen für die Analyse und Untersuchung von Sicherheitsverstößen. Weitere Informationen...

Zusätzliche Suchoptionen

Benutzer können das Feld 'Erweiterte Suche' erweitern, damit mehrere Textzeilen eingegeben werden können.

Benutzer können mithilfe der Funktion 'RuleName' nach Ereignissen suchen, durch die eine bestimmte Regel ausgelöst wurde.

Weitere Informationen...

Ariel Query Language (AQL)

Benutzern stehen neue Funktionen für AQL-Anweisungen zur Verfügung. Weitere Informationen...

Kapitel 2. QRadar Log Manager

IBM Security QRadar Log Manager ist eine Plattform für Netzsicherheitsmanagement, die durch die Korrelation, Analyse und Meldung von Sicherheitsereignissen Situationsbewusstsein und Konformitätsunterstützung bietet.

Navigation in der webbasierten Anwendung

Verwenden Sie beim Arbeiten mit QRadar Log Manager die Navigationsoptionen in der Benutzerschnittstelle und nicht die Web-Browserschaltfläche **Zurück**.

Unterstützte Web-Browser

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

Beim Zugriff auf das QRadar-System werden Sie zur Eingabe eines Benutzernamens und eines Kennworts aufgefordert. Der Benutzername und das Kennwort müssen vorher vom Administrator konfiguriert werden.

In der folgenden Tabelle werden die unterstützten Versionen der Web-Browser aufgelistet.

Tabelle 1. Unterstützte Web-Browser für QRadar-Produkte

Web-Browser	Unterstützte Versionen
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32-Bit-Version von Microsoft Internet Explorer mit aktiviertem Dokumentmodus und Browsermodus	9.0 10.0
Google Chrome	Die am Tag der Freigabe der Produkte von IBM Security QRadar V7.2.4 aktuelle Version

Dokumentmodus und Browsermodus im Internet Explorer aktivieren

Wenn Sie Microsoft Internet Explorer zum Zugriff auf IBM Security QRadar-Produkte verwenden, ist die Aktivierung des Dokumentmodus und des Browsermodus erforderlich.

Vorgehensweise

1. Drücken Sie in Ihrem Internet Explorer-Web-Browser F12, um das Fenster **Developer Tools** (Entwickler-Tools) zu öffnen.
2. Klicken Sie auf **Browser Mode** (Browsermodus) und wählen Sie Ihre Web-Browser-Version aus.
3. Klicken Sie auf **Document Mode** (Dokumentmodus).
   - Wählen Sie für Internet Explorer V9.0 den Eintrag **Internet Explorer 9 standards** (Internet Explorer 9-Standards) aus.

- Wählen Sie für Internet Explorer V10.0 den Eintrag **Internet Explorer 10 standards** (Internet Explorer 10-Standards) aus.

Anmeldung bei IBM Security QRadar

IBM Security QRadar ist eine webbasierte Anwendung. QRadar verwendet Standardanmeldeinformationen für URL, Benutzername und Kennwort.

Verwenden Sie zur Anmeldung bei Ihrer IBM Security QRadar-Konsole die Angaben aus der folgenden Tabelle.

Tabelle 2. Standardanmeldeinformationen für QRadar

Anmelde-informationen	Standard
URL	https://<IP-Adresse>. Dabei bezeichnet <IP-Adresse> die IP-Adresse der QRadar-Konsole. Wenn Sie sich in einer IPv6-Umgebung oder in einer heterogenen Umgebung bei QRadar anmelden möchten, schließen Sie die IP-Adresse in eckige Klammern ein: `https://[<IP-Adresse>]`
Benutzername	admin
Kennwort	Das QRadar während der Installation zugeordnete Kennwort.
Lizenzschlüssel	Mit einem Standardlizenzschlüssel erhalten Sie für 5 Wochen Zugriff auf das System.

REST-konforme API

Mit der REST-API (Representational State Transfer-Anwendungsprogrammierschnittstelle) können Sie HTTPS-Abfragen vornehmen und IBM Security QRadar in andere Lösungen integrieren.

Zugriff und Berechtigungen der Benutzerrolle

Damit Sie auf REST-konforme APIs zugreifen und diese verwenden können, benötigen Sie in QRadar Benutzerrollen mit Verwaltungsrechten. Weitere Informationen zur Verwaltung von Benutzerrollenberechtigungen finden Sie im *IBM Security QRadar SIEM - Verwaltungshandbuch*.

Zugriff auf die Benutzerschnittstelle für die technische Dokumentation zu REST-APIs

Die API-Benutzerschnittstelle stellt Beschreibungen und Funktionen für die folgenden REST-API-Schnittstellen bereit:

Tabelle 3. REST-API-Schnittstellen

REST-API	Beschreibung
`/api/ariel`	Abfrage von Datenbanken, Suchvorgängen, Such-IDs und Suchergebnissen.

Tabelle 3. REST-API-Schnittstellen (Forts.)

REST-API	Beschreibung
`/api/asset_model`	Gibt eine Liste aller Assets im Modell zurück. Sie können auch eine Auflistung aller verfügbaren Asseteigenschaftstypen und gespeicherten Suchläufe erhalten und Assets aktualisieren.
`/api/auth`	Abmeldung und Inaktivierung der aktuellen Sitzung.
`/api/help`	Rückgabe einer Liste der API-Funktionen.
`/api/siem`	Gibt eine Liste aller Angriffe zurück.
`/api/qvm`	Ermöglicht die Überprüfung und Verwaltung von QRadar Vulnerability Manager-Daten.
`/api/reference_data`	Ermöglicht die Anzeige und Verwaltung von Referenzdatensammlungen.
`/api/qvm`	Ermöglicht den Abruf von Assets, Schwachstellen, Netzen, offenen Services und Filtern. Sie können auch Korrekturtickets erstellen oder aktualisieren.
`/api/scanner`	Sie können eine ferne Prüfung, die einem Scanprofil zugeordnet ist, anzeigen, erstellen oder starten.

Die Schnittstelle für die technische Dokumentation von REST-APIs stellt ein Framework bereit, mit dem Sie den Code erfassen können, den Sie zur Implementierung von QRadar-Funktionen in anderen Produkten benötigen.

1. Sie können die Schnittstelle für die technische Dokumentation aufrufen, indem Sie in Ihrem Web-Browser die folgende URL eingeben: `https://`*`IP-Adresse_der_Konsole`*`/api_doc/`.
2. Klicken Sie auf den Header der API, auf die zugegriffen werden soll (beispielsweise **/ariel**).
3. Klicken Sie auf den untergeordneten Header des Endpunkts, auf den zugegriffen werden soll (beispielsweise **/databases**).
4. Klicken Sie auf den untergeordneten Header 'Experimental' (Experimentell) oder 'Provisional' (Temporär).

   Anmerkung:

   Die API-Endpunkte haben entweder die Anmerkung *experimental* (Experimentell) oder *stable* (Dauerhaft).

   Experimental
   Weist darauf hin, dass der API-Endpunkt möglicherweise noch nicht vollständig getestet wurde und ohne vorherige Ankündigung geändert oder auch entfernt werden kann.

   Stable Weist darauf hin, dass der API-Endpunkt vollständig getestet wurde und unterstützt wird.
5. Klicken Sie auf **Try it out** (Testen), um korrekt formatierte HTTPS-Antworten zu erhalten.
6. Sie können die Informationen überprüfen und sammeln, die in Ihre von einem anderen Anbieter erworbene Lösung implementiert werden sollen.

Forum und Codebeispiele für die QRadar-API

Das API-Forum stellt weitere Informationen zur REST-API bereit, beispielsweise Antworten auf häufig gestellte Fragen sowie mit Kommentaren versehene Codebeispiele, die Sie in einer Testumgebung einsetzen können. Weitere Informationen finden Sie im API-Forum (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

Registerkarten der Benutzerschnittstelle

Die verschiedenen Funktionen sind über verschiedene Registerkarten verfügbar. Bei der Anmeldung wird die Registerkarte **Dashboard** angezeigt.

Sie können die Registerkarten ganz einfach aufrufen und die gewünschten Daten bzw. Funktionen suchen.

Registerkarte 'Dashboard'

Die Registerkarte **Dashboard** wird standardmäßig bei der Anmeldung angezeigt.

Die Registerkarte **Dashboard** wird standardmäßig bei der Anmeldung bei IBM Security QRadar Log Manager angezeigt. Sie bietet eine Arbeitsbereichsumgebung mit zusammengefassten und ausführlichen Informationen zu den Ereignissen in Ihrem Netz.

Registerkarte 'Protokollaktivität'

Über die Registerkarte **Protokollaktivität** können Sie an QRadar gesendete Ereignisprotokolle in Echtzeit untersuchen, leistungsstarke Suchen durchführen und die Protokollaktivität in konfigurierbaren Zeitreihendiagrammen anzeigen.

Über die Registerkarte **Protokollaktivität** können Sie umfassende Untersuchungen zu Ereignisdaten vornehmen.

Weitere Informationen finden Sie im Abschnitt Untersuchung der Protokollaktivität.

Registerkarte 'Assets'

Die in Ihrem Netz betriebenen Assets, Server und Hosts werden von QRadar automatisch erkannt.

Assetprofile enthalten Informationen zu allen bekannten Assets in Ihrem Netz, darunter auch Identitätsinformationen, sofern verfügbar. Außerdem ist auch angegeben, welche Services auf den einzelnen Assets ausgeführt werden. Diese Profildaten werden zu Korrelationszwecken verwendet, um die Anzahl der Fehlalarme zu verringern.

Ein Beispiel: Bei einem Angriff wird versucht, einen bestimmten Service zu nutzen, der auf einem bestimmten Asset ausgeführt wird. In dieser Situation kann QRadar den Angriff mit dem Assetprofil korrelieren und so feststellen, ob das Asset für den betreffenden Angriff anfällig ist. Über die Registerkarte **Assets** können Sie die ermittelten Assets anzeigen oder nach bestimmten Assets suchen, um deren Profile anzuzeigen.

Weitere Informationen finden Sie im Abschnitt Asset-Management.

Registerkarte 'Berichte'

Über die Registerkarte **Berichte** können Sie zu allen Daten in QRadar Berichte erstellen, verteilen und verwalten.

Mit der Berichtsfunktion können Sie benutzerdefinierte Berichte zur betrieblichen Verwendung sowie für Führungskräfte erstellen. Beim Erstellen von Berichten können Sie Informationen (z. B. zur Sicherheit oder zum Netz) in einem Bericht kombinieren. Sie können auch die vorinstallierten Berichtsvorlagen aus QRadar verwenden.

Auf der Registerkarte **Berichte** haben Sie außerdem die Möglichkeit, Ihre Berichte mit angepassten Logos zu kennzeichnen. Diese Anpassung ist hilfreich, wenn Berichte an verschiedene Zielgruppen verteilt werden.

Weitere Informationen zu Berichten finden Sie im Abschnitt Berichtsverwaltung.

Registerkarte 'IBM Security QRadar Vulnerability Manager'

IBM Security QRadar Vulnerability Manager ist eine separat erhältliche QRadar-Komponente. QRadar Vulnerability Manager wird über einen Lizenzschlüssel aktiviert.

QRadar Vulnerability Manager ist eine Plattform für Netzscans, die auf die in den Anwendungen, Systemen oder Geräten im Netz vorhandenen Schwachstellen aufmerksam macht. Nach Ermittlung der Schwachstellen können Sie Daten zu den Schwachstellen durchsuchen und prüfen, Schwachstellen korrigieren und zur Bewertung des neuen Risikoniveaus Scanvorgänge erneut ausführen.

Wenn IBM Security QRadar Vulnerability Manager aktiviert ist, können Sie auf der Registerkarte 'Schwachstellen' Schwachstellenanalysen durchführen. Über die Registerkarte 'Assets' können Sie IBM Security QRadar Vulnerability Manager-Suchläufe auf ausgewählten Assets durchführen.

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

Registerkarte 'Verwaltung'

Administratoren können über die Registerkarte 'Verwaltung' Benutzer, Systeme, Netze, Plug-ins und Komponenten konfigurieren und verwalten. Der Zugriff auf die Registerkarte **Verwaltung** ist für Benutzer mit Administratorberechtigung möglich.

Die Verwaltungstools, auf die Administratoren über die Registerkarte **Verwaltung** zugreifen können, werden in Tabelle 1 beschrieben.

Tabelle 4. Verfügbare Administrationsverwaltungstools in QRadar

Verwaltungstool	Beschreibung
Systemkonfiguration	Konfiguration von System- und Benutzerverwaltungsoptionen
Datenquellen	Konfiguration von Protokollquellen
Konfiguration ferner Netze und Services	Konfiguration ferner Netze und Servicegruppen

Tabelle 4. Verfügbare Administrationsverwaltungstools in QRadar (Forts.)

Verwaltungstool	Beschreibung
Plug-ins	Zugriff auf Plug-in-Komponenten wie z. B. das IBM Security QRadar Risk Manager-Plug-in. Diese Option wird nur angezeigt, wenn auf Ihrer Konsole Plug-ins installiert sind.
Implementierungseditor	Verwaltung der verschiedenen Komponenten Ihrer QRadar-Bereitstellung.

Alle Konfigurationsaktualisierungen, die Sie auf der Registerkarte **Verwaltung** vornehmen, werden in einem Staging-Bereich gespeichert. Nach Abschluss aller Änderungen können Sie die Konfigurationsaktualisierungen an dem verwalteten Host in Ihrer Implementierung bereitstellen.

Allgemeine Verfahren in QRadar

Verschiedene Steuerelemente der QRadar-Benutzerschnittstelle sind auf den meisten Benutzerschnittstellen-Registerkarten zu finden.

Informationen zu diesen allgemeinen Prozeduren finden Sie in den folgenden Abschnitten.

Nachrichten anzeigen

Über das Menü **Nachrichten** oben rechts in der Benutzerschnittstelle erhalten Sie Zugriff auf ein Fenster, in dem Sie Ihre Systembenachrichtigungen lesen und verwalten können.

Vorbereitende Schritte

Um die Anzeige von Systembenachrichtigungen im Fenster **Nachrichten** zu ermöglichen, muss der Administrator für jeden Benachrichtigungstyp eine Regel erstellen und das Kontrollkästchen **Benachrichtigen** im **Assistent für angepasste Regeln** aktivieren.

Informationen zu diesem Vorgang

Im Menü **Nachrichten** wird angezeigt, wie viele ungelesene Systembenachrichtigungen sich in Ihrem System befinden. Die Anzahl in dieser Anzeige wird so lange weiter erhöht, bis Sie die Systembenachrichtigungen schließen. Im Fenster **Nachrichten** steht für jede Systembenachrichtigung eine Zusammenfassung und eine auf das Datum der Erstellung der Systembenachrichtigung verweisende Datumszeitmarke zur Verfügung. Bewegen Sie den Mauszeiger über eine Benachrichtigung, um weitere Details anzuzeigen. Mithilfe dieser Funktion im Fenster **Nachrichten** können Sie Systembenachrichtigungen verwalten.

Systembenachrichtigungen sind zudem auf der Registerkarte **Dashboard** und in einem optionalen Popup-Fenster verfügbar, das unten links in der Benutzerschnittstelle angezeigt werden kann. Aktionen, die Sie im Fenster **Nachrichten** ausführen, werden an die Registerkarte **Dashboard** und das Popup-Fenster weitergegeben. Wenn Sie beispielsweise eine Systembenachrichtigung im Fenster **Nachrichten** schließen, wird diese aus allen Systembenachrichtigungsanzeigen entfernt.

Weitere Informationen zu Dashboard-Systembenachrichtigungen finden Sie im Abschnitt Systembenachrichtigungen.

Über das Fenster **Nachrichten** sind die folgenden Funktionen verfügbar:

Tabelle 5. Über das Fenster 'Nachrichten' verfügbare Funktionen

Funktion	Beschreibung
Alle	Klicken Sie auf **Alle**, um alle Systembenachrichtigungen anzuzeigen. Diese Option ist die Standardeinstellung, klicken Sie daher nur auf **Alle**, wenn Sie eine andere Option ausgewählt hatten und erneut alle Systembenachrichtigungen anzeigen möchten.
Status	Klicken Sie auf **Status**, um ausschließlich Systembenachrichtigungen anzuzeigen, die über eine Status-Prioritätsstufe verfügen.
Fehler	Klicken Sie auf **Fehler**, um ausschließlich Systembenachrichtigungen anzuzeigen, die über eine Fehler-Prioritätsstufe verfügen.
Warnungen	Klicken Sie auf **Warnungen**, um ausschließlich Systembenachrichtigungen anzuzeigen, die über eine Warnungs-Prioritätsstufe verfügen.
Information	Klicken Sie auf **Information**, um ausschließlich Systembenachrichtigungen anzuzeigen, die über eine Informations-Prioritätsstufe verfügen.
Alle ablehnen	Klicken Sie auf **Alle ablehnen**, um alle Systembenachrichtigung in Ihrem System zu schließen. Wenn Sie die Liste der Systembenachrichtigungen mithilfe der Symbole **Status**, **Fehler**, **Warnungen** oder **Information** gefiltert haben, wird statt des Symbols **Alle anzeigen** eine der folgenden Optionen angezeigt: • **Alle Fehler ablehnen** • **Alle Status ablehnen** • **Alle Warnungen ablehnen** • **Alle Warnungen ablehnen** • **Alle Informationen ablehnen**
Alle anzeigen	Klicken Sie auf **Alle anzeigen**, um die Systembenachrichtigungsereignisse auf der Registerkarte **Protokollaktivität** anzuzeigen. Wenn Sie die Liste der Systembenachrichtigungen mithilfe der Symbole **Status**, **Fehler**, **Warnungen** oder **Information** gefiltert haben, wird statt des Symbols **Alle anzeigen** eine der folgenden Optionen angezeigt: • **Alle Fehler anzeigen** • **Alle Status anzeigen** • **Alle Warnungen anzeigen** • **Alle Informationen anzeigen**

Tabelle 5. Über das Fenster 'Nachrichten' verfügbare Funktionen (Forts.)

Funktion	Beschreibung
Ablehnen	Klicken Sie auf das Symbol **Ablehnen** neben einer Systembenachrichtigung, um die Systembenachrichtigung in Ihrem System zu schließen.

Vorgehensweise

1. Melden Sie sich bei QRadar an.
2. Klicken Sie oben rechts in der Benutzerschnittstelle auf **Nachrichten**.
3. Zeigen Sie die Systembenachrichtigungsdetails im Fenster **Nachrichten** an.
4. Optional. Klicken Sie, um die Liste der Systembenachrichtigungen einzugrenzen, auf eine der folgenden Optionen:
   - **Fehler**
   - **Warnungen**
   - **Information**
5. Optional. Schließen Sie die Systembenachrichtigungen unter Verwendung einer der folgenden Optionen:

Option	Bezeichnung
Alle ablehnen	Klicken Sie auf diese Option, um alle Systembenachrichtigungen zu schließen.
Ablehnen	Klicken Sie auf das Symbol **Ablehnen** neben der Systembenachrichtigung, die Sie schließen möchten.

6. Optional. Bewegen Sie den Mauszeiger über die Systembenachrichtigung, um die Systembenachrichtigungsdetails anzuzeigen.

Ergebnisse sortieren

Ergebnisse können durch Anklicken einer Spaltenüberschrift in Tabellen sortiert werden. Ein Pfeil am Spaltenanfang zeigt die Richtung der Sortierung an.

Vorgehensweise

1. Melden Sie sich bei QRadar an.
2. Klicken Sie einmal auf die Spaltenüberschrift, um die Tabelle in absteigender Reihenfolge zu sortieren, zweimal, um sie in aufsteigender Reihenfolge zu sortieren.

Benutzerschnittstelle aktualisieren und anhalten

Sie können Daten, die auf Registerkarten angezeigt werden, manuell aktualisieren, anhalten und wiedergeben

Informationen zu diesem Vorgang

Im Modus 'Letztes Intervall (automatisches Aktualisieren)' wird die Registerkarte **Protokollaktivität** automatisch alle 60 Sekunden aktualisiert.

Der Zeitgeber, der sich in der rechten oberen Ecke der Schnittstelle befindet, gibt die Zeitspanne bis zur automatischen Aktualisierung der Registerkarte an.

Wenn Sie die Registerkarte **Protokollaktivität** im Modus 'Echtzeit (Streaming)' oder 'In letzter Minute (automatische Aktualisierung)' anzeigen, können Sie mit dem **Pause**-Symbol die aktuelle Anzeige anhalten.

Sie können auch die aktuelle Anzeige auf der Registerkarte **Dashboard** anhalten. Wenn Sie auf eine beliebige Stelle innerhalb eines Dashboard-Elements klicken, wird die Registerkarte automatisch angehalten. Der Zeitgeber blinkt rot, um anzugeben, dass die aktuelle Anzeige gerade angehalten wird.

Vorgehensweise

1. Melden Sie sich bei QRadar an.
2. Klicken Sie auf die Registerkarte, die Sie anzeigen möchten.
3. Wählen Sie eine der folgenden Optionen:

Option	Bezeichnung
Aktualisieren	Klicken Sie in der rechten Ecke der Registerkarte auf **Aktualisieren**, um die Registerkarte zu aktualisieren.
Anhalten	Klicken Sie hierauf, um die Anzeige in der Registerkarte anzuhalten.
Wiedergeben	Klicken Sie hierauf, um den Zeitgeber nach einer Pause erneut zu starten.

IP-Adressen untersuchen

Sie können mehrere Methoden verwenden, um Informationen über IP-Adressen auf den Registerkarten 'Dashboard', 'Protokollaktivität' und 'Netzaktivität' zu untersuchen.

Informationen zu diesem Vorgang

Sie können weitere Informationen über eine IP-Adresse mit einer der Methoden finden, die in der folgenden Tabelle aufgelistet werden.

Tabelle 6. IP-Adressinformationen

Option	Beschreibung
Information > **DNS-Suche**	Sucht nach DNS-Einträgen, die auf der IP-Adresse basieren.
Information > **WHOIS-Suche**	Sucht nach dem registrierten Eigentümer einer fernen IP-Adresse. Der Standard-WHOIS-Server ist whois.arin.net.
Information > **Portsuche**	Führt einen Netz-Mapper-Scan (NMAP) der ausgewählten IP-Adresse aus. Diese Option ist nur verfügbar, wenn NMAP auf dem System installiert ist. Weitere Informationen zur Installation von NMAP entnehmen Sie Ihrer Anbieterdokumentation.

Tabelle 6. IP-Adressinformationen (Forts.)

Option	Beschreibung
Information > **Assetprofil**	Zeigt Assetprofilinformationen an. Diese Option wird angezeigt, wenn IBM Security QRadar Vulnerability Manager gekauft und lizenziert wird. Weitere Informationen finden Sie im *IBM Security QRadar Vulnerability Manager - Benutzerhandbuch*. Diese Menüoption ist verfügbar, wenn QRadar Profildaten aktiv durch einen Scan bezogen hat.
Information > **Ereignisse suchen**	Sucht nach Ereignissen, die mit dieser IP-Adresse verknüpft sind.
Information > **Verbindungen durchsuchen**	Sucht nach Verbindungen, die mit dieser IP-Adresse verknüpft sind. Diese Option wird nur angezeigt, wenn Sie IBM Security QRadar Risk Manager gekauft und QRadar sowie die IBM Security QRadar Risk Manager-Appliance verbunden haben. Weitere Informationen hierzu finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.
Information > **Switch Port Lookup (Switch-Port-Suche)**	
Information > **Topologie anzeigen**	Dies zeigt die Registerkarte (Risiken) an, auf der die Layer-3-Topologie Ihres Netzwerks zu sehen ist. Diese Option ist verfügbar, wenn Sie IBM Security QRadar Risk Manager gekauft und QRadar sowie die IBM Security QRadar Risk Manager-Appliance verbunden haben.
Information > **QVM-Überprüfung ausführen**	Wählen Sie die Option 'QVM-Überprüfung ausführen' aus, um einen IBM Security QRadar Vulnerability Manager-Scan für diese IP-Adresse auszuführen. Diese Option wird nur angezeigt, wenn IBM Security QRadar Vulnerability Manager gekauft und lizenziert worden ist. Weitere Informationen finden Sie im *IBM Security QRadar Vulnerability Manager - Benutzerhandbuch*.

Weitere Informationen zur Registerkarte 'Risiken' oder IBM Security QRadar Risk Manager finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Vorgehensweise

1. Melden Sie sich bei QRadar an.
2. Klicken Sie auf die Registerkarte, die Sie anzeigen möchten.
3. Bewegen Sie den Mauszeiger über eine IP-Adresse, um deren Position anzuzeigen.
4. Klicken Sie mit der rechten Maustaste auf die IP-Adresse oder den Assetnamen und wählen Sie eine der folgenden Optionen aus:

Überprüfung von Benutzernamen

Wenn Sie mit der rechten Maustaste auf einen Benutzernamen klicken, können Sie auf weitere Menüoptionen zugreifen. Verwenden Sie diese Optionen, um weitere Informationen zu dem Benutzernamen oder der IP-Adresse anzuzeigen.

Die Überprüfung von Benutzernamen ist möglich, wenn IBM Security QRadar Vulnerability Manager erworben und lizenziert wurde. Weitere Informationen hierzu finden Sie im *IBM Security QRadar Vulnerability Manager - Benutzerhandbuch*.

Wenn Sie mit der rechten Maustaste auf einen Benutzernamen klicken, können Sie die folgenden Menüoptionen auswählen.

Tabelle 7. Menüoptionen für die Überprüfung von Benutzernamen

Option	Beschreibung
Assets anzeigen	Die dem ausgewählten Benutzernamen zugeordneten aktuellen Assets werden angezeigt. Weitere Informationen zum Anzeigen von Assets finden Sie im Abschnitt Asset-Management.
Benutzerprotokoll anzeigen	Alle dem ausgewählten Benutzernamen in den letzten 24 Stunden zugeordneten Assets werden angezeigt.
Ereignisse anzeigen	Die dem ausgewählten Benutzernamen zugeordneten Ereignisse werden angezeigt. Weitere Informationen zum Fenster **Liste der Ereignisse** finden Sie im Abschnitt Überwachung der Protokollaktivität.

Weitere Informationen zur Anpassung des Kontextmenüs finden Sie im *Verwaltungshandbuch* zu Ihrem Produkt.

Systemzeit

In der QRadar-Benutzerschnittstelle wird rechts die Systemzeit angezeigt. Hierbei handelt es sich um die Konsolenzeit.

Über die Konsolenzeit werden die QRadar-Systeme innerhalb der QRadar-Bereitstellung synchronisiert. Anhand der Konsolenzeit wird für eine korrekte Zeitsynchronisationskorrelation festgestellt, zu welcher Zeit Ereignisse von anderen Geräten empfangen wurden.

Bei einer verteilten Bereitstellung könnte sich die Konsole in einer anderen Zeitzone als Ihr Desktop-Computer befinden.

Wenn Sie auf der Registerkarte **Protokollaktivität** zeitbasierte Filter und Suchen anwenden, müssen Sie über die Konsolensystemzeit einen Zeitbereich angeben.

Benutzervorgaben aktualisieren

Sie können Ihre Benutzervorgaben (zum Beispiel die Ländereinstellung) in der Hauptbenutzerschnittstelle von QRadar festlegen.

Vorgehensweise

1. Klicken Sie auf **Vorgaben**, um auf Ihre Benutzerdaten zuzugreifen.
2. Aktualisieren Sie Ihre Vorgaben.

Option	Bezeichnung
Benutzername	Zeigt Ihren Benutzernamen an. Dieses Feld kann nicht bearbeitet werden.
Kennwort	Das Kennwort muss den folgenden Kriterien entsprechen: • Mindestens sechs Zeichen • Höchstens 255 Zeichen • Enthält mindestens ein Sonderzeichen • Enthält einen Großbuchstaben
Kennwort (Bestätigen)	Kennwortbestätigung
E-Mail-Adresse	Die E-Mail-Adresse muss den folgenden Anforderungen entsprechen: • Mindestens 10 Zeichen • Höchstens 255 Zeichen
Ländereinstellung	QRadar ist in folgenden Sprachen verfügbar: Englisch, vereinfachtes Chinesisch, traditionelles Chinesisch, Japanisch, Koreanisch, Französisch, Deutsch, Italienisch, Spanisch, Russisch und Portugiesisch (Brasilien). Wenn eine Ländereinstellung nicht aufgelistet wird, wurde die Benutzerschnittstelle nicht in die zugehörige Sprache übersetzt. Sonstige zugehörige kulturelle Konventionen, zum Beispiel der Zeichentyp, die Sortierung, das Datums- und Uhrzeitformat oder die Währungseinheit, werden jedoch unterstützt.
Popup-Benachrichtigungen aktivieren	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Anzeige von Popup-Benachrichtigungen in der Benutzerschnittstelle ermöglichen möchten.

Änderung der Spaltengröße

Die Spaltengröße kann auf verschiedenen Registerkarten in QRadar geändert werden.

Bewegen Sie den Mauscursor auf die Linie zwischen den Spalten und verschieben Sie den Spaltenrand an die neue Stelle. Sie können die Spaltengröße auch ändern, indem Sie doppelt auf die Zeile zwischen den Spalten klicken. Die Größe der Spalte wird dann automatisch entsprechend der Breite des breitesten Feldes angepasst.

Anmerkung: Bei Microsoft Internet Explorer Version 7.0-Web-Browsern funktioniert die Änderung der Spaltengröße nicht, wenn auf Registerkarten Datensätze im Datenstrommodus angezeigt werden.

Seitengröße

Benutzer mit Administratorberechtigung können die maximale Anzahl Ergebnisse konfigurieren, die in den Tabellen auf verschiedenen Registerkarten in QRadar angezeigt werden.

Kapitel 3. Dashboardverwaltung

Die Registerkarte **Dashboard** wird standardmäßig bei der Anmeldung angezeigt.

Sie bietet eine Arbeitsbereichsumgebung, in der Sie die Ansichten mit den erfassten Daten anzeigen können.

Über die Registerkarte 'Dashboard' können Sie das Verhalten bei Sicherheitsereignissen überwachen.

Das Dashboard kann angepasst werden. Die auf der Registerkarte **Dashboard** angezeigten Inhalte sind benutzerspezifisch. Änderungen innerhalb einer Sitzung betreffen nur Ihr System.

Die Registerkarte **Dashboard** kann wie folgt angepasst werden:

- Hinzufügen und Entfernen von Dashboardelementen aus den Dashboards.
- Verschieben und Positionieren der Elemente nach Bedarf. Bei der Positionierung von Elementen wird die Größe jedes Element automatisch proportional zum Dashboard angepasst.
- Hinzufügen von benutzerdefinierten Dashboardelementen auf der Basis von Daten.

  Beispielsweise können Sie ein Dashboardelement hinzufügen, das ein Zeitreihendiagramm oder ein Balkendiagramm zur Darstellung der Top 10-Netzaktivität bereitstellt.

  Zum Erstellen benutzerdefinierter Elemente können Sie gespeicherte Suchen auf der Registerkarte **Protokollaktivität** erstellen und wählen, wie die Ergebnisse in Ihrem Dashboard angezeigt werden sollen. In den Dashboarddiagrammen werden zeitnahe Echtzeitdaten angezeigt. Die Zeitreihendiagramme im Dashboard werden alle 5 Minuten aktualisiert.

Protokollaktivität

Über die Elemente des Dashboards **Protokollaktivität** können Sie Ereignisse in Echtzeit überwachen und untersuchen.

Anmerkung: Ausgeblendete oder geschlossene Ereignisse sind bei den auf der Registerkarte **Dashboard** angezeigten Werten nicht mit einbezogen.

Tabelle 8. Elemente des Dashboards 'Protokollaktivität'

Dashboardelement	Beschreibung
Ereignissuche	Auf der Registerkarte 'Protokollaktivität' können Sie ein benutzerdefiniertes, auf gespeicherten Suchkriterien basierendes Dashboardelement anzeigen. Ereignissuchelemente sind im Menü **Element hinzufügen** > **Protokollaktivität** > **Ereignissuche** aufgeführt. Der Name des Ereignissuchelements entspricht dem Namen der gespeicherten Suchkriterien, auf denen das Element basiert. In QRadar sind standardmäßige gespeicherte Suchkriterien enthalten, die für die Anzeige von Ereignissuchelementen in Ihrem Registerkartenmenü **Dashboard** vorkonfiguriert sind. Sie können dem Registerkartenmenü **Dashboard** weitere Ereignissuchelemente hinzufügen. Weitere Informationen hierzu finden Sie im Abschnitt 'Hinzufügen suchbasierter Dashboardelemente zur Liste "Element hinzufügen"'. In den Elementen des Dashboards **Protokollaktivität** werden als Suchergebnisse neueste Echtzeitdaten in einem Diagramm angezeigt. Unterstützte Diagrammtypen: Zeitreihe, Tabelle, Kreis und Balken. Der Standarddiagrammtyp lautet 'Balken'. Diese Diagramme sind konfigurierbar. Zeitreihendiagramme sind interaktiv. Zur Untersuchung der Protokollaktivität können Sie einen Zeitplan vergrößern und durchsuchen.
Ereignisse nach Wertigkeit	Im Dashboardelement **Ereignisse nach Wertigkeit** wird die Anzahl der aktiven Ereignisse, die nach Wertigkeit gruppiert sind, angezeigt. Anhand dieses Elements können Sie feststellen, wie viele Ereignisse von der zugeordneten Wertigkeitsstufe empfangen werden. Die Wertigkeit gibt an, wie groß die Bedrohung durch eine Angriffsquelle im Verhältnis dazu ist, wie gut das Ziel auf den Angriff vorbereitet ist. Der Wertigkeitsbereich reicht von 0 (niedrig) bis 10 (hoch). Unterstützte Diagrammtypen: Tabelle, Kreis und Balken.

Tabelle 8. Elemente des Dashboards 'Protokollaktivität' (Forts.)

Dashboardelement	Beschreibung
Häufigste Protokollquellen	Das Dashboardelement **Häufigste Protokollquellen** zeigt die 5 wichtigsten Protokollquellen an, die in den letzten 5 Minuten Ereignisse an QRadar Log Manager gesendet haben. In dem Kreisdiagramm ist dargestellt, wie viele Ereignisse von der angegebenen Protokollquelle gesendet werden. Mithilfe dieses Elements können Sie mögliche Verhaltensänderungen erkennen. Wenn beispielsweise eine Firewallprotokollquelle, die normalerweise nicht in der Liste der 10 häufigsten Protokollquellen aufgeführt ist, nun einen großen Anteil an der Gesamtnachrichtenzahl hat, sollten Sie dies prüfen. Unterstützte Diagrammtypen: Tabelle, Kreis und Balken.

Neueste Berichte

Im Dashboardelement **Neueste Berichte** werden die zuletzt generierten Berichte angezeigt.

In der Anzeige sind der Berichtstitel, Datum und Uhrzeit der Berichtserstellung sowie das Berichtsformat angegeben.

Systemübersicht

Das Dashboardelement **Systemübersicht** bietet eine allgemeine Übersicht über die Aktivitäten der letzten 24 Stunden.

Im Übersichtselement finden Sie folgende Informationen:

- **Aktuelle Ereignisse pro Sekunde** - Zeigt die Ereignisrate pro Sekunde an.
- **Neue Ereignisse (letzte 24 Stunden)** - Zeigt die Gesamtzahl der neuen Ereignisse an, die in den letzten 24 Stunden empfangen wurden.

Elemente für das Schwachstellenmanagement

Die Elemente des Dashboards für das Schwachstellenmanagement werden nur angezeigt, wenn IBM Security QRadar Vulnerability Manager erworben und lizenziert wurde.

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

Auf der Registerkarte **Schwachstellen** können Sie ein angepasstes, auf gespeicherten Suchkriterien basierendes Dashboardelement anzeigen. Suchelemente sind im Menü **Element hinzufügen** > **Schwachstellenmanagement** > **Suche nach Schwachstellen** aufgeführt. Der Name des Suchelements stimmt mit dem Namen der gespeicherten Suchkriterien überein, auf denen das Element basiert.

In QRadar sind standardmäßige gespeicherte Suchkriterien enthalten, die für die Anzeige von Suchelementen im Registerkartenmenü **Dashboard** vorkonfiguriert sind. Sie können dem Registerkartenmenü **Dashboard** weitere Suchdashboardelemente hinzufügen.

Unterstützte Diagrammtypen: Tabelle, Kreis und Balken. Der Standarddiagrammtyp lautet 'Balken'. Diese Diagramme sind konfigurierbar.

Systembenachrichtigung

Im Dashboardelement 'Systembenachrichtigung' werden die vom System empfangenen Ereignisbenachrichtigungen angezeigt.

Damit Benachrichtigungen im Dashboardelement **Systembenachrichtigung** angezeigt werden, muss der Administrator eine auf dem jeweiligen Benachrichtigungstyp basierende Regel erstellen und im Assistenten für angepasste Regeln das Kontrollkästchen **Benachrichtigen** auswählen.

Weitere Informationen zur Konfiguration von Ereignisbenachrichtigungen sowie zum Erstellen von Ereignisregeln finden Sie im *IBM Security QRadar Log Manager - Verwaltungshandbuch*.

Im Dashboardelement **Systembenachrichtigungen** finden Sie folgende Informationen:

- **Flag** - Zeigt ein Symbol zur Angabe der Wertigkeitsstufe der Benachrichtigung an. Ziehen Sie den Mauszeiger auf das Symbol, um weitere Informationen zur Wertigkeitsstufe abzurufen.
  - Symbol **Fehlerfreier Zustand**
  - Symbol **Information** (?)
  - Symbol **Fehler** (X)
  - Symbol **Warnung** (!)
- **Erstellt** - Zeigt an, wie viel Zeit seit dem Erstellen der Benachrichtigung vergangen ist.
- **Beschreibung** - Zeigt Informationen zu der Benachrichtigung an.
- **Symbol für Ablehnen (x)** - Über dieses Symbol können Sie eine Systembenachrichtigung schließen.

Wenn Sie den Mauszeiger über eine Benachrichtigung bewegen, können Sie weitere Details anzeigen:

- **Host-IP** - Zeigt die Host-IP-Adresse des Hosts an, von dem die Benachrichtigung stammt.
- **Wertigkeit** - Zeigt die Wertigkeitsstufe des Vorfalls an, aufgrund dessen diese Benachrichtigung erstellt wurde.
- **Untergeordnete Kategorie** - Zeigt die untergeordnete Kategorie an, die dem Vorfall zugeordnet ist, aufgrund dessen diese Benachrichtigung erstellt wurde. Beispiel: Serviceunterbrechung.
- **Nutzlast** - Zeigt den Nutzdateninhalt an, der dem Vorfall zugeordnet ist, aufgrund dessen diese Benachrichtigung erstellt wurde.
- **Erstellt** - Zeigt an, wie viel Zeit seit dem Erstellen der Benachrichtigung vergangen ist.

Wenn Sie das Dashboardelement **Systembenachrichtigungen** hinzufügen, können Systembenachrichtigungen auch als Popup-Benachrichtigungen in der QRadar-Be-

nutzerschnittstelle angezeigt werden. Diese Popup-Benachrichtigungen werden unabhängig davon, welche Registerkarte Sie gerade ausgewählt haben, rechts unten in der Benutzerschnittstelle angezeigt.

Popup-Benachrichtigungen sind nur für Benutzer mit Administratorberechtigung verfügbar und sind standardmäßig aktiviert. Wenn Sie die Popup-Benachrichtigungen inaktivieren möchten, wählen Sie die Option **Benutzereinstellungen** aus und heben Sie die Markierung des Kontrollkästchens **Popup-Benachrichtigungen aktivieren** auf.

Im Popup-Fenster **Systembenachrichtigungen** ist die Anzahl der Benachrichtigungen in der Warteschlange hervorgehoben. Wenn im Header beispielsweise (1 - 12) angezeigt wird, handelt es sich bei der aktuellen Benachrichtigung um 1 von 12 anzuzeigenden Benachrichtigungen.

Im Popup-Fenster **Systembenachrichtigung** sind folgende Optionen verfügbar:

- **Symbol 'Weiter' (>)** - Zeigt die nächste Benachrichtigung an. Wenn es sich bei der aktuellen Benachrichtigung beispielsweise um Nachricht 3 von 6 handelt, klicken Sie auf das Symbol, um Nachricht 4 von 6 anzuzeigen.
- **Symbol 'Schließen' (X)** - Schließt dieses Popup-Benachrichtigungsfenster.
- **(Details)** - Zeigt weitere Informationen zu dieser Systembenachrichtigung an.

Dashboardelemente hinzufügen

Sie können der Registerkarte 'Dashboard' mehrere Dashboardelemente hinzufügen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Dashboard**.
2. Klicken Sie in der Symbolleiste auf **Element hinzufügen**.
3. Wählen Sie das hinzuzufügende Element aus. Weitere Informationen finden Sie unter 'Verfügbare Dashboardelemente'.

Protokollaktivität über das Dashboard untersuchen

Suchbasierte Dashboardelemente enthalten einen Link zur Registerkarte **Protokollaktivität**, auf der Sie die Protokollaktivität eingehender untersuchen können.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um über ein Element des Dashboards **Protokollaktivität** Datenflüsse zu untersuchen:

1. Klicken Sie auf den Link **View in Log Activity** (In Protokollaktivität anzeigen). Die Registerkarte **Protokollaktivität** wird aufgerufen. Darin sind die Ergebnisse sowie zwei Diagramme entsprechend den Parametern Ihres Dashboardelements aufgeführt.

Welche Diagrammtypen auf der Registerkarte **Protokollaktivität** angezeigt werden, hängt davon ab, welches Diagramm in dem Dashboardelement konfiguriert ist:

Diagrammtyp	Beschreibung
Balken, Kreis und Tabelle	Auf der Registerkarte **Protokollaktivität** werden ein Balken- und ein Kreisdiagramm sowie eine Tabelle mit Details angezeigt.

Diagrammtyp	Beschreibung
Zeitreihe	Auf der Registerkarte **Protokollaktivität** werden Diagramme gemäß den folgenden Kriterien angezeigt: 1. Bei einem Zeitbereich von maximal 1 Stunde werden ein Zeitreihendiagramm, ein Balkendiagramm und eine Tabelle mit Ereignisdetails angezeigt. 2. Bei einem Zeitbereich von mehr als 1 Stunde wird ein Zeitreihendiagramm angezeigt und Sie werden aufgefordert, auf 'Details aktualisieren' zu klicken. Dadurch wird die Suche gestartet, bei der die Ereignisdetails ausgefüllt werden und das Balkendiagramm erstellt wird. Nach Abschluss der Suche werden das Balkendiagramm und die Tabelle mit den Ereignisdetails angezeigt.

Diagramme konfigurieren

Sie können die Elemente der Dashboards **Protokollaktivität**, **Netzaktivität** und **Verbindungen** (sofern zutreffend) konfigurieren und dabei den Diagrammtyp sowie die Anzahl der anzuzeigenden Datenobjekte angeben.

Informationen zu diesem Vorgang

Tabelle 9. Diagramme konfigurieren. Parameteroptionen.

Option	Beschreibung
Wert zu Diagramm	Wählen Sie im Listenfeld den Objekttyp aus, den Sie in dem Diagramm darstellen möchten. Zu den möglichen Optionen gehören alle in Ihren Suchparametern enthaltenen normalisierten und benutzerdefinierten Ereignis- oder Datenflussparameter.
Diagrammtyp	Wählen Sie im Listenfeld den Diagrammtyp aus, der angezeigt werden soll. Mögliche Optionen: 1. **Balkendiagramm** - Daten werden in einem Balkendiagramm angezeigt. Diese Option ist nur für gruppierte Ereignisse verfügbar. 2. **Kreisdiagramm** - Die Daten werden in einem Kreisdiagramm angezeigt. Diese Option ist nur für gruppierte Ereignisse verfügbar. 3. **Tabelle** - Die Daten werden in einer Tabelle angezeigt. Diese Option ist nur für gruppierte Ereignisse verfügbar. 4. **Zeitreihe** - Bei Verwendung dieser Option wird ein interaktives Kurvendiagramm angezeigt, in dem die Datensätze dargestellt sind, die mit einem bestimmten Zeitintervall abgeglichen wurden.

Tabelle 9. Diagramme konfigurieren (Forts.). Parameteroptionen.

Option	Beschreibung
Wichtigste anzeigen	Wählen Sie im Listenfeld die Anzahl der im Diagramm anzuzeigenden Objekte aus. Mögliche Optionen: **5** und **10**. Der Standardwert ist **10**.
Zeitreihendaten erfassen	Wählen Sie dieses Kontrollkästchen aus, um die Zeitreihenerfassung zu aktivieren. Bei Auswahl dieses Kontrollkästchens beginnt die Diagrammfunktion damit, Daten für Zeitreihendiagramme zu kumulieren. Standardmäßig ist diese Option inaktiviert.
Zeitraum	Wählen Sie im Listenfeld den Zeitraum aus, der angezeigt werden soll.

Ihre Konfigurationen für das benutzerdefinierte Diagramm werden beibehalten. Immer wenn Sie auf die Registerkarte **Dashboard** zugreifen, werden sie also wie konfiguriert angezeigt.

QRadar Log Manager sammelt Daten. Wenn Sie eine gespeicherte Zeitreihensuche durchführen, ist daher ein Cache mit Ereignis- oder Datenflussdaten verfügbar, sodass die Daten des letzten Zeitraums angezeigt werden können. Kumulierte Parameter sind im Listenfeld **Wert zu Diagramm** mit einem Stern (*) gekennzeichnet. Wenn Sie einen nicht kumulierten Wert (ohne Stern) auswählen, sind keine Zeitreihendaten verfügbar.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Dashboard**.
2. Wählen Sie im Listenfeld **Dashboard anzeigen** das Dashboard mit dem anzupassenden Element aus.
3. Klicken Sie im Header des zu konfigurierenden Dashboardelements auf das Symbol **Einstellungen**.
4. Konfigurieren Sie die in Tabelle 1 beschriebenen Diagrammparameter.

Dashboardelemente entfernen

Sie können Elemente von einem Dashboard entfernen und jederzeit erneut hinzufügen.

Informationen zu diesem Vorgang

Wenn Sie ein Element vom Dashboard entfernen, wird das Element nicht vollkommen entfernt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Dashboard**.
2. Wählen Sie im Listenfeld **Dashboard anzeigen** das Dashboard aus, von dem Sie ein Element entfernen möchten.
3. Klicken Sie in der Dashboardelementüberschrift auf das rote [x]-Symbol, um das Element vom Dashboard zu entfernen.

Dashboardelemente freigeben

Sie können ein Element vom Dashboard freigeben und es in einem neuen Fenster auf Ihrem Desktopsystem anzeigen.

Informationen zu diesem Vorgang

Wenn Sie ein Dashboardelement freigeben, bleibt das ursprüngliche Dashboardelement auf der Registerkarte **Dashboard**, während ein freigegebenes Fenster mit einem duplizierten Dashboardelement geöffnet bleibt und während geplanter Intervalle aktualisiert wird. Wenn Sie die QRadar-Anwendung schließen, bleibt das freigegebene Fenster offen für die Überwachung und fährt mit den Aktualisierungen fort, bis Sie das Fenster manuell schließen oder Ihr Computersystem herunterfahren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Dashboard**.
2. Wählen Sie im Listenfeld **Dashboard anzeigen** das Dashboard aus, von dem ein Element freigegeben werden soll.
3. Klicken Sie auf der Dashboardelementüberschrift auf das grüne Symbol, um das Dashboardelement freizugeben und es in einem separatem Fenster zu öffnen.

Dashboard umbenennen

Sie können ein Dashboard umbenennen und die Beschreibung aktualisieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Dashboard**.
2. Wählen Sie im Listenfeld **Dashboard anzeigen** das Dashboard aus, das bearbeitet werden soll.
3. Klicken Sie in der Symbolleiste auf **Dashboard umbenennen**.
4. Geben Sie im Feld **Name** einen neuen Namen für das Dashboard ein. Die maximale Länge beträgt 65 Zeichen.
5. Geben Sie im Feld **Beschreibung** eine neue Beschreibung für das Dashboard ein. Die maximale Länge beträgt 255 Zeichen.
6. Klicken Sie auf **OK**.

Dashboard löschen

Sie können ein Dashboard löschen.

Informationen zu diesem Vorgang

Nachdem Sie ein Dashboard gelöscht haben, wird die Registerkarte **Dashboard** aktualisiert, und das erste Dashboard, das im Listenfeld **Dashboard anzeigen** aufgeführt ist, wird angezeigt. Das Dashboard, das Sie gelöscht haben, wird nicht mehr im Listenfeld **Dashboard anzeigen** aufgeführt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Dashboard**.
2. Wählen Sie im Listenfeld **Dashboard anzeigen** das Dashboard aus, das gelöscht werden soll.

3. Klicken Sie in der Symbolleiste auf **Dashboard löschen**.
4. Klicken Sie auf **Ja**.

Systembenachrichtigungen verwalten

Sie können die Anzahl der Benachrichtigungen angeben, die auf dem **Systembenachrichtigung**-Dashboardelement angezeigt werden sollen, und die Systembenachrichtigungen nach dem Lesen schließen.

Vorbereitende Schritte

Stellen Sie sicher, dass das **Systembenachrichtigung**-Dashboardelement Ihrem Dashboard hinzugefügt wurde.

Vorgehensweise

1. Klicken Sie auf der Systembenachrichtigung-Dashboardelementüberschrift auf das Symbol **Einstellungen**.
2. Wählen Sie im Listenfeld **Anzeigen** die Anzahl der Systembenachrichtigungen aus, die Sie sehen möchten.
   - Die verfügbaren Optionen sind **5**, **10** (Standard), **20**, **50** und **Alle**.
   - Um alle Systembenachrichtigungen anzuzeigen, die in den letzten 24 Stunden protokolliert wurden, klicken Sie auf **Alle**.
3. Um eine Systembenachrichtigung zu schließen, klicken Sie auf das **Löschen**-Symbol.

Hinzufügen suchbasierter Dashboardelemente zur Liste 'Element hinzufügen'

Dem Menü **Element hinzufügen** können suchbasierte Dashboardelemente hinzugefügt werden.

Vorbereitende Schritte

Wenn Sie dem Menü **Element hinzufügen** auf der Registerkarte **Dashboard** ein Ereignisdashboardelement hinzufügen möchten, müssen Sie über die Registerkarte **Protokollaktivität** Suchkriterien erstellen, wonach die Suchergebnisse auf der Registerkarte **Dashboard** angezeigt werden können. In den Suchkriterien muss auch angegeben sein, dass die Ergebnisse nach einem Parameter gruppiert werden.

Vorgehensweise

1. Gehen Sie wie folgt vor:
   - Wenn Sie ein Dashboardelement für die Ereignissuche hinzufügen möchten, klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Suchen** eine der folgenden Optionen aus:
   - Wählen Sie **Neue Suche** aus, um eine Suche zu erstellen.
   - Wählen Sie **Suche bearbeiten** aus, um eine gespeicherte Suche zu bearbeiten.
3. Konfigurieren oder bearbeiten Sie die Suchparameter nach Bedarf.
   - Wählen Sie im Fensterbereich 'Suche bearbeiten' die Option **In mein Dashboard aufnehmen** aus.
   - Wählen Sie im Fensterbereich 'Spaltendefinition' eine Spalte aus und klicken Sie auf das Symbol **Spalte hinzufügen**, um die Spalte in die Liste **Gruppieren nach** zu verschieben.

4. Klicken Sie auf **Filter**. Die Suchergebnisse werden angezeigt.
5. Klicken Sie auf **Kriterien speichern**. Beachten Sie die Informationen zum Speichern von Suchkriterien auf der Registerkarte 'Angriff'.
6. Klicken Sie auf **OK**.
7. Prüfen Sie, ob das Dashboardelement für die Ereignis- oder Datenflusssuche mithilfe der gespeicherten Suchkriterien erfolgreich zur Liste **Element hinzufügen** hinzugefügt wurde.
8. Klicken Sie auf die Registerkarte **Dashboard**.
9. Wenn Sie ein Ereignissuchelement prüfen möchten, wählen Sie **Element hinzufügen** > **Protokollaktivität** > **Ereignissuche** > **Element hinzufügen** aus.

Kapitel 4. Untersuchung der Protokollaktivität

Sie können Ereignisse in Echtzeit überwachen und untersuchen oder erweiterte Suchläufe ausführen.

Mithilfe der Registerkarte **Protokollaktivität** können Sie Protokollaktivität (Ereignisse) in Echtzeit überwachen oder erweiterte Suchläufe ausführen.

Übersicht über die Registerkarte 'Protokollaktivität'

Bei einem Ereignis handelt es sich um einen Datensatz von einer Protokollquelle, wie z. B. einem Firewall- oder Routergerät, in dem eine Aktion in einem Netz oder auf einem Host beschrieben wird.

Sie benötigen die Berechtigung, die Registerkarte **Protokollaktivität** anzuzeigen.

Symbolleiste der Registerkarte 'Protokollaktivität'

Über die Symbolleiste 'Protokollaktivität' können Sie auf verschiedene Optionen zugreifen.

Über die Symbolleiste können Sie auf die folgenden Optionen zugreifen:

Tabelle 10. Optionen der Symbolleiste 'Protokollaktivität'

Option	Beschreibung
Suchen	Klicken Sie auf **Suchen**, um eine erweiterte Suche nach Ereignissen durchzuführen. Mögliche Optionen: • **Neue Suche** - Wählen Sie diese Option aus, um eine neue Ereignissuche zu erstellen. • **Suche bearbeiten** - Wählen Sie diese Option aus, um eine Ereignissuche auszuwählen und zu bearbeiten. • **Suchergebnisse verwalten** - Wählen Sie diese Option aus, um Suchergebnisse anzuzeigen und zu verwalten.
Schnellsuchvorgänge	Über dieses Listenfeld können Sie zuvor gespeicherte Suchläufe ausführen. Im Listenfeld **Schnellsuchvorgänge** werden nur Optionen angezeigt, wenn Sie Suchkriterien gespeichert haben, in denen die Option **In meine Schnellsuche aufnehmen** angegeben ist.
Filter hinzufügen	Klicken Sie auf **Filter hinzufügen**, um den aktuellen Suchergebnissen einen Filter hinzuzufügen.
Kriterien speichern	Klicken Sie auf **Kriterien speichern**, um die aktuellen Suchkriterien zu speichern.
Ergebnisse speichern	Klicken Sie auf **Ergebnisse speichern**, um die aktuellen Suchergebnisse zu speichern. Diese Option wird nur nach Abschluss einer Suche angezeigt. Im Datenstrommodus ist diese Option inaktiviert.
Abbrechen	Klicken Sie auf **Abbrechen**, um eine laufende Suche abzubrechen. Im Datenstrommodus ist diese Option inaktiviert.

Tabelle 10. Optionen der Symbolleiste 'Protokollaktivität' (Forts.)

Option	Beschreibung
Regeln	Die Option 'Regeln' wird nur angezeigt, wenn Sie zur Anzeige von Regeln berechtigt sind. Klicken Sie auf **Regeln**, um angepasste Ereignisregeln zu konfigurieren. Mögliche Optionen: • **Regeln** - Wählen Sie diese Option aus, um eine Regel anzuzeigen oder zu erstellen. Wenn Sie nur zur Anzeige von Regeln berechtigt sind, wird die Übersichtsseite des Assistenten 'Regeln' angezeigt. Falls Sie über die Berechtigung zur Verwaltung angepasster Regeln verfügen, wird der Assistent 'Regeln' angezeigt und Sie können die Regel bearbeiten. Um die Optionen für die Regeln zur Erkennung von Unregelmäßigkeiten (Schwellenwertregel hinzufügen, Verhaltensregel hinzufügen und Unregelmäßigkeitsregel hinzufügen) zu aktivieren, müssen Sie zusammengefasste Suchkriterien speichern, da in den gespeicherten Suchkriterien die erforderlichen Parameter angegeben sind. **Anmerkung:** Die Optionen für die Regeln zur Erkennung von Unregelmäßigkeiten werden nur angezeigt, wenn Sie über die Berechtigung **Protokollaktivität** > **Maintain Custom Rules** (Angepasste Regeln verwalten) verfügen. • **Schwellenwertregel hinzufügen** - Wählen Sie diese Option aus, um eine Schwellenwertregel zu erstellen. Mit einer Schwellenwertregel werden auftretende Ereignisse auf Aktivitäten getestet, bei denen ein konfigurierter Schwellenwert überschritten wird. Die Schwellenwerte können auf allen von QRadar erfassten Daten basieren. Wenn Sie beispielsweise eine Schwellenwertregel erstellen, die besagt, dass sich maximal 220 Clients zwischen 8 und 17 Uhr beim Server anmelden dürfen, generiert die Regel beim Anmeldeversuch des 221. Clients eine Benachrichtigung. Bei Auswahl der Option **Schwellenwertregel hinzufügen** wird der Assistent 'Regeln' angezeigt. Dabei sind die entsprechenden Optionen zum Erstellen einer Schwellenwertregel bereits vorab ausgefüllt.

Tabelle 10. Optionen der Symbolleiste 'Protokollaktivität' (Forts.)

Option	Beschreibung
Regeln (Fortsetzung)	• **Verhaltensregel hinzufügen** - Wählen Sie diese Option aus, um eine Verhaltensregel zu erstellen. Mit einer Verhaltensregel werden auftretende Ereignisse auf abnormale Aktivitäten getestet, also beispielsweise auf das Vorhandensein von neuem oder unbekanntem Datenverkehr. Hierbei kann es sich um plötzlich zurückgegangenen Datenverkehr oder eine prozentuale Änderung der Zeitdauer handeln, die ein Objekt aktiv ist. So können Sie beispielsweise eine Verhaltensregel erstellen, um den durchschnittlichen Datenverkehr der letzten 5 Minuten mit dem durchschnittlichen Datenverkehr in der letzten Stunde zu vergleichen. Bei einer Änderung von mehr als 40 % generiert die Regel eine Antwort. Bei Auswahl der Option **Verhaltensregel hinzufügen** wird der Assistent 'Regeln' angezeigt. Dabei sind die entsprechenden Optionen zum Erstellen einer Verhaltensregel bereits vorab ausgefüllt. • **Unregelmäßigkeitsregel hinzufügen** - Wählen Sie diese Option aus, um eine Unregelmäßigkeitsregel zu erstellen. Mit einer Unregelmäßigkeitsregel werden auftretende Ereignisse auf abnormale Aktivitäten getestet, also beispielsweise auf das Vorhandensein von neuem oder unbekanntem Datenverkehr. Hierbei kann es sich um plötzlich zurückgegangenen Datenverkehr oder eine prozentuale Änderung der Zeitdauer handeln, die ein Objekt aktiv ist. Wenn beispielsweise ein Netzbereich, der normalerweise nie mit Asien kommuniziert, plötzlich anfängt, mit Hosts in Asien zu kommunizieren, generiert die Unregelmäßigkeitsregel eine Benachrichtigung. Bei Auswahl der Option **Unregelmäßigkeitsregel hinzufügen** wird der Assistent 'Regeln' angezeigt. Dabei sind die entsprechenden Optionen zum Erstellen einer Unregelmäßigkeitsregel bereits vorab ausgefüllt.

Tabelle 10. Optionen der Symbolleiste 'Protokollaktivität' (Forts.)

Option	Beschreibung
Aktionen	Klicken Sie auf **Aktionen**, um die folgenden Aktionen auszuführen: • **Alle anzeigen** - Wählen Sie diese Option aus, um alle Filter für die Suchkriterien zu entfernen und alle ungefilterten Ereignisse anzuzeigen. • **Drucken** - Wählen Sie diese Option aus, um die Ereignisse zu drucken, die auf der Seite angezeigt werden. • **In XML exportieren** > **Angezeigte Spalten** - Wählen Sie diese Option aus, wenn Sie nur die Spalten exportieren möchten, die auf der Registerkarte 'Protokollaktivität' sichtbar sind. Diese Option wird empfohlen. Weitere Informationen hierzu finden Sie unter Abschnitt 'Ereignisse exportieren'. • **In XML exportieren** > **Vollständiger Export (Alle Spalten)** - Wählen Sie diese Option aus, wenn Sie alle Ereignisparameter exportieren möchten. Ein vollständiger Export kann einige Zeit dauern. Weitere Informationen hierzu finden Sie im Abschnitt Ereignisse exportieren. • **In CSV-Datei exportieren** > **Angezeigte Spalten** - Wählen Sie diese Option aus, wenn Sie nur die Spalten exportieren möchten, die auf der Registerkarte 'Protokollaktivität' sichtbar sind. Diese Option wird empfohlen. Weitere Informationen hierzu finden Sie im Abschnitt Ereignisse exportieren. • **In CSV-Datei exportieren** > **Vollständiger Export (Alle Spalten)** - Wählen Sie diese Option aus, wenn Sie alle Ereignisparameter exportieren möchten. Ein vollständiger Export kann einige Zeit dauern. Weitere Informationen hierzu finden Sie im Abschnitt Ereignisse exportieren. • **Löschen** - Wählen Sie diese Option aus, um ein Suchergebnis zu löschen. Weitere Informationen hierzu finden Sie im Abschnitt Ereignis- und Datenflusssuchergebnisse verwalten. • **Benachrichtigen** - Wählen Sie diese Option aus, wenn Ihnen per E-Mail eine Benachrichtigung zugesandt werden soll, sobald die ausgewählten Suchvorgänge beendet sind. Diese Option ist nur für laufende Suchen aktiviert. **Anmerkung:** Im Datenstrommodus und bei der Anzeige partieller Suchergebnisse sind die Optionen **Drucken**, **In XML exportieren** und **In CSV-Datei exportieren** inaktiviert.
Symbolleiste für Suche	**Erweiterte Suche** Wählen Sie im Listenfeld die Option **Erweiterte Suche** aus und geben Sie einen AQL-Suchbegriff (Ariel Query Language) unter Angabe der Felder ein, die zurückgegeben werden sollen. **Schnellfilter** Wählen Sie im Listenfeld die Option 'Schnellfilter' aus, um Nutzdaten anhand einfacher Wörter oder Wortfolgen zu durchsuchen.

Kontextmenüoptionen

Auf der Registerkarte **Protokollaktivität** können Sie mit der rechten Maustaste auf ein Ereignis klicken, um auf weitere Ereignisfilterinformationen zuzugreifen.

Folgende Kontextmenüoptionen sind verfügbar:

Tabelle 11. Kontextmenüoptionen

Option	Beschreibung
Filter für	Wählen Sie diese Option aus, um abhängig von dem im Ereignis ausgewählten Parameter für das ausgewählte Ereignis zu filtern.
Weitere Optionen:	Wählen Sie der dieser Option aus, um eine IP-Adresse oder einen Benutzernamen zu untersuchen. Weitere Informationen zur Untersuchung einer IP-Adresse finden Sie im Abschnitt 'IP-Adressen untersuchen'. Weitere Informationen zur Untersuchung von Benutzernamen finden Sie im Abschnitt Benutzernamen untersuchen. **Anmerkung:** Im Datenstrommodus wird diese Option nicht angezeigt.

Statusleiste

Beim Streaming von Ereignissen wird in der Statusleiste die durchschnittlich pro Sekunde empfangene Ergebniszahl angezeigt.

Hierbei handelt es sich um die Anzahl der Ergebnisse, die die Konsole erfolgreich von den Ereignisprozessoren erhalten hat. Ist diese Zahl größer als 40 Ergebnisse pro Sekunde, werden nur 40 Ergebnisse angezeigt. Die übrigen Ergebnisse werden im Ergebnispuffer gesammelt. Um weitere Statusinformationen anzuzeigen, bewegen Sie den Mauszeiger über die Statusleiste.

Wenn kein Ereignisstreaming erfolgt, ist in der Statusleiste die Anzahl der Suchergebnisse aufgeführt, die derzeit auf der Registerkarte angezeigt werden. Außerdem ist angegeben, wie lange die Verarbeitung der Suchergebnisse dauert.

Überwachung der Protokollaktivität

Auf der Registerkarte **Protokollaktivität** werden Ereignisse standardmäßig im Datenstrommodus angezeigt, sodass Sie Ereignisse in Echtzeit verfolgen können.

Weitere Informationen zum Datenstrommodus erhalten Sie im Abschnitt Streaming-Ereignisse anzeigen. Über das Listenfeld **Ansicht** können Sie einen anderen Zeitraum für die Ereignisfilterung angeben.

Falls Sie bereits zuvor gespeicherte Suchkriterien als Standardeinstellungen konfiguriert haben, werden die Ergebnisse der betreffenden Suche automatisch angezeigt, wenn Sie auf die Registerkarte **Protokollaktivität** zugreifen. Weitere Informationen zum Speichern von Suchkriterien finden Sie im Abschnitt Ereignis- und Datenflusssuchkriterien speichern.

Streaming-Ereignisse anzeigen

Der Datenstrommodus ermöglicht Ihnen das Anzeigen von Ereignisdaten in Ihrem System. Dieser Modus stellt Ihnen eine Echtzeitansicht Ihrer aktuellen Ereignisaktivität durch Anzeige der letzten 50 Ereignisse bereit.

Informationen zu diesem Vorgang

Wenn Sie vor der Aktivierung des Datenstrommodus auf der Registerkarte **Protokollaktivität** oder in Ihren Suchkriterien Filter angewendet haben, bleiben diese Filter im Datenstrommodus erhalten. Der Datenstrommodus unterstützt jedoch keine Suchvorgänge, die gruppierte Ereignisse beinhalten. Wenn Sie den Datenstrommodus für gruppierte Ereignisse oder Suchkriterien aktivieren, werden die normalisierten Ereignisse auf der Registerkarte **Protokollaktivität** angezeigt. Weitere Informationen hierzu finden Sie unter Normalisierte Ereignisse anzeigen.

Wenn Sie ein Ereignis auswählen möchten, um Details anzuzeigen oder eine Aktion auszuführen, müssen Sie den Streaming-Vorgang anhalten, bevor Sie doppelt auf ein Ereignis klicken. Nach dem Anhalten des Streaming-Vorgangs werden die letzten 1.000 Ereignisse angezeigt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Ansicht** die Option **Echtzeit (Streaming)** aus. Informationen zu den Symbolleistenoptionen finden Sie in Tabelle 4-1. Weitere Informationen zu den Parametern, die im Datenstrommodus angezeigt werden, finden Sie in Tabelle 4-7.
3. Optional. Halten Sie die Streaming-Ereignisse an bzw. spielen Sie sie ab. Wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie bei der Auswahl eines Ereignisdatensatzes auf das Symbol **Anhalten**, um den Streaming-Vorgang anzuhalten.
   - Um den Datenstrommodus erneut zu starten, klicken Sie auf das Symbol **Play** (Abspielen).

Normalisierte Ereignisse anzeigen

Ereignisse werden unformatiert erfasst und dann für die Anzeige auf der Registerkarte **Protokollaktivität** normalisiert.

Informationen zu diesem Vorgang

Die Normalisierung beinhaltet die Syntaxanalyse unformatierter Ereignisdaten und die Vorbereitung der Daten mit dem Ziel, lesbare Informationen zur Registerkarte anzeigen zu können. Bei der Normalisierung von Ereignissen werden auch die Namen durch das System normalisiert. Daher stimmt der auf der Registerkarte **Protokollaktivität** angezeigte Name eventuell nicht mit dem im Ereignis angezeigten Namen überein.

Anmerkung: Wenn Sie einen anzuzeigenden Zeitrahmen ausgewählt haben, wird ein Zeitreihendiagramm angezeigt. Weitere Informationen zur Verwendung von Zeitreihendiagrammen finden Sie im Abschnitt Time series chart overview (Zeitreihendiagrammübersicht).

Bei der Anzeige von normalisierten Ereignissen werden die folgenden Parameter auf der Registerkarte **Protokollaktivität** angezeigt:

Tabelle 12. Registerkarte 'Protokollaktivität' - Standardparameter (Normalisierte Parameter)

Parameter	Beschreibung
Aktuelle Filter	Oben in der Tabelle werden die Details zu den Filtern angezeigt, die auf die Suchergebnisse angewendet werden. Klicken Sie, um diese Filterwerte zu löschen, auf **Filter löschen**. **Anmerkung:** Dieser Parameter wird erst angezeigt, wenn Sie einen Filter angewendet haben.
Ansicht	Wählen Sie in diesem Listenfeld den Zeitraum aus, für den der Filter gelten soll.
Aktuelle Statistik	Außer im Echtzeitmodus (Streaming) oder bei Web-Ausführungen in letzter Minute (automatisches Aktualisieren) wird die aktuelle Statistik angezeigt: **Anmerkung:** Klicken Sie auf den Pfeil neben **Aktuelle Statistik**, um die statistischen Daten anzuzeigen oder auszublenden • **Gesamtergebnisse** - Gibt die Gesamtzahl der mit Ihren Suchkriterien übereinstimmenden Ergebnisse an. • **Durchsuchte Datendateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten Datendateien an. • **Durchsuchte, komprimierte Datendateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten, komprimierten Datendateien an. • **Anzahl indexierter Dateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten, indexierten Dateien an. • **Dauer** - Gibt die Dauer der Suche an. **Anmerkung:** Aktuelle Statistiken sind bei der Fehlerbehebung hilfreich. Wenn Sie sich zur Fehlerbehebung an die Kundenunterstützung wenden, werden Sie vermutlich nach diesen Daten gefragt.

Tabelle 12. Registerkarte 'Protokollaktivität' - Standardparameter (Normalisierte Parameter) (Forts.)

Parameter	Beschreibung
Diagramme	Zeigt konfigurierbare Diagramme an, die die mit dem Zeitintervall und der Gruppierungsoption übereinstimmenden Datensätze darstellen. Klicken Sie auf **Diagramme ausblenden**, wenn Sie die Diagramme von Ihrem Bildschirm entfernen möchten. Die Diagramme werden erst angezeigt, wenn Sie einen Zeitrahmen für 'Letztes Intervall (automatisches Aktualisieren)' oder darüber hinaus und die Gruppierungsoption, die angezeigt werden soll, ausgewählt haben. Weitere Informationen zur Konfiguration von Diagrammen finden Sie im Abschnitt Chart management (Diagrammverwaltung). **Anmerkung:** Wenn Sie Mozilla Firefox als Ihren Browser verwenden und eine Werbeblocker-Browsererweiterung installiert haben, werden keine Diagramme angezeigt. Um Diagramme anzuzeigen, muss die Werbeblocker-Browsererweiterung gelöscht werden. Ihre Browserdokumentation enthält weitere Informationen hierzu.
Symbol 'Angriffe'	Klicken Sie auf dieses Symbol, um Details zu dem Angriff anzuzeigen, der diesem Ereignis zugeordnet ist. Weitere Informationen finden Sie im Abschnitt Chart management (Diagrammverwaltung). **Anmerkung:** Abhängig von Ihrem Produkt ist dieses Symbol eventuell nicht verfügbar. Sie müssen über IBM Security QRadar SIEM verfügen.
Startzeit	Gibt den Zeitpunkt des ersten Ereignisses laut dem Bericht der Protokollquelle an QRadar an.
Ereignisname	Gibt den normalisierten Namen des Ereignisses an.
Protokollquelle	Gibt die Protokollquelle an, aus der das Ereignis stammt. Wenn diesem Ereignis mehrere Protokollquellen zugeordnet sind, ist der Begriff 'Mehrere' und die Zahl der Protokollquellen in diesem Feld definiert.
Ereignisanzahl	Gibt die Gesamtzahl der Ereignisse an, die in diesem normalisierten Ereignis gebündelt sind. Ereignisse werden gebündelt, wenn innerhalb kurzer Zeit zahlreiche Ereignisse desselben Typs mit derselben Quellen- und Ziel-IP-Adresse festgestellt werden.
Zeit	Gibt Datum und Uhrzeit des Ereignisempfangs durch QRadar an.

Tabelle 12. Registerkarte 'Protokollaktivität' - Standardparameter (Normalisierte Parameter) (Forts.)

Parameter	Beschreibung
Untergeordnete Kategorie	Gibt die untergeordnete Kategorie an, die diesem Ereignis zugeordnet ist. Weitere Informationen zu Ereigniskategorien finden Sie in der Veröffentlichung *IBM Security QRadar Log Manager - Verwaltungshandbuch*.
Quellen-IP	Gibt die Quellen-IP-Adresse des Ereignisses an.
Quellenport	Gibt den Quellenport des Ereignisses an.
Ziel-IP	Gibt die Ziel-IP-Adresse des Ereignisses an.
Zielport	Gibt den Zielport des Ereignisses an.
Benutzername	Gibt den Benutzernamen an, der diesem Ereignis zugeordnet ist. Benutzernamen sind häufig bei authentifizierungsbezogenen Ereignissen verfügbar. Für alle anderen Ereignistypen, bei denen kein Benutzername verfügbar ist, ist in diesem Feld 'N/A' angegeben.
Ausmaß	Gibt das Ausmaß dieses Ereignisses an. Variablen sind u. a. Zuverlässigkeit, Relevanz und Wertigkeit. Berühren Sie den Ausmaßbalken mit dem Mauszeiger, um die Werte und das berechnete Ausmaß anzuzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Anzeigen** die Option **Standard (Normalisiert)** aus.
3. Wählen Sie im Listenfeld **Ansicht** die Zeitspanne aus, die Sie anzeigen möchten.
4. Klicken Sie auf das Symbol **Anhalten**, um den Datenstrom anzuhalten.
5. Doppelklicken Sie auf das Ereignis, das Sie detaillierter anzeigen möchten. Weitere Informationen finden Sie im Abschnitt Ereignisdetails.

Unformatierte Ereignisse anzeigen

Sie können Daten unformatierter Ereignisse, d. h. Daten nicht analysierter Ereignisse über die Protokollquelle anzeigen.

Informationen zu diesem Vorgang

Bei der Anzeige von Daten unformatierter Ereignisse stehen auf der Registerkarte **Protokollaktivität** die folgenden Parameter für die einzelnen Ereignisse zur Verfügung.

Tabelle 13. Parameter unformatierter Ereignisse

Parameter	Beschreibung
Aktuelle Filter	Oben in der Tabelle werden die Details zu den Filtern angezeigt, die auf die Suchergebnisse angewendet werden. Klicken Sie, um diese Filterwerte zu löschen, auf **Filter löschen**. **Anmerkung:** Dieser Parameter wird erst angezeigt, wenn Sie einen Filter angewendet haben.
Ansicht	Wählen Sie in diesem Listenfeld den Zeitraum aus, für den der Filter gelten soll.
Aktuelle Statistik	Außer im Echtzeitmodus (Streaming) oder bei Web-Ausführungen in letzter Minute (automatisches Aktualisieren) wird die aktuelle Statistik angezeigt: **Anmerkung:** Klicken Sie auf den Pfeil neben **Aktuelle Statistik**, um die statistischen Daten anzuzeigen oder auszublenden • **Gesamtergebnisse** - Gibt die Gesamtzahl der mit Ihren Suchkriterien übereinstimmenden Ergebnisse an. • **Durchsuchte Datendateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten Datendateien an. • **Durchsuchte komprimierte Datendateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten, komprimierten Datendateien an. • **Anzahl indexierter Dateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten, indexierten Dateien an. • **Dauer** - Gibt die Dauer der Suche an. **Anmerkung:** Aktuelle Statistiken sind bei der Fehlerbehebung hilfreich. Wenn Sie sich zur Fehlerbehebung an die Kundenunterstützung wenden, werden Sie vermutlich nach diesen Daten gefragt.

Tabelle 13. Parameter unformatierter Ereignisse (Forts.)

Parameter	Beschreibung
Diagramme	Zeigt konfigurierbare Diagramme an, die die mit dem Zeitintervall und der Gruppierungsoption übereinstimmenden Datensätze darstellen. Klicken Sie auf **Diagramme ausblenden**, wenn Sie die Diagramme von Ihrem Bildschirm entfernen möchten. Die Diagramme werden erst angezeigt, wenn Sie einen Zeitrahmen für 'Letztes Intervall (automatisches Aktualisieren)' oder darüber hinaus und die Gruppierungsoption, die angezeigt werden soll, ausgewählt haben. **Anmerkung:** Wenn Sie Mozilla Firefox als Ihren Browser verwenden und eine Werbeblocker-Browsererweiterung installiert haben, werden keine Diagramme angezeigt. Um Diagramme anzuzeigen, muss die Werbeblocker-Browsererweiterung gelöscht werden. Ihre Browserdokumentation enthält weitere Informationen hierzu.
Startzeit	Gibt den Zeitpunkt des ersten Ereignisses laut dem Bericht der Protokollquelle an QRadar an.
Protokollquelle	Gibt die Protokollquelle an, aus der das Ereignis stammt. Wenn diesem Ereignis mehrere Protokollquellen zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Protokollquellen in diesem Feld definiert.
Nutzdaten	Gibt die Nutzdateninformationen des ursprünglichen Ereignisses im UTF-8-Format an.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Anzeigen** die Option **Unformatierte Ereignisse** aus.
3. Wählen Sie im Listenfeld **Ansicht** die Zeitspanne aus, die Sie anzeigen möchten.
4. Doppelklicken Sie auf das Ereignis, das Sie detaillierter anzeigen möchten. Weitere Informationen hierzu finden Sie unter Ereignisdetails.

Gruppierte Ereignisse anzeigen

Mithilfe der Registerkarte **Protokollaktivität** können nach verschiedenen Angaben gruppierte Ereignisse angezeigt werden. Im Listenfeld **Anzeigen** können Sie die Parameter auswählen, nach denen Ereignisse gruppiert werden sollen.

Informationen zu diesem Vorgang

Das Listenfeld 'Anzeigen' wird im Datenstrommodus nicht angezeigt, da der Datenstrommodus gruppierte Ereignisse nicht unterstützt. Wenn Sie den Datenstrommodus unter Verwendung von Suchkriterien ohne Gruppierung aufgerufen haben, wird diese Option angezeigt.

Im Listenfeld 'Anzeigen' stehen die folgenden Optionen zur Verfügung:

Tabelle 14. Optionen 'Gruppierte Ereignisse'

Option 'Gruppieren'	**Beschreibung**
Untergeordnete Kategorie	Zeigt eine zusammenfassende Liste von nach untergeordneten Ereigniskategorien gruppierten Ereignissen an.
Ereignisname	Zeigt eine zusammenfassende Liste von nach normalisierten Ereignisnamen gruppierten Ereignissen an.
Ziel-IP	Zeigt eine zusammenfassende Liste von nach Ziel-IP-Adressen gruppierten Ereignissen an.
Zielport	Zeigt eine zusammenfassende Liste von nach Zielportadressen gruppierten Ereignissen an.
Quellen-IP	Zeigt eine zusammenfassende Liste von nach Quellen-IP-Adressen gruppierten Ereignissen an.
Angepasste Regel	Zeigt eine zusammenfassende Liste von nach den zugehörigen angepassten Regeln gruppierten Ereignissen an.
Benutzername	Zeigt eine zusammenfassende Liste von nach den zugeordneten Benutzernamen gruppierten Ereignissen an.
Protokollquelle	Zeigt eine zusammenfassende Liste von nach den Protokollquellen gruppierten Ereignissen an, die das Ereignis an QRadar gesendet haben.
Übergeordnete Kategorie	Zeigt eine zusammenfassende Liste von nach übergeordneten Ereigniskategorien gruppierten Ereignissen an.
Netzwerk	Zeigt eine zusammenfassende Liste von nach den zugeordneten Netzwerken gruppierten Ereignissen an.
Quellenport	Zeigt eine zusammenfassende Liste von nach Quellenportadressen gruppierten Ereignissen an.

Nach Auswahl einer Option im Listenfeld **Anzeigen** hängt die Spaltenanordnung der Daten von der gewählten Gruppierung ab. Jede Zeile in der Ereignistabelle steht für eine Ereignisgruppe. Auf der Registerkarte **Protokollaktivität** stehen die folgenden Informationen zu den einzelnen Ereignisgruppen zur Verfügung

Tabelle 15. Parameter für gruppierte Ereignisse

Parameter	**Beschreibung**
Gruppierung nach	Gibt den Parameter an, nach dem die Suche gruppiert ist.
Aktuelle Filter	Oben in der Tabelle werden die Details zu dem Filter angezeigt, der auf die Suchergebnisse angewendet wird. Klicken Sie, um diese Filterwerte zu löschen, auf **Filter löschen**.

Tabelle 15. Parameter für gruppierte Ereignisse (Forts.)

Parameter	Beschreibung
Ansicht	Wählen Sie im Listenfeld den Zeitraum aus, für den der Filter gelten soll.
Aktuelle Statistik	Außer im Echtzeitmodus (Streaming) oder bei Web-Ausführungen in letzter Minute (automatisches Aktualisieren) wird die aktuelle Statistik angezeigt: **Anmerkung:** Klicken Sie auf den Pfeil neben **Aktuelle Statistik**, um die statistischen Daten anzuzeigen oder auszublenden. • **Gesamtergebnisse** - Gibt die Gesamtzahl der mit Ihren Suchkriterien übereinstimmenden Ergebnisse an. • **Durchsuchte Datendateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten Datendateien an. • **Durchsuchte komprimierte Datendateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten, komprimierten Datendateien an. • **Anzahl indexierter Dateien** - Gibt die Gesamtzahl der während des angegebenen Zeitraums durchsuchten, indexierten Dateien an. • **Dauer** - Gibt die Dauer der Suche an. **Anmerkung:** Aktuelle Statistiken sind bei der Fehlerbehebung hilfreich. Wenn Sie sich zur Fehlerbehebung an die Kundenunterstützung wenden, werden Sie vermutlich nach diesen Daten gefragt.

Tabelle 15. Parameter für gruppierte Ereignisse (Forts.)

Parameter	Beschreibung
Diagramme	Zeigt konfigurierbare Diagramme an, die die mit dem Zeitintervall und der Gruppierungsoption übereinstimmenden Datensätze darstellen. Klicken Sie auf **Diagramme ausblenden**, wenn Sie das Diagramm von Ihrem Bildschirm entfernen möchten. Jedes Diagramm stellt eine Legende als visuelle Referenz bereit, die Ihnen dabei helfen soll, die Diagrammobjekte den Parametern zuzuordnen, die sie repräsentieren. Mithilfe der Legendenfunktion können Sie die folgenden Aktionen ausführen: • Bewegen des Mauszeigers über ein Legendenelement, um weitere Informationen zu den Parametern anzuzeigen, die es repräsentiert. • Anklicken des Legendenelements mit der rechten Maustaste, um es weiter zu untersuchen. • Anklicken eines Legendenelements, um es aus dem Diagramm auszublenden. Erneutes Anklicken des Legendenelements, um das ausgeblendete Element anzuzeigen. Elemente können auch durch Anklicken des entsprechenden Diagrammelements aus- bzw. eingeblendet werden. • Anklicken der Option **Legende**, um die Legende aus der Diagrammanzeige zu löschen. **Anmerkung:** Die Diagramme werden erst angezeigt, wenn Sie einen Zeitrahmen für 'Letztes Intervall (automatisches Aktualisieren)' oder darüber hinaus und die Gruppierungsoption, die angezeigt werden soll, ausgewählt haben. **Anmerkung:** Wenn Sie Mozilla Firefox als Ihren Browser verwenden und eine Werbeblocker-Browsererweiterung installiert haben, werden keine Diagramme angezeigt. Um Diagramme anzuzeigen, muss die Werbeblocker-Browsererweiterung gelöscht werden. Ihre Browserdokumentation enthält weitere Informationen hierzu.
Quellen-IP (Eindeutige Anzahl)	Gibt die Quellen-IP-Adresse an, die diesem Ereignis zugeordnet ist. Wenn diesem Ereignis mehrere IP-Adressen zugeordnet sind, sind Begriff 'Mehrere' und die Zahl der IP-Adressen in diesem Feld definiert.
Ziel-IP (Eindeutige Anzahl)	Gibt die Ziel-IP-Adresse an, die diesem Ereignis zugeordnet ist. Wenn diesem Ereignis mehrere IP-Adressen zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der IP-Adressen in diesem Feld definiert.

Tabelle 15. Parameter für gruppierte Ereignisse (Forts.)

Parameter	Beschreibung
Zielport (Eindeutige Anzahl)	Gibt die Zielports an, die diesem Ereignis zugeordnet sind. Wenn diesem Ereignis mehrere Ports zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Ports in diesem Feld definiert.
Ereignisname	Gibt den normalisierten Namen des Ereignisses an.
Protokollquelle (Eindeutige Anzahl)	Gibt die Protokollquellen an, die das Ereignis an QRadar gesendet haben. Wenn diesem Ereignis mehrere Protokollquellen zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Protokollquellen in diesem Feld definiert.
Übergeordnete Kategorie (Eindeutige Anzahl)	Gibt die übergeordnete Kategorie dieses Ereignisses an. Wenn diesem Ereignis mehrere Kategorien zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Kategorien in diesem Feld definiert. Weitere Informationen zu Kategorien finden Sie in der Veröffentlichung *IBM Security QRadar Log Manager - Verwaltungshandbuch*.
Untergeordnete Kategorie (Eindeutige Anzahl)	Gibt die untergeordnete Kategorie dieses Ereignisses an. Wenn diesem Ereignis mehrere Kategorien zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Kategorien in diesem Feld definiert.
Protokoll (Eindeutige Anzahl)	Gibt die Protokoll-ID an, die diesem Ereignis zugeordnet ist. Wenn diesem Ereignis mehrere Protokolle zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Protokoll-IDs in diesem Feld definiert.
Benutzername (Eindeutige Anzahl)	Gibt, falls verfügbar, den Benutzernamen an, der diesem Ereignis zugeordnet ist. Wenn diesem Ereignis mehrere Benutzernamen zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Benutzernamen in diesem Feld definiert.
Ausmaß (Maximum)	Gibt das berechnete maximale Ausmaß für gruppierte Ereignisse an. Zur Berechnung des Ausmaßes verwendete Variablen sind u. a. Zuverlässigkeit, Relevanz und Wertigkeit. Weitere Informationen zu Zuverlässigkeit, Relevanz und Wertigkeit finden Sie im „Glossar" auf Seite 163.
Ereignisanzahl (Summe)	Gibt die Gesamtzahl der Ereignisse an, die in diesem normalisierten Ereignis gebündelt sind. Ereignisse werden gebündelt, wenn innerhalb kurzer Zeit zahlreiche Ereignisse desselben Typs mit derselben Quellen- und Ziel-IP-Adresse auftreten.
Anzahl	Gibt die Gesamtzahl der normalisierten Ereignisse in dieser Ereignisgruppe an.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Ansicht** die Zeitspanne aus, die Sie anzeigen möchten.
3. Wählen Sie im Listenfeld 'Anzeigen' den Parameter, nach dem Ereignisse gruppiert werden sollen. Weitere Informationen hierzu finden Sie in Tabelle 2. Die Ereignisgruppen sind aufgelistet. Detailliertere Informationen zu Ereignisgruppen finden Sie in Tabelle 1.
4. Um die Seite **Liste der Ereignisse** für eine Gruppe anzuzeigen, doppelklicken Sie auf die Ereignisgruppe, die Sie untersuchen möchten. Die Seite **Liste der Ereignisse** behält eventuell von Ihnen auf der Registerkarte **Protokollaktivität** definierte Diagrammkonfigurationen nicht bei. Weitere Informationen zu den Parametern auf der Seite **Liste der Ereignisse** finden Sie in Tabelle 1.
5. Doppelklicken Sie, um die Details eines Ereignisses anzuzeigen, auf das Ereignis, das Sie untersuchen möchten. Weitere Informationen zu Ereignisdetails finden Sie in Tabelle 2.

Ereignisdetails

Ereignislisten können in verschiedenen Modi, u. a. im Datenstrommodus oder in Ereignisgruppen, angezeigt werden. In jedem Modus, den Sie zur Anzeige von Ereignissen auswählen, können Sie die Details zu einem einzelnen Ereignis lokalisieren und anzeigen.

Auf der Seite 'Ereignisdetails' finden Sie folgende Informationen:

Tabelle 16. Ereignisdetails

Parameter	Beschreibung
Ereignisname	Gibt den normalisierten Namen des Ereignisses an.
Untergeordnete Kategorie	Gibt die untergeordnete Kategorie dieses Ereignisses an.
Ereignisbeschreibung	Gibt eine Beschreibung des Ereignisses an, sofern verfügbar.
Ausmaß	Gibt das Ausmaß des Ereignisses an. Weitere Informationen zum Ausmaß finden Sie im Glossar.
Relevanz	Gibt die Relevanz des Ereignisses an. Weitere Informationen zur Relevanz finden Sie im Glossar.
Wertigkeit	Gibt die Wertigkeit dieses Ereignisses an. Weitere Informationen zur Wertigkeit finden Sie im Glossar.
Zuverlässigkeit	Gibt die Zuverlässigkeit dieses Ereignisses an. Weitere Informationen zur Zuverlässigkeit finden Sie im Glossar.
Benutzername	Gibt den diesem Ereignis zugeordneten Benutzernamen an, sofern verfügbar.
Startzeit	Gibt an, wann das Ereignis von der Protokollquelle empfangen wurde.
Uhrzeit der Speicherung	Gibt an, wann das Ereignis in der QRadar-Datenbank gespeichert wurde.
Protokollquellenzeit	Gibt die von der Protokollquelle in den Ereignisnutzdaten gemeldete Systemzeit an.

Tabelle 16. Ereignisdetails (Forts.)

Parameter	Beschreibung
Quell- und Zielangaben	
Quellen-IP	Gibt die Quellen-IP-Adresse des Ereignisses an.
Ziel-IP	Gibt die Ziel-IP-Adresse des Ereignisses an.
Quellenassetname	Gibt den benutzerdefinierten Assetnamen der Ereignisquelle an. Weitere Informationen zu Assets finden Sie im Abschnitt 'Asset-Management'.
Zielassetname	Gibt den benutzerdefinierten Assetnamen des Ereignisziels an. Weitere Informationen zu Assets finden Sie im Abschnitt 'Asset-Management.
Quellenport	Gibt den Quellenport dieses Ereignisses an.
Zielport	Gibt den Zielport dieses Ereignisses an.
Prä-NAT Quellen-IP	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Network Address Translation - Netzadressumsetzung) gibt dieser Parameter die Quellen-IP-Adresse vor Anwendung der NAT-Werte an. Bei der Netzadressumsetzung wird eine IP-Adresse in einem Netz in eine andere IP-Adresse in einem anderen Netz übersetzt.
Prä-NAT Ziel-IP	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter die Ziel-IP-Adresse vor Anwendung der NAT-Werte an.
Prä-NAT Quellenport	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter den Quellenport vor Anwendung der NAT-Werte an.
Prä-NAT Zielport	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter den Zielport vor Anwendung der NAT-Werte an.
Post-NAT Quellen-IP	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter die Quellen-IP-Adresse nach Anwendung der NAT-Werte an.

Tabelle 16. Ereignisdetails (Forts.)

Parameter	Beschreibung
Post-NAT Ziel-IP	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter die Ziel-IP-Adresse nach Anwendung der NAT-Werte an.
Post-NAT Quellenport	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter den Quellenport nach Anwendung der NAT-Werte an.
Post-NAT Zielport	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter den Zielport nach Anwendung der NAT-Werte an.
Post-NAT Quellenport	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter den Quellenport nach Anwendung der NAT-Werte an.
Post-NAT Zielport	Bei einer Firewall oder einem anderen NAT-fähigen Gerät (NAT = Netzadressumsetzung) gibt dieser Parameter den Zielport nach Anwendung der NAT-Werte an.
IPv6-Quelle	Gibt die Quellen-IPv6-Adresse des Ereignisses an.
IPv6-Ziel	Gibt die Ziel-IPv6-Adresse des Ereignisses an.
Quellen-MAC	Gibt die Quellen-MAC-Adresse des Ereignisses an.
Ziel-MAC	Gibt die Ziel-MAC-Adresse des Ereignisses an.
Angaben zu den Nutzdaten	
Nutzdaten	Gibt den Nutzdateninhalt des Ereignisses an. In diesem Feld stehen 3 Registerkarten zur Anzeige der Nutzdaten zur Verfügung: • Universal Transformation Format (UTF) - Klicken Sie auf 'UTF'. • Hexadezimal - Klicken Sie auf 'HEX'. • Base64 - Klicken Sie auf 'Base64'.
Weitere Informationen	
Protokoll	Gibt das diesem Ereignis zugeordnete Protokoll an.
QID	Gibt die qualifizierte Kennung (QID) für dieses Ereignis an. Zu jedem Ereignis gibt es eine eindeutige QID. Weitere Informationen zur QID-Zuordnung finden Sie im Abschnitt Ereigniszuordnung ändern.

Tabelle 16. Ereignisdetails (Forts.)

Parameter	Beschreibung
Protokollquelle	Gibt die Protokollquelle an, von der das Ereignis an QRadar gesendet wurde. Wenn es mehrere Protokollquellen gibt, die diesem Ereignis zugeordnet sind, ist in diesem Feld der Begriff 'Mehrere' und die Anzahl der Protokollquellen angegeben.
Ereigniszähler	Gibt die Gesamtzahl der Ereignisse an, die in diesem normalisierten Ereignis zusammengefasst sind. Ereignisse werden zusammengefasst, wenn innerhalb kurzer Zeit viele Ereignisse desselben Typs für dieselbe Quellen- und Ziel-IP-Adresse erkannt werden.
Angepasste Regeln	Gibt angepasste Regeln an, die mit diesem Ereignis übereinstimmen. .
Angepasste Regeln teilweise eingehalten	Gibt angepasste Regeln an, die mit diesem Ereignis teilweise übereinstimmen.
Anmerkungen	Gibt die Anmerkung zu diesem Ereignis an. Anmerkungen sind Textbeschreibungen, die von den Regeln im Rahmen der Regelantwort automatisch zu Ereignissen hinzugefügt werden können.
Identitätsinformationen - Sofern verfügbar, erfasst QRadar Identitätsinformationen aus Protokollquellennachrichten. Identitätsinformationen enthalten zusätzliche Details zu den Assets in Ihrem Netz. Identitätsinformationen werden von den Protokollquellen nur generiert, wenn die an QRadar gesendete Protokollnachricht eine IP-Adresse und mindestens eines der folgenden Elemente umfasst: Benutzername oder MAC-Adresse. Nicht alle Protokollquellen generieren Identitätsinformationen. Weitere Informationen zu Identität und Assets finden Sie im Abschnitt Asset-Management.	
Benutzername als Identität	Gibt den Benutzernamen des diesem Ereignis zugeordneten Assets an.
IP als Identität	Gibt die IP-Adresse des diesem Ereignis zugeordneten Assets an.
Identität NetBIOS-Name	Gibt den NetBIOS-Namen (Network Base Input/Output System) des diesem Ereignis zugeordneten Assets an.
Erweitertes Identitätsfeld	Gibt weitere Informationen zu dem diesem Ereignis zugeordneten Asset an. Dieses Feld enthält benutzerdefinierten Text, der Inhalt hängt davon ab, welche Geräte in Ihrem Netz Identitätsinformationen bereitstellen können. Beispiele: physischer Standort von Geräten, relevante Richtlinien, Netzswitch und Portnamen.
Hat Identität (Flag)	Hier ist 'Wahr' angegeben, wenn QRadar Identitätsinformationen für das diesem Ereignis zugeordnete Asset erfasst hat. Welche Geräte Identitätsinformationen senden, können Sie im *IBM Security QRadar DSM Configuration Guide* nachlesen.
Hostname als Identität	Gibt den Hostnamen des diesem Ereignis zugeordneten Assets an.

Tabelle 16. Ereignisdetails (Forts.)

Parameter	Beschreibung
MAC als Identität	Gibt die MAC-Adresse des diesem Ereignis zugeordneten Assets an.
Gruppenname als Identität	Gibt den Gruppennamen des diesem Ereignis zugeordneten Assets an.

Symbolleiste 'Ereignisdetails'

Auf der Symbolleiste 'Ereignisdetails' stehen verschiedene Funktionen zur Anzeige der Ereignisdetails zur Verfügung.

Auf der Symbolleiste **Ereignisdetails** stehen die folgenden Funktionen zur Verfügung:

Tabelle 17. Symbolleiste 'Ereignisdetails'

Zur Ereignisliste zurückkehren	Klicken Sie auf **Zur Ereignisliste zurückkehren**, um zur Ereignisliste zurückzukehren.
Ereignis zuordnen	Klicken Sie auf **Ereignis zuordnen**, um die Ereigniszuordnung zu bearbeiten. Weitere Informationen finden Sie im Abschnitt Ereigniszuordnung ändern.
Falscher Alarm	Klicken Sie auf **Falscher Alarm**, um QRadar zu optimieren und so zu verhindern, dass bei Fehlalarmereignissen Angriffe generiert werden.
Eigenschaft extrahieren	Klicken Sie auf **Eigenschaft extrahieren**, um aus dem ausgewählten Ereignis eine angepasste Ereigniseigenschaft zu erstellen.
Zurück	Klicken Sie auf **Zurück**, um das vorherige Ereignis in der Ereignisliste anzuzeigen.
Weiter	Klicken Sie auf **Weiter**, um das nächste Ereignis in der Ereignisliste anzuzeigen.
PCAP-Daten	**Anmerkung:** Diese Option wird nur angezeigt, wenn Ihre QRadar-Konsole für die Integration in den Juniper JunOS Platform DSM konfiguriert ist. Weitere Informationen zur Verwaltung von PCAP-Daten finden Sie im Abschnitt PCAP-Daten verwalten. • **PCAP-Informationen anzeigen** - Wählen Sie diese Option aus, um die PCAP-Informationen anzuzeigen. Weitere Informationen finden Sie im Abschnitt PCAP-Informationen anzeigen. • **PCAP-Datei herunterladen** - Wählen Sie diese Option aus, um die PCAP-Datei auf Ihr Desktopsystem herunterzuladen. Weitere Informationen finden Sie im Abschnitt PCAP-Datei auf Desktopsystem herunterladen.

Tabelle 17. Symbolleiste 'Ereignisdetails' (Forts.)

Drucken	Klicken Sie auf **Drucken**, um die Ereignisdetails zu drucken.

Zugeordnete Angriffe anzeigen

Auf der Registerkarte 'Protokollaktivität' können Sie den Angriff anzeigen, der dem Ereignis zugeordnet ist.

Informationen zu diesem Vorgang

Erfüllt ein Ereignis eine Regel, kann auf der Registerkarte **Angriffe** ein Angriff generiert werden.

Bei Anzeige eines Angriffs über die Registerkarte **Protokollaktivität** wird der dem ausgewählten Ereignis zugeordnete Angriff unter Umständen nicht angezeigt, wenn er von der Magistrate-Komponente noch nicht auf der Festplatte gespeichert oder aus der Datenbank gelöscht wurde. In diesem Fall erhalten Sie vom System eine entsprechende Benachrichtigung.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Optional. Bei der Anzeige von Ereignissen im Datenstrommodus können Sie das Streaming durch Klicken auf das Symbol **Pause** anhalten.
3. Klicken Sie auf das Symbol **Angriff** neben dem Ereignis, das untersucht werden soll.
4. Zeigen Sie den zugeordneten Angriff an.

Ereigniszuordnung ändern

Sie können manuell ein normalisiertes oder unformatiertes Ereignis einer übergeordneten und untergeordneten Kategorie (oder QID) zuordnen.

Vorbereitende Schritte

Diese manuelle Aktion wird verwendet, um unbekannte Protokollquellenereignisse bekannten QRadar-Ereignissen zuzuordnen, so dass sie angemessen kategorisiert und verarbeitet werden können.

Informationen zu diesem Vorgang

Für Normalisierungszwecke ordnet QRadar automatisch Ereignisse von Protokollquellen über- und untergeordneten Kategorien zu.

Weitere Informationen zu Ereigniskategorien finden Sie in der Veröffentlichung *IBM Security QRadar Log Manager - Verwaltungshandbuch*.

Wenn Ereignisse empfangen werden, die von Protokollquellen stammen, die das System nicht kategorisieren kann, werden die Ereignisse als unbekannt kategorisiert. Diese Ereignisse treten aus mehreren Gründen auf, wie z. B.:

- **Benutzerdefinierte Ereignisse** - Einige Protokollquellen, wie z. B. Snort, ermöglichen Ihnen, benutzerdefinierte Ereignisse zu erstellen.

- **Neue Ereignisse oder ältere Ereignisse** - Anbieter von Protokollquellen aktualisieren ihre Software möglicherweise durch Wartungsreleases, die neue Ereignisse unterstützen, die von QRadar nicht unterstützt werden.

Anmerkung: Das Symbol **Ereignis zuordnen** ist für Ereignisse inaktiviert, wenn die übergeordnete Kategorie SIM-Audit heißt oder der Protokollquellentyp Simple Object Access Protocol (SOAP) ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Optional. Wenn Sie Ereignisse im Datenstrommodus anzeigen, klicken Sie auf das **Pause**-Symbol, um das Streaming anzuhalten.
3. Doppelklicken Sie auf das Ereignis, das Sie zuordnen möchten.
4. Klicken Sie auf **Ereignis zuordnen**.
5. Wenn Sie die QID kennen, die Sie diesem Ereignis zuordnen wollen, geben Sie die QID im Feld **QIDs eingeben** ein.
6. Wenn Sie die QID, die Sie diesem Ereignis zuordnen wollen, nicht kennen, können Sie nach einer bestimmten QID suchen.
   a. Wählen Sie eine der folgenden Optionen aus: `Um anhand der Kategorie nach einer QID zu suchen, wählen Sie im Listenfeld 'Übergeordnete Kategorie' die übergeordnete Kategorie aus. Um anhand der Kategorie nach einer QID zu suchen, wählen Sie im Listenfeld 'Untergeordnete Kategorie' die untergeordnete Kategorie aus. Um anhand des Protokollquellentyps nach einer QID zu suchen, wählen Sie im Listenfeld 'Protokollquellentyp' einen Protokollquellentyp aus. Um anhand des Namens nach einer QID zu suchen, geben Sie im Feld 'QID/Name' einen Namen ein.`
   b. Klicken Sie auf **Suchen**.
   c. Wählen Sie die **QID** aus, mit der Sie dieses Ereignis verknüpfen wollen.
7. Klicken Sie auf **OK**.

PCAP-Daten

Falls Ihre QRadar-Konsole für die Integration in den Juniper JunOS Platform DSM konfiguriert ist, kann eine Paketaufzeichnung (Packet Capture - PCAP) empfangen und verarbeitet werden und Daten von einer Juniper SRX-Series Services Gateway-Protokollquelle können gespeichert werden.

Weitere Informationen zum Juniper JunOS Platform DSM finden Sie im *IBM Security QRadar DSM Configuration Guide*.

PCAP-Datenspalte anzeigen

Die Spalte **PCAP-Daten** wird nicht standardmäßig auf der Registerkarte **Protokollaktivität** angezeigt. Wenn Sie Suchkriterien erstellen, müssen Sie die Spalte **PCAP-Daten** im Fensterbereich 'Spaltendefinition' auswählen.

Vorbereitende Schritte

Bevor Sie PCAP-Daten auf der Registerkarte **Protokollaktivität** anzeigen können, muss die Juniper SRX-Series Services Gateway-Protokollquelle mit dem PCAP Syslog Combination-Protokoll konfiguriert werden. Weitere Informationen zur Konfiguration von Protokollquellenprotokollen finden Sie im *Managing Log Sources Guide*.

Informationen zu diesem Vorgang

Wenn Sie eine Suche ausführen, die die Spalte **PCAP-Daten** enthält, wird ein Symbol in der Spalte **PCAP-Daten** der Suchergebnisse angezeigt, wenn PCAP-Daten für ein Ereignis verfügbar sind. Mithilfe des **PCAP**-Symbols können Sie die PCAP-Daten anzeigen oder die **PCAP**-Datei auf Ihr Desktopsystem herunterladen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Suchen** den Eintrag **Neue Suche** aus.
3. Optional. Um nach Ereignissen zu suchen, die PCAP-Daten aufweisen, konfigurieren Sie die folgenden Suchkriterien:
   a. Wählen Sie im ersten Listenfeld **PCAP-Daten** aus.
   b. Wählen Sie im zweiten Listenfeld **Gleich** aus.
   c. Wählen Sie im dritten Listenfeld **Wahr** aus.
   d. Klicken Sie auf **Filter hinzufügen**.
4. Konfigurieren Sie die Spaltendefinitionen so, dass die Spalte **PCAP-Daten** eingeschlossen wird:
   a. Klicken Sie im Fensterbereich 'Spaltendefinition' in der Liste **Verfügbare Spalten** auf **PCAP-Daten**.
   b. Klicken Sie in der unteren Symbolgruppe auf das Symbol **Spalte hinzufügen**, um die Spalte **PCAP-Daten** zur Liste **Spalte** zu verschieben.
   c. Optional. Klicken Sie in der oberen Symbolgruppe auf das Symbol **Spalte hinzufügen**, um die Spalte **PCAP-Daten** zur Liste **Gruppieren nach** zu verschieben.
5. Klicken Sie auf **Filter**.
6. Optional. Wenn Sie Ereignisse in Datenstrommodus anzeigen, klicken Sie auf das **Pause**-Symbol, um das Streaming anzuhalten.
7. Doppelklicken Sie auf das Ereignis, das Sie untersuchen möchten.

Nächste Schritte

Weitere Informationen zum Anzeigen und Herunterladen von PCAP-Daten finden Sie in den folgenden Abschnitten:

- PCAP-Informationen anzeigen
- PCAP-Datei auf Desktopsystem herunterladen

PCAP-Informationen anzeigen

Über das Symbolleistenmenü **PCAP-Daten** kann eine lesbare Version der Daten in der PCAP-Datei angezeigt bzw. die PCAP-Datei auf Ihr Desktopsystem heruntergeladen werden.

Vorbereitende Schritte

Bevor Sie PCAP-Informationen anzeigen können, muss ein Suchvorgang durchgeführt bzw. ausgewählt werden, um die Spalte **PCAP-Daten** anzuzeigen.

Informationen zu diesem Vorgang

Bevor PCAP-Daten angezeigt werden können, muss die PCAP-Datei zur Anzeige in der Benutzerschnittstelle abgerufen werden. Wenn der Downloadprozess einen

längeren Zeitraum in Anspruch nimmt, wird das Fenster **PCAP-Informationen werden heruntergeladen** angezeigt. In den meisten Fällen ist der Downloadprozess schnell und dieses Fenster wird nicht angezeigt.

Nach dem Abrufen der Datei wird eine lesbare Version der PCAP-Datei in einem Popup-Fenster bereitgestellt. Sie können die im Fenster angezeigten Informationen lesen oder die Informationen in Ihr Desktopsystem herunterladen

Vorgehensweise

1. Wählen Sie für das Ereignis, das Sie untersuchen möchten, eine der folgenden Optionen:
   - Wählen Sie das Ereignis aus und klicken Sie auf das Symbol **PCAP**.
   - Klicken Sie mit der rechten Maustaste auf das Symbol **PCAP** für das Ereignis und wählen Sie **Weitere Optionen** > **PCAP-Informationen anzeigen** aus.
   - Doppelklicken Sie auf das Ereignis, das Sie untersuchen möchten, und klicken Sie in der Symbolleiste der Ereignisdetails dann auf **PCAP-Daten** > **PCAP-Informationen anzeigen**.
2. Wenn Sie die Informationen in Ihr Desktopsystem herunterladen möchten, wählen Sie eine der folgenden Optionen:
   - Klicken Sie auf **PCAP-Datei herunterladen**, um die ursprüngliche PCAP-Datei zur Verwendung in einer externen Anwendung herunterzuladen.
   - Klicken Sie auf **PCAP-Text herunterladen**, um die PCAP-Informationen im .TXT-Format herunterzuladen
3. Wählen Sie eine der folgenden Optionen aus:
   - Wenn Sie die Datei zur unmittelbaren Anzeige öffnen möchten, wählen Sie die Option **Open with** (Öffnen mit) und dann eine Anwendung im Listenfeld aus.
   - Wenn Sie die Liste speichern möchten, wählen Sie die Option **Save File** (Datei speichern) aus.
4. Klicken Sie auf **OK**.

PCAP-Datei auf Desktopsystem herunterladen

Sie können die PCAP-Datei auf Ihr Desktopsystem zum Speichern oder zur Verwendung in anderen Anwendungen herunterladen.

Vorbereitende Schritte

Damit Sie PCAP-Informationen anzeigen können, müssen Sie eine Suche ausführen bzw. auswählen, in der dieSpalte 'PCAP-Daten' angezeigt wird. Informationen hierzu erhalten Sie im Abschnitt **PCAP-Datenspalte anzeigen**.

Vorgehensweise

1. Wählen Sie für das Ereignis, das Sie untersuchen wollen, eine der folgenden Optionen aus:
   - Wählen Sie das Ereignis aus und klicken Sie auf das **PCAP**-Symbol.
   - Klicken Sie mit der rechten Maustaste auf das PCAP-Symbol für das Ereignis und wählen Sie **Weitere Optionen** > **PCAP-Datei herunterladen** aus.
   - Doppelklicken Sie auf das Ereignis, das Sie untersuchen wollen, und wählen Sie dann **PCAP-Daten** > **PCAP-Datei herunterladen** in der Ereignisdetailsymbolleiste.
2. Wählen Sie eine der folgenden Optionen aus:

- Wenn Sie die Datei öffnen wollen, um sie umgehend anzuzeigen, wählen Sie die Option **Öffnen mit** aus und anschließend eine Anwendung aus dem Listenfeld.
- Wenn Sie die Liste sichern wollen, wählen Sie die Option **Datei speichern** aus.

3. Klicken Sie auf **OK**.

Ereignisse exportieren

Ereignisse können in den Formaten XML oder CSV exportiert werden.

Vorbereitende Schritte

Die erforderliche Zeit zum Exportieren von Daten hängt von der Anzahl angegebener Parameter ab.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Optional. Wenn Sie Ereignisse im Datenstrommodus anzeigen, klicken Sie auf das **Pause**-Symbol, um das Streaming anzuhalten.
3. Wählen Sie im Listenfeld **Aktionen** eine der folgenden Optionen aus.
   - **In XML exportieren** > **Angezeigte Spalten** - Wählen Sie diese Option aus, um nur die Spalten zu exportieren, die auf der Protokollaktivitäts-Registerkarte sichtbar sind. Dies ist die empfohlene Option.
   - **In XML exportieren** > **Vollständiger Export (Alle Spalten)** - Wählen Sie diese Option aus, um alle Ereignisparameter zu exportieren. Ein vollständiger Export kann etwas mehr Zeit in Anspruch nehmen.
   - **In CSV exportieren** > **Angezeigte Spalten** - Wählen Sie diese Option aus, um nur die Spalten zu exportieren, die auf der Protokollaktivitäts-Registerkarte sichtbar sind. Dies ist die empfohlene Option.
   - **In CSV exportieren** > **Vollständiger Export (Alle Spalten)** - Wählen Sie diese Option aus, um alle Ereignisparameter zu exportieren. Ein vollständiger Export kann etwas mehr Zeit in Anspruch nehmen.
4. Wenn Sie Ihre Aktivitäten fortsetzen wollen, während der Export in Bearbeitung ist, klicken Sie auf **Bei Abschluss benachrichtigen**.

Ergebnisse

Wenn der Export vollständig ausgeführt wurde, erhalten Sie eine Benachrichtigung, dass er abgeschlossen ist. Wenn Sie das Symbol **Status** nicht ausgewählt haben, wird das Statusfenster angezeigt.

Kapitel 5. Diagrammverwaltung

Zur Anzeige Ihrer Daten können Sie verschiedene Diagrammkonfigurationsoptionen verwenden.

Wenn Sie einen Zeitrahmen oder eine Gruppierungsoption auswählen, um Ihre Daten anzuzeigen, werden die Diagramme über der Ereignisliste angezeigt.

Im Datenstrommodus werden keine Diagramme angezeigt.

Sie können ein Diagramm konfigurieren, um auszuwählen, welche Daten Sie darstellen möchten. Sie können Diagramme unabhängig voneinander konfigurieren, um Ihre Suchergebnisse aus unterschiedlichen Perspektiven anzuzeigen.

Mögliche Diagrammtypen:

- Balkendiagramm - die Daten werden in einem Balkendiagramm angezeigt. Diese Option ist nur für gruppierte Ereignisse verfügbar.
- Kreisdiagramm - die Daten werden in einem Kreisdiagramm angezeigt. Diese Option ist nur für gruppierte Ereignisse verfügbar.
- Tabelle - die Daten werden in einer Tabelle angezeigt. Diese Option ist nur für gruppierte Ereignisse verfügbar.
- Zeitreihe - bei Verwendung dieser Option wird ein interaktives Kurvendiagramm angezeigt, in dem die Datensätze dargestellt sind, die mit einem bestimmten Zeitintervall abgeglichen wurden. Informationen zur Konfiguration von Suchkriterien für Zeitreihen finden Sie im Abschnitt Zeitreihendiagramm - Übersicht.

Nachdem Sie ein Diagramm konfiguriert haben, bleibt Ihre Diagrammkonfiguration erhalten, wenn Sie:

- die Ansicht über das Listenfeld **Anzeige** ändern
- einen Filter anwenden
- die Suchkriterien speichern.

Ihre Diagrammkonfiguration bleibt nicht erhalten, wenn Sie:

- einen neuen Suchvorgang starten
- auf eine Schnellsuche zugreifen
- gruppierte Ergebnisse in einem Verzweigungsfenster anzeigen
- die Suchergebnisse speichern.

Anmerkung: Wenn Sie den Web-Browser Mozilla Firefox verwenden und eine Anzeigenblocker-Browsererweiterung installiert ist, werden keine Diagramme angezeigt. Um Diagramme anzuzeigen, müssen Sie die Anzeigenblocker-Browsererweiterung entfernen. Weitere Informationen finden Sie in Ihrer Browserdokumentation.

Zeitreihendiagramm - Übersicht

Zeitreihendiagramme sind grafische Darstellungen Ihrer Aktivität im Lauf der Zeit.

Die in den Diagrammen dargestellten Spitzenwerte und Tiefpunkte stellen Zeitpunkte mit besonders starker Aktivität bzw. geringer Aktivität dar. Zeitreihendiagramme eignen sich zur kurz- und langfristigen Datentrendermittlung.

Über die Zeitreihendiagramme können Sie von verschiedenen Ansichten und Perspektiven auf die Protokoll- bzw. Netzaktivität zugreifen, darin navigieren und sie untersuchen.

Anmerkung: Sie benötigen die entsprechenden Rollenberechtigungen zum Verwalten und Anzeigen von Zeitreihendiagrammen.

Wenn Sie Zeitreihendiagramme anzeigen möchten, müssen Sie eine Suche mit Zeitreihen- und Gruppierungsoptionen erstellen und speichern. Sie können bis zu 100 Zeitreihensuchen speichern.

Mit der Standardzeitreihe gespeicherte Suchen sind über die Liste der verfügbaren Suchen auf der Seite zur Ereignissuche zugänglich.

Gespeicherte Zeitreihensuchen sind im Menü **Schnellsuchvorgänge** ganz leicht zu erkennen, da dem Namen der Suche der in den Suchkriterien angegebene Zeitraum angehängt ist.

Falls Ihre Suchparameter mit einer zuvor gespeicherten Suche nach Spaltendefinitions- und Gruppierungsoptionen übereinstimmen, wird möglicherweise für Ihre Suchergebnisse automatisch ein Zeitreihendiagramm angezeigt. Falls für Ihre nicht gespeicherten Suchkriterien nicht automatisch ein Zeitreihendiagramm angezeigt wird, gibt es keine zuvor gespeicherten Suchkriterien, die Ihren Suchparametern entsprechen. In diesem Fall müssen Sie die Erfassung von Zeitreihendaten aktivieren und die Suchkriterien speichern.

Sie haben die Möglichkeit, die Zeitachse in einem Zeitreihendiagramm zu vergrößern und zu durchsuchen, um die Aktivitäten genau zu prüfen. In der folgenden Tabelle sind die Funktionen aufgeführt, die zur Anzeige von Zeitreihendiagrammen verwendet werden können.

Tabelle 18. Funktionen von Zeitreihendiagrammen

Funktion	Beschreibung
View data in greater detail (Daten genauer anzeigen)	Mit dem Zoomfeature können Sie kleinere Zeitsegmente des Auftretens von Ereignissen untersuchen. • Bewegen Sie den Mauszeiger über das Diagramm und vergrößern Sie das Diagramm durch Drehen des Mausrads (drehen Sie das Mausrad nach oben). • Markieren Sie den zu vergrößernden Bereich des Diagramms. Wenn Sie die Maustaste loslassen, wird in dem Diagramm ein kleineres Zeitsegment angezeigt. Sie können nun auf das Diagramm klicken und es ziehen und so genau durchsuchen. Wenn Sie ein Zeitreihendiagramm vergrößern, wird das Diagramm aktualisiert und es wird ein kleineres Zeitsegment angezeigt.

Tabelle 18. Funktionen von Zeitreihendiagrammen (Forts.)

Funktion	Beschreibung
View a larger time span of data (Größere Zeitspanne von Daten anzeigen)	Mit dem Zoomfeature können Sie größere Zeitsegmente untersuchen oder wieder zum maximalen Zeitraum zurückkehren. Zeiträume können wie folgt erweitert werden: • Klicken Sie auf 'Zoom zurücksetzen' oben links in dem Diagramm. • Bewegen Sie den Mauszeiger über das Diagramm und erweitern Sie die Anzeige durch Drehen des Mausrads (drehen Sie das Mausrad nach unten).
Scan the chart (Diagramm durchsuchen)	Wenn Sie ein Zeitreihendiagramm vergrößert haben, können Sie darauf klicken und das Diagramm nach links oder rechts ziehen, um die Zeitachse zu durchsuchen.

Diagrammlegenden

Zu jedem Diagramm gibt es eine Legende. Hierbei handelt es sich um einen visuellen Verweis zur leichteren Zuordnung der Diagrammobjekte zu den Parametern, die sie darstellen.

Mit der Legendenfunktion können Sie die folgenden Aktionen ausführen:

- Bewegen des Mauszeigers über ein Legendenelement oder den Legendenfarbblock, um weitere Informationen zu den betreffenden Parametern anzuzeigen.
- Anklicken des Legendenelements mit der rechten Maustaste, um weitere Informationen zu dem betreffenden Element abzurufen.
- Anklicken eines Legendenelements eines Kreis- oder Balkendiagramms, um das betreffende Element aus dem Diagramm auszublenden. Erneutes Anklicken des Legendenelements, um das ausgeblendete Element wieder anzuzeigen. Sie können auch auf das entsprechende Diagrammelement klicken, um das Element auszublenden und anzuzeigen.
- Anklicken der Option **Legende** oder des Pfeils neben dieser Option, wenn Sie die Legende aus der Diagrammanzeige entfernen möchten.

Diagramme konfigurieren

Mithilfe von Konfigurationsoptionen können Sie den Diagrammtyp, den darzustellenden Objekttyp und die Anzahl der im Diagramm dargestellten Objekte ändern. Bei Zeitreihendiagrammen können Sie außerdem einen Zeitraum auswählen und die Erfassung von Zeitreihendaten aktivieren.

Vorbereitende Schritte

Wenn Sie Ereignisse im Echtzeitmodus (Datenstrommodus) anzeigen, werden keine Diagramme angezeigt. Um Diagramme anzuzeigen, müssen Sie die Registerkarte **Protokollaktivität** aufrufen und eine der folgenden Optionen auswählen:

- Wählen Sie in den Listenfeldern **Ansicht** und **Anzeigen** Optionen aus und klicken Sie anschließend in der Symbolleiste auf **Kriterien speichern**. Weitere Informationen hierzu finden Sie in Abschnitt Ereignis- und Datenflusssuchkriterien speichern.

- Wählen Sie in der Symbolleiste eine gespeicherte Suche aus der Liste **Schnellsuche** aus.
- Führen Sie eine gruppierte Suche durch und klicken Sie anschließend in der Symbolleiste auf **Kriterien speichern**.

Wenn Sie ein Zeitreihendiagramm konfigurieren möchten, stellen Sie sicher, dass die gespeicherten Suchkriterien gruppiert sind und ein Zeitraum angegeben ist.

Informationen zu diesem Vorgang

Daten können kumuliert werden. Wenn Sie eine Zeitreihensuche durchführen, ist daher ein Cache mit Daten verfügbar, sodass die Daten des letzten Zeitraums angezeigt werden können. Wenn Sie die Erfassung von Zeitreihendaten für einen ausgewählten Parameter aktiviert haben, wird im Listenfeld 'Wert zu Diagramm' neben dem Parameter ein Stern (*) angezeigt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie im Diagrammbereich auf das Symbol **Konfigurieren**.
3. Konfigurieren Sie Werte für die folgenden Parameter:

Option	**Bezeichnung**
Parameter	Beschreibung
Wert zu Diagramm	Wählen Sie im Listenfeld den Objekttyp aus, den Sie auf der Y-Achse des Diagramms darstellen möchten. Zu den möglichen Optionen gehören alle in Ihren Suchparametern enthaltenen normalisierten und angepassten Ereignisparameter.
Wichtigste anzeigen	Wählen Sie im Listenfeld aus, wie viele Objekte im Diagramm angezeigt werden sollen. Der Standardwert ist 10. Wenn Sie mehr als 10 Elemente grafisch darstellen, besteht die Gefahr, dass die Diagrammdaten nicht mehr gut lesbar sind.
Diagrammtyp	Wählen Sie im Listenfeld den Diagrammtyp aus, der angezeigt werden soll. Wenn Ihr Balken-, Kreis- oder Tabellendiagramm auf gespeicherten Suchkriterien mit einem Zeitraum von mehr als 1 Stunde basieren, müssen Sie auf **Details aktualisieren** klicken, damit das Diagramm aktualisiert wird und die Ereignisdetails ausgefüllt werden.
Zeitreihendaten erfassen	Wählen Sie dieses Kontrollkästchen aus, wenn Sie die Erfassung von Zeitreihendaten aktivieren möchten. Bei Auswahl dieses Kontrollkästchens beginnt die Diagrammfunktion damit, Daten für Zeitreihendiagramme zu kumulieren. Standardmäßig ist diese Option inaktiviert. Diese Option ist nur bei Zeitreihendiagrammen verfügbar.

Option	Bezeichnung
Zeitraum	Wählen Sie im Listenfeld den Zeitraum aus, der angezeigt werden soll. Diese Option ist nur bei Zeitreihendiagrammen verfügbar.

4. Klicken Sie in der Symbolleiste auf **Kriterien speichern**, wenn Sie die Diagrammoption **Zeitreihe** ausgewählt und die Option **Zeitreihendaten erfassen** aktiviert haben.
5. Klicken Sie auf **Details aktualisieren**, um die Liste der Ereignisse anzuzeigen, wenn der Zeitraum mehr als 1 Stunde umfasst.

Kapitel 6. Datensuche

Auf der Registerkarte **Protokollaktivität** können Sie unter Verwendung bestimmter Kriterien Ereignisse durchsuchen.

Sie können eine Suche erstellen oder eine zuvor gespeicherte Gruppe von Suchkriterien laden. Sie können die Spalten mit den in den Suchergebnissen anzuzeigenden Daten auswählen, organisieren und gruppieren.

Nachdem Sie eine Suche ausgeführt haben, können Sie die Suchkriterien und die Suchergebnisse speichern.

Nach Elementen suchen, die mit Ihren Kriterien übereinstimmen

Sie können nach Daten suchen, die mit Ihren Suchkriterien übereinstimmen.

Informationen zu diesem Vorgang

Da die gesamte Datenbank durchsucht wird, können manche Suchvorgänge abhängig von der Datenbankgröße mehr Zeit in Anspruch nehmen.

Sie können den Suchparameter **Schnellfilter** verwenden, um nach Elementen zu suchen, die mit einer Textzeichenfolge in den Ereignisnutzdaten übereinstimmen.

In der folgenden Tabelle werden die Suchoptionen beschrieben, mit denen Sie Ereignis- und Datenflussdaten suchen können:

Tabelle 19. Suchoptionen

Optionen	Beschreibung
Gruppe	Wählen Sie eine Ereignissuchgruppe für die Anzeige in der Liste **Verfügbare gespeicherte Suchvorgänge** aus.
Geben Sie den gespeicherten Suchvorgang ein oder treffen Sie eine Auswahl in der Liste	Geben Sie den Namen einer gespeicherten Suche oder ein Schlüsselwort ein, um die Liste **Verfügbare gespeicherte Suchvorgänge** zu filtern.
Verfügbare gespeicherte Suchvorgänge	In dieser Liste werden alle verfügbaren Suchen angezeigt, außer Sie verwenden die Option **Geben Sie den gespeicherten Suchvorgang ein** oder **treffen Sie eine Auswahl in der Liste**, um einen Filter auf die Liste anzuwenden. Sie können eine gespeicherte Suche in dieser Liste zum Anzeigen oder Bearbeiten auswählen.
Suchen	Das **Suchen**-Symbol ist in mehreren Teilfenstern auf der Suchseite verfügbar. Sie können auf 'Suchen' klicken, wenn Sie mit dem Konfigurieren der Suche fertig sind und die Ergebnisse anzeigen wollen.
In meine Schnellsuche aufnehmen	Wählen Sie dieses Kontrollkästchen aus, um diese Suche im Menü **Schnellsuche** einzubeziehen.

Tabelle 19. Suchoptionen (Forts.)

Optionen	Beschreibung
In mein Dashboard aufnehmen	Wählen Sie dieses Kontrollkästchen aus, um die Daten aus Ihrer gespeicherten Suche auf der Registerkarte **Dashboard** einzuschließen. Weitere Informationen zur Registerkarte **Dashboard** erhalten Sie im Abschnitt Dashboard-Verwaltung. **Anmerkung:** Dieser Parameter wird nur angezeigt, wenn die Suche gruppiert ist.
Als Standardwert definieren	Wählen Sie dieses Kontrollkästchen aus, um diese Suche als Standardsuche festzulegen.
Freigeben für jeden	Wählen Sie dieses Kontrollkästchen aus, um diese Suche für alle anderen Benutzern freizugeben.
Echtzeit (Streaming)	Zeigt Ergebnisse im Datenstrommodus an. Weitere Informationen zum Datenstrommodus erhalten Sie im Abschnitt Streaming-Ereignisse anzeigen. **Anmerkung:** Wenn 'Echtzeit (Streaming)' aktiviert ist, sind Sie nicht in der Lage, Ihre Suchergebnisse zu gruppieren. Wenn Sie eine Gruppierungsoption im Spaltendefinitions-Teilfenster auswählen, wird eine Fehlernachricht angezeigt.
Letztes Intervall (automatisches Aktualisieren)	Zeigt die Suchergebnisse im Modus für automatische Aktualisierung an. Im Modus für automatische Aktualisierung wird die Registerkarte **Protokollaktivität** in Ein-Minuten-Intervallen aktualisiert, um die neuesten Informationen anzuzeigen.
Aktuelle	Wählen Sie einen vordefinierten Zeitbereich für Ihre Suche aus. Nachdem Sie diese Option ausgewählt haben, müssen Sie eine Zeitbereichsoption aus dem Listenfeld auswählen.
Bestimmtes Intervall	Wählen Sie einen angepassten Zeitbereich für Ihre Suche aus. Nachdem Sie diese Option ausgewählt haben, müssen Sie den Datums-/Zeitbereich aus den Kalendern **Startzeit** und **Endzeit** auswählen.

Tabelle 19. Suchoptionen (Forts.)

Optionen	Beschreibung
Datenzusammenfassung	Dieser Fensterbereich wird nur angezeigt, wenn Sie eine gespeicherte Suche laden. Die Aktivierung eindeutiger Zähler für aufgelaufene Daten, die auch in anderen gespeicherten Suchvorgängen und Berichten genutzt werden, kann die Systemleistung beeinträchtigen. Wenn Sie eine gespeicherte Suche laden, zeigt dieses Teilfenster die folgenden Optionen an: • Wenn sich keine Daten für diese gespeicherte Suche summieren, wird die folgende Informationsnachricht angezeigt: `Es werden keine Daten für diese Suche zusammengefasst`. • Wenn sich Daten für diese gespeicherte Suche summieren, werden folgende Optionen angezeigt: – **Spalten** - Wenn Sie den Mauszeiger über diesen Link bewegen oder ihn anklicken, wird eine Liste mit den Spalten angezeigt, die Daten zusammenfassen. – **Eindeutige Zähler aktivieren/ Eindeutige Zähler inaktivieren** - Dieser Link ermöglicht Ihnen, die Suchergebnisse für die Anzeige von eindeutigen Ereigniszählern anstatt von Durchschnittszählern über die Zeit anzuzeigen. Nachdem Sie auf den Link **Eindeutige Zähler aktivieren** geklickt haben, wird ein Dialogfenster geöffnet und angegeben, welche gespeicherten Suchen und Berichte die zusammengefassten Daten freigeben.
Aktuelle Filter	Diese Liste zeigt die Filter an, die auf diese Suche angewendet werden. Die Optionen zum Hinzufügen eines Filters befinden sich über der Liste **Aktuelle Filter**.
Ergebnisse nach Abschluss des Suchvorgangs speichern	Wählen Sie dieses Kontrollkästchen aus, um die Suchergebnisse zu sichern und zu benennen.
Anzeigen	Wählen Sie diese Liste aus, um eine vordefinierte Spalte anzugeben, die in den Suchergebnissen angezeigt werden soll.

Tabelle 19. Suchoptionen (Forts.)

Optionen	Beschreibung
Geben Sie die Spalte ein oder treffen Sie eine Auswahl in der Liste	Mit diesem Feld können Sie die Spalten filtern, die in der Liste 'Verfügbare Spalten' aufgeführt werden. Geben Sie den Namen der Spalte ein, die Sie lokalisieren wollen, oder geben Sie ein Schlüsselwort ein, um eine Liste von Spaltennamen anzuzeigen. Geben Sie zum Beispiel `Gerät` ein, um eine Liste von Spalten anzuzeigen, die 'Gerät' im Spaltennamen enthalten.
Verfügbare Spalten	Diese Liste zeigt verfügbare Spalten an. Spalten, die gegenwärtig in Verwendung für diese gespeicherte Suche sind, werden hervorgehoben und in der Liste **Spalten** angezeigt.
Spaltensymbole hinzufügen und entfernen (obere Reihe)	Verwenden Sie die obere Reihe von Symbolen, um die Liste **Gruppieren nach** anzupassen. • **Spalte hinzufügen** - Wählen Sie eine oder mehrere Spalten aus der Liste **Verfügbare Spalten** aus und klicken Sie auf das Symbol **Spalte hinzufügen**. • **Spalte entfernen** - Wählen Sie eine oder mehrere Spalten aus der Liste **Gruppieren nach** aus und klicken Sie auf das Symbol **Spalte entfernen**.
Spaltensymbole hinzufügen und entfernen (untere Reihe)	Verwenden Sie die untere Reihe von Symbolen, um die Liste **Spalten** anzupassen. • **Spalte hinzufügen** - Wählen Sie eine oder mehrere Spalten aus der Liste 'Verfügbare Spalten' aus und klicken Sie auf das Symbol **Spalte hinzufügen**. • **Spalte entfernen** - Wählen Sie eine oder mehrere Spalten aus der Liste 'Spalten' aus und klicken Sie auf das Symbol **Spalte entfernen**.

Tabelle 19. Suchoptionen (Forts.)

Optionen	Beschreibung
Gruppieren nach	Diese Liste gibt die Spalten an, in denen die gespeicherte Suche die Ergebnisse gruppiert. Verwenden Sie die folgenden Optionen, um die Liste 'Gruppieren nach' weiter anzupassen: • Nach oben - Wählen Sie eine Spalte aus, und verschieben Sie sie mithilfe des Symbols **Nach oben** in der Prioritätenliste nach oben. • Nach unten - Wählen Sie eine Spalte aus, und verschieben Sie sie mithilfe des Symbols **Nach unten** in der Prioritätenliste nach unten. Die Prioritätenliste gibt an, in welcher Reihenfolge die Ergebnisse gruppiert werden. Die Suchergebnisse werden nach der ersten Spalte in der Liste **Gruppieren nach** gruppiert und danach nach der nächsten Spalte der Liste.
Spalten	Gibt Spalten an, die für die Suche ausgewählt werden. Sie können mehr Spalten in der Liste **Verfügbare Spalten** auswählen. Sie können die Liste **Spalten** mithilfe der folgenden Optionen weiter anpassen: • **Nach oben** - Verschiebt die ausgewählte Spalte in der Prioritätenliste nach oben. • **Nach unten** - Verschiebt die ausgewählte Spalte in der Prioritätenliste nach unten. Wenn der Spaltentyp numerisch oder zeitbasiert ist und es gibt einen Eintrag in der Liste **Gruppieren nach**, dann schließt die Spalte ein Listenfeld ein. Verwenden Sie das Listenfeld, um auszuwählen, wie Sie die Spalte gruppieren wollen. Wenn der Spaltentyp 'Gruppe' ist, schließt die Spalte ein Listenfeld ein, um auszuwählen, wie viele Ebenen Sie für die Gruppe einschließen wollen.
Sortieren nach	Wählen Sie im ersten Listenfeld die Spalte aus, nach der Sie die Suchergebnisse sortieren wollen. Wählen Sie dann vom zweiten Listenfeld die Reihenfolge aus, die Sie für die Suchergebnisse verwenden wollen. Zu den Optionen gehören **Absteigend** und **Aufsteigend**.

Tabelle 19. Suchoptionen (Forts.)

Optionen	Beschreibung
Grenzwert für die Ergebnisse	Sie können im Fenster **Suche bearbeiten** die Anzahl der Zeilen angeben, die eine Suche zurückgibt. Das Feld **Grenzwert für die Ergebnisse** ist ebenfalls im Fenster **Ergebnisse** zu sehen. • Für eine gespeicherte Suche wird die Begrenzung in der gespeicherten Suche gespeichert und wieder angewendet, wenn die Suche geladen wird. • Wenn man in einer Spalte in dem Suchergebnis sortiert, das eine Zeilenbegrenzung aufweist, wird die Sortierung innerhalb der beschränkten Zeilen ausgeführt, die im Datengrid angezeigt werden. • Bei einer Suche mit 'Gruppiert nach' und aktiviertem Zeitreihe-Diagramm gilt die Zeilenbegrenzung nur für den Datengrid. Über das Dropdown-Element **Top N** im Zeitreihe-Diagramm wird weiterhin bestimmt, wie viele Zeitreihen im Diagramm gezeichnet werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Suchen** den Eintrag **Neue Suche** aus.
3. So wählen Sie eine zuvor gespeicherte Suche aus:
   a. Wählen Sie eine der folgenden Optionen aus: `Wählen Sie in der Liste 'Verfügbare gespeicherte Suchvorgänge' die gespeicherte Suche aus, die geladen werden soll.Geben Sie im Feld 'Geben Sie den gespeicherten Suchvorgang ein oder treffen Sie eine Auswahl in der Liste' den Namen der Suche ein, die geladen werden soll.`
   b. Klicken Sie auf **Laden**.
   c. Wählen Sie im Teilfenster 'Suche bearbeiten' die gewünschten Optionen für diese Suche aus. Weitere Informationen hierzu finden Sie in Tabelle 1.
4. Um eine Suche zu erstellen, wählen Sie im Teilfenster 'Zeitraum' die Optionen für den Zeitraum aus, den Sie für diese Suche erfassen wollen.
5. Optional. Aktivieren Sie im Teilfenster 'Datenzusammenfassung' eindeutige Zähler:
   a. Klicken Sie auf **Eindeutige Zähler aktivieren**.
   b. Lesen Sie im Fenster **Warnung** den Warnhinweis und klicken Sie auf **Fortfahren**. Weitere Informationen zur Aktivierung eindeutiger Zähler erhalten Sie in Tabelle 1.
6. Definieren Sie im Suchparameter-Teilfenster Ihre Suchkriterien:
   a. Wählen Sie im ersten Listenfeld einen Parameter aus, nach dem Sie suchen wollen. Beispiel: Einheit, Quellenport oder Ereignisname.
   b. Wählen Sie im zweiten Listenfeld den Modifikator aus, den Sie für die Suche verwenden wollen.
   c. Geben Sie im Eingabefeld spezifische Informationen ein, die zu Ihrem Suchparameter gehören.

d. Klicken Sie auf **Filter hinzufügen**.
e. Wiederholen Sie die Schritte a bis d für jeden Filter, den Sie den Suchkriterien hinzufügen wollen.

7. Optional. Um die Suchergebnisse automatisch zu sichern, wenn der Suchvorgang abgeschlossen ist, wählen Sie das Kontrollkästchen **Ergebnisse nach Abschluss des Suchvorgangs speichern** aus und geben Sie anschließend einen Namen für die gespeicherte Suche ein.
8. Definieren Sie im Spaltendefinition-Teilfenster die Spalten und das Spaltenlayout, die Sie verwenden wollen, um die Ergebnisse anzuzeigen:
   a. Wählen Sie im Listenfeld **Anzeigen** die vorkonfigurierte Spalte aus, die mit dieser Suche verknüpft wird.
   b. Klicken Sie auf den Pfeil neben **Erweiterte Ansichtsdefinition**, um erweiterte Suchparameter anzuzeigen.
   c. Passen Sie die in den Suchergebnissen anzuzeigenden Spalten an. Weitere Informationen hierzu finden Sie in Tabelle 1.
   d. Optional. Geben Sie im Feld **Grenzwert für die Ergebnisse** die Anzahl der Zeilen ein, die die Suche zurückgeben soll.
9. Klicken Sie auf **Filter**.

Ergebnisse

Der Status **In Bearbeitung (<Prozent>% abgeschlossen)** wird in der rechten oberen Ecke angezeigt.

.

Während partielle Suchergebnisse angezeigt werden, ist die Suchmaschine im Hintergrund aktiv, um die Suche auszuführen, und aktualisiert die partiellen Ergebnisse für Ihre Ansicht.

Wenn die Suche fertig ist, wird der Status **Abgeschlossen** in der rechten oberen Ecke angezeigt.

Zugehörige Konzepte:

„Erweiterte Suchoptionen” auf Seite 66
Im Feld **Erweiterte Suche** können Sie für die Ausführung einer Abfrage einen AQL-Suchbegriff (Ariel Query Language) eingeben, in dem festgelegt wird, welche Felder zurückgegeben und wie sie angeordnet werden sollen.

„Beispiele für AQL-Suchbegriffe” auf Seite 67
Mit AQL (Ariel Query Language) können Sie aus Ereignissen, Datenflüssen und simarc-Tabellen in der Ariel-Datenbank bestimmte Felder abrufen.

Suchkriterien speichern

Sie können konfigurierte Suchkriterien sichern, so dass Sie die Kriterien wiederverwenden und in anderen Komponenten, wie z. B. Berichte, nutzen können. Gespeicherte Suchkriterien verfallen nicht.

Informationen zu diesem Vorgang

Wenn Sie einen Zeitbereich für Ihre Suche angeben, wird Ihr Suchname mit dem angegebenen Zeitbereich angehängt. Beispiel: Eine gespeicherte Suche mit dem Namen 'Exploits von Quelle' mit dem Zeitraum der letzten 5 Minuten wird zu 'Exploits von Quelle - Letzte 5 Minuten'.

Wenn Sie eine Spaltengruppe in einer zuvor gespeicherten Suche ändern und dann die Suchkriterien mit dem gleichen Namen sichern, gehen vorherige Zusammenfassungen für Zeitreihendiagramme verloren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Führen Sie eine Suche durch.
3. Klicken Sie auf **Kriterien speichern**.
4. Folgende Parameter müssen angegeben werden:

Option	**Bezeichnung**
Parameter	Beschreibung
Name der Suche	Geben Sie den eindeutigen Namen ein, den Sie diesen Suchkriterien zuweisen wollen.
Suche zu Gruppe(n) zuordnen	Wählen Sie das Kontrollkästchen für die Gruppe aus, der Sie diese gespeicherte Suche zuweisen wollen. Wenn Sie keine Gruppe auswählen, wird diese gespeicherte Suche standardmäßig der Gruppe 'Sonstige' zugewiesen. Weitere Informationen finden Sie im Abschnitt Suchgruppen verwalten.
Gruppen verwalten	Klicken Sie auf **Gruppen verwalten**, um Suchgruppen zu verwalten. Weitere Informationen finden Sie im Abschnitt Suchgruppen verwalten.
Zeitraumoptionen:	Wählen Sie eine der folgenden Optionen: • **Echtzeit (Streaming)** - Wählen Sie diese Option aus, um Ihre Suchergebnisse während des Datenstrommodus zu filtern. • **Letztes Intervall (automatisches Aktualisieren)** - Wählen Sie diese Option aus, um Ihre Suchergebnisse während des automatischen Aktualisierungsmodus zu filtern. Die Registerkarten **Protokollaktivität** und **Netzaktivität** werden in Ein-Minuten-Intervallen aktualisiert, um die neuesten Informationen anzuzeigen. • **Aktuelle** - Wählen Sie diese Option und dann in diesem Listenfeld den Zeitbereich aus, für den Sie filtern wollen. • **Bestimmtes Intervall** - Wählen Sie diese Option und dann im Kalender das Datum und den Zeitraum aus, für die Sie filtern wollen.
In meine Schnellsuche aufnehmen	Wählen Sie dieses Kontrollkästchen aus, um diese Suche im Listenfeld **Schnellsuche** der Symbolleiste einzubeziehen.
In mein Dashboard aufnehmen	Wählen Sie dieses Kontrollkästchen aus, um die Daten aus Ihrer gespeicherten Suche auf der Registerkarte **Dashboard** einzuschließen. Weitere Informationen zur Registerkarte **Dashboard** erhalten Sie im Abschnitt Dashboard-Verwaltung. **Anmerkung:** Dieser Parameter wird nur angezeigt, wenn die Suche gruppiert ist.

Option	Bezeichnung
Als Standardwert definieren	
Freigeben für jeden	Wählen Sie dieses Kontrollkästchen aus, um diese Suchanforderungen für alle Benutzer freizugeben.

5. Klicken Sie auf **OK**.

Geplanter Suchvorgang

Über die Option 'Geplanter Suchvorgang' können Sie eine Suche terminieren und die Ergebnisse anzeigen.

Sie können eine Suche für eine bestimmte Tages- oder Nachtzeit terminieren.

Beispiel:
Wenn Sie die Ausführung einer Suche nachts ansetzen, können Sie die Ergebnisse am nächsten Morgen untersuchen. Im Gegensatz zu Berichten können Sie Suchergebnisse zusammenfassen und eingehender untersuchen. Sie haben die Möglichkeit, nach der Anzahl fehlgeschlagener Anmeldungen in Ihrer Netzgruppe zu suchen. Wenn die Anzahl in der Regel bei 10 liegt, die Suche aber 100 ergibt, können Sie die Suchergebnisse in Gruppen zusammenfassen, um die Untersuchung zu erleichtern. Um festzustellen, für welchen Benutzer die meisten fehlgeschlagenen Anmeldungen verzeichnet werden, können Sie eine Gruppierung nach Benutzername vornehmen. Anschließend können Sie eine weitergehende Untersuchung vornehmen.

Auf der Registerkarte **Berichte** können Sie eine Suche in Ereignissen oder Datenflüssen terminieren. Dazu müssen Sie zunächst eine zuvor gespeicherte Gruppe von Suchkriterien auswählen.

1. Bericht erstellen

   Geben Sie im Fenster **Berichtsassistent** die folgenden Informationen ein:

   - Der Diagrammtyp ist 'Ereignisse/Protokolle' oder 'Datenflüsse'.
   - Der Bericht basiert auf einer gespeicherten Suche.
   - Angriff generieren

     Sie können die Option **Einen individuellen Angriff generieren** oder die Option **Ergebnis zu einem bestehenden Angriff hinzufügen** auswählen.

     Sie können auch eine manuelle Suche generieren.
2. Suchergebnisse anzeigen

Sie können die Ergebnisse Ihrer geplanten Suche auf der Registerkarte **Angriffe** anzeigen.

- Angriffe in geplanten Suchvorgängen werden in der Spalte **Angriffstyp** angegeben.

  Wenn Sie einen Einzelangriff erstellen, wird bei jeder Ausführung eines Berichts ein Angriff generiert. Wenn Sie das Ergebnis der gespeicherten Suche einem vorhandenen Angriff hinzufügen, wird bei der ersten Ausführung des Berichts ein Angriff erstellt. Nachfolgende Berichtsausführungen werden an diesen Angriff angehängt. Werden keine Ergebnisse zurückgegeben, hängt das System keinen Angriff an bzw. erstellt keinen Angriff.
- Damit im Fenster **Zusammenfassung des Angriffs** die aktuellsten Suchergebnisse angezeigt werden, doppelklicken Sie in der Liste mit Angriffen auf einen An-

griff in einer geplante Suche. Um eine Liste sämtlicher geplanter Suchausführungen anzuzeigen, klicken Sie im Fenster **Letzte 5 Suchergebnisse** auf **Suchergebnisse**.

Sie können einen Angriff in einer geplanten Suche einem Benutzer zuweisen.

Zugehörige Konzepte:

„Erweiterte Suchoptionen"
Im Feld **Erweiterte Suche** können Sie für die Ausführung einer Abfrage einen AQL-Suchbegriff (Ariel Query Language) eingeben, in dem festgelegt wird, welche Felder zurückgegeben und wie sie angeordnet werden sollen.

„Beispiele für AQL-Suchbegriffe" auf Seite 67
Mit AQL (Ariel Query Language) können Sie aus Ereignissen, Datenflüssen und simarc-Tabellen in der Ariel-Datenbank bestimmte Felder abrufen.

Erweiterte Suchoptionen

Im Feld **Erweiterte Suche** können Sie für die Ausführung einer Abfrage einen AQL-Suchbegriff (Ariel Query Language) eingeben, in dem festgelegt wird, welche Felder zurückgegeben und wie sie angeordnet werden sollen.

Eingaben in das Feld **Erweiterte Suche** werden automatisch vervollständigt, die Syntax wird hervorgehoben.

Diese beiden Funktionen (automatische Vervollständigung und Syntaxhervorhebung) sind bei der Erstellung von Abfragen hilfreich. Informationen zu den unterstützten Web-Browsern finden Sie im Abschnitt „Unterstützte Web-Browser" auf Seite 3.

Zugriff auf 'Erweiterte Suche'

Zugriff auf die Option **Erweiterte Suche** zur Eingabe einer AQL-Abfrage erhalten Sie in der Symbolleiste **Suchen** auf der Registerkarte **Protokollaktivität**.

Wählen Sie im Listenfeld der Symbolleiste **Suchen** die Option **Erweiterte Suche** aus.

Blenden Sie wie folgt das Feld **Erweiterte Suche** ein:

1. Ziehen Sie das Symbol zum Einblenden rechts im Feld.
2. Springen Sie mit der Tastenkombination Umschaltetaste+Eingabetaste in die nächste Zeile.
3. Drücken Sie die Eingabetaste.

Sie können mit der rechten Maustaste auf einen beliebigen Wert in den Suchergebnissen klicken und eine Filterung anhand dieses Wertes vornehmen.

Bei Doppelklicken auf eine Zeile in den Suchergebnissen werden weitere Informationen angezeigt.

Alle Suchvorgänge, einschließlich AQL-Suchläufe, sind im Prüfprotokoll enthalten.

Beispiele für AQL-Suchbegriffe

Die folgende Tabelle enthält Beispiele für AQL-Suchbegriffe.

Tabelle 20. AQL-Suchbegriffe - Beispiele

Beschreibung	Beispiel
Standardspalten in Ereignissen auswählen:	`SELECT * FROM events`
Bestimmte Spalten auswählen:	`SELECT sourceip, destinationip FROM events`
Bestimmte Spalten auswählen und Ergebnisse sortieren:	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
Zusammengefasste Suchabfrage ausführen:	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
Funktionsaufruf in einer SELECT-Klausel ausführen:	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
Suchergebnisse anhand einer WHERE-Klausel filtern:	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
Nach Ereignissen suchen, die eine bestimmte Regel ausgelöst haben (der Regelname oder Teile des Regelnamens werden angegeben):	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
Auf Feldnamen verweisen, die Sonderzeichen (beispielsweise arithmetische Zeichen oder Leerzeichen) enthalten, indem der Feldname in Anführungszeichen gesetzt wird:	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

Weitere Informationen zu Funktionen, simarc-Feldern und Operatoren finden Sie im Handbuch zu Ariel Query Language.

Zugehörige Konzepte:

„Geplanter Suchvorgang” auf Seite 65
Über die Option 'Geplanter Suchvorgang' können Sie eine Suche terminieren und die Ergebnisse anzeigen.

„Suche mit Filtern” auf Seite 70
Sie können Ereignis- und Datenflussnutzdaten durch Eingabe von Textsuchbegriffen (einfache Wörter oder Wortfolgen) durchsuchen.

Zugehörige Tasks:

„Nach Elementen suchen, die mit Ihren Kriterien übereinstimmen” auf Seite 57
Sie können nach Daten suchen, die mit Ihren Suchkriterien übereinstimmen.

Beispiele für AQL-Suchbegriffe

Mit AQL (Ariel Query Language) können Sie aus Ereignissen, Datenflüssen und simarc-Tabellen in der Ariel-Datenbank bestimmte Felder abrufen.

Berichte zur Accountnutzung

Für unterschiedliche Benutzercommunitys kann es unterschiedliche Hinweise auf Bedrohungen und die Nutzung geben.

Über Referenzdaten können Sie Berichte zu mehreren Benutzereigenschaften (beispielsweise Abteilung, Standort Manager) erstellen.

Sie haben die Möglichkeit, externe Referenzdaten zu verwenden.

Mit der folgenden Abfrage werden Metadateninformationen zum Benutzer über deren Anmeldeereignisse zurückgegeben.

```
SELECT
REFERENCETABLE('user_data','FullName',username) as 'Full Name',
REFERENCETABLE('user_data','Location',username) as 'Location',
REFERENCETABLE('user_data','Manager',username) as 'Manager',
UNIQUECOUNT(username) as 'Userid Count',
UNIQUECOUNT(sourceip) as 'Source IP Count',
COUNT(*) as 'Event Count'
FROM events
WHERE qidname(qid) ILIKE '%logon%'
GROUP BY 'Full Name', 'Location', 'Manager'
LAST 1 days
```

Anzeige bei mehreren Account-IDs

In diesem Beispiel verfügen einzelne Benutzer über mehrere Accounts im Netz. Das Unternehmen benötigt eine zentrale Übersicht über die Aktivität eines Benutzers.

Ordnen Sie lokale Benutzer-IDs mithilfe von Referenzdaten einer globalen ID zu.

Mit der folgenden Abfrage werden die Benutzeraccounts, die von einer globalen ID verwendet werden, in Ereignissen zurückgegeben, die als verdächtig markiert sind.

```
SELECT
REFERENCEMAP('GlobalID Mapping',username) as 'Global ID',
REFERENCETABLE('user_data','FullName', 'Global ID') as 'Full Name',
UNIQUECOUNT(username),
COUNT(*) as 'Event count'
FROM events
WHERE RULENAME(creEventlist) ILIKE '%suspicious%'
GROUP BY 'Global ID'
LAST 1 days
```

Mit der folgenden Abfrage werden die Aktivitäten zurückgegeben, die von einer globalen ID ausgeführt wurden.

```
SELECT
QIDNAME(qid) as 'Event name,
starttime as Time,
sourceip as 'Source IP', destinationip as 'Destination IP',
username as 'Event  Username',
REFERENCEMAP('GlobalID_Mapping', username)as 'Global User'
FROM events
WHERE 'Global User' = 'John Doe'
LAST 1 days
```

Verdächtigen Beaconbetrieb über einen längeren Zeitraum ermitteln

Viele Bedrohungen kommunizieren tage-, wochen- oder monatelang unter Verwendung von Command-and-Control.

Mithilfe einer erweiterten Suche können die Verbindungsmuster über die Zeit ermittelt werden. So können Sie beispielsweise abfragen, ob zwischen IP-Adressen oder zwischen einer IP-Adresse und einem Standort täglich, wöchentlich oder monatlich konsistente oder kurze Verbindungen bzw. Verbindungen mit geringen Datenmengen hergestellt werden oder auch wie viele Verbindungen hergestellt werden.

Mit der REST-API von IBM Security QRadar können Sie einen Angriff generieren bzw. ein Referenzset oder eine Referenztabelle füllen.

Mit der folgenden Abfrage über Proxy-Protokollereignisse wird festgestellt, ob täglich Beaconnachrichten an eine Domäne gesandt werden. Die Beaconingzeiten variieren von Tag zu Tag, die Intervalle zwischen den einzelnen Signalen sind kurz.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG(hourofday*hourofday) - (AVG(hourofday)^2)) as variance,
COUNT(*) as 'total events'
FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist) ILIKE '%proxy%'
GROUP BY url_domain
HAVING variance < 0.1 and 'total events' < 10
LAST 7 days
```

Die Eigenschaft **url_domain** ist eine angepasste Eigenschaft aus Proxy-Protokollen.

Informationen zu externen Bedrohungen

Nutzungs- und Sicherheitsdaten, die mit Informationen zu externen Bedrohungen korreliert werden, können wichtige Hinweise auf Bedrohungen liefern.

Erweiterte Suchvorgänge können Hinweise auf externe Bedrohungen mit anderen Sicherheitsereignissen und Nutzungsdaten abgleichen.

Mit der folgenden Abfrage können Sie mithilfe von Daten zu einer externen Bedrohung, die über viele Tage, Wochen oder Monate gesammelt werden, ein Profil erstellen, um die Risikostufe für Assets und Accounts zu ermitteln und eine entsprechende Priorität zu vergeben.

```
Select
REFERENCETABLE('ip_threat_data','Category',destinationip) as 'Category',
REFERENCETABLE('ip_threat_data','Rating', destinationip) as 'Threat Rating',
UNIQUECOUNT(sourceip) as 'Source IP Count',
UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 days
```

Informationen zu Assets und Konfiguration

Hinweise auf Bedrohungen und Nutzungsindikatoren variieren je nach Assettyp, Betriebssystem, Schwachstellenanfälligkeit, Servertyp, Klassifikation usw.

Mit der folgenden Abfrage geben erweiterte Suchvorgänge und das Assetmodell Einblick in den Betrieb eines Standorts.

Mit der Funktion **Assetproperty** werden Eigenschaftswerte aus Assets abgerufen, sodass Assetdaten in die Ergebnisse aufgenommen werden können.

```
SELECT
ASSETPROPERTY('Location',sourceip) as location,
COUNT(*) as 'event count'
FROM events
GROUP BY location
LAST 1 days
```

Mit der Funktion **AssetUser** wird der Benutzername aus der Assetdatenbank abgerufen.

Funktion 'Network LOOKUP'

Mit der Funktion **Network LOOKUP** können Sie den einer IP-Adresse zugeordneten Netznamen abrufen.

```
SELECT NETWORKNAME(sourceip) as srcnet,
NETWORKNAME(destinationip) as dstnet
FROM events
```

Funktion 'Rule LOOKUP'

Mit der Funktion **Rule LOOKUP** können Sie den Namen einer Regel anhand der ID abrufen.

```
SELECT RULENAME(123) FROM events
```

Die folgende Abfrage gibt Ereignisse zurück, die eine Regel mit einem bestimmten Regelnamen ausgelöst haben.

```
SELECT * FROM events
WHERE RULENAME(creEventList) ILIKE '%my rule name%'
```

Zugehörige Konzepte:

„Geplanter Suchvorgang" auf Seite 65
Über die Option 'Geplanter Suchvorgang' können Sie eine Suche terminieren und die Ergebnisse anzeigen.

„Suche mit Filtern"
Sie können Ereignis- und Datenflussnutzdaten durch Eingabe von Textsuchbegriffen (einfache Wörter oder Wortfolgen) durchsuchen.

Zugehörige Tasks:

„Nach Elementen suchen, die mit Ihren Kriterien übereinstimmen" auf Seite 57
Sie können nach Daten suchen, die mit Ihren Suchkriterien übereinstimmen.

Suche mit Filtern

Sie können Ereignis- und Datenflussnutzdaten durch Eingabe von Textsuchbegriffen (einfache Wörter oder Wortfolgen) durchsuchen.

Möglichkeiten zum Filtern von Suchvorgängen:

Über die Symbolleisten Protokollaktivität und
Wählen Sie im Listenfeld der Symbolleiste **Suchen** die Option **Schnellfilter** aus und geben Sie den gewünschten Textsuchbegriff ein. Klicken Sie auf das Symbol **Schnellfilter**, um Ihren auf die Liste mit Ereignissen oder Datenflüssen anzuwenden.

Über das Dialogfeld Filter hinzufügen
Klicken Sie auf der Registerkarte **Protokollaktivität** oder auf das Symbol **Filter hinzufügen**.

Wählen Sie **Schnellfilter** als Filterparameter aus und geben Sie den gewünschten Textsuchbegriff ein.

Über die Seiten zum Durchsuchen von Datenflüssen
Fügen Sie Ihrer Liste mit Filtern einen Schnellfilter hinzu.

Bei der Anzeige von im Echtzeitmodus (Datenstrommodus) oder im Modus 'Letztes Intervall' können Sie im Feld **Schnellfilter** nur einfache Wörter oder Wortfolgen eingeben. Halten Sie sich bei der Anzeige von **Ereignissen** oder mit einem Zeitbereich and die Syntaxrichtlinien in der folgenden Tabelle:

Tabelle 21. Syntaxrichtlinien für Schnellfilter

Beschreibung	Beispiel
Geben Sie einen einfachen Text ein, von dem Sie erwarten, dass er in den Nutzdaten enthalten ist.	`Firewall`
Suchen Sie nach exakten Wortfolgen, indem Sie sie in Anführungszeichen setzen.	`"Alle Firewalls"`
Suchbegriffe können Platzhalterzeichen für einzelne und mehrere Zeichen enthalten, sie dürfen jedoch nicht mit einem Platzhalterzeichen beginnen.	`F?rewall` oder `F??ew*`
Sie könnten Begriffe unter Verwendung von logischen Ausdrücken (AND, OR und NOT) eingeben. Damit logische Ausdrücke als solche erkannt und nicht als Suchbegriffe interpretiert werden, müssen Syntax und Operationen in Großbuchstaben eingegeben werden.	`(%PIX* AND ("Aufgerufene URL" OR "udp src verweigern") AND 10.100.100.*)`
Bei der Angabe von Suchkriterien, die den logischen Ausdruck NOT enthalten, müssen Sie mindestens einen weiteren logischen Ausdruck angeben, da andernfalls keine Ergebnisse zurückgegeben werden.	`(%PIX* AND ("Aufgerufene URL" OR "udp src verweigern") NOT 10.100.100.*)`
Wenn die folgenden Zeichen Teil Ihres Suchbegriffs sind, müssen Sie ihnen einen umgekehrten Schrägstrich voranstellen: `+ - && || ! () {} [] ^ " ~ * ? : \.`	`"%PIX\-5\-304001"`

Suchbegriffe werden der Reihenfolge nach, beginnend mit dem ersten Zeichen in dem Wort oder Ausdruck aus den Nutzdaten, abgeglichen. So ergibt der Begriff 'user' beispielsweise eine Übereinstimmung mit `user_1` und `user_2`, nicht aber mit `ruser`, `myuser` oder `anyuser`.

Zugehörige Konzepte:

„Erweiterte Suchoptionen" auf Seite 66
Im Feld **Erweiterte Suche** können Sie für die Ausführung einer Abfrage einen AQL-Suchbegriff (Ariel Query Language) eingeben, in dem festgelegt wird, welche Felder zurückgegeben und wie sie angeordnet werden sollen.

„Beispiele für AQL-Suchbegriffe" auf Seite 67
Mit AQL (Ariel Query Language) können Sie aus Ereignissen, Datenflüssen und simarc-Tabellen in der Ariel-Datenbank bestimmte Felder abrufen.

Suchergebnisse mithilfe einer Untersuche eingrenzen

Sie können eine Untersuche verwenden, um innerhalb einer Reihe fertiger Suchergebnisse zu suchen. Mithilfe der Untersuche werden Suchergebnisse eingegrenzt, ohne die Datenbank erneut zu durchsuchen.

Vorbereitende Schritte

Wenn Sie eine Suche definieren, die Sie als Grundlage für eine Untersuche verwenden wollen, vergewissern Sie sich, dass die Option 'Echtzeit (Streaming)' inaktiviert und die Suche nicht gruppiert ist.

Informationen zu diesem Vorgang

Diese Funktion ist nicht für gruppierte Suchen, aktive Suchen oder im Datenstrommodus verfügbar.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Führen Sie eine Suche durch.
3. Wenn Ihre Suche fertig ist, fügen Sie einen weiteren Filter hinzu:
   a. Klicken Sie auf **Filter hinzufügen**.
   b. Wählen Sie im ersten Listenfeld einen Parameter aus, nach dem Sie suchen wollen.
   c. Wählen Sie im zweiten Listenfeld den Modifikator aus, den Sie für die Suche verwenden wollen. Die Liste von Modifikatoren, die verfügbar sind, hängt von dem Attribut ab, das in der ersten Liste ausgewählt ist.
   d. Geben Sie im Eingabefeld spezifische Informationen ein, die zu Ihrer Suche gehören.
   e. Klicken Sie auf **Filter hinzufügen**.

Ergebnisse

Im Teilfenster 'Ursprüngliche Filter' werden die ursprünglichen Filter angegeben, die auf die Basissuche angewendet werden. Im Filterteilfenster 'Aktuell' werden die ursprünglichen Filter angegeben, die auf die Untersuche angewendet werden. Sie können Untersuchfilter löschen, ohne die Basissuche erneut zu starten. Klicken Sie auf den Link **Filter löschen** neben dem Filter, den Sie löschen wollen. Wenn Sie einen Filter aus dem Teilfenster 'Ursprünglicher Filter' löschen, wird die Basissuche erneut gestartet.

Wenn Sie die Basissuchkriterien für gesicherte Untersuchkriterien löschen, haben Sie trotzdem weiterhin Zugriff auf gesicherte Untersuchkriterien. Wenn Sie einen Filter hinzufügen, durchsucht die Untersuche die ganze Datenbank, da die Suchfunktion nicht mehr die Suche auf eine früher durchsuchte Datenmenge basiert.

Nächste Schritte

Suchkriterien speichern

Suchergebnisse verwalten

Sie können mehrere Suchvorgänge einleiten und dann zu anderen Registerkarten navigieren, um andere Aufgaben auszuführen, während Ihre Suchen im Hintergrund durchgeführt werden.

Sie können bei der Konfiguration einer Suche festlegen, dass Ihnen eine E-Mail-Benachrichtigung gesendet werden soll, wenn die Suche abgeschlossen ist.

Sie haben jederzeit während einer Suche die Möglichkeit, zur Registerkarte **Protokollaktivität** zurückzukehren, um partielle oder vollständige Suchergebnisse anzuzeigen.

Suchkriterien löschen

Sie können Suchkriterien löschen.

Informationen zu diesem Vorgang

Wenn Sie eine gespeicherte Suche löschen, funktionieren zugehörige Objekte möglicherweise nicht. Berichte und Anomalieerkennungsregeln sind QRadar-Objekte, die gespeicherte Suchkriterien verwenden. Nachdem Sie eine gespeicherte Suche gelöscht haben, bearbeiten Sie die zugehörigen Objekte, um sicherzustellen, dass sie weiterhin funktionieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Suchen** den Eintrag **Neue Suche** oder **Suche bearbeiten** aus.
3. Wählen Sie im Fensterbereich 'Gespeicherte Suchvorgänge' eine gespeicherte Suche im Listenfeld **Verfügbare gespeicherte Suchvorgänge** aus.
4. Klicken Sie auf **Löschen**.
   - Wenn die gespeicherten Suchkriterien nicht mit anderen QRadar-Objekten verknüpft sind, wird ein Bestätigungsfenster angezeigt.
   - Wenn die gespeicherten Suchkriterien mit anderen Objekten verknüpft sind, wird das Fenster **Gespeicherten Suchvorgang löschen** angezeigt. Im Fenster werden die Objekte aufgeführt, die zur gespeicherten Suche gehören, die Sie löschen möchten. Notieren Sie die zugehörigen Objekte.
5. Klicken Sie auf **OK**.
6. Wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie auf **OK**, um fortzufahren.
   - Klicken Sie auf **Abbrechen**, um das Fenster **Gespeicherten Suchvorgang löschen** zu schließen.

Nächste Schritte

Wenn die gespeicherten Suchkriterien mit anderen QRadar-Objekten verknüpft waren, rufen Sie die zugehörigen Objekte auf, die Sie notiert haben, und bearbeiten Sie sie, um die Verknüpfung mit der gelöschten gespeicherten Suche zu entfernen oder zu ersetzen.

Suchergebnisse speichern

Sie können die Suchergebnisse sichern.

Informationen zu diesem Vorgang

Wenn Sie eine Suche ausführen und die Suchergebnisse nicht explizit sichern, sind die Suchergebnisse 24 Stunden lang im Fenster **Suchergebnisse verwalten** verfügbar und werden dann automatisch gelöscht.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Führen Sie einen Suchvorgang aus.
3. Klicken Sie auf **Ergebnisse speichern**.
4. Geben Sie im Fenster **Suchergebnis speichern** einen eindeutigen Namen für die Suchergebnisse ein.
5. Klicken Sie auf **OK**.

Verwaltete Suchergebnisse anzeigen

Über die Seite **Suchergebnisse verwalten** können Suchergebnisse teilweise oder vollständig angezeigt werden.

Informationen zu diesem Vorgang

Gespeicherte Suchergebnisse behalten Diagrammkonfigurationen der zugehörigen Suchkriterien bei. Wenn jedoch das Suchergebnis auf bereits gelöschten Suchkriterien basiert, werden die Standarddiagramme (Balken- und Kreisdiagramm) angezeigt.

Auf der Seite **Suchergebnisse verwalten** stehen die folgenden Parameter zur Verfügung

Tabelle 22. Parameter der Seite 'Suchergebnisse verwalten'

Parameter	Beschreibung
Flags	Zeigt an, dass eine E-Mail-Benachrichtigung für den Abschluss der Suche ansteht.
Benutzer	Gibt den Namen des Benutzers an, der die Suche gestartet hat.
Name	Gibt den Namen der Suche an, wenn die Suche gespeichert wurde. Weitere Informationen zum Speichern einer Suche finden Sie im Abschnitt Suchergebnisse speichern.
Gestartet am	Gibt Datum und Uhrzeit des Starts der Suche an.
Beendet am	Gibt Datum und Uhrzeit des Endes der Suche an.
Dauer	Gibt die Zeitspanne an, die zur Durchführung des Suchvorgangs benötigt wurde. Während der Durchführung der Suche gibt der Parameter **Dauer** an, wie lange der Suchvorgang bisher gedauert hat. Wenn der Suchvorgang abgebrochen wurde, gibt der Parameter **Dauer** an, wie lange die Suche vor ihrem Abbruch ausgeführt wurde.
Ablaufdatum	Gibt Ablaufdatum und -uhrzeit eines ungespeicherten Suchergebnisses an. Der Wert für die Aufbewahrungsdauer einer gespeicherten Suche wird in den Systemeinstellungen konfiguriert. Weitere Informationen zur Konfiguration von Systemeinstellungen finden Sie im *IBM Security QRadar Log Manager*-Verwaltungshandbuch.

Tabelle 22. Parameter der Seite 'Suchergebnisse verwalten' (Forts.)

Parameter	Beschreibung
Status	Gibt den Status des Suchvorgangs an. Für den Status kann Folgendes angegeben werden: • **In Warteschlange** - Gibt an, dass sich der Suchvorgang in der Warteschlange für den Start befindet. • **<Prozent>%Abgeschlossen** - Gibt den Fortschritt des Suchvorgangs in Prozent an. Klicken Sie auf den Link, um Teilergebnisse anzuzeigen. • **Sortierung** - Gibt an, dass das Erfassen von Ergebnissen innerhalb des Suchvorgangs abgeschlossen ist und die Ergebnisse derzeit zur Ansicht vorbereitet werden. • **Abgebrochen** - Gibt an, dass der Suchvorgang abgebrochen wurde. Klicken Sie auf den Link, um die Ergebnisse anzuzeigen, die vor dem Abbruch erfasst wurden. • **Abgeschlossen** - Gibt an, dass der Suchvorgang abgeschlossen ist. Klicken Sie auf den Link, um die Ergebnisse anzuzeigen. Weitere Informationen hierzu finden Sie unter Log activity monitoring (Protokollaktivitätsüberwachung)
Größe	Gibt die Dateigröße der Suchergebnisliste an.

Über die Symbolleiste des Fensters **Suchergebnisse verwalten** stehen die folgenden Funktionen zur Verfügung

Tabelle 23. Symbolleiste 'Suchergebnisse verwalten'

Funktion	Beschreibung
Neue Suche	Klicken Sie auf **Neue Suche**, um einen neuen Suchvorgang zu erstellen. Durch Anklicken dieses Symbols wird die Suchseite angezeigt.
Ergebnisse speichern	Klicken Sie auf **Ergebnisse speichern**, um die ausgewählten Suchergebnisse zu speichern. Weitere Informationen hierzu finden Sie unter 'Suchergebnisse speichern'.
Abbrechen	Klicken Sie auf **Abbrechen**, um das ausgewählte Suchergebnis, das sich in Bearbeitung bzw. in der Warteschlange befindet, abzubrechen. Weitere Informationen hierzu finden Sie unter 'Canceling a search' (Suche abbrechen).
Löschen	Klicken Sie auf **Löschen**, um das ausgewählte Suchergebnis zu löschen. Weitere Informationen hierzu finden Sie unter 'Deleting a search result' (Suchergebnis löschen).

Tabelle 23. Symbolleiste 'Suchergebnisse verwalten' (Forts.)

Funktion	Beschreibung
Benachrichtigen	Klicken Sie auf **Benachrichtigen**, um eine E-Mail-Benachrichtigung zu aktivieren, wenn die ausgewählte Suche abgeschlossen ist.
Ansicht	In diesem Listenfeld können Sie auswählen, welche Suchergebnisse auf der Seite **Suchergebnisse** aufgeführt werden sollen. Folgende Optionen stehen zur Verfügung: • Ergebnisse des gespeicherten Suchvorgangs • Alle Suchergebnisse • Abgebrochene/fehlerhafte Suchvorgänge • Derzeit bearbeitete Suchvorgänge

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Menü **Suchen** die Option **Suchergebnisse verwalten** aus.
3. Zeigen Sie die Liste der Suchergebnisse an.

Suche abbrechen

Während eine Suche in die Warteschlange eingereiht oder in Bearbeitung ist, können Sie die Suche auf der Seite **Suchergebnisse verwalten** abbrechen.

Informationen zu diesem Vorgang

Wenn Sie eine gerade laufende Suche abbrechen, bleiben die bis zu dem Abbruch kumulierten Ergebnisse erhalten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Menü **Suchen** die Option **Suchergebnisse verwalten** aus.
3. Wählen Sie das in die Warteschlange eingereihte oder in Bearbeitung befindliche Suchergebnis aus, das Sie abbrechen möchten.
4. Klicken Sie auf **Abbrechen**.
5. Klicken Sie auf **Ja**.

Suche löschen

Wenn ein Suchergebnis nicht mehr benötigt wird, können Sie es auf der Seite **Suchergebnisse verwalten** löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Menü **Suchen** den Eintrag **Suchergebnisse verwalten** aus.
3. Wählen Sie das Suchergebnis aus, das Sie löschen wollen.
4. Klicken Sie auf **Löschen**.
5. Klicken Sie auf **Ja**.

Suchgruppen verwalten

Über das Fenster **Search Groups** (Suchgruppen) können Sie Ereignis-, Datenfluss- und Angriffssuchgruppen erstellen und verwalten.

Mithilfe dieser Gruppen können Sie gespeicherte Suchkriterien ganz einfach auf der Registerkarte **Protokollaktivität** sowie im Berichtsassistenten lokalisieren.

Suchgruppen anzeigen

Ein Standardset von Gruppen und Untergruppen ist verfügbar.

Informationen zu diesem Vorgang

Sie können Suchgruppen im Fenster **Ereignissuchgruppe** anzeigen.

Alle gespeicherten Suchen, die keiner Gruppe zugeordnet sind, befinden sich in der Gruppe **Sonstige**.

Im Fenster **Ereignissuchgruppe** werden für jede Gruppe die folgenden Parameter angezeigt.

Tabelle 24. Parameter der Suchgruppenfenster

Parameter	Beschreibung
Name	Gibt den Namen der Suchgruppe an.
Benutzer	Gibt den Namen des Benutzers an, der die Suchgruppe erstellt hat.
Beschreibung	Gibt die Beschreibung der Suchgruppe an.
Änderungsdatum	Gibt das Datum der Änderung der Suchgruppe an.

Über die Symbolleiste des Fensters **Ereignissuchgruppe** stehen die folgenden Funktionen zur Verfügung.

Tabelle 25. Symbolleistenfunktionen der Suchgruppenfenster

Funktion	Beschreibung
Neue Gruppe	Klicken Sie zum Erstellen einer neuen Suchgruppe auf **Neue Gruppe**. Weitere Informationen hierzu finden Sie unter Neue Suchgruppe erstellen.
Bearbeiten	Klicken Sie zum Bearbeiten einer bestehenden Suchgruppe auf **Bearbeiten**. Weitere Informationen hierzu finden Sie unter Suchgruppe bearbeiten.
Kopieren	Klicken Sie zum Kopieren einer gespeicherten Suche in eine andere Suchgruppe auf **Kopieren**. Weitere Informationen hierzu finden Sie unter Gespeicherte Suche in eine andere Gruppe kopieren.

Tabelle 25. Symbolleistenfunktionen der Suchgruppenfenster (Forts.)

Funktion	Beschreibung
Entfernen	Wählen Sie zum Entfernen einer Suchgruppe oder einer gespeicherten Suche aus einer Suchgruppe das Element aus, das entfernt werden soll, und klicken Sie dann auf **Entfernen**. Weitere Informationen hierzu finden Sie unter Gruppe oder gespeicherte Suche aus einer Gruppe entfernen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie **Suchen** >**Suche bearbeiten** aus.
3. Klicken Sie auf **Gruppen verwalten**.
4. Zeigen Sie die Suchgruppen an.

Neue Suchgruppe erstellen

Sie können eine neue Suchgruppe erstellen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie **Suchen Suche bearbeiten** aus.
3. Klicken Sie auf **Gruppen verwalten**.
4. Wählen Sie den Ordner für die Gruppe aus, unter der Sie die neue Gruppe erstellen möchten.
5. Klicken Sie auf **Neue Gruppe**.
6. Geben Sie im Feld **Name** einen eindeutigen Namen für die neue Gruppe ein.
7. Optional. Geben Sie im Feld **Beschreibung** eine Beschreibung ein.
8. Klicken Sie auf **OK**.

Suchgruppe bearbeiten

Sie können die Felder **Name** und **Beschreibung** einer Suchgruppe bearbeiten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie **Suchen** > **Suche bearbeiten** aus.
3. Klicken Sie auf **Gruppen verwalten**.
4. Wählen Sie die Gruppe aus, die Sie bearbeiten wollen.
5. Klicken Sie auf **Bearbeiten**.
6. Bearbeiten Sie die Parameter:
   - Geben Sie in das Feld **Name** einen neuen Namen ein.
   - Geben Sie in das Feld **Beschreibung** eine neue Beschreibung ein.
7. Klicken Sie auf **OK**.

Gespeicherte Suche in eine andere Gruppe kopieren

Sie können eine gespeicherte Suche in eine oder mehrere Gruppen kopieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie **Suchen** > **Suche bearbeiten** aus.
3. Klicken Sie auf **Gruppen verwalten**.
4. Wählen Sie die gespeicherte Suche aus, die Sie kopieren möchten.
5. Klicken Sie auf **Kopieren**.
6. Wählen Sie im Fenster **Elementgruppen** das Kontrollkästchen für die Gruppe aus, in die die gespeicherte Suche kopiert werden soll.
7. Klicken Sie auf **Gruppen zuordnen**.

Gruppe oder gespeicherte Suche aus einer Gruppe entfernen

Sie können mit dem **Entfernen**-Symbol eine Suche aus einer Gruppe entfernen oder eine Suchgruppe entfernen.

Informationen zu diesem Vorgang

Wenn Sie eine gespeicherte Suche aus einer Gruppe entfernen, wird die gespeicherte Suche nicht aus Ihrem System gelöscht. Die gespeicherte Suche wird aus der Gruppe entfernt und automatisch zur Gruppe **Sonstige** verschoben.

Sie können Ereignissuchgruppen nicht von Ihrem System entfernen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie **Suchen** > **Suche bearbeiten** aus.
3. Klicken Sie auf **Gruppen verwalten**.
4. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie die gespeicherte Suche aus, die Sie aus der Gruppe entfernen wollen.
   - Wählen Sie die Gruppe aus, die Sie entfernen wollen.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **OK**.

Kapitel 7. Angepasste Ereigniseigenschaften

Mithilfe der angepassten Ereignis- und Datenflusseigenschaften können Sie Informationen in Protokollen suchen, anzeigen und melden, die in QRadar SIEM normalerweise nicht normalisiert und angezeigt werden.

Angepasste Ereigniseigenschaften können von mehreren Stellen der Registerkarte **Protokollaktivität** aus erstellt werden:

- Ereignisdetails - Sie können ein Ereignis in der Registerkarte **Protokollaktivität** auswählen, um eine aus den Nutzdaten abgeleitete angepasste Ereigniseigenschaft zu erstellen.
- Suchseite - Sie können von der Seite **Suche** aus ein angepasstes Ereignis bzw. eine angepasste Eigenschaft erstellen und bearbeiten. Wenn Sie auf der Seite **Suche** eine neue angepasste Eigenschaft erstellen, wird die Eigenschaft nicht von einem bestimmten Ereignis abgeleitet. Daher wird das Fenster **Custom Property Definition** (Definition angepasster Eigenschaften) nicht vorab mit Daten ausgefüllt. Sie haben die Möglichkeit, Nutzdaten aus einer anderen Quelle zu kopieren und einzufügen.

Erforderliche Berechtigungen

Wenn Sie über die entsprechende Berechtigung verfügen, können Sie angepasste Eigenschaften erstellen.

Sie benötigen die Berechtigung 'User Defined Event Properties (Benutzerdefinierte Ereigniseigenschaften)'.

Wenn Sie über Administratorrechte verfügen, können Sie auch über die Registerkarte 'Verwaltung' angepasste Eigenschaften erstellen und ändern.

Klicken Sie auf **Verwaltung** > **Datenquellen** > **Angepasste Ereigniseigenschaften**.

Klären Sie mit Ihrem Administrator, ob Sie über die entsprechenden Berechtigungen verfügen.

Weitere Informationen finden Sie im *IBM Security QRadar Log Manager Administration Guide*.

Typen angepasster Eigenschaften

Sie können verschiedene Arten angepasster Eigenschaften erstellen.

Beim Erstellen einer angepassten Eigenschaft können Sie wählen, ob Sie eine Regex-Eigenschaft oder eine berechnete Eigenschaft erstellen möchten.

Bei Verwendung von Regex-Anweisungen (Regex = Regular Expression - regulärer Ausdruck) können Sie nicht normalisierte Daten aus Ereignisnutzdaten extrahieren.

So wird beispielsweise ein Bericht zur Meldung aller Benutzer erstellt, die Änderungen an den Benutzerberechtigungen auf einem Oracle-Server vornehmen. Es wird eine Liste der Benutzer aufgeführt und angegeben, wie oft diese eine Änderung an der Berechtigung eines anderen Kontos vorgenommen haben. Allerdings

kann normalerweise das eigentliche Benutzerkonto oder die geänderte Berechtigung nicht angezeigt werden. Sie können eine angepasste Eigenschaft erstellen, um diese Informationen aus den Protokollen zu extrahieren, und diese Eigenschaft dann in Suchen und Berichten verwenden. Für die Verwendung dieser Funktion sind weiterreichende Kenntnisse über reguläre Ausdrücke (regex) erforderlich.

In dem regulären Ausdruck wird das Feld definiert, das zur angepassten Eigenschaft werden soll. Nach der Eingabe können Sie die Regex-Anweisung unter Verwendung der Nutzdaten prüfen. Beachten Sie bei der Definition angepasster Regex-Muster die in der Programmiersprache Java™ definierten Regex-Regeln.

Weitere Informationen hierzu finden Sie in den Regex-Lernprogrammen im Web. Eine angepasste Eigenschaft kann mehreren regulären Ausdrücken zugeordnet werden.

Bei der Analyse eines Ereignisses wird jedes Regex-Muster an dem Ereignis getestet, bis ein Regex-Muster mit den Nutzdaten übereinstimmt. Das erste Regex-Muster, das mit den Ereignisnutzdaten übereinstimmt, entscheidet, welche Daten extrahiert werden.

Mit auf Berechnungen basierenden angepassten Eigenschaften können Sie Berechnungen mit vorhandenen numerischen Ereignis- oder Datenflusseigenschaften durchführen und so eine berechnete Eigenschaft erstellen.

So können Sie beispielsweise durch Teilen einer numerischen Eigenschaft durch eine andere numerische Eigenschaft eine Eigenschaft erstellen, die einen Prozentsatz anzeigt.

Auf regulärem Ausdruck basierte angepasste Eigenschaft erstellen

Sie können eine auf einem regulären Ausdruck basierende angepasste Eigenschaft erstellen, um Ereignis- oder Datenflussnutzdaten einem regulären Ausdruck zuzuordnen.

Informationen zu diesem Vorgang

Wenn Sie eine auf einem regulären Ausdruck basierende angepasste Eigenschaft konfigurieren, werden im Fenster **Custom Event Property** (Angepasste Ereigniseigenschaft) Parameter bereitgestellt. In der folgenden Tabelle werden einige dieser Parameter beschrieben.

Tabelle 26. Parameter im Fenster **Angepasste Ereigniseigenschaften** *(regulärer Ausdruck)*

Parameter	Beschreibung
Testfeld	Gibt die Nutzdaten an, die vom unnormalisierten Ereignis oder Datenfluss extrahiert wurden. Gibt die Nutzdaten an, die vom unnormalisierten Ereignis extrahiert wurden.
Neue Eigenschaft	Der neue Eigenschaftsname kann nicht der Name einer normalisierten Eigenschaft sein, wie z. B. `Benutzername`, `Quellen-IP` oder `Ziel-IP`.

Tabelle 26. Parameter im Fenster **Angepasste Ereigniseigenschaften** *(regulärer Ausdruck) (Forts.)*

Parameter	Beschreibung
Parsing für Regeln, Berichte und Suchen optimieren	Analysiert und speichert die Eigenschaft beim ersten Empfang des Ereignisses oder Datenflusses. Wenn Sie das Kontrollkästchen auswählen, erfordert die Eigenschaft keine weitere Analyse für Berichte, Suchen oder Regeltests. Wenn Sie dieses Kontrollkästchen abwählen, wird die Eigenschaft bei jeder Ausführung eines Berichts, einer Suche oder eines Regeltests analysiert.
Protokollquelle	Wenn diesem Ereignis mehrere Protokollquellen zugeordnet sind, sind der Begriff 'Mehrere' und die Zahl der Protokollquellen in diesem Feld definiert.
Regulärer Ausdruck	Der reguläre Ausdruck, den Sie für die Extraktion der Daten aus den Nutzdaten verwenden möchten. Reguläre Ausdrücke beachten Groß-/Kleinschreibung. In den folgenden Beispielen sind einige reguläre Ausdrücke zur Veranschaulichung dargestellt: • E-Mail: `(.+@[^\.].*\.[a-z]{2,}$)` • URL: `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • Domänenname: `(http[s]?://(.+?)["/?:])` • Gleitkommazahl: `([-+]?\d*\.?\d*$)` • Ganzzahl: `([-+]?\d*$)` • IP-Adresse: `(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` Erfassungsgruppen müssen in Klammern eingeschlossen werden.
Erfassungsgruppe	Erfassungsgruppen betrachten mehrere Zeichen als eine einzelne Einheit. In einer Erfassungsgruppe werden Zeichen zwischen runden Klammern gruppiert.
Aktiviert	Wenn Sie das Kontrollkästchen abwählen, wird diese angepasste Eigenschaft nicht in Suchfiltern oder Spaltenlisten angezeigt und die Eigenschaft wird nicht von Nutzdaten analysiert.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wenn Sie Ereignisse im Datenstrommodus anzeigen, klicken Sie auf das **Pause**-Symbol, um das Streaming anzuhalten.

3. Doppelklicken Sie auf das Ereignis, auf das Sie die angepasste Eigenschaft basieren wollen.
4. Klicken Sie auf **Eigenschaft extrahieren**.
5. Wählen Sie im Teilfenster **Eigenschaftstypauswahl** die Option **Auf Basis von regulärem Ausdruck** aus.
6. Konfigurieren Sie die Parameter der angepassten Eigenschaft.
7. Klicken Sie auf **Test**, um den regulären Ausdruck in Bezug auf die Nutzdaten zu testen.
8. Klicken Sie auf **Speichern**.

Ergebnisse

Die angepasste Eigenschaft wird als Option in der Liste der verfügbaren Spalten auf der Suchseite angezeigt. Wenn Sie eine angepasste Eigenschaft in eine Ereignis- oder Datenflussliste aufnehmen möchten, müssen Sie die angepasste Eigenschaft beim Erstellen einer Suche in der Liste der verfügbaren Spalten auswählen.

Berechnungsbasierte angepasste Eigenschaft erstellen

Zum Abgleich von Nutzdaten mit einem regulären Ausdruck können Sie eine berechnungsbasierte angepasste Eigenschaft erstellen.

Informationen zu diesem Vorgang

Wenn Sie eine berechnungsbasierte angepasste Eigenschaft konfigurieren, werden im Fenster **Custom Event Property** (Angepasste Ereigniseigenschaft) oder **Custom Flow Property** (Angepasste Datenflusseigenschaft) die folgenden Parameter bereitgestellt:

Tabelle 27. Parameter des Fensters 'Angepasste Eigenschaftsdefinition' (Berechnung)

Parameter	Beschreibung
Eigenschaftsdefinition	
Eigenschaftsname	Geben Sie einen eindeutigen Namen für diese angepasste Eigenschaft ein. Der neue Eigenschaftsname darf nicht mit dem Namen einer normalisierten Eigenschaft wie z. B. Benutzername, Quellen-IP oder Ziel-IP übereinstimmen.
Beschreibung	Geben Sie eine Beschreibung der angepassten Eigenschaft ein.
Eigenschaftenberechnungsdefinition	
Eigenschaft 1	Wählen Sie im Listenfeld die erste Eigenschaft aus, die Sie in der Berechnung verwenden möchten. Möglich sind alle numerischen normalisierten und numerischen angepassten Eigenschaften. Sie können auch einen bestimmten numerischen Wert angeben. Wählen Sie im Listenfeld **Eigenschaft 1** die Option **Benutzerdefiniert** aus. Der Parameter **Numerische Eigenschaft** wird angezeigt. Geben Sie einen bestimmten numerischen Wert ein.

Tabelle 27. Parameter des Fensters 'Angepasste Eigenschaftsdefinition' (Berechnung) (Forts.)

Parameter	Beschreibung
Operator	Wählen Sie im Listenfeld den Operator aus, den Sie auf die ausgewählten Eigenschaften in der Berechnung anwenden möchten. Mögliche Optionen: • Hinzufügen • Subtrahieren • Multiplizieren • Dividieren
Eigenschaft 2	Wählen Sie im Listenfeld die zweite Eigenschaft aus, die Sie in der Berechnung verwenden möchten. Möglich sind alle numerischen normalisierten und numerischen angepassten Eigenschaften. Sie können auch einen bestimmten numerischen Wert angeben. Wählen Sie im Listenfeld **Eigenschaft 1** die Option **Benutzerdefiniert** aus. Der Parameter **Numerische Eigenschaft** wird angezeigt. Geben Sie einen bestimmten numerischen Wert ein.
Aktiviert	Wählen Sie dieses Kontrollkästchen aus, um die angepasste Eigenschaft zu aktivieren. Wenn Sie die Markierung des Kontrollkästchens aufheben, wird die betreffende angepasste Eigenschaft nicht in Ereignissuchfiltern oder Spaltenlisten angezeigt und es erfolgt keine Analyse der Ereignis- bzw. Datenflusseigenschaft aus den Nutzdaten.

Vorgehensweise

1. Sie haben folgende Möglichkeiten: Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Optional. Wenn Sie Ereignisse oder Datenflüsse im Datenstrommodus anzeigen, können Sie den Streaming-Vorgang über das Symbol **Pause** anhalten.
3. Doppelklicken Sie auf das Ereignis, auf dem die angepasste Eigenschaft basieren soll.
4. Klicken Sie auf **Eigenschaft extrahieren**.
5. Wählen Sie im Fensterbereich 'Eigenschaftstypauswahl' die Option **Berechnungsbasiert** aus.
6. Konfigurieren Sie die Parameter der angepassten Eigenschaft.
7. Klicken Sie auf **Test**, um den regulären Ausdruck anhand der Nutzdaten zu testen.
8. Klicken Sie auf **Speichern**.

Ergebnisse

Die angepasste Eigenschaft wird jetzt als Option in der Liste der verfügbaren Spalten auf der Suchseite angezeigt. Wenn Sie eine angepasste Eigenschaft in eine Ereignis- oder Datenflussliste aufnehmen möchten, müssen Sie die angepasste Eigenschaft beim Erstellen einer Suche in der Liste der verfügbaren Spalten auswählen.

Angepasste Eigenschaften ändern

Sie können eine angepasste Eigenschaft ändern.

Informationen zu diesem Vorgang

Mit dem Fenster **Angepasste Ereigniseigenschaften** können Sie eine angepasste Eigenschaft ändern.

Die angepassten Eigenschaften werden in der folgenden Tabelle beschrieben.

Tabelle 28. Spalten des Fensters 'Angepasste Eigenschaften'

Spalte	Beschreibung
Eigenschaftsname	Gibt einen eindeutigen Namen für diese angepasste Eigenschaft an.
Typ	Gibt den Typ für diese angepasste Eigenschaft an.
Eigenschaftenbeschreibung	Gibt eine Beschreibung für diese angepasste Eigenschaft an.
Protokollquellentyp	Gibt den Namen des Protokollquellentyps an, für den diese angepasste Eigenschaft gilt. Diese Spalte wird nur im Fenster **Angepasste Ereigniseigenschaften** angezeigt.
Protokollquelle	Gibt die Protokollquelle an, für die diese angepasste Eigenschaft gilt. Wenn es mehrere Protokollquellen gibt, die mit diesem Ereignis verknüpft sind, gibt dieses Feld den Begriff 'Mehrere' und die Anzahl der Protokollquellen an. Diese Spalte wird nur im Fenster **Angepasste Ereigniseigenschaften** angezeigt.

Tabelle 28. Spalten des Fensters 'Angepasste Eigenschaften' (Forts.)

Spalte	Beschreibung
Ausdruck	Gibt den Ausdruck für diese angepasste Eigenschaft an. Der Ausdruck hängt vom angepassten Eigenschaftstyp ab: Für eine auf einem regulären Ausdruck basierende angepasste Eigenschaft gibt dieser Parameter den regulären Ausdruck an, den Sie für das Extrahieren der Daten aus den Nutzdaten verwenden möchten. Für eine berechnungsbasierte angepasste Eigenschaft gibt dieser Parameter die Berechnung an, die Sie für die Erstellung des angepassten Eigenschaftswerts verwenden wollen.
Benutzername	Gibt den Namen des Benutzers an, der diese angepasste Eigenschaft erstellt hat.
Aktiviert	Gibt an, ob diese angepasste Eigenschaft aktiviert ist. Dieses Feld gibt entweder 'Wahr' oder 'Falsch' an.
Erstellungsdatum	Gibt das Datum an, an dem diese angepasste Eigenschaft erstellt wurde.
Änderungsdatum	Gibt an, wann diese angepasste Eigenschaft zuletzt geändert wurde.

Die Symbolleiste für 'Angepasste Ereigniseigenschaften' stellt die folgenden Funktionen bereit:

Tabelle 29. Optionen der Symbolleiste für angepasste Eigenschaften

Option	Beschreibung
Hinzufügen	Klicken Sie auf **Hinzufügen**, um eine neue angepasste Eigenschaft hinzuzufügen.
Bearbeiten	Klicken Sie auf **Bearbeiten**, um die ausgewählte angepasste Eigenschaft zu bearbeiten.
Kopieren	Klicken Sie auf **Kopieren**, um ausgewählte angepasste Eigenschaften zu kopieren.
Löschen	Klicken Sie auf **Löschen**, um ausgewählte angepasste Eigenschaften zu löschen.
Aktivieren/Inaktivieren	Klicken Sie auf **Aktivieren/Inaktivieren**, um die ausgewählten angepassten Eigenschaften für das Parsing und Anzeigen in den Suchfiltern oder Spaltenlisten zu aktivieren oder zu inaktivieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Suchen** den Eintrag **Suche bearbeiten** aus.
3. Klicken Sie auf **Angepasste Eigenschaften verwalten**.

4. Wählen Sie die angepasste Eigenschaft aus, die Sie bearbeiten wollen, und klicken Sie auf **Bearbeiten**.
5. Bearbeiten Sie die erforderlichen Parameter.
6. Optional. Wenn Sie den regulären Ausdruck bearbeitet haben, klicken Sie auf **Test**, um den regulären Ausdruck in Bezug auf die Nutzdaten zu testen.
7. Klicken Sie auf **Speichern**.

Angepasste Eigenschaft kopieren

Wenn Sie basierend auf einer bereits vorhandenen angepassten Eigenschaft eine neue angepasste Eigenschaft erstellen möchten, können Sie die vorhandene angepasste Eigenschaft kopieren und dann die Parameter ändern.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Wählen Sie im Listenfeld **Suchen** die Option **Suche bearbeiten** aus.
3. Klicken Sie auf **Angepasste Eigenschaften verwalten**.
4. Wählen Sie die zu kopierende angepasste Eigenschaft aus und klicken Sie auf **Kopieren**.
5. Bearbeiten Sie die erforderlichen Parameter.
6. Optional. Wenn Sie den regulären Ausdruck bearbeitet haben, können Sie auf **Test** klicken, um den regulären Ausdruck anhand der Nutzdaten zu testen.
7. Klicken Sie auf **Speichern**.

Benutzerdefinierte Eigenschaften löschen

Sie können eine benutzerdefinierte Eigenschaft löschen, vorausgesetzt diese ist nicht einer anderen benutzerdefinierten Eigenschaft zugehörig.

Vorgehensweise

1. Wählen Sie im Listenfeld **Suchen** den Eintrag **Suche bearbeiten** aus.
2. Klicken Sie auf **Angepasste Eigenschaften verwalten**.
3. Wählen Sie die benutzerdefinierte Eigenschaft aus, die Sie löschen wollen, und klicken Sie auf **Löschen**.
4. Klicken Sie auf **Ja**.

Kapitel 8. Regelmanagement

Auf der Registerkarte **Protokollaktivität** können Sie Regeln anzeigen und verwalten.

Dieses Thema betrifft Benutzer mit der Benutzerrollenberechtigung **View Custom Rules (Angepasste Regeln anzeigen)** oder **Maintain Custom Rules (Angepasste Regeln verwalten)**.

Überlegungen zu Regelberechtigungen

Wenn Sie über die Benutzerrollenberechtigungen 'View Custom Rules (Angepasste Regeln anzeigen)' und 'Maintain Custom Rules (Angepasste Regeln verwalten)' können Sie Regeln für die Netzbereiche anzeigen und verwalten, auf die Sie Zugriff haben.

Zum Erstellen von Regeln zur Erkennung von Unregelmäßigkeiten müssen Sie über die entsprechende Berechtigung **Maintain Custom Rules (Angepasste Regeln verwalten)** für die Registerkarte verfügen, auf der Sie die Regel erstellen möchten. Um Beispielsweise eine Regel zur Erkennung von Unregelmäßigkeiten auf der Registerkarte 'Protokollaktivität' erstellen zu können, benötigen Sie die Berechtigung **Protokollaktivität** > **Maintain Custom Rules (Angepasste Regeln verwalten)**.

Weitere Informationen zu Benutzerrollenberechtigungen finden Sie im *IBM Security QRadar Log Manager Administration Guide*.

Regeln - Übersicht

Regeln führen Tests auf Ereignisse aus und generieren eine Antwort, wenn alle Bedingungen eines Test erfüllt sind.

Bei den Tests der jeweiligen Regel kann auch auf andere Bausteine und Regeln verwiesen werden. Die Regeln müssen nicht in einer bestimmten Reihenfolge erstellt werden, da das System immer eine Prüfung auf Abhängigkeiten durchführt, wenn eine neue Regel hinzugefügt, bearbeitet oder gelöscht wird. Wenn eine Regel, auf die von einer anderen Regel verwiesen wird, gelöscht oder inaktiviert wird, wird eine Warnung angezeigt und keine Aktion durchgeführt.

Eine vollständige Liste der Standardregeln finden Sie im *IBM Security QRadar SIEM Administration Guide*.

Ereignisregel

Ereignisregeln führen Tests auf Ereignisse durch, wenn sie in Echtzeit vom Ereignisprozessor verarbeitet werden.

Sie können eine Ereignisregel erstellen, um ein einzelnes Ereignis innerhalb bestimmter Eigenschaften oder Ereignissequenzen zu finden. Wenn Sie beispielsweise Ihr Netz auf erfolglose Anmeldeversuche, den Zugriff auf mehrere Hosts oder ein Ausspähereignis mit anschließendem Exploit überwachen möchten, können Sie eine Ereignisregel erstellen. Im Allgemeinen werden von den Ereignisregeln als Antwort Angriffe erstellt.

Regelbedingungen

Jede Regel könnte Funktionen, Bausteine oder Tests enthalten.

In Verbindung mit Funktionen können Sie Bausteine und andere Regeln verwenden und so eine Funktion für mehrere Ereignisse erstellen. Mithilfe von Funktionen, die boolesche Operatoren wie OR und AND unterstützen, können Regeln verbunden werden. Wenn Sie beispielsweise Ereignisregeln verbinden möchten, können Sie die Funktion für den Fall, dass ein Ereignis einer | allen folgenden Regel(n) entspricht, verwenden.

Ein Baustein ist eine Regel ohne Antwort und wird als allgemeine Variable in mehreren Regeln oder zum Erstellen komplexer Regeln oder von Logik verwendet, die in anderen Regeln verwendet werden soll(en). Sie können eine Gruppe von Tests als Bausteine für die Verwendung mit anderen Funktionen speichern. Mithilfe von Bausteinen können Sie bestimmte Regeltests in anderen Regeln wiederverwenden. So können Sie beispielsweise einen Baustein speichern, der die IP-Adressen aller Mail-Server in Ihrem Netz umfasst, und mithilfe dieses Bausteins dann die betreffenden Mail-Server von einer anderen Regel ausschließen. Die Standardbausteine werden als Leitlinien bereitgestellt, die geprüft und den Anforderungen Ihres Netzes entsprechend bearbeitet werden sollten.

Anmerkung: Bausteine werden nicht standardmäßig geladen. Sie müssen eine Regel zur Erstellung von Bausteinen definieren.

Sie können Tests für die Eigenschaft eines Ereignisses durchführen, beispielsweise für die Quellen-IP-Adresse oder die Wertigkeit des Ereignisses.

Domänenspezifische Regeln

Wenn für eine Regel ein Domänentest festgelegt ist, können Sie die Regel so einschränken, dass sie nur für Ereignisse gilt, die innerhalb einer angegebenen Domäne auftreten. Ein Ereignis mit einem Domänentag, der sich von der in der Regel festgelegten Domäne unterscheidet, löst keine Ereignisantwort aus.

Um eine Regel zu erstellen, mit der Bedingungen für Vorgänge, die im gesamten System auftreten, getestet werden, müssen Sie die Domänenbedingung auf **Beliebige Domäne** setzen.

Regelantworten

Wenn die Regelbedingungen erfüllt sind, kann die betreffende Regel eine oder mehrere Antworten generieren.

Die Regeln können eine oder mehrere der folgenden Antworten generieren:

- Einen Angriff erstellen
- Eine E-Mail senden
- Systembenachrichtigungen in der Funktion 'Dashboard' generieren
- Daten zu Referenzsets hinzufügen
- Daten zu Referenzdatensammlungen hinzufügen
- Antwort an ein externes System generieren
- Daten zu Referenzdatensammlungen hinzufügen, die bei Regeltests verwendet werden können.

Arten von Referenzdatensammlungen

Bevor Sie eine Regelantwort konfigurieren können, um einer Referenzdatensammlung Daten zu senden, müssen Sie die Referenzdatensammlung über die Befehlszeilenschnittstelle (CLI) erstellen. QRadar unterstützt die folgenden Arten von Datensammlungen:

Referenzset
Eine Gruppe von Elementen, beispielsweise eine Liste mit IP-Adressen oder Benutzernamen, die von Ereignissen und Datenflüssen in Ihrem Netz abgeleitet werden.

Referenzzuordnung
Die Daten werden in Datensätzen gespeichert, in denen ein Schlüssel zu einem Wert zugeordnet wird. Zum Korrelieren der Benutzeraktivität in Ihrem Netz beispielsweise können Sie eine Referenzzuordnung erstellen, in der der Parameter **Benutzername** als Schlüssel und die globale ID (**Global ID**) des Benutzers als Wert verwendet wird.

Referenzzuordnung von Sets
Die Daten werden in Datensätzen gespeichert, in denen ein Schlüssel mehreren Werten zugeordnet wird. Verwenden Sie beispielsweise zum Testen, ob ein berechtigter Zugriff auf ein Patent erfolgt, eine angepasste Ereigniseigenschaft für die **Patent-ID** als Schlüssel und den Parameter **Benutzername** als Wert. Mithilfe einer Zuordnung von Sets können Sie eine Liste berechtigter Benutzer ausfüllen.

Referenzzuordnung von Zuordnungen
Die Daten werden in Datensätzen gespeichert, in denen ein Schlüssel einem anderen Schlüssel zugeordnet wird, der dann einem einzelnen Wert zugeordnet wird. Sie können beispielsweise eine Zuordnung von Zuordnungen erstellen, um zu testen, ob die Netzbandbreite nicht eingehalten wurde. Verwenden Sie den Parameter **Quellen-IP** als ersten Schlüssel, den Parameter **Anwendung** als zweiten Schlüssel und den Parameter **Gesamtzahl Bytes** als Wert.

Referenztabelle
Bei Verwendung einer Referenztabelle werden die Daten in einer Tabelle gespeichert, in der ein Schlüssel einem anderen Schlüssel zugeordnet wird, der dann wiederum einem einzelnen Wert zugeordnet wird. Dem zweiten Schlüssel ist ein Typ zugewiesen. Diese Zuordnung ist einer Datenbanktabelle ähnlich, bei der jede Tabellenspalte einem Typ zugeordnet ist. So können Sie beispielsweise eine Referenztabelle erstellen, in der der Parameter **Benutzername** als erster Schlüssel gespeichert ist und in der es mehrere Sekundärschlüssel mit einem zugeordneten benutzerdefinierten Typ wie z. B. **IP Type** (IP-Typ) mit dem Parameter **Quellen-IP** oder **Quellenport** als Wert gibt. Sie können eine Regelantwort konfigurieren, um einen oder mehrere in der Tabelle definierte Schlüssel hinzuzufügen. Außerdem können Sie der Regelantwort benutzerdefinierte Werte hinzufügen. Der benutzerdefinierte Wert muss für den Typ des Sekundärschlüssels gültig sein.

Anmerkung: Informationen zu Referenzsets und Referenzdatensammlungen finden Sie im *Administratorhandbuch* für Ihr Produkt.

Regeln anzeigen

Sie können die Details einer Regel einschließlich der Tests, Bausteine und Antworten anzeigen.

Vorbereitende Schritte

Anhängig von Ihren Benutzerrollenberechtigungen können Sie über die Registerkarte **Protokollaktivität** auf die Regelseite zugreifen. Weitere Informationen zu Benutzerrollenberechtigungen finden Sie in der Veröffentlichung *IBM Security QRadar Log Manager - Verwaltungshandbuch*.

Informationen zu diesem Vorgang

Auf der Regelseite wird eine Liste der Regeln mit den ihnen zugeordneten Parametern angezeigt. Um die Regel zu lokalisieren, die Sie öffnen und deren Details Sie anzeigen möchten, können Sie das Listenfeld 'Gruppe' oder das Feld **Suchregeln** in der Symbolleiste verwenden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität** und wählen Sie im Listenfeld **Regeln** in der Symbolleiste dann die Option **Regeln** aus.
2. Wählen Sie im Listenfeld **Anzeigen** die Option **Regeln** aus.
3. Doppelklicken Sie auf die Regel, die Sie anzeigen möchten.
4. Überprüfen Sie die Regeldetails.

Ergebnisse

Wenn Sie über die Berechtigung **View Custom Rules** (Angepasste Regeln anzeigen) jedoch nicht über die Berechtigung **Maintain Custom Rules** (Angepasste Regeln verwalten) verfügen, wird die Seite **Regelzusammenfassung** angezeigt und die Regel kann nicht bearbeitet werden. Wenn Sie über die Berechtigung **Maintain Custom Rules** (Angepasste Regeln verwalten) verfügen, wird die Seite **Editor für Regelteststack** angezeigt. Sie können die Regeldetails bearbeiten und überprüfen.

Angepasste Regel erstellen

Sie können neue Regeln erstellen, um die Anforderungen Ihrer Bereitstellung zu erfüllen.

Informationen zu diesem Vorgang

Zum Erstellen einer neuen Regel benötigen Sie die Berechtigung **Angriffe** > **Maintain Custom Rules (Angepasste Regeln verwalten)**.

Regeln können lokal oder global getestet werden. Bei einem lokalen Test wird die Regel im lokalen Ereignisprozessor getestet und nicht im System gemeinsam genutzt. Bei einem globalen Test wird die Regel gemeinsam genutzt und kann von allen Ereignisprozessoren im System getestet werden. Globale Regeln senden Ereignisse und Datenflüsse an den zentralen Ereignisprozessor, wodurch die Leistung des zentralen Ereignisprozessors unter Umständen herabgesetzt sein kann.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie in der Liste **Aktionen** die Option **Neue Ereignisregel** aus.
4. Lesen Sie den Einleitungstext im Regelassistenten. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Weiter**, um die Seite **Editor für Regelteststack** anzuzeigen.

6. Geben Sie in das Feld **Enter rule name here** (Hier Regelnamen eingeben) im Fensterbereich 'Regel' einen eindeutigen Namen ein, den Sie dieser Regel zuweisen möchten.
7. Wählen Sie im Listenfeld **Lokal** oder **Global** aus.
8. Fügen Sie einer Regel einen oder mehrere Tests hinzu:
   a. Optional. Wenn Sie die Optionen im Listenfeld **Testgruppe** filtern möchten, geben Sie den Text, nach dem gefiltert werden soll, in das Feld 'Filtertyp' ein.
   b. Wählen Sie im Listenfeld **Testgruppe** den Testtyp aus, den Sie dieser Regel hinzufügen möchten.
   c. Wählen Sie für jeden Test, den Sie der Regel hinzufügen möchten, das Pluszeichen (+) neben dem Test aus.
   d. Optional. Wenn Sie einen Test als ausgeschlossenen Test kennzeichnen möchten, klicken Sie im Fensterbereich 'Regel' am Anfang des Tests auf **and** (und). Anstelle von **and** (und) wird daraufhin **and not** (und nicht) angezeigt.
   e. Klicken Sie auf die unterstrichenen konfigurierbaren Parameter, um die Testvariablen anzupassen.
   f. Wählen Sie im Dialogfeld Werte für die Variable aus und klicken Sie auf **Übergeben**.
9. So können Sie die konfigurierte Regel als Baustein zur Verwendung mit anderen Regeln exportieren:
   a. Klicken Sie auf **Als Baustein exportieren**.
   b. Geben Sie einen eindeutigen Namen für den Baustein ein.
   c. Klicken Sie auf **Speichern**.
10. Wählen Sie im Fensterbereich 'Gruppen' die Kontrollkästchen der Gruppen aus, denen Sie diese Regel zuweisen möchten.
11. Geben Sie im Feld **Hinweise** einen Hinweis ein, den Sie für diese Regel angeben möchten. Klicken Sie auf **Weiter**.
12. Konfigurieren Sie auf der Seite **Regelantworten** die Antworten, die von dieser Regel generiert werden sollen.
13. Klicken Sie auf **Weiter**.
14. Prüfen Sie auf der Seite **Regelzusammenfassung**, ob die Einstellungen korrekt sind. Nehmen Sie gegebenenfalls Änderungen vor und klicken Sie anschließend auf **Beenden**.

Regel zur Erkennung von Unregelmäßigkeiten erstellen

Über den Assistenten für Regeln zur Erkennung von Unregelmäßigkeiten können Sie Regeln erstellen, die unter Verwendung von Datums- und Uhrzeittests Zeitraumkriterien anwenden.

Vorbereitende Schritte

Zum Erstellen einer neuen Regel zur Erkennung von Unregelmäßigkeiten müssen folgende Anforderungen erfüllt werden:

- Sie müssen über die Berechtigung 'Maintain Custom Rules (Angepasste Regeln verwalten)' verfügen.
- Sie müssen eine gruppierte Suche ausführen.

Die Optionen für die Erkennung von Unregelmäßigkeiten werden angezeigt, wenn Sie eine gruppierte Suche durchgeführt und die Suchkriterien gespeichert haben.

Informationen zu diesem Vorgang

Um eine Regel zur Erkennung von Unregelmäßigkeiten erstellen zu können, müssen Sie über die entsprechende Rollenberechtigung verfügen.

Wenn Sie Regeln zur Erkennung von Unregelmäßigkeiten auf der Registerkarte **Protokollaktivität** erstellen möchten, benötigen Sie hierfür die Rollenberechtigung **Protokollaktivität Maintain Custom Rules (Angepasste Regeln verwalten)**.

Wenn Sie Regeln zur Erkennung von Unregelmäßigkeiten auf der Registerkarte **Netzaktivität** erstellen möchten, benötigen Sie hierfür die Rollenberechtigung **Netzaktivität Maintain Custom Rules (Angepasste Regeln verwalten)**.

Die Regeln zur Erkennung von Unregelmäßigkeiten verwenden alle Gruppierungs- und Filterkriterien aus den gespeicherten Suchkriterien, auf denen die Regel basiert, die Zeitbereiche werden jedoch nicht aus den Suchkriterien übernommen.

Wenn Sie eine Regel zur Erkennung von Unregelmäßigkeiten erstellen, wird die Regel mit einem Standardteststack aufgefüllt. Sie können die Standardtests bearbeiten oder dem Teststack Tests hinzufügen. Im Teststack muss mindestens ein Test für eine kumulierte Eigenschaft enthalten sein.

Standardmäßig ist auf der Seite **Editor für Regelteststack** die Option **Den [ausgewählte kumulierte Eigenschaft]-Wert jeder [Gruppe]-Instanz gesondert testen** ausgewählt.

Bei Verwendung dieser Option testet die Regel zur Erkennung von Unregelmäßigkeiten die ausgewählte kumulierte Eigenschaft für jede Ereignisgruppe separat. Lautet der ausgewählte kumulierte Wert beispielsweise **UniqueCount(sourceIP)** (Eindeutiger Zähler (Quellen-IP)), testet die Regel jede eindeutige Quellen-IP-Adresse für jede Ereignisgruppe.

Bei der Option **Den [ausgewählte kumulierte Eigenschaft]-Wert jeder [Gruppe]-Instanz gesondert testen** handelt es sich um eine dynamische Option. Der Wert für **[ausgewählte kumulierte Eigenschaft]** hängt davon ab, welche Option Sie für das Feld **this accumulated property test** (Test dieser kumulierten Eigenschaft) des Standardteststacks auswählen. Der Wert für **[Gruppe]** hängt von den in den gespeicherten Suchkriterien angegebenen Gruppierungsoptionen ab. Bei Angabe mehrerer Gruppierungsoptionen kann es sein, dass der Text abgeschnitten wird. Bewegen Sie den Mauszeiger über den Text, um alle Gruppen anzuzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Führen Sie eine Suche durch.
3. Wählen Sie im Menü **Regeln** den Regeltyp aus, den Sie erstellen möchten. Mögliche Optionen:
   - Anomalieregel hinzufügen
   - Schwellenwertregel hinzufügen
   - Verhaltensregel hinzufügen
4. Lesen Sie den Einleitungstext im Regelassistenten. Klicken Sie auf **Weiter**. Die zuvor ausgewählte Regel wird ausgewählt.

5. Klicken Sie auf **Weiter**, um die Seite **Editor für Regelteststack** anzuzeigen.
6. Geben Sie in das Feld **Enter rule name here** (Hier Regelnamen eingeben) einen eindeutigen Namen ein, den Sie dieser Regel zuweisen möchten.
7. So fügen Sie einer Regel einen Test hinzu:
   a. Optional. Wenn Sie die Optionen im Listenfeld 'Testgruppe' filtern möchten, geben Sie den Text, nach dem gefiltert werden soll, in das Feld 'Filtertyp' ein.
   b. Wählen Sie im Listenfeld 'Testgruppe' den Testtyp aus, den Sie dieser Regel hinzufügen möchten.
   c. Wählen Sie für jeden Test, den Sie der Regel hinzufügen möchten, das Zeichen '+' neben dem Test aus.
   d. Optional. Wenn Sie einen Test als ausgeschlossenen Test kennzeichnen möchten, klicken Sie im Fensterbereich 'Regel' am Anfang des Tests auf 'and' (und). Anstelle von 'and' (und) wird daraufhin 'and not' (und nicht) angezeigt.
   e. Klicken Sie auf die unterstrichenen konfigurierbaren Parameter, um die Testvariablen anzupassen.
   f. Wählen Sie im Dialogfeld Werte für die Variable aus und klicken Sie auf **Übergeben**.
8. Optional. Wenn Sie die gesamten ausgewählten kumulierten Eigenschaften für jede Ereignis- oder Datenflussgruppe testen möchten, heben Sie die Markierung des Kontrollkästchens **Den [ausgewählte kumulierte Eigenschaft]-Wert jeder [Gruppe]-Instanz gesondert testen** auf.
9. Wählen Sie im Fensterbereich 'Gruppen' die Kontrollkästchen der Gruppen, denen Sie diese Regel zuweisen möchten. Weitere Informationen finden Sie im Abschnitt Verwaltung von Regelgruppen.
10. Geben Sie im Feld **Hinweise** alle Hinweise ein, die Sie für diese Regel angeben möchten. Klicken Sie auf **Weiter**.
11. Konfigurieren Sie auf der Seite **Regelantworten** die Antworten, die von dieser Regel generiert werden sollen. „Parameter der Seite 'Regelantwort'" auf Seite 103
12. Klicken Sie auf **Weiter**.
13. Prüfen Sie die konfigurierte Regel. Klicken Sie auf **Beenden**.

Regelmanagementtasks

Sie können angepasste Regeln und Anomalieregeln verwalten.

Regeln können nach Bedarf aktiviert und inaktiviert werden. Außerdem können Sie Regeln bearbeiten, kopieren oder löschen.

Regeln zur Erkennung von Unregelmäßigkeiten können nur auf der Registerkarte **Protokollaktivität** erstellt werden.

Regeln aktivieren und inaktivieren

Wenn Sie Ihr System optimieren, können Sie die erforderlichen Regeln aktivieren bzw. inaktivieren, um sicherzustellen, dass Ihr System aussagefähige Angriffe für Ihre Umgebung generiert.

Informationen zu diesem Vorgang

Sie benötigen die Rollenberechtigung **Protokollaktivität** > **Maintain Custom Rules** (Angepasste Regeln verwalten), um eine Regel zu aktivieren oder zu inaktivieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie im Listenfeld **Anzeigen** auf der Seite **Regeln** den Eintrag **Regeln** aus.
4. Wählen Sie die Regel aus, die Sie aktivieren oder inaktivieren wollen.
5. Wählen Sie im Listenfeld **Aktionen** den Eintrag **Aktivieren/Inaktivieren** aus.

Regeln bearbeiten

Sie können eine Regel bearbeiten, um den Regelnamen, Regeltyp, Tests oder Antworten zu ändern.

Informationen zu diesem Vorgang

Sie benötigen die Rollenberechtigung **Protokollaktivität** > **Maintain Custom Rules** (Angepasste Regeln verwalten), um eine Regel zu aktivieren oder zu inaktivieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie im Listenfeld **Anzeigen** auf der Seite **Regeln** den Eintrag **Regeln** aus.
4. Doppelklicken Sie auf die Regel, die Sie bearbeiten möchten.
5. Wählen Sie im Listenfeld **Aktionen** den Eintrag **Öffnen** aus.
6. Optional. Wenn Sie den Regeltyp ändern wollen, klicken Sie auf **Zurück** und wählen Sie einen neuen Regeltyp aus.
7. Bearbeiten Sie die Parameter auf der Seite **Editor für Regelteststack**.
8. Klicken Sie auf **Weiter**.
9. Bearbeiten Sie die Parameter auf der Seite **Regelantwort**.
10. Klicken Sie auf **Weiter**.
11. Prüfen Sie die bearbeitete Regel. Klicken Sie auf **Fertigstellen**.

Regel kopieren

Sie können eine vorhandene Regel kopieren, einen neuen Namen für die Regel eingeben und dann die Parameter in der neuen Regel nach Bedarf anpassen.

Informationen zu diesem Vorgang

Zum Aktivieren oder Inaktivieren einer Regel benötigen Sie die Rollenberechtigung **Protokollaktivität** > **Maintain Custom Rules (Angepasste Regeln verwalten)**.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie im Listenfeld **Anzeige** die Option **Regeln** aus.

4. Wählen Sie die zu duplizierende Regel aus.
5. Wählen Sie im Listenfeld **Aktionen** die Option **Duplizieren** aus.
6. Geben Sie im Feld 'Geben Sie den Namen für die kopierte Regel ein' einen Namen für die neue Regel ein. Klicken Sie auf **OK**.

Regeln löschen

Sie können eine Regel aus Ihrem System löschen.

Informationen zu diesem Vorgang

Sie benötigen die Rollenberechtigung **Protokollaktivität** > **Maintain Custom Rules** (Angepasste Regeln verwalten), um eine Regel zu aktivieren oder zu inaktivieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie im Listenfeld **Anzeigen** den Eintrag **Regeln** aus.
4. Wählen Sie die Regel aus, die Sie löschen wollen.
5. Wählen Sie im Listenfeld **Aktionen** den Eintrag **Löschen** aus.

Verwaltung von Regelgruppen

Als Administrator können Sie Gruppen von Regeln erstellen, bearbeiten und löschen. Durch die Kategorisierung Ihrer Regeln oder Bausteine in Gruppen können Sie die Regeln effizient anzeigen und nachverfolgen.

Sie können zum Beispiel alle Regeln in Bezug auf Konformität anzeigen.

Beim Erstellen neuer Regeln können Sie diese vorhandenen Gruppen zuweisen. Informationen zur Zuweisung einer Gruppe über den Regelassistenten finden Sie in den Abschnitten Erstellen einer angepassten Regel oder Erstellen einer Regel zur Erkennung von Unregelmäßigkeiten.

Regelgruppe anzeigen

Sie können die Regeln oder Bausteine auf der Seite **Regeln** filtern, um nur die zu einer bestimmten Gruppe gehörigen Regeln oder Bausteine anzuzeigen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Legen Sie im Listenfeld **Anzeigen** fest, ob Regeln oder Bausteine angezeigt werden sollen.
4. Wählen Sie im Listenfeld **Filter** die Gruppenkategorie aus, die Sie anzeigen möchten.

Gruppen erstellen

Auf der Seite **Regeln** werden Standardregelgruppen bereitgestellt, allerdings können Sie eine neue Gruppe erstellen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Navigationsstruktur die Gruppe aus, unter der Sie eine neue Gruppe erstellen wollen.
5. Klicken Sie auf **Neue Gruppe**.
6. Folgende Parameter müssen angegeben werden:
   - **Name** - Geben Sie einen eindeutigen Namen ein, der der neuen Gruppe zugewiesen wird. Der Name kann bis zu 255 Zeichen lang sein.
   - **Beschreibung** - Geben Sie eine Beschreibung ein, die Sie dieser Gruppe zuweisen wollen. Die Beschreibung kann bis zu 255 Zeichen lang sein.
7. Klicken Sie auf **OK**.
8. Optional. Um die Position der neuen Gruppe zu ändern, klicken Sie auf die neue Gruppe und ziehen Sie den Ordner zur neuen Position in der Navigationsstruktur.

Element zu einer Gruppe zuweisen

Sie können eine ausgewählte Regel oder einen Baustein einer Gruppe zuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie die Regel bzw. den Baustein aus, den Sie einer Gruppe zuweisen möchten.
4. Wählen Sie im Listenfeld **Aktionen** die Option **Gruppen zuordnen** aus.
5. Wählen Sie die Gruppe aus, der Sie die Regel bzw. den Baustein zuweisen möchten.
6. Klicken Sie auf **Gruppen zuordnen**.
7. Schließen Sie das Fenster **Gruppe auswählen**.

Gruppen bearbeiten

Sie können eine Gruppe bearbeiten, um den Namen oder die Beschreibung zu ändern.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Navigationsstruktur die Gruppe aus, die Sie bearbeiten wollen.
5. Klicken Sie auf **Bearbeiten**.
6. Folgende Parameter müssen aktualisiert werden:
   - **Name** - Geben Sie einen eindeutigen Namen ein, der der neuen Gruppe zugewiesen wird. Der Name kann bis zu 255 Zeichen lang sein.
   - **Beschreibung** - Geben Sie eine Beschreibung ein, die Sie dieser Gruppe zuweisen wollen. Die Beschreibung kann bis zu 255 Zeichen lang sein.
7. Klicken Sie auf **OK**.

8. Optional. Um die Position der Gruppe zu ändern, klicken Sie auf die neue Gruppe und ziehen Sie den Ordner zur neuen Position in der Navigationsstruktur.

Element in eine andere Gruppe kopieren

Sie können eine Regel oder einen Baustein von einer Gruppe in andere Gruppen kopieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Klicken Sie auf **Gruppen**.
4. Wählen Sie in der Navigationsstruktur die Regel bzw. den Baustein aus, die/der in eine andere Gruppe kopiert werden soll.
5. Klicken Sie auf **Kopieren**.
6. Wählen Sie das Kontrollkästchen für die Gruppe aus, in die Sie die Regel bzw. den Baustein kopieren möchten.
7. Klicken Sie auf **Kopieren**.

Element aus einer Gruppe löschen

Sie können ein Element aus einer Gruppe löschen. Wenn Sie ein Element aus einer Gruppe löschen, wird die Regel bzw. der Baustein nur aus der Gruppe gelöscht und bleibt auf der Seite **Regeln** weiterhin verfügbar.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Klicken Sie auf **Gruppen**.
4. Navigieren Sie über die Navigationsstruktur zu dem zu löschenden Element und wählen Sie dieses aus.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **OK**.

Gruppen löschen

Sie können eine Gruppe löschen. Wenn Sie eine Gruppe löschen, bleiben die Regeln oder Bausteine jener Gruppe auf der Seite **Regeln** verfügbar.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Klicken Sie auf **Gruppen**.
4. Navigieren Sie über die Navigationsstruktur zur Gruppe, die gelöscht werden soll, und wählen Sie sie aus.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **OK**.

Bausteine bearbeiten

Sie können einen der Standardbausteine bearbeiten, um die Anforderungen Ihrer Implementierung zu erfüllen.

Informationen zu diesem Vorgang

Ein Baustein ist ein wiederverwendbares Regelteststack, das man als Komponente in andere Regeln einbeziehen kann.

Zum Beispiel können Sie den Baustein 'BB:HostDefinition: Mail Servers' bearbeiten, um alle Mail-Server in Ihrer Implementierung zu identifizieren. Dann können Sie eine Regel konfigurieren, um Ihre Mail-Server aus den Regeltests auszuschließen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Protokollaktivität**.
2. Klicken Sie in der Symbolleiste auf **Regeln**.
3. Wählen Sie im Listenfeld **Anzeigen** den Eintrag **Bausteine** aus.
4. Doppelklicken Sie auf den Baustein, den Sie bearbeiten möchten.
5. Aktualisieren Sie den Baustein nach Bedarf.
6. Klicken Sie auf **Weiter**.
7. Fahren Sie mit dem Assistenten fort. Weitere Informationen finden Sie im Abschnitt Angepasste Regel erstellen.
8. Klicken Sie auf **Fertigstellen**.

Parameter der Seite 'Regeln'

Eine Beschreibung der Parameter auf der Seite **Regeln**.

In der Liste der bereitgestellten Regeln sind zu jeder Regel folgende Informationen angegeben:

Tabelle 30. Parameter der Seite 'Regeln'

Parameter	Beschreibung
Regelname	Zeigt den Namen der Regel an.
Gruppe	Zeigt die Gruppe an, der diese Regel zugewiesen ist. Weitere Informationen zu Gruppen finden Sie im Abschnitt Verwaltung von Regelgruppen.
Regelkategorie	Zeigt die Regelkategorie für die Regel an. Mögliche Optionen sind u. a. 'Angepasste Regel' und 'Regel zur Erkennung von Unregelmäßigkeiten'.
Regeltyp	Zeigt den Regeltyp an.
Aktiviert	Gibt an, ob die Regel aktiviert oder inaktiviert ist. Weitere Informationen zum Aktivieren und Inaktivieren von Regeln finden Sie im Abschnitt Regeln aktivieren und inaktivieren.

Tabelle 30. Parameter der Seite 'Regeln' (Forts.)

Parameter	Beschreibung
Antwort	Zeigt die Regelantwort an, sofern vorhanden. Mögliche Regelantworten: • Neues Ereignis senden • E-Mail • Log Notification (Protokollbenachrichtigung) • SNMP • Referenzset • Reference Data (Referenzdaten) • IF-MAP Response (IF-MAP-Antwort) Weitere Informationen zu Regelantworten finden Sie im Abschnitt Regelantworten.
Ereigniszähler	Zeigt an, wie viele Ereignisse dieser Regel zugewiesen werden, wenn die Regel zu einem Angriff beiträgt.
Ursprung	Gibt an, ob es sich um eine Standardregel (System) oder eine angepasste Regel (Benutzer) handelt.
Erstellungsdatum	Gibt an, wann diese Regel erstellt wurde (Datum und Uhrzeit).
Änderungsdatum	Gibt an, wann diese Regel geändert wurde (Datum und Uhrzeit).

Symbolleiste der Seite 'Regeln'

Über die Symbolleiste der Seite **Regeln** können Sie Regeln, Bausteine oder Gruppen anzeigen. Außerdem ist es möglich, Regelgruppen zu verwalten und mit Regeln zu arbeiten.

Auf der Symbolleiste der Seite **Regeln** stehen die folgenden Funktionen zur Verfügung:

Tabelle 31. Funktionen auf der Symbolleiste der Seite 'Regeln'

Funktion	Beschreibung
Anzeige	Wählen Sie in dem Listenfeld aus, ob in der Regelliste Regeln oder Bausteine angezeigt werden sollen.
Gruppe	Wählen Sie in dem Listenfeld aus, welche Regelgruppe in der Regelliste angezeigt werden soll.
Gruppen	Klicken Sie auf **Gruppen**, um Regelgruppen zu verwalten.

Tabelle 31. Funktionen auf der Symbolleiste der Seite 'Regeln' (Forts.)

Funktion	Beschreibung
Aktionen	Klicken Sie auf **Aktionen** und wählen Sie eine der folgenden Optionen aus: • **Neue Ereignisregel** - Wählen Sie diese Option aus, um eine neue Ereignisregel zu erstellen. • **Aktivieren/Inaktivieren** - Wählen Sie diese Option aus, um ausgewählte Regeln zu aktivieren oder zu inaktivieren. • **Duplizieren** - Wählen Sie diese Option aus, um eine ausgewählte Regel zu kopieren. • **Bearbeiten** - Wählen Sie diese Option aus, um eine ausgewählte Regel zu bearbeiten. • **Löschen** - Wählen Sie diese Option aus, um eine ausgewählte Regel zu löschen. • **Gruppen zuordnen** - Wählen Sie diese Option aus, um ausgewählte Regeln zu Regelgruppen zuzuordnen.
Regel zurücksetzen	Klicken Sie auf **Regel zurücksetzen**, um eine geänderte Systemregel auf den Standardwert zurückzusetzen. Wenn Sie auf **Regel zurücksetzen** klicken, wird ein Bestätigungsfenster angezeigt. Wenn Sie eine Regel zurücksetzen, werden vorherige Änderungen dauerhaft entfernt. Wenn Sie die Regel zurücksetzen und eine geänderte Version beibehalten möchten, duplizieren Sie die Regel und verwenden Sie die Option **Regel zurücksetzen** für die geänderte Regel.
Suchregeln	Geben Sie Ihre Suchkriterien in das Feld **Suchregeln** ein und klicken Sie auf das Symbol **Suchregeln** oder drücken Sie die Eingabetaste. Alle Regeln, die mit Ihren Suchkriterien übereinstimmen, werden in der Regelliste angezeigt. Die folgenden Parameter werden auf eine Übereinstimmung mit Ihren Suchkriterien durchsucht: • Regelname • Rule (description) (Regel (Beschreibung)) • Hinweise • Antwort Die Funktion 'Suchregel' versucht, eine direkte Textfolgenübereinstimmung ausfindig zu machen. Wenn keine Übereinstimmung gefunden wird, versucht die Funktion 'Suchregel' einen Abgleich mit einem regulären Ausdruck (regex).

Parameter der Seite 'Regelantwort'

Es gibt verschiedene Parameter für die Seite **Regelantwort**.

In der folgenden Tabelle sind die Parameter der Seite **Regelantwort** aufgeführt.

Tabelle 32. Parameter der Seite mit Antworten von Ereignis- und Datenflussregeln sowie allgemeinen Regeln

Parameter	Beschreibung
Wertigkeit	Wählen Sie dieses Kontrollkästchen aus, wenn mit dieser Regel die Wertigkeit definiert oder angepasst werden soll. Ist dieses Kontrollkästchen ausgewählt, können Sie die entsprechende Wertigkeitsstufe über die Listenfelder konfigurieren.
Zuverlässigkeit	Wählen Sie dieses Kontrollkästchen aus, wenn mit dieser Regel die Zuverlässigkeit definiert oder angepasst werden soll. Ist dieses Kontrollkästchen ausgewählt, können Sie die entsprechende Zuverlässigkeitsstufe über die Listenfelder konfigurieren.
Relevanz	Wählen Sie dieses Kontrollkästchen aus, wenn mit dieser Regel die Relevanz definiert oder angepasst werden soll. Ist dieses Kontrollkästchen ausgewählt, können Sie die entsprechende Relevanzstufe über die Listenfelder konfigurieren.
Annotate event (Ereignis mit Anmerkungen versehen)	Wählen Sie dieses Kontrollkästchen aus, wenn Sie zu diesem Ereignis eine Anmerkung hinzufügen möchten, und geben Sie die gewünschte Anmerkung ein.
Erkanntes Ereignis löschen	Wählen Sie dieses Kontrollkästchen aus, um zu erzwingen, dass ein Ereignis, das normalerweise an die Magistrate-Komponente gesendet wird, zu Berichtszwecken oder für die Suche an die Ariel-Datenbank gesendet wird.
Neues Ereignis senden	Wählen Sie dieses Kontrollkästchen aus, wenn Sie zusätzlich zu dem ursprünglichen Ereignis ein neues Ereignis senden möchten, das wie alle anderen Ereignisse im System verarbeitet wird. Bei Auswahl dieses Kontrollkästchens werden die Parameter **Neues Ereignis senden** angezeigt. Standardmäßig ist dieses Kontrollkästchen nicht ausgewählt.
Ereignisname	Geben Sie einen eindeutigen Namen für das Ereignis ein, der auf der Registerkarte **Protokollaktivität** angezeigt werden soll.
Ereignisbeschreibung	Geben Sie eine Beschreibung für das Ereignis ein. Die Beschreibung wird im Fensterbereich **Anmerkungen** der Ereignisdetails angezeigt.
Wertigkeit	Wählen Sie im Listenfeld die Wertigkeit für das Ereignis aus. Der Bereich reicht von 0 (niedrigste Stufe) bis 10 (höchste Stufe), der Standardwert lautet '0'. Die Wertigkeit wird im Fensterbereich **Anmerkung** der Ereignisdetails angezeigt.
Zuverlässigkeit	Wählen Sie im Listenfeld die Zuverlässigkeit für das Ereignis aus. Der Bereich reicht von 0 (niedrigste Stufe) bis 10 (höchste Stufe), der Standardwert lautet '10'. Die Zuverlässigkeit wird im Fensterbereich **Anmerkung** der Ereignisdetails angezeigt.

Tabelle 32. Parameter der Seite mit Antworten von Ereignis- und Datenflussregeln sowie allgemeinen Regeln (Forts.)

Parameter	Beschreibung
Relevanz	Wählen Sie im Listenfeld die Relevanz des Ereignisses aus. Der Bereich reicht von 0 (niedrigste Stufe) bis 10 (höchste Stufe), der Standardwert lautet '10'. Die Relevanz wird im Fensterbereich **Anmerkung** der Ereignisdetails angezeigt.
Übergeordnete Kategorie	Wählen Sie im Listenfeld die übergeordnete Ereigniskategorie aus, die von dieser Regel bei der Ereignisverarbeitung verwendet werden soll.
Untergeordnete Kategorie	Wählen Sie im Listenfeld die untergeordnete Ereigniskategorie aus, die von dieser Regel bei der Ereignisverarbeitung verwendet werden soll.
E-Mail	Wählen Sie dieses Kontrollkästchen aus, um die E-Mail-Optionen anzuzeigen. **Anmerkung:** Soll die **E-Mail-Ländereinstellung** geändert werden, wählen Sie auf der Registerkarte **Verwaltung** die Option **Systemeinstellungen** aus.
E-Mail-Adresse für Benachrichtigungen eingeben	Geben Sie die E-Mail-Adresse ein, an die eine Benachrichtigung gesendet werden soll, wenn diese Regel generiert wird. Geben Sie mehrere E-Mail-Adressen durch Kommas getrennt an.
SNMP-Alarmnachricht	Dieser Parameter wird nur angezeigt, wenn die Parameter für die SNMP-Einstellungen in den Systemeinstellungen konfiguriert sind. Wählen Sie dieses Kontrollkästchen aus, wenn diese Regel in der Lage sein soll, eine SNMP-Benachrichtigung (Alarmnachricht) zu senden. In der Ausgabe der SNMP-Alarmnachricht sind die Systemzeit, die Objektkennung der Alarmnachricht und die Benachrichtigungsdaten wie im Nachrichteninformationsblock definiert angegeben.
An lokales Systemprotokoll senden	Wählen Sie dieses Kontrollkästchen aus, wenn das Ereignis lokal protokolliert werden soll. Dieses Kontrollkästchen ist standardmäßig nicht ausgewählt. **Anmerkung:** Nur normalisierte Ereignisse können lokal auf einem System protokolliert werden. Wenn Sie unformatierte Ereignisdaten senden möchten, müssen Sie die Daten mit der Option 'An Weiterleitungsziele senden' an einen fernen Syslog-Host senden.

Tabelle 32. Parameter der Seite mit Antworten von Ereignis- und Datenflussregeln sowie allgemeinen Regeln (Forts.)

Parameter	Beschreibung
An Weiterleitungsziele senden	Dieses Kontrollkästchen wird nur für Ereignisregeln angezeigt. Wählen Sie dieses Kontrollkästchen aus, wenn das Ereignis bzw. der Datenfluss auf einem Weiterleitungsziel protokolliert werden soll. Bei einem Weiterleitungsziel handelt es sich um ein Anbietersystem wie z. B. SIEM, Etikettierungs- oder Alertingsysteme. Bei Auswahl dieses Kontrollkästchens wird eine Liste mit Weiterleitungszielen angezeigt. Wählen Sie das Kontrollkästchen für das Weiterleitungsziel aus, an das dieses Ereignis bzw. dieser Datenfluss gesendet werden soll. Klicken Sie auf den Link **Ziele verwalten**, wenn Sie ein Weiterleitungsziel hinzufügen, bearbeiten oder löschen möchten.
Benachrichtigen	Wählen Sie dieses Kontrollkästchen aus, wenn Ereignisse, die infolge dieser Regel generiert werden, unter dem Eintrag 'Systembenachrichtigungen' auf der Registerkarte 'Dashboard' angezeigt werden sollen. Konfigurieren Sie den Parameter **Antwortbegrenzer**, falls Sie Benachrichtigungen aktivieren.
Zu Referenzset hinzufügen	Wählen Sie dieses Kontrollkästchen aus, wenn Ereignisse, die infolge dieser Regel generiert werden, Daten zu einem Referenzset hinzufügen sollen. So fügen Sie einem Referenzset Daten hinzu: 1. Wählen Sie über das erste Listenfeld die hinzuzufügenden Daten aus. In Frage kommen alle normalisierten oder benutzerdefinierten Daten. 2. Wählen Sie im zweiten Listenfeld das Referenzset aus, dem die angegebenen Daten hinzugefügt werden sollen. Die Regelantwort **Zu Referenzset hinzufügen** bietet folgende Funktionen: **Aktualisieren** Aktualisieren Sie das erste Listenfeld durch Anklicken von **Aktualisieren** und stellen Sie so sicher, dass die Liste aktuell ist. **Referenzsätze konfigurieren** Klicken Sie auf **Referenzsätze konfigurieren**, um das Referenzset zu konfigurieren. Diese Option ist nur verfügbar, wenn Sie über Administratorberechtigung verfügen.

Tabelle 32. Parameter der Seite mit Antworten von Ereignis- und Datenflussregeln sowie allgemeinen Regeln (Forts.)

Parameter	Beschreibung
Zu Referenzdaten hinzufügen	Diese Regelantwort können Sie erst verwenden, nachdem Sie über die Befehlszeilenschnittstelle die Referenzdatensammlung erstellt haben. Weitere Informationen zum Erstellen und zur Verwendung von Referenzdatensammlungen finden Sie im *Verwaltungshandbuch* für Ihr Produkt. Wählen Sie dieses Kontrollkästchen aus, wenn Ereignisse, die infolge dieser Regel generiert werden, Daten zu einer Referenzdatensammlung hinzufügen sollen. Wählen Sie nach Auswahl des Kontrollkästchens eine der folgenden Optionen aus: **Zu einer Referenzzuordnung hinzufügen** Wählen Sie diese Option aus, wenn Sie Daten an eine Sammlung von Paaren 'einzelner Schlüssel/ mehrere Werte' senden möchten. Sie müssen zunächst den Schlüssel und Wert für den Datensatz und anschließend die Referenzzuordnung auswählen, zu der der Datensatz hinzugefügt werden soll. **Zu einer Referenzzuordnung von Sets hinzufügen** Wählen Sie diese Option aus, wenn Sie Daten an eine Sammlung von Paaren 'Schlüssel/einzelner Wert' senden möchten. Sie müssen zunächst den Schlüssel und Wert für den Datensatz und anschließend die Referenzzuordnung von Sets auswählen, zu der der Datensatz hinzugefügt werden soll. **Zu einer Referenzzuordnung von Zuordnungen hinzufügen** Wählen Sie diese Option aus, wenn Sie Daten an eine Sammlung von Paaren 'mehrere Schlüssel/ einzelner Wert' senden möchten. Sie müssen einen Schlüssel für die erste Zuordnung, einen Schlüssel für die zweite Zuordnung und dann den Wert für den Datensatz auswählen. Sie müssen auch die Referenzzuordnung von Zuordnungen auswählen, zu der der Datensatz hinzugefügt werden soll. **Zu einer Referenztabelle hinzufügen** Wählen Sie diese Option aus, wenn Sie Daten an eine Sammlung von Paaren 'mehrere Schlüssel/ einzelner Wert' senden möchten, wobei den Sekundärschlüsseln ein Typ zugeordnet wurde. Wählen Sie die Referenztabelle, der Sie Daten hinzufügen möchten, und dann einen Primärschlüssel aus. Wählen Sie die inneren Schlüssel (Sekundärschlüssel) und ihre Werte für die Datensätze aus.
Auf dem IF-MAP-Server veröffentlichen	Wenn die IF-MAP-Parameter konfiguriert und in den Systemeinstellungen bereitgestellt sind, wählen Sie diese Option aus, um die Ereignisdaten zum IF-MAP-Server zu veröffentlichen.
Antwortbegrenzer	Wählen Sie dieses Kontrollkästchen aus und konfigurieren Sie über die Listenfelder die gewünschte Häufigkeit der Antworten dieser Regel.

Tabelle 32. Parameter der Seite mit Antworten von Ereignis- und Datenflussregeln sowie allgemeinen Regeln (Forts.)

Parameter	Beschreibung
Regel aktivieren	Wählen Sie dieses Kontrollkästchen aus, um diese Regel zu aktivieren.

Eine SNMP-Benachrichtigung könnte ungefähr wie folgt aussehen:

```
"Mi 28. Sept 12:20:57 GMT 2005, Benachrichtigung der Engine für angepasste Regeln -
 Regel 'SNMPTRAPTst' ausgelöst. 172.16.20.98:0 -> 172.16.60.75:0 1, Ereignisname:
 ICMP-Ziel nicht erreichbar, die Kommunikation mit dem Zielhost ist
 verwaltungstechnisch untersagt, QID: 1000156, Kategorie: 1014, Hinweise:
 Beschreibung des Angriffs"
```

Eine Systemprotokollausgabe könnte ungefähr wie folgt aussehen:

```
28. Sept 12:39:01 localhost.localdomain ECS:
 Regel 'Name der Regel' ausgelöst: 172.16.60.219:12642
 -> 172.16.210.126:6666 6, Ereignisname: SCAN SYN FIN, QID:
 1000398, Kategorie: 1011, Hinweise: Ereignisbeschreibung
```

Kapitel 9. Integration des IBM Security X-Force Threat Intelligence-Feeds

Mit dem IBM Security X-Force Threat Intelligence-Feed wird eine Echtzeitliste potenziell zerstörerischer IP-Adressen bereitgestellt. Mithilfe dieser IP-Adressen können Sie zusammen mit IBM QRadar Security Intelligence Platform verdächtige Aktivitäten in Ihrer Umgebung ermitteln.

Sie müssen über eine Subskription für den X-Force Threat Intelligence-Feed verfügen, damit dieser Feed zusammen mit QRadar eingesetzt werden kann.

Für den Inhalt des X-Force-Feeds wird eine relative Risikobewertung vergeben. QRadar-Benutzer können Vorfällen bzw. Verstößen, die durch diesen Inhalt entstehen, anhand dieser Risikobewertung Prioritäten zuweisen. Die Daten aus diesen Informationsquellen werden automatisch in die Korrelations- und Analysefunktionen von QRadar übernommen; die Funktionen des Produkts zur Erkennung von Sicherheitsbedrohungen werden somit durch aktuellste Daten zu Bedrohungen aus dem Internet erweitert. Alle Daten zu sicherheitsrelevanten Ereignissen oder Netzaktivitäten in Zusammenhang mit diesen Adressen werden automatisch markiert; dadurch erhält man wertvolle Kontextinformationen für die Analyse und Untersuchung von Sicherheitsverstößen.

Um eine Priorität für die Bedrohung zu vergeben und Sicherheitsverstöße zu ermitteln, die einer eingehenderen Untersuchung bedürfen, können Sie die X-Force-Feeds auswählen, die in die QRadar-Regeln, -Angriffe und -Ereignisse eingefügt werden sollen. So können Sie beispielsweise mit den Feeds folgende Vorfälle ermitteln:

- Eine Reihe von Anmeldeversuchen für einen dynamischen IP-Adressenbereich
- Eine anonyme Proxy-Verbindung zum Portal eines Geschäftspartners
- Eine Verbindung zwischen einem internen Endpunkt und einem bekannten Botnet Command-and-Control-Server
- Die Kommunikation zwischen einem Endpunkt und einer bekannten Site, die Malware verteilt

Der X-Force Threat Intelligence-Feed teilt IP-Adressen in Kategorien ein und nimmt anschließend eine Konfidenzeinstufung vor, anhand derer die Bedrohung beurteilt wird. Die IP-Adressen werden in die folgenden Kategorien eingeteilt:

- Malware-Hosts
- SPAM-Quellen
- Dynamische IP-Adressen
- Anonyme Proxys
- Botnet Command-and-Control

Der X-Force Threat Intelligence-Feed teilt auch URL-Adressen in Kategorien ein, beispielsweise in Sites für Partnerschaftssuche oder Glücksspiele oder pornografische Sites. Ein vollständige Liste der Kategorien zur Einteilung von URL-Adressen finden Sie auf der X-Force-Website (www.xforce-security.com).

Vor einer Verwendung URL-basierter Regeln müssen Sie eine angepasste Ereigniseigenschaft erstellen, um die URL aus den Nutzdaten abzurufen. Für Ereignisse

aus einer Reihe von Quellen wie beispielsweise Blue Coat SG- und Juniper Networks Secure Access-Protokollquellen ist das angepasste URL-Ereignis bereits definiert.

Erweiterte X-Force-Regeln

Sobald Sie den X-Force Threat Intelligence-Feed zu IBM QRadar Security Intelligence Platform hinzugefügt haben, können Sie sofort erweiterte Daten zu Bedrohungen empfangen.

Die folgenden Regeln gehören zur Gruppe **Erweiterte X-Force-Regeln**. Sie können diese Regeln unverändert einsetzen oder anpassen.

Diese Regeln sind IP-basiert:

X-Force Premium: Internal Connection to Possible Malware Host
Die Kommunikation deutet mit großer Wahrscheinlichkeit darauf hin, dass ein Versuch unternommen wurde, das Clientsystem zu infizieren, oder dass Malware heruntergeladen wurde.

X-Force Premium: Internal Hosts Communicating With Anonymous Proxies
Anonyme Proxys sind Adressen, die bekannt dafür sind, dass sie ihre Identität verschleiern. Diese Adressen werden häufig von Malware oder bei professionellen permanenten Bedrohungen eingesetzt, um den Ursprung der Kommunikation mit externen Quellen zu verbergen. Die Adressen können in Zusammenhang mit Aktivitäten wie Malware-Kommunikation oder dem unerlaubten Kopieren von Daten stehen.

X-Force Premium: Internal Mail Server Sending Mail to Possible SPAM Host
In der Regel werden Mail-Server, die mit SPAM-Hosts kommunizieren, missbraucht.

X-Force Premium: Non-Mail Servers Communicating with Known SPAM Sending Hosts
Dieses Verhalten weist mit großer Wahrscheinlichkeit darauf hin, dass der Server infiziert wurde und als SPAM-Relais verwendet wird.

X-Force Premium: Non-Servers Communicating with an External Dynamic IP
Dynamisch zugeordnete IP-Adressen, die typischerweise keinen legitimen Servern im Internet zugeordnet sind. Wenn interne Workstations mit dynamischen Adressen kommunizieren, weist dies unter Umständen auf verdächtige interne Aktivitäten oder Malware- oder Botnet-Aktivitäten hin.

X-Force Premium: Server Initiated Connection to Dynamic Hosts
Normalerweise kommunizieren Server mit Hosts, die eine feste Identität haben, keine dynamischen IP-Adressen.

Da die URL einen spezifischeren Hinweis auf die Daten gibt, die übertragen werden, sind URL-basierte Regeln unter Umstänen akkurater als IP-basierte Regeln.

Diese Regeln sind URL-basiert:

X-Force Premium: Internal Host Communicating with Botnet Command and Control URL
Hin und wieder werden legitime Server dazu verwendet, Botnet-Konnektivität an bestimmten URL-Adressen bereitstellen.

X-Force Premium: Internal Host Communication with Malware URL
Hin und wieder werden legitime Server dazu verwendet, Malware an bestimmten URL-Adressen bereitzustellen.

Beispiel: Regel unter Verwendung der URL-Kategorisierung erstellen, um den Zugriff auf bestimmte Websitetypen zu überwachen

Sie können eine Regel erstellen, die eine E-Mail-Benachrichtigung sendet, wenn Benutzer des internen Netzes auf URL-Adressen zugreifen, die unter die Kategorie "Websites für Glücksspiele" fallen.

Vorbereitende Schritte

Damit URL-Kategorisierungsregeln verwendet werden können, müssen Sie über eine Subskription für den X-Force Threat Intelligence-Feed verfügen.

Zum Erstellen einer neuen Regel benötigen Sie die Berechtigung **Angriffe** > **Maintain Custom Rules (Angepasste Regeln verwalten)**.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Angriffe**.
2. Klicken Sie im Navigationsmenü auf **Regeln**.
3. Wählen Sie in der Liste **Aktionen** die Option **Neue Ereignisregel** aus.
4. Lesen Sie die Einführung im Regelassistenten und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Ereignisse** und anschließend auf **Weiter**.
6. Wählen Sie im Listenfeld **Testgruppe** die Option **X-Force Tests** (X-Force-Tests) aus.
7. Klicken Sie auf das Pluszeichen (+) neben dem Test **when this URL property is categorized by X-Force as one of the following categories** (wenn diese URL-Eigenschaft von X-Force einer der folgenden Kategorien zugeordnet wurde).
8. Geben Sie in das Feld **hier Regelnamen eingeben** im Fensterbereich 'Regel' einen eindeutigen Namen ein, den Sie dieser Regel zuweisen möchten.
9. Wählen Sie im Listenfeld **Lokal** oder **Global** aus.
10. Klicken Sie auf die unterstrichenen konfigurierbaren Parameter, um die Testvariablen anzupassen.
    a. Klicken Sie auf **URL (custom)** (URL (angepasst)).
    b. Wählen Sie die URL-Eigenschaft aus, die die aus den Nutzdaten abgerufene URL enthält, und klicken Sie auf **Übergeben**.
    c. Klicken Sie auf **one of the following categories** (eine der folgenden Kategorien).
    d. Wählen Sie unter den URL-Kategorien von X-Force die Kategorie **Gambling / Lottery** (Glücksspiel/Lotterie) aus und klicken Sie auf **Hinzufügen +** und anschließend auf **Übergeben**.
11. So können Sie die konfigurierte Regel als Baustein zur Verwendung mit anderen Regeln exportieren:
    a. Klicken Sie auf **Als Baustein exportieren**.
    b. Geben Sie einen eindeutigen Namen für den Baustein ein.
    c. Klicken Sie auf **Speichern**.
12. Wählen Sie im Fensterbereich 'Gruppen' die Kontrollkästchen der Gruppen aus, denen Sie diese Regel zuweisen möchten.
13. Geben Sie im Feld **Hinweise** den Hinweis ein, der dieser Regel hinzugefügt werden soll, und klicken Sie auf **Weiter**.

14. Klicken Sie auf der Seite **Regelantworten** auf **E-Mail** und geben Sie die E-Mail-Adressen ein, die diese Benachrichtigung erhalten sollen. Informationen zu weiteren Antwortparametern für eine Ereignisregel finden Sie unter Parameter der Seite mit Antworten von Ereignis- und Datenflussregeln sowie allgemeinen Regeln.
15. Klicken Sie auf **Weiter**.
16. Wenn die Regel korrekt ist, klicken Sie auf **Fertigstellen**.

Kapitel 10. Assetprofile

Assetprofile enthalten Informationen zu den bekannten Assets im Netz, darunter auch Angaben zu den Services, die auf den einzelnen Assets ausgeführt werden.

Assetprofilinformationen werden zu Korrelationszwecken verwendet, um die Anzahl falscher Alarme zu reduzieren. Wenn eine Quelle versucht, einen bestimmten auf einem Asset ausgeführten Service zu nutzen, stellt QRadar zum Beispiel fest, ob das Asset für diese Attacke anfällig ist. Hierfür wird die Attacke mit dem Assetprofil korreliert.

Wenn Scans zur Schwachstellenanalyse (VA) konfiguriert sind, werden Assetprofile automatisch erkannt.

Schwachstellen

Schwachstellen können mithilfe von QRadar Vulnerability Manager und Scannern anderer Anbieter ermittelt werden.

Mithilfe von Scannern anderer Anbieter können Schwachstellen ermittelt und gemeldet werden. Dabei werden externe Referenzen wie OSVDB (Open Source Vulnerability Database), NVDB (National Vulnerability Database) und Critical Watch verwendet. Zu den Scannern anderer Anbieter gehören beispielsweise QualysGuard und nCircle ip360. OSVDB ordnet jeder Schwachstelle eine eindeutige Referenz-ID (OSVDB ID) zu. Bei Verwendung externer Referenzen wird jeder Schwachstelle eine eindeutige Referenz-ID zugeordnet. Zu den Referenz-IDs für externe Daten gehören beispielsweise die CVE-ID (CVE = Common Vulnerability and Exposures) oder die Bugtraq-ID. Weitere Informationen zu Scannern sowie zur Schwachstellenanalyse finden Sie im *IBM Security QRadar Vulnerability Manager - Benutzerhandbuch*.

QRadar Vulnerability Manager ist eine separat erhältliche Komponente, die über einen Lizenzschlüssel aktiviert werden kann. QRadar Vulnerability Manager ist eine Plattform für Netzscans, die auf die in den Anwendungen, Systemen oder Geräten im Netz vorhandenen Schwachstellen aufmerksam macht. Nach Ermittlung der Schwachstellen können Sie Daten zu den Schwachstellen durchsuchen und prüfen, Schwachstellen korrigieren und zur Bewertung des neuen Risikoniveaus Scanvorgänge erneut ausführen.

Wenn QRadar Vulnerability Manager aktiviert ist, können Sie auf der Registerkarte **Schwachstellen** Tasks zur Schwachstellenanalyse durchführen. Über die Registerkarte **Assets** können Sie Scanvorgänge auf ausgewählten Assets durchführen.

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

Übersicht über die Registerkarte 'Assets'

Auf der Registerkarte **Assets** finden Sie einen Arbeitsbereich, von dem aus Sie Ihre Netzassets verwalten und Schwachstellen, Ports, Anwendungen, das Verlaufsprotokoll und sonstige Zuordnungen zu einem Asset überprüfen können.

Über die Registerkarte **Assets** können Sie folgende Aktionen ausführen:

- Alle erkannten Assets anzeigen
- Manuell Assetprofile hinzufügen
- Nach bestimmten Assets suchen
- Informationen zu erkannten Assets anzeigen
- Assetprofile für manuell hinzugefügte oder erkannte Assets bearbeiten
- Falsch positive Schwachstellen optimieren
- Assets importieren
- Assetprofile drucken oder exportieren
- Assets erkennen
- Schwachstellensuche von Drittanbietern konfigurieren und verwalten
- QRadar Vulnerability Manager-Scans starten

Weitere Informationen zur Option 'VA-Scan' im Fensterbereich 'Navigation' finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Liste der Registerkarte 'Asset'

Auf der Seite **Assetprofile** finden Sie Informationen zur ID, IP-Adresse, zum Assetnamen, zur zusammengefassten CVSS-Bewertung, zu Schwachstellen und Services.

Auf der Seite **Assetprofile** finden Sie folgende Informationen zu jedem Asset:

Tabelle 33. Parameter der Seite 'Assetprofile'

Parameter	Beschreibung
ID	Hier wird die ID-Nummer des Assets angezeigt. Die Asset-ID-Nummer wird automatisch erstellt, wenn Sie ein Assetprofil manuell hinzufügen oder wenn Assets bei Ereignis- oder Schwachstellensuchläufen erkannt werden.
IP-Adresse	Hier wird die letzte bekannte IP-Adresse des Assets angezeigt.
Assetname	Hier wird der angegebene Name, der NetBios-Name, der DSN-Name oder die MAC-Adresse des Assets angezeigt. Sind diese Angaben nicht bekannt, wird hier die letzte bekannte IP-Adresse angezeigt. **Anmerkung:** Die Werte werden in der Reihenfolge ihrer Priorität angezeigt. Gibt es zu einem Asset beispielsweise keinen angegebenen Namen wird der zusammengefasste NetBIOS-Name angezeigt. Bei einer automatischen Erkennung des Assets wird dieses Feld automatisch belegt, Sie können den Assetnamen jedoch bei Bedarf bearbeiten.

Tabelle 33. Parameter der Seite 'Assetprofile' (Forts.)

Parameter	Beschreibung
Risikobewertung	Hier wird eine der folgenden CVSS-Bewertungen (CVSS = Common Vulnerability Scoring System) angezeigt: • Verbundene zusammengefasste CVSS-Bewertung der Umgebung • Zusammengefasste zeitliche CVSS-Bewertung • Zusammengefasste CVSS-Basisbewertung • Diese Bewertungen werden in der Reihenfolge ihrer Priorität angezeigt. Ist beispielsweise die verbundene zusammengefasste CVSS-Bewertung der Umgebung nicht verfügbar, wird die zusammengefasste zeitliche CVSS-Bewertung angezeigt. Bei der CVSS-Bewertung handelt es sich um eine Messgröße zur Bewertung des Schweregrads einer Schwachstelle. Mithilfe der CVSS-Bewertungen können Sie beurteilen, wie gravierend eine Schwachstelle im Vergleich zu anderen Schwachstellen anzusehen ist. Die CVSS-Bewertung wird unter Verwendung der folgenden benutzerdefinierten Parameter berechnet: • Nebenschadenpotenzial • Vertraulichkeitsanforderungen • Verfügbarkeitsanforderungen • Integritätsanforderungen Weitere Informationen zur Konfiguration dieser Parameter finden Sie im Abschnitt „Assetprofil hinzufügen oder bearbeiten" auf Seite 120. Weitere Informationen zu CVSS finden Sie unter http://www.first.org/cvss/.
Schwachstellen	Hier wird angezeigt, wie viele eindeutige Schwachstellen auf dem Asset erkannt wurden. Zu diesem Wert werden auch die aktiven und passiven Schwachstellen gezählt.
Services	Hier wird angezeigt, wie viele eindeutige Schicht 7-Anwendungen auf diesem Asset ausgeführt werden.
Letzter Benutzer	Hier wird der letzte diesem Asset zugeordnete Benutzer angezeigt.
Benutzer zuletzt gesehen	Hier wird angezeigt, wann der letzte dem Asset zugeordnete Benutzer zuletzt gesehen wurde.

Symbolleiste der Registerkarte 'Assets'

Über die Symbolleiste der Seite **Assetprofile** können Sie Assets suchen, speichern, hinzufügen, löschen, bearbeiten und weitere Aktionen ausführen.

Über die Symbolleiste der Seite **Assetprofile** sind folgende Funktionen verfügbar:

Tabelle 34. Symbolleistenfunktionen der Seite 'Assetprofile'

Funktion	Beschreibung
Suchen	Klicken Sie auf **Suchen**, wenn Sie erweiterte Suchläufe auf Assets durchführen möchten. Mögliche Optionen: • **Neue Suche**- Wählen Sie diese Option aus, wenn Sie eine neue Assetsuche erstellen möchten. • **Suche bearbeiten** - Wählen Sie diese Option aus, um eine Assetsuche zu bearbeiten. Weitere Informationen zur Suchfunktion finden Sie im Abschnitt Assetprofile durchsuchen .
Schnellsuchvorgänge	Über dieses Listenfeld können Sie zuvor gespeicherte Suchläufe ausführen. Im Listenfeld **Schnellsuchvorgänge** werden nur Optionen angezeigt, wenn Sie Suchkriterien gespeichert haben, in denen die Option **In meine Schnellsuche aufnehmen** angegeben ist.
Kriterien speichern	Klicken Sie auf **Kriterien speichern**, um die aktuellen Suchkriterien zu speichern.
Filter hinzufügen	Klicken Sie auf **Filter hinzufügen**, um den aktuellen Suchergebnissen einen Filter hinzuzufügen.
Asset hinzufügen	Klicken Sie auf **Asset hinzufügen**, um ein Assetprofil hinzuzufügen. Beachten Sie die Informationen im Abschnitt Assetprofil hinzufügen oder bearbeiten.
Asset bearbeiten	Klicken Sie auf **Asset bearbeiten**, um ein Assetprofil zu bearbeiten. Diese Option ist nur aktiviert, wenn Sie ein Assetprofil aus der Ergebnisliste ausgewählt haben. Weitere Informationen hierzu finden Sie im Abschnitt „Assetprofil hinzufügen oder bearbeiten” auf Seite 120.

Tabelle 34. Symbolleistenfunktionen der Seite 'Assetprofile' (Forts.)

Funktion	Beschreibung
Aktionen	Klicken Sie auf **Aktionen**, um die folgenden Aktionen auszuführen: • **Asset löschen** - Wählen Sie diese Option aus, um die ausgewählten Assetprofile zu löschen. Weitere Informationen hierzu finden Sie im Abschnitt Assets löschen. • **Aufgelistete löschen** - Wählen Sie diese Option aus, um alle in der Ergebnisliste aufgeführten Assetprofile zu löschen. Weitere Informationen hierzu finden Sie im Abschnitt Assets löschen. • **Assets importieren** - Wählen Sie diese Option zum Importieren von Assets aus. Weitere Informationen hierzu finden Sie im Abschnitt Assetprofile importieren. • **In XML exportieren** - Wählen Sie diese Option aus, um Assetprofile in XML-Format zu exportieren. Weitere Informationen hierzu finden Sie im Abschnitt Assets exportieren. • **In CSV-Datei exportieren** - Wählen Sie diese Option aus, um Assetprofile in CSV-Format zu exportieren. Weitere Informationen hierzu finden Sie im Abschnitt Assets exportieren. • **Drucken** - Wählen Sie diese Option aus, um die Assetprofile zu drucken, die auf der Seite angezeigt werden. • Das Menü **Aktionen** ist nur für Benutzer mit Administratorberechtigung verfügbar.
Filter löschen	Nach Anwendung eines Filters mit der Option **Filter hinzufügen** können Sie den Filter mit der Option **Filter löschen** entfernen.

Kontextmenüoptionen

Wenn Sie in der Registerkarte 'Asset' mit der rechten Maustaste auf ein Asset klicken, werden Menüs für weitere Ereignisfilterinformationen angezeigt.

Auf der Registerkarte **Assets** können Sie durch Klicken mit der rechten Maustaste auf ein Asset auf weitere Ereignisfilterinformationen zugreifen.

Tabelle 35. Kontextmenüoptionen

Option	Beschreibung
Information	Im Menü **Information** finden Sie folgende Optionen: • **DNS-Suche** - Suche nach DNS-Einträgen auf der Basis der IP-Adresse. • **WHOIS-Suche** - Suche nach dem registrierten Eigner einer fernen IP-Adresse. Der WHOIS-Standardserver ist whois.arin.net. • **Portsuche** - Es wird eine NMAP-Suche (NMAP = Network Mapper - Netzzuordnungsfunktion) der ausgewählten IP-Adresse durchgeführt. Diese Option ist nur verfügbar, wenn NMAP in Ihrem System installiert ist. Weitere Informationen zur NMAP-Installation finden Sie in der Dokumentation des betreffenden Anbieters. • **Assetprofil** - Anzeige von Assetprofilinformationen. Diese Menüoption ist nur verfügbar, wenn Profildaten aktiv von einem Suchlauf übernommen werden. • **Ereignisse suchen** - Wählen Sie die Option **Ereignisse suchen** aus, um nach Ereignissen im Zusammenhang mit dieser IP-Adresse zu suchen.
QVM-Überprüfung ausführen	Wählen Sie der dieser Option aus, um einen Vulnerability Manager-Scan auf dem ausgewählten Asset auszuführen. Diese Option wird erst nach Installation von QRadar Vulnerability Manager angezeigt.

Assetprofil anzeigen

Aus der Assetliste auf der Registerkarte **Assets** können Assetprofile ausgewählt und angezeigt werden. Ein Assetprofil stellt Informationen zu den einzelnen Profilen bereit.

Informationen zu diesem Vorgang

Assetprofilinformationen werden mithilfe der Servererkennung automatisch erkannt bzw. manuell konfiguriert. Sie können automatisch generierte Assetprofilinformationen bearbeiten.

Die Seite **Assetprofil** stellt die Informationen zu dem Asset in mehreren Teilfenstern bereit. Wenn Sie ein Teilfenster anzeigen möchten, können Sie entweder den Pfeil **(>)** auf dem Teilfenster anklicken, um weitere Details anzuzeigen, oder das Teilfenster im Listenfeld **Anzeigen** in der Symbolleiste auswählen.

Über die Symbolleiste der Seite **Assetprofil** sind die folgenden Funktionen verfügbar:

Tabelle 36. Symbolleistenfunktionen der Seite 'Assetprofil'

Optionen	Beschreibung
Zur Assetliste zurückkehren	Klicken Sie auf diese Option, um zur Assetliste zurückzukehren.
Anzeigen	Im Listenfeld können Sie das Teilfenster auswählen, das im Teilfenster 'Assetprofil' angezeigt werden soll. Die Teilfenster 'Assetzusammenfassung' und 'Netzschnittstellenzusammenfassung' werden immer angezeigt. Weitere Informationen zu den in den einzelnen Teilfenstern angezeigten Parametern finden Sie im Abschnitt Assets profile page parameters (Parameter der Assetprofilseite).
Asset bearbeiten	Klicken Sie auf diese Option, um das Assetprofil zu bearbeiten. Weitere Informationen hierzu finden Sie unter „Assetprofil hinzufügen oder bearbeiten” auf Seite 120.
Zielzusammenfassung anzeigen	Wenn dieses Asset das Ziel eines Angriffs ist, ermöglicht Ihnen diese Option die Anzeige der Zielübersichtsdaten.
Protokoll	Klicken Sie auf die Option **Protokoll**, um Ereignisprotokollinformationen für dieses Asset anzuzeigen. Beim Anklicken des Symbols **Protokoll** wird das Fenster **Ereignissuche** mit vorab ausgefüllten Ereignissuchkriterien angezeigt: Die Suchparameter können bei Bedarf angepasst werden. Klicken Sie auf **Suchen**, um die Ereignisprotokollinformationen anzuzeigen.
Anwendungen	Klicken Sie auf die Option **Anwendungen**, um die Anwendungsinformationen für dieses Asset anzuzeigen. Beim Anklicken des Symbols **Anwendungen** wird das Fenster **Datenflusssuche** mit vorab ausgefüllten Ereignissuchkriterien angezeigt. Die Suchparameter können bei Bedarf angepasst werden. Klicken Sie auf **Suchen**, um die Anwendungsinformationen anzuzeigen.
Verbindungen durchsuchen	Klicken Sie auf **Verbindungen durchsuchen**, um nach Verbindungen zu suchen. Das Fenster **Verbindung suchen** wird angezeigt. Diese Option wird nur angezeigt, wenn IBM Security QRadar Risk Manager gekauft und lizenziert wurde. Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.
Topologie anzeigen	Diese Option wird nur angezeigt, wenn IBM Security QRadar Risk Manager gekauft und lizenziert wurde. Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Tabelle 36. Symbolleistenfunktionen der Seite 'Assetprofil' (Forts.)

Optionen	Beschreibung
Aktionen	Wählen Sie in der Liste **Aktionen** die Option **Protokoll der Schwachstellen** aus. Diese Option wird nur angezeigt, wenn IBM Security QRadar Risk Manager gekauft und lizenziert wurde. Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager-Benutzerhandbuch*.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**
3. Doppelklicken Sie auf das Asset, das Sie anzeigen möchten.
4. Verwenden Sie die Optionen auf der Symbolleiste, um die verschiedenen Teilfenster der Assetprofilinformationen anzuzeigen. Weitere Informationen hierzu finden Sie unter Assetprofil bearbeiten.
5. Klicken Sie, um die zugehörigen Schwachstellen zu untersuchen, im Teilfenster 'Schwachstellen' auf die einzelnen Schwachstellen. Weitere Informationen hierzu finden Sie in Tabelle 10-10
6. Bearbeiten Sie das Assetprofil, falls erforderlich. Weitere Informationen hierzu finden Sie unter Assetprofil bearbeiten.
7. Klicken Sie auf **Return to Assets List** (Zur Assetliste zurückkehren), um ggf. ein anderes Asset auszuwählen und anzuzeigen.

Assetprofil hinzufügen oder bearbeiten

Assetprofile werden automatisch erkannt und hinzugefügt; allerdings kann es erforderlich sein, ein Profil manuell hinzuzufügen

Informationen zu diesem Vorgang

Wenn Assets mithilfe der Servererkennungsoption erkannt werden, werden einige Assetprofildetails automatisch ausgefüllt. Sie können manuell Informationen zum Assetprofil hinzufügen und bestimmte Parameter bearbeiten.

Es können nur die Parameter bearbeitet werden, die manuell eingegeben wurden. Parameter, die vom System generiert wurden, werden in Kursivschrift angezeigt und können nicht bearbeitet werden. Sie können vom System generierte Parameter löschen, falls dies erforderlich ist.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie eine der folgenden Optionen aus:
   - Klicken Sie zum Hinzufügen eines Assets auf **Asset hinzufügen** und geben Sie die IP-Adresse oder den CIDR-Bereich des Assets im Feld **Neue IP-Adresse** ein.
   - Doppelklicken Sie zum Bearbeiten eines Assets auf das Asset, das Sie anzeigen möchten, und klicken Sie dann auf **Asset bearbeiten**.

4. Konfigurieren Sie die Parameter im Teilfenster 'MAC- & IP-Adresse'. Konfigurieren Sie eine oder mehrere der folgenden Optionen:
   - Klicken Sie auf das Symbol **Neue MAC-Adresse** und geben Sie eine MAC-Adresse im Dialogfenster ein.
   - Klicken Sie auf das Symbol **Neue IP-Adresse** und geben Sie eine IP-Adresse im Dialogfenster ein.
   - Wenn **Unbekanntes NIC** aufgeführt wird, können Sie dieses Element auswählen, das Symbol **Bearbeiten** anklicken und eine neue MAC-Adresse im Dialogfenster eingeben.
   - Wählen Sie eine MAC- oder IP-Adresse aus der Liste aus, klicken Sie auf das Symbol **Bearbeiten** und geben Sie eine neue MAC-Adresse im Dialogfenster ein.
   - Wählen Sie eine MAC- oder IP-Adresse aus der Liste aus und klicken Sie auf das Symbol **Entfernen**.
5. Konfigurieren Sie die Parameter im Teilfenster 'Namen & Beschreibungen'. Konfigurieren Sie eine oder mehrere der folgenden Optionen:

Parameter	Beschreibung
DNS	Wählen Sie eine der folgenden Optionen aus: • Geben Sie einen DNS-Namen ein und klicken Sie auf **Hinzufügen**. • Wählen Sie einen DNS-Namen aus der Liste aus und klicken Sie auf **Bearbeiten**. • Wählen Sie einen DNS-Namen aus der Liste aus und klicken Sie auf **Entfernen**.
NetBIOS	Wählen Sie eine der folgenden Optionen aus: • Geben Sie einen NetBIOS-Namen ein und klicken Sie auf **Hinzufügen**. • Wählen Sie einen NetBIOS-Namen aus der Liste aus und klicken Sie auf **Bearbeiten**. • Wählen Sie einen NetBIOS-Namen aus der Liste aus und klicken Sie auf **Entfernen**.
Angegebener Name	Geben Sie einen Namen für dieses Assetprofil ein.
Position	Geben Sie eine Position für dieses Assetprofil ein.
Beschreibung	Geben Sie eine Beschreibung für dieses Assetprofil ein.
Wireless AP	Geben Sie den drahtlosen Netzzugang (AP) für dieses Assetprofil ein.
Wireless SSID	Geben Sie die drahtlose Service-Set-ID (SSID) für dieses Assetprofil ein.
Switch-ID	Geben Sie die Switch-ID für dieses Assetprofil ein.
Switch-Port-ID	Geben Sie die Switch-Port-ID für dieses Assetprofil ein.

6. Konfigurieren Sie die Parameter im Teilfenster 'Betriebssystem':
   a. Wählen Sie im Listenfeld **Anbieter** einen Betriebssystemanbieter aus.
   b. Wählen Sie im Listenfeld **Produkt** das Betriebssystem für das Assetprofil aus.
   c. Wählen Sie im Listenfeld **Version** die Version des ausgewählten Betriebssystems aus.
   d. Klicken Sie auf das Symbol **Hinzufügen**.
   e. Wählen Sie im Listenfeld **Überschreiben** eine der folgenden Optionen aus:
      - **Bis zum nächsten Scan** - Wählen Sie diese Option aus, um anzugeben, dass der Scanner Betriebssysteminformationen bereitstellt und die Informationen vorübergehend bearbeitet werden können. Wenn Sie die Betriebssystemparameter bearbeiten, stellt der Scanner die Informationen beim nächsten Scan wieder her.
      - **Dauerhaft** - Wählen Sie diese Option aus, um anzugeben, dass Sie Betriebssysteminformationen manuell eingeben und die Aktualisierung der Informationen durch den Scanner inaktivieren möchten.
   f. Wählen Sie ein Betriebssystem aus der Liste aus.
   g. Wählen Sie ein Betriebssystem aus und klicken Sie auf das Symbol **Überschreibung umschalten**.
7. Konfigurieren Sie die Parameter im Teilfenster 'CVSS & Gewichtung'. Konfigurieren Sie eine oder mehrere der folgenden Optionen:

Parameter	Beschreibung
Nebenschadenpotenzial	Konfigurieren Sie diesen Parameter, um das Potenzial für den Verlust von Menschenleben oder Vermögensgegenständen durch Beschädigung oder Diebstahl dieses Assets anzuzeigen. Sie können diesen Parameter auch dazu verwenden, das Potenzial für wirtschaftlichen Schaden durch Produktivitäts- oder Umsatzverluste anzuzeigen. Ein erhöhtes Nebenschadenpotenzial hat eine Zunahme des errechneten Werts des Parameters 'CVSS-Bewertung' zur Folge. Wählen Sie im Listenfeld **Nebenschadenpotenzial** eine der folgenden Optionen aus: • Keine • Niedrig • Niedrig-Mittel • Mittel-Hoch • Hoch • Nicht definiert Wenn Sie den Parameter **Nebenschadenpotenzial** konfigurieren, wird der Parameter **Gewichtung** automatisch aktualisiert.

Parameter	Beschreibung
Vertraulichkeitsanforderungen	Konfigurieren Sie diesen Parameter, um die Auswirkung anzuzeigen, die eine erfolgreich genutzte Sicherheitslücke auf diesem Asset auf die Vertraulichkeit besitzt. Eine größere Auswirkung auf die Vertraulichkeit hat eine Zunahme des errechneten Werts des Parameters 'CVSS-Bewertung' zur Folge. Wählen Sie im Listenfeld **Vertraulichkeitsanforderungen** eine der folgenden Optionen aus: • Niedrig • Mittel • Hoch • Nicht definiert
Verfügbarkeitsanforderungen	Konfigurieren Sie diesen Parameter, um die Auswirkung anzuzeigen, die eine erfolgreich genutzte Sicherheitslücke auf die Verfügbarkeit des Assets besitzt. Angriffe, die Netzbandbreite, Prozessorzyklen oder Plattenspeicherplatz verbrauchen, wirken sich auf die Verfügbarkeit eines Assets aus. Eine größere Auswirkung auf die Verfügbarkeit hat eine Zunahme des errechneten Werts des Parameters 'CVSS-Bewertung' zur Folge. Wählen Sie im Listenfeld **Verfügbarkeitsanforderungen** eine der folgenden Optionen aus: • Niedrig • Mittel • Hoch • Nicht definiert
Integritätsanforderungen	Konfigurieren Sie diesen Parameter, um die Auswirkung anzuzeigen, die eine erfolgreich genutzte Sicherheitslücke auf die Integrität des Assets besitzt. Integrität bezeichnet die Vertrauenswürdigkeit und garantierte Richtigkeit von Informationen. Eine größere Auswirkung auf die Integrität hat eine Zunahme des errechneten Werts des Parameters 'CVSS-Bewertung' zur Folge. Wählen Sie im Listenfeld **Integritätsanforderungen** eine der folgenden Optionen aus: • Niedrig • Mittel • Hoch • Nicht definiert

Parameter	Beschreibung
Gewichtung	Wählen Sie im Listenfeld **Gewichtung** eine Gewichtung für dieses Assetprofil aus. Es steht ein Bereich von 0 bis 10 zur Verfügung. Wenn Sie den Parameter **Gewichtung** konfigurieren, wird der Parameter **Nebenschadenpotenzial** automatisch aktualisiert.

8. Konfigurieren Sie die Parameter im Teilfenster 'Eigner'. Wählen Sie eine oder mehrere der folgenden Optionen aus:

Parameter	Beschreibung
Geschäftseigentümer	Geben Sie den Namen des Geschäftseigentümers des Assets ein. Ein Geschäftseigentümer ist beispielsweise ein Abteilungsleiter. Die maximale Länge beträgt 255 Zeichen.
Kontakt zum Geschäftseigentümer	Geben Sie die Kontaktinformationen des Geschäftseigentümers ein. Die maximale Länge beträgt 255 Zeichen.
Fachansprechpartner	Geben Sie den Fachansprechpartner für das Asset ein. Ein Fachansprechpartner ist beispielsweise der IT-Manager oder Direktor. Die maximale Länge beträgt 255 Zeichen.
Kontakt zum Fachansprechpartner	Geben Sie die Kontaktinformationen des Fachansprechpartners ein. Die maximale Länge beträgt 255 Zeichen.
Technischer Benutzer	Wählen Sie im Listenfeld den Benutzernamen aus, der diesem Assetprofil zugeordnet werden soll. Sie können diesen Parameter auch dazu verwenden, eine automatische Korrektur von Sicherheitslücken für IBM Security QRadar Vulnerability Manager zu aktivieren. Weitere Informationen zur automatischen Korrektur finden Sie im Benutzerhandbuch von *IBM Security QRadar Vulnerability Manager*.

9. Klicken Sie auf **Speichern**.

Assetprofile durchsuchen

Sie können Suchparameter konfigurieren, um im Teilfenster **Asset** auf der Registerkarte **Assets** nur die Assetprofile anzuzeigen, die Sie überprüfen möchten.

Informationen zu diesem Vorgang

Beim Zugriff auf die Registerkarte **Assets** wird das Teilfenster **Asset** mit allen erkannten Assets in Ihrem Netz angezeigt. Zur Eingrenzung dieser Liste können Sie Suchparameter konfigurieren, um nur die Assetprofile anzuzeigen, die Sie überprüfen möchten.

Über das Teilfenster **Assetsuche** können Assetsuchgruppen verwaltet werden. Weitere Informationen zu Assetsuchgruppen finden Sie im Abschnitt Assetsuchgruppen.

Mithilfe der Suchfunktion können Sie Hostprofile, Assets und Identitätsinformationen durchsuchen. Identitätsinformationen stellen weitere Details zu Protokollquellen auf Ihrem Netz einschließlich DNS-Informationen, Benutzeranmeldungen und MAC-Adressen bereit.

Die Assetsuchfunktion ermöglicht die Assetsuche nach externen Datenreferenzen, um zu ermitteln, ob bekannte Schwachstellen in Ihrer Implementierung existieren.

Beispiel:

Sie erhalten eine Benachrichtigung, dass CVE ID: CVE-2010-000 aktiv im Feld verwendet wird. Um zu prüfen, ob ein Host in Ihrer Implementierung durch dieses Exploit gefährdet ist, können Sie in der Liste der Suchparameter die Option **Schwachstelle externe Referenz** und anschließend **CVE** auswählen und dann

```
2010-000
```

eingeben, um eine Liste aller Hosts anzuzeigen, die durch diese spezielle CVE-ID gefährdet sind.

Anmerkung: Weitere Informationen zur OSVDB finden Sie unter *http://osvdb.org/* . Weitere Informationen zur NVDB finden Sie unter *http://nvd.nist.gov/* .

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Klicken Sie in der Symbolleiste auf **Suchen** > **Neue Suche**.
4. Wählen Sie eine der folgenden Optionen aus:
   - Um eine zuvor gespeicherte Suche zu laden, gehen Sie zu Schritt 5.
   - Um eine neue Suche zu erstellen, gehen Sie zu Schritt 6.
5. Wählen Sie eine zuvor gespeicherte Suche aus:
   a. Wählen Sie eine der folgenden Optionen aus:
      - Optional. Wählen Sie im Listenfeld **Gruppe** die Assetsuchgruppe, die in der Liste **Verfügbare gespeicherte Suchvorgänge** angezeigt werden soll.
      - Wählen Sie in der Liste **Verfügbare gespeicherte Suchvorgänge** die gespeicherte Suche aus, die Sie laden möchten.
      - Geben Sie im Feld **Geben Sie den gespeicherten Suchvorgang ein oder treffen Sie eine Auswahl in der Liste** den Namen der Suche ein, die geladen werden soll.

   b. Klicken Sie auf **Laden**.
6. Definieren Sie im Teilfenster 'Suchparameter' Ihre Suchkriterien:
   a. Wählen Sie im ersten Listenfeld den Assetparameter aus, nach dem gesucht werden soll. Beispielsweise **Hostname**, **Schwachstelle Risikoklassifizierung** oder **Fachansprechpartner**.
   b. Wählen Sie im zweiten Listenfeld den Änderungswert, der für die Suche verwendet werden soll.
   c. Geben Sie im Eingabefeld spezielle Informationen in Verbindung mit Ihrem Suchparameter ein.
   d. Klicken Sie auf **Filter hinzufügen**.

e. Wiederholen Sie diese Schritte für jeden Filter, den Sie zu den Suchkriterien hinzufügen möchten.

7. Klicken Sie auf **Suchen**.

Ergebnisse

Sie können Ihre Assetsuchkriterien speichern. Weitere Informationen hierzu finden Sie unter Assetsuchkriterien speichern.

Assetsuchkriterien speichern

Auf der Registerkarte **Asset** können Sie konfigurierte Suchkriterien zur späteren Wiederverwendung speichern. Gespeicherte Suchkriterien verfallen nicht.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Führen Sie einen Suchvorgang aus. Details finden Sie im Abschnitt Assetprofile durchsuchen.
4. Klicken Sie auf **Kriterien speichern**.
5. Geben Sie Werte für die folgenden Parameter ein:

Parameter	Beschreibung
Geben Sie den Namen dieser Suche ein	Geben Sie den eindeutigen Namen ein, den Sie diesen Suchkriterien zuweisen möchten.
Gruppen verwalten	Klicken Sie auf **Gruppen verwalten**, um Suchgruppen zu verwalten. Weitere Informationen finden Sie im Abschnitt Asset search groups (Assetsuchgruppen). Diese Option wird nur angezeigt, wenn Sie über Administratorberechtigungen verfügen.
Suche zu Gruppe(n) zuordnen	Aktivieren Sie das Kontrollkästchen für die Gruppe, der Sie diese gespeicherte Suche zuweisen möchten. Wenn Sie keine Gruppe auswählen, wird diese gespeicherte Suche standardmäßig der Gruppe **Sonstige** zugeordnet. Weitere Informationen finden Sie im Abschnitt Asset search groups (Assetsuchgruppen).
In meine Schnellsuche aufnehmen	Aktivieren Sie dieses Kontrollkästchen, um diese Suche in Ihr Listenfeld **Schnellsuche** aufzunehmen, das sich in der Symbolleiste der Registerkarte **Assets** befindet.
Als Standardwert definieren	Aktivieren Sie dieses Kontrollkästchen, um diese Suche beim Zugriff auf die Registerkarte **Assets** als Ihre Standardsuche festzulegen.
Freigeben für jeden	Aktivieren Sie dieses Kontrollkästchen, um diese Suchanforderungen für alle Benutzer freizugeben.

Assetsuchgruppen

Über das Fenster **Assetsuchgruppen** können Sie Assetsuchgruppen erstellen und verwalten.

Mithilfe dieser Gruppen können Sie gespeicherte Suchkriterien ganz einfach auf der Registerkarte **Assets** lokalisieren.

Suchgruppen anzeigen

Verwenden Sie das Fenster **Assetsuchgruppen**, um eine Liste von Gruppen und Untergruppen anzuzeigen.

Informationen zu diesem Vorgang

Im Fenster **Assetsuchgruppen** können Sie Details zu jeder Gruppe anzeigen, einschließlich einer Beschreibung und des Datums der letzten Änderung.

Alle gespeicherten Suchen, die keiner Gruppe zugeordnet sind, befinden sich in der Gruppe **Sonstige**.

Im Fenster **Assetsuchgruppen** werden für jede Gruppe die folgenden Parameter angezeigt:

Tabelle 37. Die Symbolleistenfunktionen des Fensters 'Assetsuchgruppen'

Funktion	Beschreibung
Neue Gruppe	Klicken Sie zum Erstellen einer neuen Suchgruppe auf **Neue Gruppe**. Weitere Informationen hierzu finden Sie unter Neue Suchgruppe erstellen.
Bearbeiten	Klicken Sie zum Bearbeiten einer bestehenden Suchgruppe auf **Bearbeiten**. Weitere Informationen hierzu finden Sie unter Suchgruppe bearbeiten.
Kopieren	Klicken Sie zum Kopieren einer gespeicherten Suche in eine andere Suchgruppe auf **Kopieren**. Weitere Informationen hierzu finden Sie unter Gespeicherte Suche in eine andere Gruppe kopieren.
Entfernen	Wählen Sie zum Entfernen einer Suchgruppe oder einer gespeicherten Suche aus einer Suchgruppe das Element aus, das entfernt werden soll, und klicken Sie dann auf **Entfernen**. Weitere Informationen hierzu finden Sie unter Gruppe oder gespeicherte Suche aus einer Gruppe entfernen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie **Suchen** > **Neue Suche** aus.
4. Klicken Sie auf **Gruppen verwalten**.
5. Zeigen Sie die Suchgruppen an.

Neue Suchgruppe erstellen

Im Fenster **Assetsuchgruppen** kann eine neue Suchgruppe erstellt werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie **Suchen** > **Neue Suche** aus.
4. Klicken Sie auf **Gruppen verwalten**.
5. Wählen Sie den Ordner der Gruppe aus, unter der Sie die neue Gruppe erstellen wollen.
6. Klicken Sie auf **Neue Gruppe**.
7. Geben Sie im Feld **Name** einen eindeutigen Namen für die neue Gruppe ein.
8. Optional. Geben Sie im Feld **Beschreibung** eine Beschreibung ein.
9. Klicken Sie auf **OK**.

Suchgruppe bearbeiten

Die Felder **Name** und **Beschreibung** einer Suchgruppe können bearbeitet werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie **Suchen** > **Neue Suche** aus.
4. Klicken Sie auf **Gruppen verwalten**.
5. Wählen Sie die Gruppe aus, die bearbeitet werden soll.
6. Klicken Sie auf **Bearbeiten**.
7. Geben Sie im Feld **Name** einen neuen Namen ein.
8. Geben Sie im Feld **Beschreibung** eine neue Beschreibung ein.
9. Klicken Sie auf **OK**.

Gespeicherte Suche in eine andere Gruppe kopieren

Eine gespeicherte Suche kann in eine andere Gruppe kopiert werden. Auch das Kopieren der gespeicherten Suche in mehr als eine Gruppe ist möglich.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie **Suchen** > **Neue Suche** aus.
4. Klicken Sie auf **Gruppen verwalten**.
5. Wählen Sie die gespeicherte Suche aus, die kopiert werden soll.
6. Klicken Sie auf **Kopieren**.
7. Aktivieren Sie im Fenster **Elementgruppen** das Kontrollkästchen der Gruppe, in die die gespeicherte Suche kopiert werden soll.
8. Klicken Sie auf **Gruppen zuordnen**.

Gruppe oder gespeicherte Suche aus einer Gruppe entfernen

Das Symbol **Entfernen** kann dazu verwendet werden, eine Suche aus einer Gruppe zu entfernen bzw. eine Suchgruppe zu entfernen.

Informationen zu diesem Vorgang

Wenn Sie eine gespeicherte Suche aus einer Gruppe entfernen, wird die gespeicherte Suche nicht aus Ihrem System gelöscht. Die gespeicherte Suche wird aus der Gruppe entfernt und automatisch in die Gruppe **Sonstige** verschoben.

Die folgenden Gruppen können nicht aus Ihrem System entfernt werden:

- Assetsuchgruppen
- Sonstige

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie **Suchen** > **Neue Suche** aus.
4. Klicken Sie auf **Gruppen verwalten**.
5. Wählen Sie die gespeicherte Suche aus, die aus der Gruppe entfernt werden soll:
   - Wählen Sie die gespeicherte Suche aus, die aus der Gruppe entfernt werden soll.
   - Wählen Sie die Gruppe aus, die entfernt werden soll.

Tasks zur Assetprofilverwaltung

Über die Registerkarte 'Assets' können Sie Assetprofile löschen, importieren und exportieren.

Informationen zu diesem Vorgang

Über die Registerkarte **Assets** können Sie Assetprofile löschen, importieren und exportieren.

Assets löschen

Sie können bestimmte Assets oder alle aufgelisteten Assetprofile löschen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie das Asset aus, das gelöscht werden soll, und wählen Sie dann im Listenfeld **Aktionen** die Option **Asset löschen** aus.
4. Klicken Sie auf **OK**.

Assetprofile importieren

Sie können Assetprofilinformationen importieren.

Vorbereitende Schritte

Die importierte Datei muss eine CSV-Datei in folgendem Format sein:

```
IP-Adresse,Name,Gewichtung,Beschreibung
```

Dabei gilt:

- **IP** - Gibt eine gültige IP-Adresse in der Schreibweise mit Trennzeichen an. Beispiel: 192.168.5.34.
- **Name** - Gibt den Namen des Assets an (maximal 255 Zeichen). Kommas sind in diesem Feld nicht zulässig und machen den Importprozess ungültig. Beispiel: WebServer01 ist korrekt.
- **Gewichtung** - Gibt eine Zahl von 0 bis 10 an, die die Bedeutung des Assets im Netz beschreibt. Dabei steht 0 für eine geringe und 10 für eine sehr große Bedeutung.
- **Beschreibung** - Gibt eine Beschreibung des Assets an (maximal 255 Zeichen). Dieser Wert ist optional.

Eine CSV-Datei kann beispielsweise folgende Einträge enthalten:

- ```
  192.168.5.34,WebServer01,5,Main Production Web Server
  ```
- ```
  192.168.5.35,MailServ01,0,
  ```

Beim Importprozess werden die importierten Assetprofile mit den Assetprofilinformationen, die Sie derzeit im System gespeichert haben, zusammengeführt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie im Listenfeld **Aktionen** die Option **Assets importieren** aus.
4. Klicken Sie auf **Durchsuchen**, um die CSV-Datei, die importiert werden soll, zu suchen und auszuwählen.
5. Klicken Sie auf **Assets importieren**, um den Importprozess zu starten.

Assets exportieren

Aufgelistete Assetprofile können in eine XML- oder CSV-Datei (XML = Extended Markup Language, CSV = Comma-Separated Value) exportiert werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie im Listenfeld **Aktionen** eine der folgenden Optionen aus:
   - In XML exportieren
   - In CSV-Datei exportieren
4. Zeigen Sie das Statusfenster an, um Informationen zum Status des Exportprozesses zu erhalten.
5. Optional: Wenn Sie während des Exportvorgangs andere Registerkarten und Seiten verwenden möchten, klicken Sie auf den Link **Bei Abschluss benachrichtigen**.

   Nach Abschluss des Exportvorgangs wird das Fenster **File Download** (Dateidownload) angezeigt.
6. Wählen Sie im Fenster **File Download** (Dateidownload) eine der folgenden Optionen:
   - **Öffnen** - Wählen Sie diese Option aus, um die Exportergebnisse im Browser Ihrer Wahl zu öffnen.

- **Speichern** - Wählen Sie diese Option aus, um die Ergebnisse auf Ihrem Desktop zu speichern.

7. Klicken Sie auf **OK**.

Assetschwachstellen untersuchen

Im Teilfenster 'Schwachstellen' auf der Seite **Assetprofil** wird eine Liste der ermittelten Schwachstellen für das Asset angezeigt.

Informationen zu diesem Vorgang

Durch Doppelklicken auf die Schwachstelle werden weitere Schwachstellendetails angezeigt.

Im Fenster **Schwachstellendetails untersuchen** sind die folgenden Details angegeben:

Parameter	Beschreibung
ID der Schwachstelle	Gibt die ID der Schwachstelle an. Die Schwachstellen-ID ist eine durch das Schwachstellen-Informationssystem VIS generierte, eindeutige Kennung.
Veröffentlichungsdatum	Gibt das Datum an, an dem die Schwachstellendetails in der OSVDB veröffentlicht wurden.
Name	Gibt den Namen der Schwachstelle an.
Assets	Gibt die Zahl der Assets in Ihrem Netz an, die über diese Schwachstelle verfügen. Klicken Sie auf den Link, um die Liste der Assets anzuzeigen.
Assets, einschließlich Ausnahmen	Gibt die Zahl der Assets in Ihrem Netz an, die über Schwachstellenausnahmen verfügen. Klicken Sie auf den Link, um die Liste der Assets anzuzeigen.
CVE	Gibt die CVE-ID der Schwachstelle an. CVE-IDs werden durch die NVDB bereitgestellt. Klicken Sie für weitere Informationen auf den Link. Beim Anklicken des Links wird die NVDB-Website in einem neuen Browserfenster angezeigt.
XForce	Gibt die XForce-ID der Schwachstelle an. Klicken Sie für weitere Informationen auf den Link. Beim Anklicken des Links wird die IBM Internet Security Systems-Website in einem neuen Browserfenster angezeigt.
OSVDB	Gibt die OSVDB-ID der Schwachstelle an. Klicken Sie für weitere Informationen auf den Link. Beim Anklicken des Links wird die OSVDB-Website in einem neuen Browserfenster angezeigt.

Parameter	Beschreibung
Plug-in-Details	Gibt die ID von QRadar Vulnerability Manager an. Klicken Sie auf den Link, um OVAL-Definitionen, Windows Knowledge Base-Einträge oder UNIX-Empfehlungen für die Schwachstelle anzuzeigen. Diese Funktion stellt Informationen dazu bereit, wie QRadar Vulnerability Manager bei einem Patch-Scan überprüft, ob Details zu Schwachstellen vorliegen. Mit dieser Funktion können Sie ermitteln, warum eine Schwachstelle in einem Asset aufgetreten bzw. nicht aufgetreten ist.
CVSSB-Bewertungsbasis	Zeigt die CVSS-Gesamtbewertung (CVSS = Common Vulnerability Scoring System) der Schwachstellen dieses Assets an. Eine CVSS-Bewertung ist eine Metrik zur Bewertung des Schweregrads einer Schwachstelle. CVSS-Bewertungen können dazu verwendet werden, zu gewichten, zu wie viel Besorgnis eine Schwachstelle im Vergleich zu anderen Schwachstellen Anlass gibt. Die CVSS-Bewertung wird unter Verwendung der folgenden benutzerdefinierten Parameter berechnet: • Nebenschadenpotenzial • Vertraulichkeitsanforderungen • Verfügbarkeitsanforderungen • Integritätsanforderungen Weitere Informationen zur Konfiguration dieser Parameter finden Sie im Abschnitt „Assetprofil hinzufügen oder bearbeiten" auf Seite 120. Weitere Informationen zu CVSS finden Sie unter *http://www.first.org/cvss/* .
Auswirkung	Zeigt die Art des Schadens an, der zu erwarten ist, wenn diese Schwachstelle ausgenutzt wird.
CVSS-Basismessgröße	Zeigt die Metriken an, die zur Berechnung der CVSS-Basisbewertung verwendet werden, einschließlich: • Zugriffsvektor • Zugriffskomplexität • Authentifizierung • Auswirkungen auf die Vertraulichkeit • Auswirkungen auf die Integrität • Auswirkungen auf die Verfügbarkeit

Parameter	Beschreibung
Beschreibung	Stellt eine Beschreibung der ermittelten Schwachstelle bereit. Dieser Wert ist nur verfügbar, wenn VA-Tools in Ihrem System integriert sind.
Problemstellung	Gibt die Auswirkungen an, die die Schwachstelle auf Ihr Netz haben kann.
Lösung	Befolgen Sie die bereitgestellten Anweisungen, um die Schwachstelle zu beheben.
Virtuelles Patch	Zeigt, falls verfügbar, die Informationen des dieser Schwachstelle zugeordneten, virtuellen Patchs an. Ein virtuelles Patch ist eine kurzfristige Lösung zur Risikominderung für eine kürzlich ermittelte Schwachstelle. Diese Informationen sind von IPS-Ereignissen (IPS = Intrusion Protection System) abgeleitet. Angaben zur Installation des virtuellen Patchs finden Sie in den Informationen Ihres IPS-Anbieters.
Referenz	Zeigt eine Liste externer Referenzen an, einschließlich: • **Referenztyp** - Gibt den Typ der aufgelisteten Referenz an, beispielsweise eine Empfehlungs-URL oder eine E-Mail-Posting-Liste. • **URL** - Gibt die URL an, die Sie anklicken können, um die Referenz anzuzeigen. Klicken Sie für weitere Informationen auf den Link. Beim Anklicken des Links wird die externe Ressource in einem neuen Browserfenster angezeigt.
Produkte	Zeigt eine Liste von Produkten an, die dieser Schwachstelle zugeordnet sind. • **Anbieter** - Gibt den Anbieter des Produkts an. • **Produkt** - Gibt den Produktnamen an. • **Version** - Gibt die Versionsnummer des Produkts an.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Assets**.
2. Klicken Sie im Navigationsmenü auf **Assetprofile**.
3. Wählen Sie ein Assetprofil aus.
4. Klicken Sie im Teilfenster 'Schwachstellen' auf den Parameterwert **ID** oder **Schwachstelle** der Schwachstelle, die Sie untersuchen möchten.

Parameter der Seite 'Assetprofil'

Hier finden Sie Beschreibungen der Parameter der Seite 'Assetprofil' für die Fensterbereiche 'Assetzusammenfassung', 'Netzschnittstelle', 'Schwachstelle', 'Services', 'Pakete', 'Windows-Patches', 'Eigenschaften', 'Risikorichtlinien' und 'Produkte'.

Hier finden Sie auch Tabellen mit Beschreibungen der Parameter, die in den einzelnen Fensterbereichen der Registerkarte **Assetprofil** angezeigt werden.

Fensterbereich 'Assetzusammenfassung'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Assetzusammenfassung', auf den Sie über die Seite **Assetprofil** zugreifen können.

Im Fensterbereich 'Assetzusammenfassung' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 10-8 - Parameter des Fensterbereichs 'Assetzusammenfassung'

Parameter	Beschreibung
Asset-ID	Hier wird die dem Assetprofil zugeordnete ID-Nummer angezeigt.
IP-Adresse	Hier wird die zuletzt gemeldete IP-Adresse des Assets angezeigt.
MAC-Adresse	Hier wird die letzte bekannte MAC-Adresse des Assets angezeigt.
Netz	Hier wird das zuletzt gemeldete, dem Asset zugeordnete Netz angezeigt.
NetBIOS-Name	Hier wird der NetBIOS-Name des Assets angezeigt, sofern bekannt. Hat das Asset mehrere NetBIOS-Namen, wird in diesem Feld die Anzahl der NetBIOS-Namen angezeigt. Bewegen Sie den Mauszeiger über den Wert, um eine Liste der zugehörigen NetBIOS-Namen anzuzeigen.
DNS-Name	Hier wird die IP-Adresse oder der DNS-Name des Assets angezeigt, sofern bekannt. Hat das Asset mehrere DNS-Namen, wird in diesem Feld die Anzahl der DNS-Namen angezeigt. Bewegen Sie den Mauszeiger über den Wert, um eine Liste der zugehörigen DNS-Namen anzuzeigen.
Angegebener Name	Hier wird der Name des Assets angezeigt. Standardmäßig ist dieses Feld leer. Bearbeiten Sie das Assetprofil, wenn Sie einen Namen für das Asset angeben möchten.
Gruppenname	Hier wird die letzte bekannte Benutzergruppe des Assets anzeigt, sofern bekannt.
Letzter Benutzer	Hier wird der letzte bekannte Benutzer des Assets angezeigt. Benutzerinformationen werden von Identitätsereignissen abgeleitet. Wenn diesem Asset mehrere Benutzer zugeordnet sind, können Sie durch Klicken auf den Link alle Benutzer anzeigen.

Parameter	Beschreibung
Betriebssystem	Hier wird das Betriebssystem angezeigt, das auf dem Asset ausgeführt wird. Gibt es mehrere Betriebssysteme auf dem Asset, wird in diesem Feld die Anzahl der Betriebssysteme angegeben. Bewegen Sie den Mauszeiger über den Wert, um eine Liste der zugehörigen Betriebssysteme anzuzeigen. Sie können diesen Parameter direkt bearbeiten, wenn für den Parameter **Überschreiben Bis zum nächsten Scan überschreiben** oder **Dauerhaft überschreiben** angegeben ist.
Gewichtung	Hier ist angegeben, welche Bewertungsstufe dem betreffenden Asset zugeordnet ist. Der Bereich reicht von 0 (nicht wichtig) bis 10 (sehr wichtig). Standardmäßig ist dieses Feld leer. Wenn Sie eine Gewichtung für das Asset angeben möchten, bearbeiten Sie hierfür das Assetprofil.
CVSS-Bewertung zusammenfassen	Hier wird die zusammengefasste CVSS-Bewertung (CVSS = Common Vulnerability Scoring System) für die Schwachstellen in diesem Asset angezeigt. Bei der CVSS-Bewertung handelt es sich um eine Messgröße zur Bewertung des Schweregrads einer Schwachstelle. Mithilfe der CVSS-Bewertungen können Sie beurteilen, wie gravierend eine Schwachstelle im Vergleich zu anderen Schwachstellen anzusehen ist. Die CVSS-Bewertung wird unter Verwendung der folgenden benutzerdefinierten Parameter berechnet: • Nebenschadenpotenzial • Vertraulichkeitsanforderungen • Verfügbarkeitsanforderungen • Integritätsanforderungen Weitere Informationen zur Konfiguration dieser Parameter finden Sie im Abschnitt „Assetprofil hinzufügen oder bearbeiten" auf Seite 120. Weitere Informationen zu CVSS finden Sie unter *http://www.first.org/cvss/* .
Geschäftseigentümer	Hier wird der Name des Geschäftseigentümers des Assets angezeigt. Hierbei kann es sich beispielsweise um einen Abteilungsleiter handeln.
Kontakt zum Geschäftseigentümer	Hier werden die Kontaktinformationen für den Geschäftseigentümer angezeigt.

Parameter	Beschreibung
CVSS-Nebenschadenpotenzial	Hier wird das Potenzial dieses Assets für Nebenschäden angezeigt. Dieser Wert wird in die Formel zur Berechnung des Parameters **CVSS-Bewertung** einbezogen. Standardmäßig ist dieses Feld nicht definiert. Wenn Sie eine Position für das Asset angeben möchten, bearbeiten Sie das Assetprofil.
Fachansprechpartner	Hier wird der Fachansprechpartner für das Asset angezeigt. Hierbei kann es sich beispielsweise um einen IT-Manager oder -Leiter handeln.
Kontakt zum Fachansprechpartner	Hier werden die Kontaktinformationen des Fachansprechpartners angezeigt.
CVSS-Verfügbarkeit	Hier wird angezeigt, inwiefern es sich auf die Verfügbarkeit des Assets auswirkt, wenn eine Schwachstelle erfolgreich ausgenutzt wird.
Wireless AP	Hier wird der Wireless Access Point (AP) für das betreffende Assetprofil angezeigt.
Wireless SSID	Hier wird der Wireless Service Set Identifier (SSID) für das betreffende Assetprofil angezeigt.
Anforderungen an CVSS-Vertraulichkeit	Hier wird angezeigt, inwiefern sich eine erfolgreich ausgenutzte Schwachstelle auf diesem Asset auf die Vertraulichkeit auswirkt.
Switch-ID	Hier wird die Switch-ID für das Assetprofil angezeigt.
Switch-Port-ID	Hier wird die Switch-Port-ID für das Assetprofil angezeigt.
Anforderungen an CVSS-Integrität	Hier wird angezeigt, inwiefern es sich auf die Integrität des Assets auswirkt, wenn eine Schwachstelle erfolgreich ausgenutzt wird.
Technischer Benutzer	Hier ist der der diesem Assetprofil zugeordnete Benutzername angegeben.
Offene Services	Hier wird angezeigt, wie viele eindeutige Schicht 7-Anwendungen auf diesem Assetprofil ausgeführt werden.
Schwachstellen	Hier wird angezeigt, wie viele Schwachstellen auf dem Assetprofil erkannt wurden.
Position	Hier ist die physische Position des Assets angegeben. Standardmäßig ist dieses Feld leer. Wenn Sie eine Position für das Asset angeben möchten, bearbeiten Sie das Assetprofil.

Parameter	Beschreibung
Assetbeschreibung	Hier ist eine Beschreibung für das Asset angegeben. Standardmäßig ist dieses Feld leer. Wenn Sie eine Beschreibung für das Asset angeben möchten, bearbeiten Sie hierfür das Assetprofil.
Zusatzdaten	Hier werden auf Grundlage eines Ereignisses erweiterte Informationen angegeben.

Fensterbereich 'Netzschnittstellenzusammenfassung'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Netzschnittstellenzusammenfassung', auf den Sie über die Seite **Assetprofil** zugreifen können.

Im Fensterbereich 'Netzschnittstellenzusammenfassung' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 1 - Parameter des Fensterbereichs 'Netzschnittstellenzusammenfassung'

Parameter	Beschreibung
MAC-Adresse	Hier wird die MAC-Adresse des Assets angezeigt, sofern bekannt.
IP-Adresse	Hier wird die für die betreffende MAC-Adresse erkannte IP-Adresse angezeigt.
Netz	Hier wird das Netz angezeigt, dem die IP-Adresse zugeordnet ist, sofern bekannt.
Zuletzt gesehen	Hier wird der Zeitpunkt (Datum und Uhrzeit) angezeigt, zu dem die IP-Adresse an dieser MAC-Adresse zuletzt erkannt wurde.

Fensterbereich 'Schwachstelle'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Schwachstelle', auf den Sie über die Seite **Assetprofil** zugreifen können.

Im Fensterbereich 'Schwachstelle' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 38. Schwachstelle, Parameter des Fensterbereichs

Parameter	Beschreibung
ID	Hier wird die ID der Schwachstelle angezeigt. Die ID ist eine eindeutige Kennung, die von Vulnerability Information System (VIS) generiert wird.
Wertigkeit	Hier wird die der Schwachstelle zugeordnete PCI-Wertigkeit (PCI = Payment Security Industry) angezeigt.
Risiko	Die der Schwachstelle zugeordnete Risikostufe. Beim Sortieren nach dieser Spalte muss der zugrundeliegende Risikostufencode verwendet werden.

Tabelle 38. Schwachstelle, Parameter des Fensterbereichs (Forts.)

Parameter	Beschreibung
Service	Der der Schwachstelle zugeordnete Service (wie im Suchlauf erkannt). Falls nur 1 Service zugeordnet ist, wird hier der Service angezeigt. Andernfalls wird 'Mehrere (N)' angezeigt. N steht dabei für die Gesamtzahl der dieser Schwachstelle zugeordneten Services.
Port	Hier wird angezeigt, an welcher Portnummer die Schwachstelle erkannt wurde. Falls die Schwachstelle an mehreren Ports erkannt wurde, wird in diesem Feld die Anzahl der Portnummern angezeigt. Bewegen Sie den Mauszeiger über den Wert, um eine Liste der Portnummern anzuzeigen.
Schwachstelle	Der Name oder Titel dieser Schwachstelle.
Details	Spezieller ausführlicher Text im Zusammenhang mit dieser Schwachstelle, wie im Suchlauf festgestellt. Falls nur 1 Detail zugeordnet ist, wird hier der Text zu diesem Detail angezeigt. Andernfalls wird 'Mehrere (N)' angezeigt. N steht dabei für die Gesamtzahl der dieser Schwachstelle zugeordneten Details.
CVSS-Bewertung	Hier wird die zusammengefasste CVSS-Bewertung (CVSS = Common Vulnerability Scoring System) für die Schwachstellen auf diesem Asset angezeigt. Bei der CVSS-Bewertung handelt es sich um eine Messgröße zur Bewertung des Schweregrads einer Schwachstelle. Mithilfe der CVSS-Bewertungen können Sie beurteilen, wie gravierend eine Schwachstelle im Vergleich zu anderen Schwachstellen anzusehen ist. Die CVSS-Bewertung wird unter Verwendung der folgenden benutzerdefinierten Parameter berechnet: • Nebenschadenpotenzial • Vertraulichkeitsanforderungen • Verfügbarkeitsanforderungen • Integritätsanforderungen Weitere Informationen zur Konfiguration dieser Parameter finden Sie im Abschnitt „Assetprofil hinzufügen oder bearbeiten" auf Seite 120. Weitere Informationen zu CVSS finden Sie unter *http://www.first.org/cvss/* .
Gefunden	Hier wird das Datum angezeigt, an dem diese Schwachstelle ursprünglich in einem Suchlauf gefunden wurde.

Tabelle 38. Schwachstelle, Parameter des Fensterbereichs (Forts.)

Parameter	Beschreibung
Zuletzt gesehen	Hier wird das Datum angezeigt, an dem diese Schwachstelle zuletzt bei einem Suchlauf gesehen wurde.

Fensterbereich 'Services'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Services', auf den Sie über die Seite **Assetprofil** zugreifen können.

Im Fensterbereich 'Services' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 39. Services, Parameter des Fensterbereichs

Parameter	Beschreibung
Service	Hier wird der Name des offenen Service angezeigt.
Produkt	Sofern bekannt, wird hier das Produkt angezeigt, das auf diesem Service ausgeführt wird.
Port	Hier wird der Port angezeigt, an dem die Schicht 7-Anwendung erkannt wurde. Wenn dieser Service über mehrere Ports verfügt, wird in diesem Feld die Anzahl der Ports angezeigt. Bewegen Sie den Mauszeiger über den Wert, um eine Liste der Portnummern anzuzeigen.
Protokoll	Hier wird eine durch Kommas getrennte Liste der Protokolle angezeigt, die an dem Port, an dem der offene Service ausgeführt wird, erkannt wurden.
Zuletzt passiv gesehen	Hier wird der Zeitpunkt (Datum und Uhrzeit) angezeigt, an dem der offene Service zuletzt passiv gesehen wurde.
Zuletzt aktiv gesehen	Hier wird der Zeitpunkt (Datum und Uhrzeit) angezeigt, an dem der offene Service zuletzt aktiv gesehen wurde.
Standardport des Service	Hier wird eine durch Kommas getrennte Liste der bekannten Ports angezeigt, an denen die Schicht 7-Anwendung bekanntermaßen ausgeführt wird.
Schwachstellen	Hier wird die Anzahl der Schwachstellen im Zusammenhang mit diesem offenen Service angezeigt.

Fensterbereich 'Windows-Services'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Windows-Services', auf den Sie über die Seite **Assetprofil** zugreifen können. Der Fensterbereich 'Windows-Services' wird nur angezeigt, wenn QRadar Vulnerability Manager auf Ihrem System installiert ist.

Im Fensterbereich 'Windows-Services' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 40. Parameter des Fensterbereichs 'Windows-Services'

Parameter	Beschreibung
Name	Hier wird der Name des Windows-Service angezeigt, der auf dem Asset aktiv gesehen wurde.
Status	Hier wird der Status des Windows-Service angezeigt. Mögliche Optionen: • Aktiviert • Manuell • Inaktiviert

Fensterbereich 'Pakete'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Pakete', auf den Sie über die Seite **Assetprofil** zugreifen können.

Der Fensterbereich 'Pakete' wird nur angezeigt, wenn QRadar Vulnerability Manager auf Ihrem System installiert ist. Im Fensterbereich 'Pakete' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 41. Pakete, Parameter des Fensterbereichs

Parameter	Beschreibung
Pakete	Hier wird der Name des Pakets angezeigt, das auf das Asset angewandt wird.
Version	Hier wird die Version des Pakets angezeigt, das auf das Asset angewandt wird.
Überarbeitung	Hier wird die Überarbeitung des Pakets angezeigt, das auf das Asset angewandt wird.

Fensterbereich 'Windows-Patches'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Windows-Patches', auf den Sie über die Seite **Assetprofil** zugreifen können.

Der Fensterbereich 'Windows-Patches' wird nur angezeigt, wenn QRadar Vulnerability Manager auf Ihrem System installiert ist. Im Fensterbereich 'Windows-Patches' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 42. Parameter des Fensterbereichs 'Windows-Patches'

Parameter	Beschreibung
Nummer der Microsoft Knowledge-Base	Hier wird die Nummer der Microsoft Knowledge Base (KB) für das auf dem Asset ausgeführte Windows-Patch angezeigt.
Beschreibung	Hier wird die Beschreibung des Windows-Patches angezeigt.
Bulletin-ID	Hier wird die Bulletin-ID-Nummer des Windows-Patches angezeigt.
ID der Schwachstelle	Hier wird die Schwachstellen-ID des Windows-Patches angezeigt.

Tabelle 42. Parameter des Fensterbereichs 'Windows-Patches' (Forts.)

Parameter	Beschreibung
CVE-ID	Hier wird die dem Windows-Patch zugeordnete CVE-ID angezeigt. Wenn dem Windows-Patch mehrere CVE-IDs zugeordnet sind, können Sie die Liste der CVE-IDs anzeigen, indem Sie den Mauszeiger über den Link 'Mehrere' bewegen. Durch Anklicken eines CVE-ID-Links können Sie auf weitere Informationen zugreifen.
System	Hier wird das Windows-System für das Patch angezeigt.
Service-Pack	Hier wird das Service-Pack für das Patch angezeigt.

Fensterbereich 'Eigenschaften'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Eigenschaften', auf den Sie über die Seite **Assetprofil** zugreifen können. Der Fensterbereich 'Eigenschaften' wird nur angezeigt, wenn QRadar Vulnerability Manager auf Ihrem System installiert ist.

Im Fensterbereich 'Eigenschaften' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 43. Eigenschaften, Parameter des Fensterbereichs

Parameter	Beschreibung
Name	Hier wird der Name der Konfigurationseigenschaft angezeigt, die auf dem Asset aktiv gesehen wurde.
Wert	Hier wird der Wert für die Konfigurationseigenschaft angezeigt.

Fensterbereich 'Risikorichtlinien'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Risikorichtlinien', auf den Sie über die Seite **Assetprofil** zugreifen können. Der Fensterbereich 'Risikorichtlinien' wird nur angezeigt, wenn QRadar Vulnerability Manager auf Ihrem System installiert ist.

Im Fensterbereich 'Risikorichtlinien' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 44. Parameter des Fensterbereichs 'Risikorichtlinien'

Parameter	Beschreibung
Richtlinie	Gibt den Namen der diesem Asset zugeordneten Richtlinie an.
Bestanden/Nicht bestanden	Gibt an, ob der Status der Richtlinie **Bestanden** oder **Nicht bestanden** lautet.
Zuletzt ausgewertet	Zeigt das Datum an, an dem diese Richtlinie zuletzt ausgewertet wurde.

Fensterbereich 'Produkte'

Hier finden Sie Parameterbeschreibungen für den Fensterbereich 'Produkte', auf den Sie über die Seite **Assetprofil** zugreifen können.

Im Fensterbereich 'Produkte' der Seite **Assetprofil** finden Sie die folgenden Informationen:

Tabelle 45. Parameter des Fensterbereichs 'Produkte'

Parameter	Beschreibung
Produkt	Zeigt den Namen des auf dem Asset ausgeführten Produkts an.
Port	Zeigt den von dem Produkt verwendeten Port an.
Schwachstelle	Zeigt die Anzahl der Schwachstellen in Zusammenhang mit diesem Produkt an.
ID der Schwachstelle	Hier wird die ID der Schwachstelle angezeigt.

Kapitel 11. Berichtsverwaltung

Über die Registerkarte **Berichte** können Sie Berichte erstellen, bearbeiten, verteilen und verwalten.

Ausführliche, flexible Berichtsoptionen erfüllen die verschiedenen Regulierungsstandards, z. B. in Bezug auf PCI-Konformität.

Sie haben die Möglichkeit, Ihre eigenen angepassten Berichte zu erstellen oder Standardberichte zu verwenden. Die Standardberichte können angepasst und unter einer anderen Bezeichnung verwendet und an andere Benutzer verteilt werden. Falls es in Ihrem System viele Berichte gibt, kann die Aktualisierung der Registerkarte **Berichte** einige Zeit dauern.

Anmerkung: Bei Verwendung von Microsoft Exchange Server 5.5 werden in der Betreffzeile von per E-Mail versendeten Berichten unter Umständen nicht verfügbare Schriftartzeichen angezeigt. Laden Sie zur Behebung dieses Problems Service-Pack 4 von Microsoft Exchange Server 5.5 herunter und installieren Sie es. Weitere Informationen erhalten Sie beim Microsoft-Support.

Überlegungen zur Zeitzone

Damit die Berichtsfunktion für die Berichtsdaten das richtige Datum und die korrekte Uhrzeit verwendet, muss Ihre Sitzung mit Ihrer Zeitzone synchronisiert sein.

Die Zeitzone wird bei der Installation und Konfiguration von QRadar-Produkten konfiguriert. Klären Sie mit Ihrem Administrator, ob Ihre QRadar-Sitzung mit Ihrer Zeitzone synchronisiert ist.

Registerkarte 'Berichte' - Berechtigungen

Benutzer mit Verwaltungsaufgaben können alle Berichte anzeigen, die von anderen Benutzern erstellt werden.

Benutzer ohne Verwaltungsaufgaben können nur die selbst erstellten oder von anderen Benutzern geteilten Berichte anzeigen.

Registerkarte 'Berichte' - Parameter

Auf der Registerkarte **Berichte** wird eine Liste mit Standardberichten und benutzerdefinierten Berichten angezeigt.

Über die Registerkarte **Berichte** können Sie statistische Information zu der Berichtsvorlage anzeigen, Aktionen mit Berichtsvorlagen durchführen, die generierten Berichte anzeigen und generierte Inhalte löschen.

Wenn in einem Bericht kein Intervallplan angegeben ist, müssen Sie den Bericht manuell generieren.

Sie können den Mauscursor über einen Bericht bewegen, um in einer QuickInfo eine Berichtszusammenfassung als Vorschau anzuzeigen. In der Zusammenfassung ist die Berichtskonfiguration angegeben, außerdem geht daraus hervor, welche Art von Inhalt mit dem Bericht generiert wird.

Übersicht über die Registerkarte 'Berichte'

Sie haben die Möglichkeit, Ihre eigenen angepassten Berichte zu erstellen oder Standardberichte zu verwenden. Die Standardberichte können angepasst und unter einer anderen Bezeichnung verwendet und an andere Benutzer verteilt werden.

Falls es in Ihrem System viele Berichte gibt, kann die Aktualisierung der Registerkarte **Berichte** einige Zeit dauern.

Anmerkung: Bei Verwendung von Microsoft Exchange Server 5.5 werden in der Betreffzeile von per E-Mail versendeten Berichten unter Umständen nicht verfügbare Schriftartzeichen angezeigt. Laden Sie zur Behebung dieses Problems Service-Pack 4 von Microsoft Exchange Server 5.5 herunter und installieren Sie es. Weitere Informationen erhalten Sie beim Microsoft-Support.

Überlegungen zur Zeitzone

Damit die Berichtsfunktion für die Berichtsdaten das richtige Datum und die korrekte Uhrzeit verwendet, muss Ihre Sitzung mit Ihrer Zeitzone synchronisiert sein.

Die Zeitzone wird bei der Installation und Konfiguration von QRadar-Produkten konfiguriert. Klären Sie mit Ihrem Administrator, ob Ihre QRadar-Sitzung mit Ihrer Zeitzone synchronisiert ist.

Registerkarte 'Berichte' - Berechtigungen

Benutzer mit Verwaltungsaufgaben können alle Berichte anzeigen, die von anderen Benutzern erstellt werden.

Benutzer ohne Verwaltungsaufgaben können nur die selbst erstellten oder von anderen Benutzern geteilten Berichte anzeigen.

Registerkarte 'Berichte' - Parameter

Auf der Registerkarte **Berichte** wird eine Liste mit Standardberichten und angepassten Berichten angezeigt.

Über die Registerkarte **Berichte** können Sie statistische Information zu der Berichtsvorlage anzeigen, Aktionen mit Berichtsvorlagen durchführen, die generierten Berichte anzeigen und generierte Inhalte löschen.

Auf der Registerkarte **Berichte** finden Sie folgende Informationen:

Tabelle 46. Registerkarte 'Berichte' - Parameter

Parameter	Beschreibung
Spalte 'Flags'	Wenn ein Fehler aufgetreten ist, aufgrund dessen die Berichterstellung fehlgeschlagen ist, wird in dieser Spalte das Symbol **Fehler** angezeigt.
Berichtsname	Gibt den Berichtsnamen an.
Gruppe	Gibt die Gruppe an, zu der dieser Bericht gehört.

Tabelle 46. Registerkarte 'Berichte' - Parameter (Forts.)

Parameter	Beschreibung
Zeitplan	Gibt an, wie oft der Bericht generiert wird. Berichte, für die ein Intervallplan angegeben ist, werden, sofern aktiviert, automatisch gemäß dem angegebenen Intervall generiert. Wenn für einen Bericht kein Intervallplan angegeben ist, müssen Sie den Bericht manuell generieren.
Nächste Ausführungszeit	Gibt die Zeitdauer in Stunden und Minuten an, bis der nächste Bericht erstellt wird.
Letzte Änderung	Gibt das Datum an, an dem dieser Bericht zuletzt geändert wurde.
Eigner	Gibt den Benutzer an, der Eigner des Berichts ist.
Autor	Gibt den Benutzer an, der den Bericht erstellt hat.
Erstellte Berichte	Wählen Sie in diesem Listenfeld die Datumszeitmarke des erstellten Berichts aus, den Sie anzeigen möchten. Wenn Sie die Datumszeitmarke auswählen, zeigt der Parameter **Format** verfügbare Formate für die erstellten Berichte an. Wenn keine Berichte generiert wurden, wird **Keine** angezeigt.
Formate	Gibt die Berichtsformate des derzeit ausgewählten Berichts in der Spalte 'Erstellte Berichte' an. Klicken Sie auf das Symbol für das Format, das Sie anzeigen möchten.

Sie können den Mauscursor über einen Bericht bewegen, um in einer QuickInfo eine Berichtszusammenfassung als Vorschau anzuzeigen. In der Zusammenfassung ist die Berichtskonfiguration angegeben, außerdem geht daraus hervor, welche Art von Inhalt mit dem Bericht generiert wird.

Sortierreihenfolge der Berichtsregisterkarte

Standardmäßig werden Berichte nach der Spalte **Letzte Änderung** sortiert. Im Menü **Reports navigation** (Berichtnavigation) sind die Berichte nach dem Intervallplan sortiert.

Wenn Sie den Bericht filtern möchten, sodass nur Berichte mit einer bestimmten Häufigkeit angezeigt werden, klicken Sie auf den Pfeil neben dem Menüpunkt **Bericht** im Navigationsmenü und wählen Sie den Ordner für die Gruppe (Häufigkeit) aus.

Symbolleiste der Berichtsregisterkarte

Über die Symbolleiste können Sie eine Reihe von Aktionen mit Berichten durchführen.

In der folgenden Tabelle sind die Optionen der Symbolleiste 'Berichte' aufgeführt und beschrieben.

Tabelle 47. Optionen der Symbolleiste 'Berichte'

Option	Beschreibung
Gruppe	
Gruppen verwalten	Klicken Sie auf **Gruppen verwalten**, um Berichtsgruppen zu verwalten. Mit der Funktion 'Gruppen verwalten' können Sie Ihre Berichte in Funktionsgruppen organisieren.

Tabelle 47. Optionen der Symbolleiste 'Berichte' (Forts.)

Option	Beschreibung
Aktionen	Klicken Sie auf **Aktionen**, um die folgenden Aktionen auszuführen: • **Erstellen** - Wählen Sie diese Option aus, wenn Sie einen neuen Bericht erstellen möchten. • **Bearbeiten** - Wählen Sie diese Option aus, um den ausgewählten Bericht zu bearbeiten. Sie können auch auf einen Bericht doppelklicken, um den Inhalt zu bearbeiten. • **Duplizieren** - Wählen Sie diese Option aus, um den ausgewählten Bericht zu duplizieren oder umzubenennen. • **Gruppen zuordnen** - Wählen Sie diese Option aus, um den ausgewählten Bericht einer Berichtsgruppe zuzuweisen. • **Freigeben** - Wählen Sie diese Option aus, um den ausgewählten Bericht für andere Benutzer freizugeben. Zum Freigeben von Berichten benötigen Sie Administratorberechtigung. • **Zeitplanung ein-/ausschalten** - Wählen Sie diese Option aus, um für den ausgewählten Bericht zum Status 'Aktiv' bzw. 'Inaktiv' zu wechseln. • **Bericht ausführen** - Wählen Sie diese Option aus, um den ausgewählten Bericht zu generieren. Wenn Sie mehrere Berichte generieren möchten, klicken Sie bei gedrückter Steuertaste auf die gewünschten Berichte. • **Bericht für Rohdaten ausführen** - Wählen Sie diese Option aus, um den ausgewählten Bericht unter Verwendung von Rohdaten zu generieren. Diese Option ist hilfreich, wenn Sie einen Bericht generieren möchten, bevor die erforderlichen kumulierten Daten verfügbar sind. So können Sie mit dieser Option beispielsweise einen Bericht generieren, wenn Sie einen wöchentlichen Bericht ausführen möchten und seit dem Erstellen des Berichts noch keine volle Woche vergangen ist. • **Bericht löschen** - Wählen Sie diese Option aus, um den ausgewählten Bericht zu löschen. Wenn Sie mehrere Berichte löschen möchten, klicken Sie bei gedrückter Steuertaste auf die gewünschten Berichte. • **Generierten Inhalt löschen** - Wählen Sie diese Option aus, um den gesamten generierten Inhalt für die ausgewählten Zeilen zu löschen. Wenn Sie mehrere generierte Berichte löschen möchten, klicken Sie bei gedrückter Steuertaste auf die betreffenden Berichte.

Tabelle 47. Optionen der Symbolleiste 'Berichte' (Forts.)

Option	Beschreibung
Inaktive Berichte ausblenden	Wählen Sie dieses Kontrollkästchen aus, wenn Sie inaktive Berichtsvorlagen ausblenden möchten. Die Registerkarte **Berichte** wird automatisch aktualisiert und es werden nur aktive Berichte angezeigt. Heben Sie die Markierung des Kontrollkästchens auf, wenn die verdeckten inaktiven Berichte wieder angezeigt werden sollen.
Berichte suchen	Geben Sie Ihre Suchkriterien in das Feld **Berichte suchen** ein und klicken Sie auf das Symbol **Berichte suchen**. Es wird eine Suche für die folgenden Parameter ausgeführt, um festzustellen, welche den angegebenen Kriterien entsprechen: • Berichtstitel • Berichtsbeschreibung • Berichtsgruppe • Berichtsgruppen • Benutzername des Berichtserstellers

Berichtslayout

Ein Bericht kann aus mehreren Datenelementen bestehen. Netz- und Sicherheitsdaten können darin auf verschiedene Art und Weise, z. B. in Tabellen, Kurven-, Kreis- und Balkendiagrammen dargestellt werden.

Wenn Sie das Layout eines Berichts auswählen, bedenken Sie auch, welchen Berichtstyp Sie erstellen möchten. So sollten Sie beispielsweise keinen kompakten Diagrammcontainer für Grafikinhalte mit vielen Objekten auswählen. Zu jeder Grafik gibt es eine Legende und eine Liste der Netze, aus denen der Inhalt abgeleitet wurde. Wählen Sie einen Container aus, der groß genug für die Daten ist. Informationen zur Vorschau der Datenanzeige in den verschiedenen Diagrammen finden Sie im Abschnitt Grafiktypen.

Diagrammtypen

Beim Erstellen eines Berichts müssen Sie einen Diagrammtyp für jedes Diagramm auswählen, das Sie in Ihren Bericht aufnehmen möchten.

Der Diagrammtyp legt fest, wie Daten und Netzobjekte in dem generierten Bericht dargestellt werden. Sie können Daten mit mehreren Kenndaten grafisch darstellen und die Diagramme in einem einzelnen generierten Bericht erstellen.

Folgende Arten von Diagrammen können verwendet werden:

- **Keine** - Verwenden Sie diese Option, um in dem Bericht einen leeren Container anzuzeigen. Diese Option ist möglicherweise zum Erstellen von Leerraum in Ihrem Bericht hilfreich. Bei Auswahl der Option **Keine** für einen Container ist keine weitere Konfiguration für diesen Container erforderlich.
- **Assetschwachstellen** - Verwenden Sie dieses Diagramm, um zu jedem definierten Asset in Ihrer Bereitstellung Angaben zu Schwachstellen anzuzeigen. Diagramme zu Assetschwachstellen können erstellt werden, wenn bei einem VA-Scan Schwachstellen festgestellt wurden. Dieses Diagramm ist nach Installation von IBM Security QRadar Vulnerability Manager verfügbar.

- **Schwachstellen** - Die Option 'Schwachstellen' wird nur angezeigt, wenn IBM Security QRadar Vulnerability Manager erworben und lizenziert wurde. Weitere Informationen hierzu finden Sie im *IBM Security QRadar Vulnerability Manager - Benutzerhandbuch*.

Grafiktypen

Jeder Diagrammtyp unterstützt verschiedene Grafiktypen, die Sie verwenden können, um Daten anzuzeigen.

Die folgenden Grafiktypen sind für QRadar Log Manager-Berichte verfügbar:

- Kurvendiagramm
- Gestapeltes Kurvendiagramm
- Balkendiagramm
- Gestapeltes Balkendiagramm
- Kreisdiagramm
- Tabellendiagramm

Um Inhalte in einer Tabelle anzuzeigen, müssen Sie einen Bericht mit einem Container mit voller Seitenbreite entwerfen.

Angepasste Berichte erstellen

Sie können den Berichtsassistenten verwenden, um einen neuen Bericht zu erstellen.

Vorbereitende Schritte

Sie müssen zutreffende Netzwerkberechtigungen haben, um einen generierten Bericht für andere Benutzer freizugeben.

Weitere Informationen zu Berechtigungen finden Sie im *IBM Security QRadar Log Manager - Verwaltungshandbuch*.

Informationen zu diesem Vorgang

Der Berichtsassistent bietet einen schrittweisen Leitfaden zum Entwerfen, Planen und Generieren von Berichten.

Der Assistent verwendet die folgenden wichtigen Elemente, um Ihnen dabei zu helfen, einen Bericht zu erstellen:

- **Layout** - Position und Größe von jedem Container
- **Container** - Platzhalter für den gezeigten Inhalt
- **Inhalt** - Definition des Diagramms, das sich im Container befindet

Nachdem ein Bericht mit wöchentlicher oder monatlicher Generierung erstellt wurde, muss der geplante Zeitpunkt vergangen sein, bevor der generierte Bericht Ergebnisse zurückgibt. Für einen geplanten Bericht müssen Sie den geplanten Zeitraum abwarten, damit Ergebnisse vorhanden sind. Zum Beispiel erfordert eine wöchentliche Suche, dass sieben Tage vergangen sind, um die Daten aufzubauen. Diese Suche gibt vor sieben Tagen keine Ergebnisse zurück.

Wenn Sie das Ausgabeformat für den Bericht angeben, sollten Sie berücksichtigen, dass die Dateigröße von generierten Berichten, abhängig vom gewählten Ausgabe-

format, 1 bis 2 Megabyte betragen kann. Das PDF-Format ist kleiner und nimmt nicht viel Plattenspeicher in Anspruch.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie im Listenfeld **Aktionen** den Eintrag **Erstellen** aus.
3. Klicken Sie bei "Willkommen beim Berichtsassistenten" auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.
4. Wählen Sie eine der folgenden Optionen aus:

Option	Bezeichnung
Manuell	Generiert einmalig einen Bericht. Dies ist die Standardeinstellung; allerdings können Sie diesen Bericht so oft wie erforderlich generieren.
Stündlich	Plant, dass der Bericht am Ende jeder Stunde anhand der Daten der vorherigen Stunde generiert wird. Wenn Sie die stündliche Option auswählen, sind weitere Konfigurationen erforderlich. Wählen Sie in den Listenfeldern einen Zeitrahmen aus, um den Berichtszyklus anzufangen und zu beenden. Es wird ein Bericht für jede Stunde innerhalb dieses Zeitrahmens generiert. Die Zeit kann in 30-Minuten-Schritten eingestellt werden. Sowohl für das Feld **Von** als auch für das Feld **Bis** ist 1:00 Uhr die Standardeinstellung.
Wöchentlich	Plant die wöchentliche Generierung des Berichts anhand von Daten der vorherigen Woche. Wenn Sie die Option **Wöchentlich** auswählen, sind weitere Konfigurationen erforderlich. Wählen Sie den Tag aus, an dem der Bericht generiert werden soll. Der Standardwert ist Montag. Wählen Sie im Listenfeld eine Zeit aus, um mit dem Berichtszyklus anzufangen. Die Zeit kann in 30-Minuten-Schritten eingestellt werden. Die Standardeinstellung ist 1:00 Uhr.
Monatlich	Plant die monatliche Generierung des Berichts anhand von Daten des Vormonats. Wenn Sie die Option **Monatlich** auswählen, sind weitere Konfigurationen erforderlich. Wählen Sie im Listenfeld das Datum aus, an dem der Bericht generiert werden soll. Die Standardeinstellung ist der erste Tag des Monats. Wählen Sie zudem im Listenfeld eine Zeit aus, um mit dem Berichtszyklus anzufangen. Die Zeit kann in 30-Minuten-Schritten eingestellt werden. Die Standardeinstellung ist 1:00 Uhr.

5. Wählen Sie im Fensterbereich **Darf dieser Bericht manuell erstellt werden?** die Option **Ja** oder **Nein** aus.

6. Konfigurieren Sie das Layout des Berichts:
   a. Wählen Sie im Listenfeld **Ausrichtung** die Seitenausrichtung aus: Hochformat oder Querformat.
   b. Wählen Sie eine der sechs Layoutoptionen aus, die im Berichtsassistenten angezeigt werden.
   c. Klicken Sie auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.
7. Folgende Parameter müssen angegeben werden:
   - **Berichtstitel** - Geben Sie einen Berichtstitel ein. Der Titel kann bis zu 100 Zeichen lang sein. Verwenden Sie keine Sonderzeichen.
   - **Logo** - Wählen Sie im Listenfeld ein Logo aus.
   -
8. Konfigurieren Sie jeden Container im Bericht:
   a. Wählen Sie im Listenfeld **Diagrammtyp** einen Diagrammtyp aus.
   b. Konfigurieren Sie im Fenster **Containerdetails - <Diagramm_Typ>** die Diagrammparameter.
   c. Klicken Sie auf **Containerdetails speichern**.
   d. Falls erforderlich, wiederholen Sie die Schritte a bis c für alle Container.
   e. Klicken Sie auf **Weiter**, um zur nächsten Seite des Berichtsassistenten zu wechseln.
9. Zeigen Sie die Seite **Layoutvorschau** an, und klicken Sie dann auf **Weiter**, um mit dem nächsten Schritt des Berichtsassistenten fortzufahren.
10. Wählen Sie die Kontrollkästchen für die Berichtsformate aus, die Sie generieren wollen, und klicken Sie dann auf **Weiter**.

    Anmerkung: Extensible Markup Language ist nur für Tabellen verfügbar.
11. Wählen Sie die Verteilungskanäle für Ihren Bericht aus, und klicken Sie dann auf **Weiter**. Folgende Verteilungskanäle gehören zu den Optionen:

Option	Bezeichnung
Berichtskonsole	Wählen Sie dieses Kontrollkästchen aus, um den generierten Bericht zur Registerkarte **Berichte** zu senden. Dies ist der Standardverteilungskanal.
Wählen Sie die Benutzer aus, die den generierten Bericht anzeigen können.	Diese Option wird angezeigt, nachdem Sie das Kontrollkästchen **Berichtskonsole** ausgewählt haben. Wählen Sie von der Liste von Benutzern die Benutzer aus, denen Sie Berechtigung erteilen wollen, die generierten Berichte anzuzeigen.
Alle Benutzer auswählen	Diese Option wird nur angezeigt, nachdem Sie das Kontrollkästchen **Berichtskonsole** ausgewählt haben. Wählen Sie dieses Kontrollkästchen aus, wenn Sie allen Benutzern die Berechtigung erteilen wollen, die generierten Berichte anzuzeigen. Sie müssen zutreffende Netzwerkberechtigungen haben, um den generierten Bericht für andere Benutzer freizugeben.

Option	Bezeichnung
E-Mail	Wählen Sie dieses Kontrollkästchen aus, wenn Sie den generierten Bericht per E-Mail verteilen wollen.
E-Mail-Adresse(n) der Berichtsziele eingeben	Diese Option wird nur angezeigt, nachdem Sie das Kontrollkästchen **E-Mail** ausgewählt haben. Geben Sie die E-Mail-Adresse für jeden generierten Berichtsempfänger ein; trennen Sie eine Liste mit E-Mail-Adressen mit Kommas ab. Dieser Parameter darf maximal 255 Zeichen aufweisen. E-Mail-Empfänger erhalten diese E-Mail von no_reply_reports@qradar.
Bericht als Anhang einschließen (nur Nicht-HTML)	Diese Option wird nur angezeigt, nachdem Sie das Kontrollkästchen **E-Mail** ausgewählt haben. Wählen Sie dieses Kontrollkästchen aus, um den generierten Bericht als Anhang zu senden.
Link zur Berichtskonsole einschließen	Diese Option wird nur angezeigt, nachdem Sie das Kontrollkästchen **E-Mail** ausgewählt haben. Wählen Sie dieses Kontrollkästchen aus, um einen Link zur Berichtskonsole in der E-Mail einzuschließen.

12. Geben Sie auf der Seite **Endbearbeitung** Werte für die folgenden Parameter ein:

Option	Bezeichnung
Berichtsbeschreibung	Geben Sie eine Beschreibung für diesen Bericht ein. Die Beschreibung wird auf der Seite **Berichtszusammenfassung** und in der generierten Berichtsverteilungs-E-Mail angezeigt.
Gruppen	Wählen Sie die Gruppen aus, denen Sie diesen Bericht zuweisen wollen. Weitere Informationen zu Gruppen finden Sie im Abschnitt Berichtsgruppen.
Soll der Bericht jetzt ausgeführt werden?	Wählen Sie dieses Kontrollkästchen aus, wenn Sie den Bericht nach Abschluss des Assistenten generieren wollen. Das Kontrollkästchen ist standardmäßig ausgewählt.

13. Klicken Sie auf **Weiter**, um die Berichtszusammenfassung anzuzeigen.
14. Wählen Sie auf der Seite **Berichtszusammenfassung** die im Zusammenfassungsbericht verfügbaren Registerkarten aus, um eine Vorschau zur Berichtskonfiguration anzuzeigen.

Ergebnisse

Der Bericht wird sofort generiert. Wenn Sie auf der letzten Seite des Assistenten das Kontrollkästchen **Soll der Bericht jetzt ausgeführt werden?** abgewählt haben, wird der Bericht gespeichert und zum geplanten Zeitpunkt generiert. Der Berichts-

titel ist der Standardtitel für den generierten Bericht. Wenn Sie einen Bericht neu konfigurieren, um einen neuen Berichtstitel einzugeben, wird der Bericht als ein neuer Bericht mit dem neuen Namen gesichert; allerdings bleibt der ursprüngliche Bericht der gleiche.

Berichtsverwaltungsaufgaben

Über die Registerkarte 'Berichte' und den Assistenten 'Berichte' können Sie Berichte verwalten.

Sie können Berichte bearbeiten, kopieren, freigeben und kennzeichnen. Außerdem können Sie generierte Berichte löschen.

Berichte bearbeiten

Mithilfe des Berichtsassistenten können Sie jeden standardmäßigen oder benutzerdefinierten Bericht bearbeiten.

Informationen zu diesem Vorgang

Sie können eine große Anzahl an Standardberichten verwenden oder anpassen. In der standardmäßigen Registerkarte **Berichte** wird die Liste mit Berichten angezeigt. Jeder Bericht erfasst die vorhandenen Daten und zeigt sie an.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Doppelklicken Sie auf den Bericht, der angepasst werden soll.
3. Ändern Sie im Berichtsassistenten die Parameter, um den Bericht anzupassen und den erforderlichen Inhalt zu generieren.

Ergebnisse

Wenn Sie einen Bericht neu konfigurieren, um einen neuen Berichtstitel einzugeben, wird der Bericht als ein neuer Bericht mit dem neuen Namen gesichert; allerdings bleibt der ursprüngliche Bericht der gleiche.

Erstellte Berichte anzeigen

Auf der Registerkarte **Berichte** wird ein Symbol in der Spalte **Formate** angezeigt, wenn ein Bericht Inhalte generiert hat. Klicken Sie auf das Symbol, um den Bericht anzuzeigen.

Informationen zu diesem Vorgang

Wenn ein Bericht Inhalte generiert hat, wird in der Spalte **Erstellte Berichte** ein Listenfeld angezeigt. Im Listenfeld werden alle generierten Inhalte nach den Zeitmarken der Berichte zusammengefasst aufgeführt. Die aktuellsten Berichte befinden sich am Anfang der Liste. Wenn ein Bericht über keine generierten Inhalte verfügt, wird der Wert **Ohne** in der Spalte **Erstellte Berichte** anzeigt.

In der Spalte **Formate** zeigen Symbole das Berichtsformat des generierten Berichts an.

Berichte können in den Formaten PDF, HTML, RTF, XML und XLS erstellt werden.

Anmerkung: Die Formate XML und XLS sind ausschließlich für Berichte verfügbar, die ein Format mit einer einzelnen Diagrammtabelle (Hoch- oder Querformat) verwenden.

Sie können nur die Berichte anzeigen, auf die Ihnen vom Administrator Zugriff gewährt wurde. Benutzer mit Verwaltungsaufgaben können auf alle Berichte zugreifen.

Wenn Sie den Web-Browser Mozilla Firefox verwenden und das RTF-Berichtsformat auswählen, öffnet Mozilla Firefox ein neues Browserfenster. Dieses neue Fenster ist auf die Web-Browser-Konfiguration von Mozilla Firefox zurückzuführen und hat keine Auswirkungen auf QRadar. Sie können das Fenster schließen und Ihre QRadar-Sitzung fortsetzen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie im Listenfeld der Spalte **Erstellte Berichte** die Zeitmarke des Berichts aus, den Sie anzeigen möchten.
3. Klicken Sie auf das Symbol des Formats, das Sie verwenden möchten.

Generierten Inhalt löschen

Wenn Sie generierten Inhalt löschen, werden alle Berichte, die von der Berichtsvorlage generiert haben, gelöscht, aber die Berichtsvorlage wird beibehalten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie die Berichte aus, für die Sie den generierten Inhalt löschen wollen.
3. Wählen Sie im Listenfeld **Aktionen** den Eintrag **Generierten Inhalt löschen** aus.

Bericht manuell erstellen

Ein Bericht kann für eine automatische Generierung konfiguriert werden; allerdings können Sie auch jederzeit einen Bericht manuell generieren.

Informationen zu diesem Vorgang

Während ein Bericht generiert wird, ist in der Spalte 'Nächste Ausführungszeit' eine der drei folgenden Nachrichten zu sehen:

- **wird erstellt** - Der Bericht wird gerade generiert.
- **Eingereiht (Position in der Warteschlange)** - Der Bericht befindet sich in der Warteschlange für die Generierung. Die Nachricht gibt die Stelle an, an der sich der Bericht in der Warteschlange befindet. Beispiel: 1 von 3.
- **(x Stunde(n) x Minute(n) y Sekunde(n))** - Die Ausführung des Berichts wurde geplant. Die Nachricht ist ein Countdown-Zähler, der angibt, wann der Bericht als Nächstes ausgeführt wird.

Sie können das Symbol **Aktualisieren** auswählen, um die Ansicht einschließlich Informationen in der Spalte **Nächste Ausführungszeit** zu aktualisieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie den Bericht aus, den Sie generieren wollen.

3. Klicken Sie auf **Bericht ausführen**.

Nächste Schritte

Nachdem der Bericht generiert wurde, können Sie in der Spalte 'Erstellte Berichte' den generierten Bericht anzeigen.

Berichte duplizieren

Um einen Bericht zu erstellen, der einem vorhandenen Bericht sehr ähnelt, können Sie den Bericht duplizieren, den Sie modellieren wollen, und ihn dann anpassen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie den Bericht aus, den Sie duplizieren wollen.
3. Klicken Sie im Listenfeld **Aktionen** auf **Duplizieren**.
4. Geben Sie einen neuen Namen ohne Leerzeichen für den Bericht ein.

Nächste Schritte

Sie können den duplizierten Bericht anpassen.

Bericht freigeben

Sie können Berichte für andere Benutzer freigeben. Wenn Sie einen Bericht freigeben, stellen Sie eine Kopie des ausgewählten Berichts für einen anderen Benutzer zur Bearbeitung oder Planung bereit.

Informationen zu diesem Vorgang

Aktualisierungen, die der Benutzer an einem freigegebenen Bericht vornimmt, wirken sich nicht auf die Originalfassung des Berichts aus.

Sie müssen über Administratorberechtigungen verfügen, um Berichte freigeben zu können. Um die Anzeige von Berichten und den Zugriff auf diese durch einen neuen Benutzer zu ermöglichen, muss ein Benutzer mit Verwaltungsaufgaben zudem alle notwendigen Berichte für den neuen Benutzer freigeben.

Ein Bericht kann nur für Benutzer freigegeben werden, die über den entsprechenden Zugriff verfügen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie die Berichte aus, die Sie freigeben möchten.
3. Klicken Sie im Listenfeld **Aktionen** auf **Freigeben**.
4. Wählen Sie in der Liste der Benutzer die Benutzer aus, für die Sie diesen Bericht freigeben wollen.

Branding von Berichten

Zum Branding von Berichten können Sie Logos und bestimmte Bilder importieren. Wenn Sie Berichte mit benutzerdefinierten Logos kennzeichnen möchten, müssen Sie die Logos vor Verwendung des Berichtsassistenten hochladen und konfigurieren.

Vorbereitende Schritte

Achten Sie darauf, eine Grafik mit 144 x 50 Pixeln und weißem Hintergrund zu verwenden.

Löschen Sie den Browser-Cache, um sicherzugehen, dass das neue Logo im Browser angezeigt wird.

Informationen zu diesem Vorgang

Das Branding von Berichten ist für Unternehmen hilfreich, die mehrere Logos unterstützen. Beim Hochladen werden die Bilder automatisch als Portable Network Graphic (PNG) gespeichert.

Wenn Sie ein neues Bild hochladen und als Standard festlegen, wird das neue Standardbild nicht auf bereits zuvor generierte Berichte angewandt. Wenn Sie das Logo auf bereits generierten Berichten aktualisieren möchten, müssen Sie manuell von dem Bericht aus neue Inhalte generieren.

Wenn Sie ein Bild hochladen, das länger ist als vom Berichtsheader unterstützt, wird die Größe des Bildes automatisch an den Header, also auf eine Höhe von ca. 50 Pixeln angepasst.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Klicken Sie im Navigationsmenü auf **Branding**.
3. Klicken Sie auf **Durchsuchen**, um die Dateien in Ihrem System zu durchsuchen.
4. Wählen Sie die Datei mit dem hochzuladenden Logo aus. Klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Upload Image** (Bild hochladen).
6. Wählen Sie das Logo aus, das Sie als Standard verwenden möchten, und klicken Sie auf **Set Default Image** (Standardbild festlegen).

Berichtsgruppen

Berichte können in Funktionsgruppen sortiert werden. Durch die Kategorisierung in Gruppen können die Berichte effizient organisiert und gesucht werden.

Sie können beispielsweise alle Berichte im Zusammenhang mit PCIDSS-Konformität (Payment Card Industry Data Security Standard) anzeigen.

Standardmäßig wird auf der Registerkarte **Berichte** die Liste aller Berichte angezeigt, Sie können die Berichte jedoch beispielsweise in folgenden Gruppen kategorisieren:

- Konformität
- Executive
- Protokollquellen
- Netzmanagement
- Sicherheit
- VoIP
- Sonstige

Wenn Sie einen neuen Bericht erstellen, können Sie den Bericht einer vorhandenen Gruppe zuweisen oder eine neue Gruppe erstellen. Zum Erstellen, Bearbeiten oder Löschen von Gruppen benötigen Sie Verwaltungszugriff.

Weitere Informationen zu Benutzerrollen finden Sie im *IBM Security QRadar Log Manager - Verwaltungshandbuch*.

Berichtsgruppe erstellen

Sie können neue Gruppen erstellen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Klicken Sie auf **Gruppen verwalten**.
3. Wählen Sie über die Navigationsstruktur die Gruppe aus, unter der Sie eine neue Gruppe erstellen möchten.
4. Klicken Sie auf **Neue Gruppe**.
5. Geben Sie Werte für die folgenden Parameter ein:
   - **Name** - Geben Sie den Namen für die neue Gruppe ein. Der Name kann bis zu 255 Zeichen umfassen.
   - **Beschreibung** - Optional. Geben Sie eine Beschreibung für die Gruppe ein. Die Beschreibung kann bis zu 255 Zeichen umfassen.
6. Klicken Sie auf **OK**.
7. Wenn Sie die Speicherposition der neuen Gruppe ändern möchten, klicken Sie auf die neue Gruppe und ziehen Sie den Ordner zu der neuen Speicherposition in der Navigationsstruktur.
8. Schließen Sie das Fenster **Berichtsgruppen**.

Gruppen bearbeiten

Sie können eine Berichtsgruppe bearbeiten, um den Namen oder die Beschreibung zu ändern.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Klicken Sie auf **Gruppen verwalten**.
3. Wählen Sie in der Navigationsstruktur die Gruppe aus, die Sie bearbeiten wollen.
4. Klicken Sie auf **Bearbeiten**
5. Aktualisieren Sie nach Bedarf Werte für die Parameter:
   - **Name** - Geben Sie den Namen für die neue Gruppe ein. Der Name kann bis zu 255 Zeichen lang sein.
   - **Beschreibung** - Optional. Geben Sie eine Beschreibung für diese Gruppe ein. Die Beschreibung kann bis zu 255 Zeichen lang sein. Dieses Feld ist optional.
6. Klicken Sie auf **OK**.
7. Schließen Sie das Fenster **Berichtsgruppen**.

Bericht zu einer Gruppe zuweisen

Mit der Option **Gruppen zuordnen** können Sie einen Bericht einer anderen Gruppe zuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Wählen Sie den Bericht aus, den Sie einer Gruppe zuweisen möchten.
3. Wählen Sie im Listenfeld **Aktionen** die Option **Gruppen zuordnen** aus.
4. Wählen Sie in der Liste **Elementgruppen** das Kontrollkästchen für die Gruppe aus, die Sie diesem Bericht zuweisen möchten.
5. Klicken Sie auf **Gruppen zuordnen**.

Bericht in eine andere Gruppe kopieren

Über das Symbol **Kopieren** können Sie einen Bericht in eine oder mehrere Berichtsgruppen kopieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Klicken Sie auf **Gruppen verwalten**.
3. Wählen Sie in der Navigationsstruktur den zu kopierenden Bericht aus.
4. Klicken Sie auf **Kopieren**.
5. Wählen Sie die Gruppe(n) aus, in die der Bericht kopiert werden soll.
6. Klicken Sie auf **Gruppen zuordnen**.
7. Schließen Sie das Fenster **Berichtsgruppen**.

Berichte entfernen

Verwenden Sie das **Entfernen**-Symbol, um einen Bericht aus einer Gruppe zu entfernen.

Informationen zu diesem Vorgang

Wenn Sie einen Bericht aus einer Gruppe entfernen, ist der Bericht noch auf der Registerkarte **Berichte** vorhanden. Der Bericht wurde nicht von Ihrem System entfernt.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Berichte**.
2. Klicken Sie auf **Gruppen verwalten**.
3. Navigieren Sie von der Navigationsstruktur zu dem Ordner, der den Bericht enthält, den Sie entfernen wollen.
4. Wählen Sie in der Liste von Gruppen den Bericht aus, den Sie entfernen möchten.
5. Klicken Sie auf **Entfernen**.
6. Klicken Sie auf **OK**.
7. Schließen Sie das Fenster **Berichtsgruppen**.

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.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

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.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

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

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

Hinweise zur Datenschutzrichtlinie

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

Je nachdem, welche Konfigurationen bereitgestellt sind, kann dieses Softwareangebot Sitzungscookies verwenden, die für das Sitzungsmanagement und die Authentifizierung die Sitzungs-ID jedes Benutzers erfassen. Diese Cookies können inaktiviert werden, 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 Online-Datenschutzerklärung, Schwerpunkte' unter http://www.ibm.com/privacy, in der 'IBM Online-Datenschutzerklärung' unter http://www.ibm.com/privacy/details im Abschnitt 'Cookies, Web-Beacons und sonstige Technologien' " und unter 'IBM Software Products and Software-as-a-Service Privacy Statement' (http://www.ibm.com/software/info/product-privacy).

Glossar

Dieses Glossar enthält Begriffe und Definitionen für Software und Produkte von IBM Security QRadar SIEM.

In diesem Glossar werden die folgenden Querverweise verwendet:

- *Siehe* verweist von einem Synonym auf den bevorzugt zu verwendenden Begriff oder von einer Abkürzung auf die Langform des Begriffs.
- *Siehe auch* verweist Sie auf einen verwandten oder entgegengesetzten Begriff.

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

A

Address Resolution Protocol (ARP)
Ein Protokoll, das eine IP-Adresse dynamisch einer Netzadapteradresse in einem lokalen Netz (LAN = Local Area Network) zuordnet.

Administrative Freigabe
Eine Netzressource, die für Benutzer ohne Administratorrechte ausgeblendet ist. Administrative Freigaben bieten Administratoren Zugriff auf alle Ressourcen in einem Netzsystem an.

Akkumulator
Ein Register, in dem ein Operand einer Operation gespeichert und später durch das Ergebnis dieser Operation ersetzt werden kann.

Aktives System
Das System in einem Hochverfügbarkeitscluster, dessen gesamte Services ausgeführt werden.

Aktualisierungszeitgeber
Ein internes Gerät, das manuell oder automatisch in Intervallen ausgelöst wird und die gegenwärtigen Netzaktivitätsdaten aktualisiert.

Angriff
Eine als Reaktion auf eine überwachte Bedingung gesendete Nachricht oder ein als Reaktion generiertes Ereignis. Beispiel: Ein Angriff liefert Informationen dazu, ob gegen eine Richtlinie verstoßen wurde oder das Netz angegriffen wird.

Anwendungssignatur
Mehrere eindeutige Merkmale, die durch die Untersuchung der Paketnutzungsdaten abgeleitet und anschließend zur Identifizierung einer bestimmten Anwendung verwendet werden.

ARP Siehe Address Resolution Protocol.

ARP-Umleitung
Eine ARP-Methode zur Benachrichtigung des Hosts, falls ein Problem in einem Netz besteht.

ASN Siehe Nummer des autonomen Systems.

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

Ausmaß
Kennzahl für den relativen Stellenwert eines bestimmten Angriffs. "Ausmaß" ist ein gewichteter Wert, der aus Relevanz, Schweregrad und Zuverlässigkeit berechnet wird.

Ausspähung (recon)
Eine Methode, durch die Informationen abgerufen werden, die die Identität der Netzressourcen betreffen. Netzscans und andere Verfahren werden verwendet, um eine Liste von Netzressourcenereignissen zu kompilieren, denen dann eine Prioritätsstufe zugeordnet wird.

B

Berechtigungsnachweis
Informationen, die einem Benutzer oder Prozess bestimmte Zugriffsrechte gewähren.

Bericht
In der Abfrageverwaltung die formatierten Daten, die sich aus dem Ausführen einer Abfrage und dem anschließenden Anwenden eines Formulars auf die Daten ergeben.

Berichtsintervall
Ein konfigurierbares Zeitintervall, an dessen Ende der Ereignisprozessor alle erfassten Ereignis- und Datenflussdaten an die Konsole senden muss.

C

CIDR Siehe Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
Methode zum Hinzufügen von Internetprotokolladressen (IP-Adressen) der Klasse C. Internet-Service-Provider (ISPs) erhalten diese Adressen von ihren Kunden. CIDR-Adressen reduzieren die Größe von Routing-Tabellen und stellen mehr IP-Adressen in Organisationen und Unternehmen bereit.

Client Ein Softwareprogramm oder Computer, das bzw. der Services von einem Server anfordert.

Cluster mit hoher Verfügbarkeit
Eine Hochverfügbarkeitskonfiguration, bestehend aus einem primären und einem sekundären Server.

Common Vulnerability Scoring System (CVSS)
Ein Scoring-System, nach dem der Schweregrad einer Schwachstelle gemessen wird.

CVSS Siehe Common Vulnerability Scoring System.

D

Datenbank-Endknotenobjekt
Letztes Objekt oder letzter Knoten in einer Datenbankhierarchie.

Dateneintrag
Ein berechneter Wert einer Metrik zu einem bestimmten Zeitpunkt.

Datenfluss
Eine einzelne Übertragung von Daten, die während einer Konversation über einen Link übergeben werden.

Datenflussprotokoll
Eine Sammlung von Datenflusseinträgen.

Datenflussquellen
Der Ursprung, aus dem der Datenfluss erfasst wird. Eine Datenflussquelle wird als intern klassifiziert, wenn der Datenfluss aus Hardware stammt, die auf einem verwalteten Host installiert ist. Sie wird als extern klassifiziert, wenn der Datenfluss an einen Datenflusskollektor gesendet wird.

Device Support Module (DSM)
Eine Konfigurationsdatei, die aus mehreren Protokollquellen empfangene Ereignisse analysiert und sie in ein Standardtaxonomieformat umwandelt, das als Ausgabe angezeigt werden kann.

DHCP Siehe Dynamic Host Configuration Protocol.

DNS Siehe Domain Name System.

Domain Name System (DNS)
Das verteilte Datenbanksystem, das Domänennamen zu IP-Adressen zuordnet.

Doppelter Datenfluss
Mehrere Instanzen derselben Datenübertragung, empfangen aus verschiedenen Datenflussquellen.

DSM Siehe Device Support Module.

Dynamic Host Configuration Protocol (DHCP)
Ein Kommunikationsprotokoll, das verwendet wird, um Konfigurationsdaten zentral zu verwalten. DHCP ordnet z. B. Computern in einem Netz automatisch IP-Adressen zu.

E

Endknoten
In einer Baumstruktur ein Eintrag oder Knoten, zu dem keine untergeordneten Elemente vorhanden sind.

Endpunkt
Die Adresse einer API oder eines Service

in einer Umgebung. Eine API macht einen Endpunkt verfügbar und ruft zur gleichen Zeit die Endpunkte anderer Services auf.

Externe Scananwendung
Eine Maschine, die mit dem Netz verbunden ist, um Schwachstelleninformationen zu Assets im Netz abzurufen.

F

Falsch-positiv
Ein als positiv eingestuftes Testergebnis (d. h., die Site ist anfällig für einen Angriff), das vom Benutzer als negativ eingestuft wird (d. h. nicht anfällig).

Fern an Fern (R2R)
Der externe Datenverkehr von einem fernen Netz an ein anderes fernes Netz.

Fern an Lokal (R2L)
Der externe Datenverkehr von einem fernen Netz an ein lokales Netz.

FQDN
Siehe Vollständig qualifizierter Domänenname.

FQNN
Siehe Vollständig qualifizierter Netzname.

G

Gateway
Ein Gerät oder Programm, das verwendet wird, um Netze oder Systeme mit anderen Netzarchitekturen zu verbinden.

H

HA Siehe Hochverfügbarkeit (High Availability, HA).

Hash-Based Message Authentication Code (HMAC)
Eine Verschlüsselungscode, der eine verschlüsselte Hashfunktion und einen geheimen Schlüssel verwendet.

HMAC
Siehe Hash-Based Message Authentication Code.

Hochverfügbarkeit (High Availability, HA)
Ein Clustersystem, das bei Auftreten eines Knoten- oder Dämonfehlers umkonfiguriert wird, sodass die vorhandenen Workloads auf die verbleibenden Clusterknoten umverteilt werden können.

Hostkontext
Ein Service, der Komponenten überwacht, um sicherzustellen, dass jede Komponente wie erwartet funktioniert.

I

ICMP Siehe Internet Control Message Protocol.

Identität
Eine Sammlung von Attributen aus einer Datenquelle, die eine Person, ein Unternehmen, einen Bereich oder ein Element darstellen.

IDS Siehe Intrusion-Detection-System.

Inhaltserfassung
Prozess, bei dem eine konfigurierbare Menge an Nutzdaten erfasst und anschließend in einem Datenflussprotokoll gespeichert wird.

Internet Control Message Protocol (ICMP)
Ein Internetprotokoll, das von einem Gateway für die Kommunikation mit einem Quellenhost verwendet wird, um beispielsweise einen Fehler in einem Datagramm zu melden.

Internet Protocol (IP)
Ein Protokoll, das Daten über ein Netz oder miteinander verbundene Netze leitet. Dieses Protokoll dient als Vermittler zwischen den höheren Protokollschichten und dem physischen Netz. Siehe auch Transmission Control Protocol.

Internet-Service-Provider (ISP)
Eine Organisation, die Zugriff auf das Internet bereitstellt.

Intrusion-Detection-System (IDS)
Software, die versuchte oder erfolgreiche Angriffe auf überwachte Ressourcen erkennt, die zu einem Netz oder Hostsystem gehören.

Intrusion-Prevention-System (IPS)
Ein System, das versucht, potenziell zerstörerische Aktivitäten abzuweisen. Zu den Abweisemechanismen könnten u.a. Filtern, Verfolgen/Protokollieren oder Festlegen von Ratengrenzwerten gehören.

IP Siehe Internet Protocol.

IP-Multicast
Übertragung eines Internet Protocol-Datagramms (IP) an eine Gruppe von Systemen, die als einzelne Multicast-Gruppe fungiert.

IPS Siehe Intrusion-Prevention-System.

ISP Siehe Internet-Service-Provider.

K

Kommunikation offener Systeme (OSI, Open Systems Interconnection)
Die Verbindung offener Systeme gemäß den ISO-Normen (International Organization for Standardization) für den Informationsaustausch.

Konsole
Ein Datensichtgerät, von dem aus ein Bediener den Systembetrieb steuern und beobachten kann.

L

LAN Siehe Local Area Network.

LDAP Siehe Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)
Ein offenes Protokoll, das TCP/IP für den Zugriff auf die Verzeichnisse, die ein X.500-Modell unterstützen, verwendet und die Ressourcenanforderungen des komplexeren X.500-DAP-Modells (Directory Access Protocol) nicht erfüllt. LDAP kann beispielsweise eingesetzt werden, um Personen, Organisationen und andere Ressourcen in einem Internet- oder Intranetverzeichnis zu lokalisieren.

Live-Scan
Eine Schwachstellensuche, die Berichtsdaten aus den Scanergebnissen generiert, die auf dem Sitzungsnamen basieren.

L2L Siehe Lokal an Lokal.

Local Area Network (LAN)
Ein Netz, das verschiedene Geräte in einem begrenzten Bereich (z. B. innerhalb eines Gebäudes oder auf einem Campus) miteinander verbindet und an ein größeres Netz angeschlossen werden kann.

Lokal an Fern (L2R)
Betrifft den internen Datenverkehr von einem lokalen Netz zu einem anderen fernen Netz.

Lokal an Lokal (L2L)
Betrifft den internen Datenverkehr von einem lokalen Netz zu einem anderen lokalen Netz.

L2R Siehe Lokal an Fern.

M

Magistrat
Eine interne Komponente, die den Datenaustausch im Netz sowie Sicherheitsereignisse mittels definierter angepasster Regeln analysiert.

N

NAT Siehe Netzadresskonvertierung (Network Address Translation).

NetFlow
Ein Cisco-Netzprotokoll, das die Daten des Netzverkehrsflusses überwacht. Zu diesen Daten gehören die Client- und Serverinformationen, welche Ports verwendet werden sowie die Anzahl der Byte und Pakete, die über die mit einem Netz verbundenen Switches und Router laufen. Die Daten werden an Netzdatenflusskollektoren gesendet und dort analysiert.

Netzebene
In der OSI-Architektur die Ebene, die Services bereitstellt, um zwischen offenen Systemen einen Pfad mit vorhersehbarer Servicequalität zu erstellen.

Netzgewicht
Auf jedes Netz angewendeter numerischer Wert, der den Stellenwert des Netzes angibt. Das Netzgewicht wird vom Benutzer definiert.

Netzhierarchie
Eine Art von Container als hierarchische Sammlung von Netzobjekten.

Netzobjekt
Eine Komponente einer Netzhierarchie.

Netzwerkadresskonvertierung (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 verwendet werden, werden maskiert.

Nummer des autonomen Systems (ASN)
In TCP/IP ist dies eine Zahl, die einem autonomen System von derselben zentralen Stelle zugewiesen wird, die auch IP-Adressen zuweist. Die Nummer des autonomen Systems ermöglicht es automatisierten Routingalgorithmen, autonome Systeme voneinander zu unterscheiden.

Nutzdaten
Anwendungsdaten, die in einem IP-Datenfluss enthalten sind, ohne Header und administrative Informationen.

O

Offsite-Quelle
Ein Gerät, das sich nicht am primären Standort befindet und das normalisierte Daten an einen Ereigniskollektor weiterleitet.

Offsite-Ziel
Ein Gerät, das sich nicht am primären Standort befindet und das Ereignis- oder Datenflüsse von einem Ereigniskollektor empfängt.

Open Source Vulnerability Database (OSVDB)
Erstellt von der Netzsicherheitscommunity für die Netzsicherheitscommunity. Eine Open Source-Datenbank, die technische Informationen zu Schwachstellen der Netzsicherheit liefert.

OSI Siehe Kommunikation offener Systeme.

OSVDB
Siehe Open Source Vulnerability Database.

P

Parsing-Reihenfolge
Eine Protokollquellendefinition, in der der Benutzer die Reihenfolge für Protokollquellen, die eine gemeinsame IP-Adresse oder einen gemeinsamen Hostnamen teilen, nach Bedeutung definieren kann.

Primärer Hochverfügbarkeitshost
Der Hauptcomputer, der mit dem Hochverfügbarkeitscluster verbunden ist.

Protokoll
Eine Reihe von Regeln, die die Kommunikation und die Übertragung von Daten zwischen mindestens zwei Geräten oder Systemen in einem Kommunikationsnetz steuern.

Protokollquelle
Entweder die Sicherheitsausrüstung oder die Netzausrüstung, aus der ein Ereignisprotokoll stammt.

Protokollquellenerweiterung
Eine XML-Datei, die alle regulären Ausdrucksmuster beinhaltet, die zur Identifikation und Kategorisierung von Ereignissen dieser Ereignisnutzdaten erforderlich sind.

Q

QID-Zuordnung
Taxonomie (Systematik), welche jedes eindeutige Ereignis identifiziert und die Ereignisse unter- und übergeordneten Kategorien zuordnet, um zu bestimmen, wie ein Ereignis korreliert und organisiert werden kann.

R

recon Siehe Ausspähung.

Referenzset
Eine Liste einzelner Elemente, die von Ereignissen oder Flüssen in einem Netz abgeleitet ist, beispielsweise eine Liste der IP-Adressen oder eine Liste der Benutzernamen.

Referenztabelle
Eine Tabelle, in der der Datensatz Schlüssel zuordnet, die über einen zugeordneten Typ für andere Schlüssel verfügen und danach einem einzelnen Wert zugeordnet werden.

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

Relevanz
Ein Maß der relativen Auswirkung eines Ereignisses, einer Kategorie oder eines Angriffs auf das Netz.

R2L Siehe Fern an Lokal.

R2R Siehe Fern an Fern.

S

Scanner
Ein automatisiertes Sicherheitsprogramm, das nach Softwareschwachstellen innerhalb von Webanwendungen sucht.

Schlüsseldatei
In der IT-Sicherheit eine Datei, die öffentliche Schlüssel, private Schlüssel, Trust-Roots und Zertifikate enthält.

Schwachstelle
Ein Sicherheitsrisiko in einer Betriebssystem-, Systemsoftware- oder einer Anwendungssoftwarekomponente.

Schweregrad
Kennzahl der relativen Sicherheitsbedrohung, die eine Quelle auf ein Ziel ausübt.

Sekundärer Hochverfügbarkeitshost
Der Standby-Computer, der mit dem Hochverfügbarkeitscluster verbunden ist. Sollte der primäre Hochverfügbarkeitshost ausfallen, übernimmt der sekundäre Hochverfügbarkeitshost dessen Verantwortung.

Simple Network Management Protocol (SNMP)
Eine Gruppe von Protokollen für die Überwachung von Systemen und Geräten in komplexen Netzen. Informationen zu den verwalteten Geräten werden in einer Management Information Base (MIB) definiert und gespeichert.

SNMP
Siehe Simple Network Management Protocol.

SOAP Ein einfaches XML-basiertes Protokoll für das Austauschen von Informationen in einer dezentralen, verteilten Umgebung. Mit SOAP können Informationen und Services im Internet abgefragt, zurückgegeben und aufgerufen werden.

Standby-System
Ein System, das automatisch aktiviert wird, wenn das aktive System ausfällt. Wenn die Datenträgerreplikation aktiviert ist, werden die Daten aus dem aktiven System repliziert.

Systemansicht
Eine visuelle Darstellung des primären und der verwalteten Hosts, aus denen sich ein System zusammensetzt.

T

TCP Siehe Transmission Control Protocol.

Teilnetz
Siehe Teilnetzwerk.

Teilnetzmaske
Für Internetteilnetze eine 32-Bit-Maske, die verwendet wird, um die Teilnetzadressbits im Hostteil einer IP-Adresse zu identifizieren.

Teilnetzwerk (Teilnetz)
Ein Netz, das in kleinere unabhängige Untergruppen unterteilt ist, die trotzdem miteinander verbunden sind.

Transmission Control Protocol (TCP)
Ein Übertragungsprotokoll, das im Internet sowie in allen Netzen verwendet wird, die die IETF-Standards (Internet Engineering Task Force) für netzübergreifende Protokolle verwenden. TCP ist ein zuverlässiges Host-to-Host-Protokoll in DFV-Netzen mit Paketvermittlung und Systemverbünden solcher Netze. Siehe auch Internet Protocol.

Truststore-Dateien
Eine Schlüsseldatei, die die öffentlichen Schlüssel für eine vertrauenswürdige Entität enthält.

U

Übergeordneter Datenfluss
Ein einzelner Datenfluss, der aus mehreren Datenflüssen mit ähnlichen Eigenschaften besteht, um die Verarbeitungskapazität durch Minderung der Speicherbeschränkungen zu erhöhen.

Unregelmäßigkeit
Eine Abweichung vom erwarteten Verhalten des Netzes.

Untergeordnete Suche
Eine Funktion, die ermöglicht, dass eine Suchabfrage in einer Gruppe bereits beendeter Suchergebnisse ausgeführt wird.

V

Verbindungsintervall
Das Intervall, in dem Ereignisse gebündelt werden. Dies geschieht alle 10 Sekunden und beginnt mit dem ersten Ereignis, das keinem aktuellen Verbindungsereignis

entspricht. Innerhalb des Verbindungsintervalls werden die ersten drei übereinstimmenden Ereignisse gebündelt und an den Ereignisprozessor gesendet.

Verhalten
Die überwachbaren Effekte einer Operation oder eines Ereignisses, einschließlich ihrer bzw. seiner Ergebnisse.

Verletzung
Vorgang, der eine unternehmensinterne Richtlinie übergeht oder dagegen verstößt.

Verschlüsselung
Bei der Computersicherheit der Prozess, durch den Daten in eine nicht verständliche Form umgewandelt werden, sodass die ursprünglichen Daten entweder gar nicht oder nur mithilfe eines Entschlüsselungsprozesses aufgerufen werden können.

Verweiszuordnung
Ein Datensatz der direkten Zuordnung eines Schlüsels zu einem Wert, beispielsweise ein Benutzername zu einer globalen ID.

Verweiszuordnung von Gruppen
Ein Datensatz eines Schlüssels, der vielen Werten zugeordnet ist, beispielsweise die Zuordnung einer Liste privilegierter Benutzer zu einem Host.

Verweiszuordnung von Zuordnungen
Ein Datensatz zweier Schlüssel, die vielen Werten zugeordnet sind, beispielsweise die Zuordnung der gesamten Bytes einer Anwendung zu einer Quellen-IP.

Virtuelle Cluster-IP-Adresse
Eine IP-Adresse, die vom primären oder sekundären Host und dem Cluster mit hoher Verfügbarkeit gemeinsam verwendet wird.

Vollständig qualifizierter Domänenname (FQDN)
In der Internetkommunikation der Name eines Hostsystems, der alle Teilnamen des Domänennamens beinhaltet. Ein Beispiel für einen vollständig qualifizierten Domänennamen ist "rchland.vnet.ibm.com".

Vollständig qualifizierter Netzname (FQNN)
In einer Netzhierarchie der Name eines Objekts, der alle Abteilungen enthält. Ein Beispiel eines vollständig qualifizierten Netznamens ist "UnternehmenA.vnet.Abteilung.Marketing".

W

Weiterleitungsregel
Bedingung, dass, wenn Ereignisdaten ihre Kriterien erfüllen, Bedingungen erfasst und entsprechend weitergeleitet werden.

Weiterleitungsziel
Mindestens ein Anbietersystem, das Rohdaten und normalisierte Daten aus Protokollquellen und Datenflussquellen empfängt.

whois-Server
Ein Server, mit dem Informationen zu registrierten Internetressourcen wie Zuordnungen von Domänennamen und IP-Adressen abgerufen werden.

Z

Zuverlässigkeit
Eine numerische Bewertung von 0-10, mit der die Integrität eines Ereignisses oder eines Angriffs bestimmt wird. Die Zuverlässigkeit nimmt zu, wenn mehrere Quellen dasselbe Ereignis bzw. denselben Angriff melden.

Index

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z