IBM Security QRadar SIEM
Version 7.1.0 (MR2)

Users Guide

IBM

Note: Before using this information and the product that it supports, read the information in "Notices and trademarks" on page 327.

CONTENTS

ABOUT THIS GUIDE

1 ABOUT QRADAR SIEM

2 DASHBOARD MANAGEMENT

3 OFFENSE MANAGEMENT

4 LOG ACTIVITY INVESTIGATION

5 NETWORK ACTIVITY INVESTIGATION

6 CHART MANAGEMENT

7 DATA SEARCHES

10 ASSET MANAGEMENT

11 REPORTS MANAGEMENT

A RULE TESTS

ABOUT THIS GUIDE

The *IBM Security QRadar SIEM Users Guide* provides information on managing IBM Security QRadar SIEM including the **Dashboard**, **Offenses**, **Log Activity**, **Network Activity**, **Assets**, and **Reports** tabs.

Intended audience

This guide is intended for all QRadar SIEM users responsible for investigating and managing network security. This guide assumes that you have QRadar SIEM access and a knowledge of your corporate network and networking technologies.

Conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION:*Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING:*Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation

For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

Contacting customer support

For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)

1 About QRadar SIEM

QRadar SIEM is a network security management platform that provides situational awareness and compliance support through the combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment.

Supported web browsers

You can access the Console from a standard web browser. QRadar SIEM supports certain versions of Mozilla Firefox and Microsoft Internet Explorer web browsers.

When you access the system, a prompt is displayed asking for a user name and a password. The user name and password must be configured in advance by the QRadar SIEM administrator.

Table 1-1 Supported web browsers

Web browser	Supported versions
Mozilla Firefox	10.0 Due to Mozilla's short release cycle, we cannot commit to testing on the latest versions of the Mozilla Firefox browser. However, we are fully committed to investigating any issues that are reported.
Microsoft® Windows Internet Explorer, with Compatibility View Enabled	• 8.0 • 9.0 For instructions on how to enable Compatibility View, see **Enabling Compatibility View for Internet Explorer**.

Enabling Compatibility View for Internet Explorer

You need to enable compatibility view if you use the Microsoft Internet Explorer web browser to access QRadar SIEM.

Procedure

Step 1 In your Microsoft Internet Explorer web browser, press F12 to open the Developer Tools window.

Step 2 To configure browser mode, from the **Browser Mode** list box, select the version of your web browser.

Step 3 To configure document mode, from the **Document Mode** list box, select **Internet Explorer 7.0 Standards**.

Logging in to QRadar SIEM

QRadar SIEM is a web-based application. To log in to QRadar SIEM, you must use the Mozilla Firefox or Microsoft Internet Explorer web browsers.

For more information on supported web browsers, see **Supported web browsers**.

About this task

If you are using the Mozilla Firefox web browser, you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla Firefox web browser documentation.

If you are using the Microsoft Internet Explorer web browser, a website security certificate message is displayed when you access the QRadar SIEM system. You must select the **Continue to this website** option to log in to QRadar SIEM.

Procedure

Step 1 Open your web browser.

Step 2 Type the following address in the address bar:

https://`<IP Address>`

Where **`<IP Address>`** is the IP address of the QRadar SIEM system.

Step 3 Type your user name and password.

Step 4 Click **Login To QRadar**.

Step 5 To log out of QRadar SIEM, click **Log out** in the top right corner of the user interface.

Result

A default license key provides you access to the user interface for five weeks. A window is displayed, providing the date that the temporary license key expires. For more information about installing a license key, see the *IBM Security QRadar SIEM Administration Guide*.

When navigating QRadar SIEM, do not use the browser **Back** button. Use the navigation options available with QRadar SIEM to navigate the user interface.

User interface tabs

QRadar SIEM divides functionality in tabs. The Dashboard tab is displayed when you log in to QRadar SIEM. You can easily navigate the tabs to locate the data or functionality you require.

Dashboard tab

The **Dashboard** tab is the default tab that is displayed when you log in to QRadar SIEM. It provides a workspace environment that supports multiple dashboards on which you can display your views of network security, activity, or data that QRadar SIEM collects. Five default dashboards are available. Each dashboard contains items that provide summary and detailed information about offenses occurring on your network. You can also create a custom dashboard to enable you to focus on your security or network operations responsibilities.

For more information about using the **Dashboard** tab, see **Dashboard management**.

Offenses tab

The **Offenses** tab allows you to view offenses occurring on your network, which you can locate using various navigation options or through powerful searches. From the **Offenses** tab, you can investigate an offense to determine the root cause of an issue. You can also resolve the issue.

For more information about **Offenses** tab, see **Offense management**.

Log Activity tab

The **Log Activity** tab allows you to investigate event logs being sent to QRadar SIEM in real-time, perform powerful searches, and view log activity using configurable time-series charts. The **Log Activity** tab allows you to perform in-depth investigations on event data.

For more information, see **Log activity investigation**.

Network Activity tab

The **Network Activity** tab allows you to investigate flows being sent to QRadar SIEM in real-time, perform powerful searches, and view network activity using configurable time-series charts. A flow is a communication session between two hosts. Viewing flow information allows you to determine how the traffic is communicated, what is communicated (if the content capture option is enabled), and who is communicating. Flow data also includes details such as protocols, ASN values, IFIndex values, and priorities.

For more information, see **Network activity investigation**.

Assets tab

QRadar SIEM automatically discovers assets (servers and hosts) operating on your network, based on passive flow data and vulnerability data, allowing QRadar SIEM to build an asset profile. Asset profiles provide information about each known asset in your network, including identity information (if available) and what services are running on each asset. This profile data is used for correlation purposes to help reduce false positives. For example, if an attack tries to exploit a specific service running on a specific asset, QRadar SIEM can determine if the asset is vulnerable to this attack by correlating the attack to the asset profile. Using the **Assets** tab, you can view the learned assets or search for specific assets to view their profiles.

For more information, see **Asset management**.

Reports tab

The **Reports** tab allows you to create, distribute, and manage reports for any data within QRadar SIEM. The Reports feature allows you to create customized reports for operational and executive use. To create a report, you can combine information (such as, security or network) into a single report. You can also use pre-installed report templates that are included with QRadar SIEM.

The **Reports** tab also allows you to brand your reports with customized logos. This is beneficial for distributing reports to different audiences.

For more information about reports, see **Reports management**.

IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager is a separately installed appliance for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network. IBM Security QRadar Risk Manager uses data collected by 7.1.0 (MR1), configuration data from network and security devices (firewalls, routers, switches, or IPSs), vulnerability feeds, and vendor security sources to identify security, policy, and compliances risks within your network security infrastructure and the probability of those risks being exploited.

Note: For more information about IBM Security QRadar Risk Manager, contact your local sales representative.

Admin tab

If you have administrative privileges, you can access the **Admin** tab. The **Admin** tab gives administrative users access to administrative functionality, including:

- **System Configuration** - Allows you to configure system and user management options.
- **Data Sources** - Allows you to configure log sources, flow sources, and vulnerability options.
- **Remote Networks and Services Configuration** - Allows you to configure remote networks and services groups.
- **Plug-ins** - Provides access to plug-in components, such as the IBM Security QRadar Risk Manager plug-in. This option is only displayed if there are plug-ins installed on your Console.
- **Deployment Editor** - Allows you to manage the individual components of your QRadar SIEM deployment.

All configuration updates you make in the **Admin** tab are saved to a staging area. When all changes are complete, you can deploy the configuration updates to the managed host in your deployment.

For more information regarding the **Admin** tab, see the *IBM Security QRadar SIEM Administration Guide*.

QRadar SIEM common procedures

Various controls on the QRadar SIEM user interface are common to most user interface tabs. This section provides information on these common procedures.

Viewing messages

The Messages menu, which is located on the top right corner of the user interface, provides access to a window in which you can read and manage your system notifications.

Before you begin

For system notifications to show on the Messages window, the Administrator must create a rule based on each notification message type and select the **Notify** check box in the Custom Rules Wizard. For more information about how to configure event notifications and create event rules, see the *IBM Security QRadar SIEM Administration Guid*e.

About this task

The Messages menu indicates how many unread system notifications you have in your system. This indicator increments the number until you dismiss system notifications. For each system notification, the Messages window provides a summary and the date stamp for when the system notification was created. You can hover your mouse pointer over a notification to view more detail. Using the functions on the Messages window, you can manage the system notifications.

System notifications are also available on the **Dashboard** tab and on an optional pop-up window that can be displayed on the lower left corner of the user interface. Actions that you perform in the Messages window are propagated to the **Dashboard** tab and the pop-up window. For example, if you dismiss a system notification from the Messages window, the system notification is removed from all system notification displays. For more information on Dashboard system notifications, see **System Notifications item**.

The Messages window provides the following functions:

Table 1-2 Messages window functions

Function	Description
All	Click **All** to view all system notifications. This is the default option, therefore, you only need to click **All** if you have selected another option and want to display all system notifications again.
Health	Click **Health** to view only system notifications that have a severity level of Health.
Errors	Click **Errors** to view only system notifications that have a severity level of Error.
Warnings	Click **Warnings** to view only the system notifications that have a severity level of Warning.

Table 1-2 Messages window functions

Function	Description
Information	Click **Information** to view only the system notifications that have a severity level of Information.
Dismiss All	Click **Dismiss All** to dismiss all system notifications from your system. If you have filtered the list of system notifications using the **Health**, **Errors**, **Warnings**, or **Information** icons, the text on the **View All** icon changes to one of the following options: • Dismiss All Errors • Dismiss All Health • Dismiss All Warnings • Dismiss All Info
View All	Click **View All** to view the system notification events in the **Log Activity** tab. If you have filtered the list of system notifications using the **Health**, **Errors**, **Warnings**, or **Information** icons, the text on the **View All** icon changes to one of the following options: • View All Errors • View All Health • View All Warnings • View All Info
Dismiss	Click the **Dismiss** icon beside a system notification to dismiss the system notification from your system.

When you click a notification, the following system notification details are displayed in a pop-up window:

Table 1-3 System notification details

Parameter	Description
Flag	Displays a symbol to indicate severity level of the notification. Point your mouse over the symbol to view more detail about the severity level. • Information icon (i) • Error icon (X) • Warning icon (!) • Health icon
Host IP	Displays the host IP address of the host that originated this system notification.
Severity	Displays the severity level of the incident that created this system notification.

Table 1-3 System notification details

Parameter	Description
Low Level Category	Displays the low-level category associated with the incident that generated this system notification. For example: Service Disruption. For more information on categories, see the *IBM Security QRadar SIEM Administration Guide*.
Payload	Displays the payload content associated with the incident that generated this system notification.
Created	Displays the amount of time that has elapsed since the system notification was created.

Procedure

Step 1 Log in to QRadar SIEM.

Step 2 On the top right corner of the user interface, click **Messages**.

Step 3 On the Messages window, view the system notification details.

Step 4 Optional. To refine the list of system notifications, click one of the following options:

- Errors
- Warnings
- Information

Step 5 Optional. To dismiss system notifications, choose of the following options:

- To dismiss all system notifications, click **Dismiss All**.
- To dismiss one system notification, click the **Dismiss** icon next to the system notification you want to dismiss.

Step 6 Optional. To view the system notification details, hover your mouse pointer over the system notification.

Sorting results

On the **Log Activity**, **Offenses**, **Network Activity**, and **Reports** tabs, you can sort tables by clicking on a column heading. An arrow at the top of the column indicates the direction of the sort.

Procedure

Step 1 Log in to QRadar SIEM.

Step 2 Click the tab you want to view:

Step 3 Choose one of the following options:

- Click the column header once to sort the table in descending order
- Click the column header twice to sort the table in ascending order.

Refreshing and pausing the user interface

The **Dashboard**, **Log Activity**, **Offenses**, and **Network Activity** tabs allow you to manually refresh, pause, and play the data displayed on the tab.

About this task

The **Dashboard** and **Offenses** tabs automatically refresh every 60 seconds. The **Log Activity** and **Network Activity** tabs automatically refresh every 60 seconds if you are viewing the tab in Last Interval (auto refresh) mode. The timer, located at the top right corner of the interface, indicates the amount of time until the tab is automatically refreshed.

When you view the **Log Activity** or **Network Activity** tab in Real Time (streaming) or Last Minute (auto refresh) mode, you can use the **Pause** icon to pause the current display.

You can also pause the current display in the **Dashboard** tab. Clicking anywhere inside a dashboard item automatically pauses the tab. The timer flashes red to indicate the current display is paused.

Procedure

Step 1 Log in to QRadar SIEM.

Step 2 Click the tab you want to view.

Step 3 Choose one of the following options:

- To refresh the tab, click the **Refresh** icon located in the right corner of the tab.
- To pause the display on the tab, click the **Pause** icon.
- If the time is paused, click the **Play** icon to restart the timer.

Investigating IP addresses

The **Dashboard**, **Log Activity**, **Offenses**, and **Network Activity** tabs provide several methods to investigate an IP address from the user interface.

About this task

If geographic information is available for an IP address, the country is visually indicated by a flag.

The right-click menu provides options for you to investigate an IP address. You can add custom right-click options to the menu. For more information on how to customize the right-click menu, see the *Customizing the Right-Click Menu Technical Note*.

Procedure

Step 1 Log in to QRadar SIEM.

Step 2 Click the tab you want to view.

Step 3 Move your mouse pointer over an IP address to view the location of the IP address.

Step 4 Right-click the IP address or asset name and select one of the following options:

Option	Description
Navigate > View by Network	Displays the List of Networks window, which displays all networks associated with the selected IP address.
Navigate > View Source Summary	Displays the List of offenses window, which displays all offenses associated with the selected source IP address.
Navigate > View Destination Summary	Displays the List of Offenses window, which displays all offenses associated to the selected destination IP address.
Information > DNS Lookup	Searches for DNS entries based on the IP address.
Information > WHOIS Lookup	Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net.
Information > Port Scan	Performs a Network Mapper (NMAP) scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information about installing NMAP, see your vendor documentation.
Information > Asset Profile	Displays asset profile information. This menu option is only available when QRadar SIEM has acquired profile data either actively through a scan or passively through flow sources. For information, see the *IBM Security QRadar SIEM Administration Guide.*
Information > Search Events	Select the **Search Events** option to search events associated with this IP address. For information, see **Searching events or flows**.
Information > Search Flows	Select the **Search Flows** option to search for flows associated with this IP address. For information, see **Searching events or flows**.
Information > Search Connections	Select the **Search Connections** option to search for connections associated with this IP address. This option is only displayed when IBM Security QRadar Risk Manager has been purchased and licensed, and you have established the connection between the Console and the IBM Security QRadar Risk Manager appliance. For more information, see the *IBM Security QRadar Risk Manager Users Guide.*
Information > Switch Port Lookup	Select the **Switch Port Lookup** to determine the switch port on a Cisco IOS device for this IP address. This option only applies to switches discovered using the Discover Devices option on the **IBM Security QRadar Risk Manager** tab. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.

Option	Description
Information > View Topology	Select the **View Topology** option to view the **IBM Security QRadar Risk Manager Topology** tab, which depicts the layer 3 topology of your network. This option is only displayed when IBM Security QRadar Risk Manager has been purchased and licensed, and you have established the connection between the Console and the IBM Security QRadar Risk Manager appliance. For more information, see the *IBM Security QRadar Risk Manager Users Guide.*

Investigating user names

Right-click a user name to access additional menu options, which allow you to further investigate that user name or IP address.

The menu options include:

Option	Description
View Assets	Displays the Assets Lists window, which displays current assets associated to the selected user name. For more information about viewing assets, see **Asset management**.
View User History	Displays the Assets Lists window, which displays all assets associated to the selected user name over the previous 24 hours. For more information about viewing assets, see **Asset management**.
View Events	Displays the List of Events window, which displays the events associated to the selected user name. For more information about the List of Events window, see **Log activity monitoring**.

Note: For more information about customizing the right-click menu, see the *Customizing the Right-Click Menu* Technical Note.

System time

The right corner of the QRadar SIEM user interface displays system time, which is the time on the Console. The Console time synchronizes all QRadar SIEM systems within the QRadar SIEM deployment, and is used to determine what time events were received from other devices for proper time synchronization correlation.

In a distributed deployment, the Console might be located in a different time zone from your desktop computer. When you apply time-based filters and searches on the **Log Activity** and **Network Activity** tabs, you must use the Console System Time when specifying a time range.

Updating user details

You can update your user details through the main QRadar SIEM user interface.

Procedure

Step 1 To access your user information, click **Preferences**.

Step 2 As required, update the following parameters:

Options	Description
Username	Displays your user name. This field is not editable
Password	Type a new password. The password must meet the following criteria: • Minimum of six characters • Maximum of 255 characters • Contain at least one special character • Contain one uppercase character
Password (Confirm)	Type the password again for confirmation.
Email Address	Type your email address. The email address must meet the following requirements: • Valid email address • Minimum of 10 characters • Maximum of 255 characters
Enable Popup Notifications	Select this check box if you want to enable popup system notifications to be displayed on your user interface.

Accessing Online Help

You can access the QRadar SIEM Online Help through the main QRadar SIEM user interface. To access the Online Help, click **Help > Help Contents**.

Resizing columns

Several QRadar SIEM tabs, including the **Offenses**, **Log Activity**, **Network Activity**, **Assets**, and **Reports** tabs allow you to resize the columns of the display. Place the pointer of your mouse over the line that separates the columns and drag the edge of the column to the new location. You can also resize columns by double-clicking the line that separates the columns to automatically resize the column to the width of the largest field.

Note: Column resizing does not function in Internet Explorer 7.0 while the **Log Activity** or **Network Activity** tabs are displaying records in streaming mode.

Configuring page size

In the **Offenses**, **Assets**, **Log Activity**, **Network Activity**, and **Reports** tab tables, QRadar SIEM displays a maximum of 40 results by default. If you have administrative privileges, you can configure the maximum number of results using the **Admin** tab. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

2 DASHBOARD MANAGEMENT

The **Dashboard** tab is the default view when you log into QRadar SIEM. It provides a workspace environment that supports multiple dashboards on which you can display your views of network security, activity, or data that QRadar SIEM collects.

Dashboard overview

Dashboards allow you to organize your dashboard items into functional views, which enables you to focus on specific areas of your network.

Default dashboards

The **Dashboard** tab provides five default dashboards focused on security, network activity, application activity, system monitoring, and compliance. Each dashboard displays a default set of dashboard items. The dashboard items act as launch points to navigate to more detailed data.

The following table defines the default dashboards.

Table 2-1 Default dashboards

Default dashboard	Items
Application Overview	The **Application Overview** dashboard includes the following default items: • Inbound Traffic by Country (Total Bytes) • Outbound Traffic by Country (Total Bytes) • Top Applications (Total Bytes) • Top Applications Inbound from Internet (Total Bytes) • Top Applications Outbound to the Internet (Total Bytes) • Top Services Denied through Firewalls (Event Count) • DSCP - Precedence (Total Bytes)

Table 2-1 Default dashboards (continued)

Default dashboard	**Items**
Compliance Overview	The **Compliance Overview** dashboard includes the following default items: • Top Authentications by User (Time Series) • Top Authentication Failures by User (Event Count) • Login Failures by User (real-time) • Compliance: Username Involved in Compliance Rules (time series) • Compliance: Source IPs Involved in Compliance Rules (time series) • Most Recent Reports
Network Overview	The **Network Overview** dashboard includes the following default items: • Top Talkers (real time) • ICMP Type/Code (Total Packets) • Top Networks by Traffic Volume (Total Bytes) • Firewall Deny by DST Port (Event Count) • Firewall Deny by DST IP (Event Count) • Firewall Deny by SRC IP (Event Count) • Top Applications (Total Bytes) • Link Utilization (real-time) • DSCP - Precedence (Total Bytes)
System Monitoring	The **System Monitoring** dashboard includes the following default items: • Top Log Sources (Event Count) • Link Utilization (real-time) • System Notifications • Event Processor Distribution (Event Count) • Event Rate (Events per Second Coalesced - Average 1 Min) • Flow Rate (Flows per Second - Peak 1 Min)

Table 2-1 Default dashboards (continued)

Default dashboard	**Items**
Threat and Security Monitoring	The **Threat and Security Monitoring** dashboard includes the following default items: • Default-IDS/IPS-All: Top Alarm Signatures (real-time) • Top Systems Attacked (Event Count) • Top Systems Sourcing Attacks (Event Count) • My Offenses • Most Severe Offenses • Most Recent Offenses • Top Services Denied through Firewalls (Event Count) • Internet Threat Information Center • Flow Bias (Total Bytes) • Top Category Types • Top Sources • Top Local Destinations

Custom dashboards

You can customize your dashboards. The content displayed on the **Dashboard** tab is user-specific. Changes made within a QRadar SIEM session affect only your system.

To customize your **Dashboard** tab, you can perform the following tasks:

- Create custom dashboards that are relevant to your responsibilities. QRadar SIEM supports up to 255 dashboards per user; however, performance issues might occur if you create more than 10 dashboards.
- Add and remove dashboard items from default or custom dashboards.
- Move and position items to meet your requirements. When you position items, each item automatically resizes in proportion to the dashboard.
- Add custom dashboard items based on any data.

  For example, you can add a dashboard item that provides a time series graph or a bar chart that represents top 10 network activity.

  To create custom items, you can create saved searches on the **Network Activity** or **Log Activity** tabs and choose how you want the results represented in your dashboard. Each dashboard chart displays real-time up-to-the-minute data. Time series graphs on the dashboard refresh every 5 minutes.

Available dashboard items

QRadar SIEM allows you to add dashboard items to your default or custom dashboards.

The following dashboard item categories are available:

- **Flow search items**
- **Offense items**
- **Log Activity items**
- **Most Recent Reports items**
- **Risk Manager items**
- **System Summary item**
- **System Notifications item**
- **Internet Threat Information Center**
- **Adding search-based dashboard items to the Add Items list**

Flow search items

You can display a custom dashboard item based on saved search criteria from the **Network Activity** tab. Flow search items are listed in the **Add Item > Network Activity > Flow Searches** menu. The name of the flow search item matches the name of the saved search criteria the item is based on.

QRadar SIEM includes default saved search criteria that is preconfigured to display flow search items on your **Dashboard** tab menu. You can add more flow search dashboard items to your **Dashboard** tab menu. For more information. **Adding search-based dashboard items to the Add Items list**.

On a flow search dashboard item, search results display real-time last minute data on a chart. The supported chart types are time series, table, pie, and bar. The default chart type is bar. These charts are configurable. For more information about chart configuration, see **Configuring charts**.

Time series charts are interactive. You can magnify and scan through a timeline to investigate network activity.

Offense items

You can add several offense-related items to your dashboard.

Note: Hidden or closed offenses are not included in the values that are displayed in the **Dashboard** tab. For more information on hidden or closed events, see **Offense management**.

The following table describes the Offense items:

Table 2-2 Offense items

Dashboard item	Description
Most Recent Offenses	The five most recent offenses are identified with a magnitude bar to inform you of the importance of the offense. Point your mouse over the offense name to view detailed information for the IP address.
Most Severe Offenses	The five most severe offenses are identified with a magnitude bar to inform you of the importance of the offense. Point your mouse over the offense name to view detailed information for the IP address.
My Offenses	The **My Offenses** item displays five of the most recent offenses assigned to you. The offenses are identified with a magnitude bar to inform you of the importance of the offense. Point your mouse over the IP address to view detailed information for the IP address.
Top Sources	The **Top Sources** item displays the top offense sources. Each source is identified with a magnitude bar to inform you of the importance of the source. Point your mouse over the IP address to view detailed information for the IP address.
Top Local Destinations	The **Top Local Destinations** item displays the top local destinations. Each destination is identified with a magnitude bar to inform you of the importance of the destination. Point your mouse over the IP address to view detailed information for the IP address.
Categories	The **Top Categories Types** item displays the top five categories associated with the highest number of offenses.

Log Activity items

The Log Activity dashboard items allow you to monitor and investigate events in real-time.

Note: Hidden or closed events are not included in the values that are displayed in the **Dashboard** tab.

The following table describes the Log Activity items:

Table 2-3 Log activity items

Dashboard item	Description
Event Searches	You can display a custom dashboard item based on saved search criteria from the **Log Activity** tab. Event search items are listed in the **Add Item > Network Activity > Event Searches** menu. The name of the event search item matches the name of the saved search criteria the item is based on. QRadar SIEM includes default saved search criteria that is preconfigured to display event search items on your **Dashboard** tab menu. You can add more event search dashboard items to your **Dashboard** tab menu. For more information, see **Adding search-based dashboard items to the Add Items list**. On a **Log Activity** dashboard item, search results display real-time last minute data on a chart. The supported chart types are time series, table, pie, and bar. The default chart type is bar. These charts are configurable. For more information about chart configuration, see **Configuring charts**. Time series charts are interactive. You can magnify and scan through a timeline to investigate log activity.
Events By Severity	The **Events By Severity** dashboard item displays the number of active events grouped by severity. This item allows you to see the number of events that are received by the level of severity that has been assigned. Severity indicates the amount of threat an offense source poses in relation to how prepared the destination is for the attack. The range of severity is 0 (low) to 10 (high). The supported chart types are Table, Pie, and Bar.
Top Log Sources	The **Top Log Sources** dashboard item displays the top five log sources that sent events to QRadar SIEM within the last 5 minutes. The number of events sent from the specified log source is indicated in the pie chart. This item allows you to view potential changes in behavior, for example, if a firewall log source that is typically not in the top 10 list now contributes to a large percentage of the overall message count, you should investigate this occurrence. The supported chart types are Table, Pie, and Bar.

Most Recent Reports items

The **Most Recent Reports** dashboard item displays the top recently generated reports. The display provides the report title, the time and date the report was generated, and the format of the report.

System Summary item

The **System Summary** dashboard item provides a high-level summary of activity within the past 24 hours. Within the summary item, you can view the following information:

- **Current Flows Per Second** - Displays the flow rate per second.
- **Flows (Past 24 Hours)** - Displays the total number of active flows seen within the last 24 hours.

- **Current Events Per Second** - Displays the event rate per second.
- **New Events (Past 24 Hours)** - Displays the total number of new events received within the last 24 hours.
- **Updated Offenses (Past 24 Hours)** - Displays the total number of offenses that have been either created or modified with new evidence within the last 24 hours.
- **Data Reduction Ratio** - Displays the ratio of data reduced based on the total events detected within the last 24 hours and the number of modified offenses within the last 24 hours.

Risk Manager items

Risk Manager dashboard items are only displayed when IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.

You can display a custom dashboard item based on saved search criteria from the **Risks** tab. Connection search items are listed in the **Add Item > Risk Manager> Connection Searches** menu. The name of the connection search item matches the name of the saved search criteria the item is based on.

QRadar SIEM includes default saved search criteria that is preconfigured to display connection search items on your **Dashboard** tab menu. You can add more connection search dashboard items to your **Dashboard** tab menu. For more information. **Adding search-based dashboard items to the Add Items list**.

On a connections search dashboard item, search results display real-time last minute data on a chart. The supported chart types are time series, table, pie, and bar. The default chart type is bar. These charts are configurable. For more information about chart configuration, see **Configuring charts**.

Time series charts are interactive. You can magnify and scan through a timeline to investigate log activity.

System Notifications item

The **Systems Notification** dashboard item displays event notifications your system receives. For notifications to show in the **System Notification** dashboard item, the Administrator must create a rule based on each notification message type and select the **Notify** check box in the Custom Rules Wizard. For more information about how to configure event notifications and create event rules, see the *IBM Security QRadar SIEM Administration Guid*e.

On the **System Notifications** dashboard item, you can view the following information:

- **Flag** - Displays a symbol to indicate severity level of the notification. Point your mouse over the symbol to view more detail about the severity level.
  - **Health** icon
  - **Information** icon (?)

  - **Error** icon (X)
  - **Warning** icon (!)
- **Created** - Displays the amount of time that has elapsed since the notification was created.
- **Description** - Displays information about the notification.
- **Dismiss icon (x)**- Allows you to dismiss a system notification.

You can point your mouse over a notification to view more details:

- **Host IP** - Displays the host IP address of the host that originated the notification.
- **Severity** - Displays the severity level of the incident that created this notification.
- **Low Level Category** - Displays the low-level category associated with the incident that generated this notification. For example: Service Disruption. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
- **Payload** - Displays the payload content associated with the incident that generated this notification.
- **Created** - Displays the amount of time that has elapsed since the notification was created.

When you add the **System Notifications** dashboard item, system notifications can also display as pop-up notifications in the QRadar SIEM user interface. These pop-up notifications are displayed in the lower right corner of the user interface, regardless of the selected tab.

Pop-up notifications are only available for users with administrative permissions and are enabled by default. To disable pop-up notifications, select **User Preferences** and clear the **Enable Pop-up Notifications** check box. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

In the System Notifications pop-up window, the number of notifications in the queue is highlighted. For example, if (1 to 12) is displayed in the header, the current notification is 1 of 12 notifications to be displayed.

The system notification pop-up window provides the following options:

- **Next icon (>)** - Displays the next notification message. For example, if the current notification message is 3 of 6, click the icon to view 4 of 6.
- **Close icon (X)** - Closes this notification pop-up window.
- **(details)** - Displays additional information about this system notification.

Internet Threat Information Center

The Internet Threat Information Center dashboard item is an embedded RSS feed that provides you with up-to-date advisories on security issues, daily threat assessments, security news, and threat repositories.

The Current Threat Level diagram indicates the current threat level and provides a link to the Current Internet Threat Level page of the IBM Internet Security Systems website.

Current advisories are listed in the dashboard item. To view a summary of the advisory, click the Arrow icon next to the advisory. The advisory expands to display a summary. Click the Arrow icon again to hide the summary.

To investigate the full advisory, click the associated link. The IBM Internet Security Systems website opens in another browser window and displays the full advisory details.

Dashboard management tasks

On the **Dashboard** tab, you can customize your dashboards to display and organize the dashboards items that meet your network security requirements.

Viewing a dashboard

QRadar SIEM provides five default dashboards, which you can access from the **Show Dashboard** list box. If you have previously viewed a dashboard and have returned to the **Dashboard** tab, the last dashboard you viewed is displayed.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the **Show Dashboard** list box, select the dashboard you want to view.

Creating a custom dashboard

You can create a custom dashboard to enable you to view a group of dashboard items that meet a particular requirement.

About this task

After you create a custom dashboard, the new dashboard is displayed in the **Dashboard** tab and is listed in the **Show Dashboard** list box. A new custom dashboard is empty by default; therefore, you must add items to the dashboard. For more information about available dashboard items, see **Available dashboard items**.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 Click the **New Dashboard** icon.

Step 3 In the **Name** field, type a unique name for the dashboard.

The maximum length is 65 characters.

Step 4 In the **Description** field, type a description of the dashboard.

The maximum length is 255 characters. This description is displayed in the tooltip for the dashboard name in the **Show Dashboard** list box.

Step 5 Click **OK**.

Step 6 For each item that you want to add, select an item from **Add Item** list box.

Investigating log or network activity from a dashboard item

You can investigate log or network activity from a dashboard item. Search-based dashboard items provide a link to the **Log Activity** or **Network Activity** tabs. For more information on dashboard items, see **Available dashboard items**.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 Choose one of the following options:

- Click the **View in Log Activity** link.
- Click the **View in Network Activity** link.

Result

When you open the **Log Activity** or **Network Activity** tab from the **Dashboard** tab, the data and two charts that match the parameters of your dashboard item are displayed. The chart types displayed on the **Log activity** or **Network Activity** tab depend on which chart is configured in the dashboard item:

- **Bar, Pie, and Table** - The **Log Activity** or **Network Activity** tab displays a bar chart, pie chart, and table of flow details.
- **Time Series** - The **Log Activity** or **Network Activity** tab displays charts according to the following criteria:
  - If your time range is less than or equal to 1 hour, a time series chart, a bar chart, and a table of event or flow details are displayed.
  - If your time range is more than 1 hour, a time series chart is displayed and you are prompted to click **Update Details**. This action starts the search that populates the event or flow details and generates the bar chart. When the search completes, the bar chart and table of event or flow details are displayed.

Configuring charts

You can configure **Log Activity**, **Network Activity**, and **Connections** (if applicable) dashboard items to specify the chart type and how many data objects you want to view. Your custom chart configurations are retained, so that they are displayed as configured each time you access the **Dashboard** tab.

About this task

QRadar SIEM accumulates data so that when you perform a time series saved search, there is a cache of event or flow data available to display the data for the previous time period. Accumulated parameters are indicated by an asterisk (*) in the **Value to Graph** list box. If you select a value to graph that is not accumulated (no asterisk), time series data is not available.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the **Show Dashboard** list box, select the dashboard that contains the item you want to customize.

Step 3 On the header of the dashboard item you want to configure, click the **Settings** icon.

Step 4 Configure the following parameters:

Option	**Description**
Value to Graph	From the list box, select the object type that you want to graph on the chart. Options include all normalized and custom event or flow parameters included in your search parameters.
Chart Type	From the list box, select the chart type you want to view. Options include: • **Bar Chart** - Displays data in a bar chart. This option is only available for grouped events or flows. • **Pie Chart** - Displays data in a pie chart. This option is only available for grouped events or flows. • **Table** - Displays data in a table. This option is only available for grouped events or flows. • **Time Series** - Displays an interactive line chart that represents the records matched by a specified time interval.
Display Top	From the list box, select the number of objects you want you view in the chart. Options include 5 and 10. The default is 10.
Capture Time Series Data	Select this check box to enable time series capture. When you select this check box, the chart feature begins to accumulate data for time series charts. By default, this option is disabled. ***Note:*** *This option is only available on time series charts. You must have the appropriate role permissions to manage and view time series charts. For more information about role permissions, see the IBM Security QRadar SIEM Administration Guide.*
Time Range	From the list box, select the time range you want to view. ***Note:*** *This option is only available on time series charts. You must have the appropriate role permissions to manage and view time series charts. For more information about role permissions, see the IBM Security QRadar SIEM Administration Guide.*

Removing items

You can remove items from a dashboard. When you remove an item from the dashboard, the item is not removed from QRadar SIEM completely. You can add the item again at any time.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the **Show Dashboard** list box, select the dashboard from which you want to remove an item.

Step 3 On the dashboard item header, click the red [x] icon to remove the item from the dashboard.

Detaching an item

You can detach the item from your dashboard and display the item in a new window on your desktop system.

When you detach a dashboard item, the original dashboard item remains on the **Dashboard** tab, while a detached window with a duplicate dashboard item remains open and refreshes during scheduled intervals. If you close the QRadar SIEM application, the detached window remains open for monitoring and continues to refresh until you manually close the window or shut down your computer system.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the **Show Dashboard** list box, select the dashboard from which you want to detach an item.

Step 3 On the dashboard item header, click the green icon to detach the dashboard item and open it in separate window.

Renaming a dashboard

You can rename a dashboard and update the description.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the **Show Dashboard** list box, select the dashboard you want to edit.

Step 3 On the toolbar, click the **Rename Dashboard** icon.

Step 4 In the **Name** field, type a new name for the dashboard. The maximum length is 65 characters.

Step 5 In the **Description** field, type a new description of the dashboard. The maximum length is 255 characters.hol

Step 6 Click **OK**.

Deleting a dashboard

You can delete a dashboard. After you delete a dashboard, the **Dashboard** tab refreshes and the first dashboard listed in the **Show Dashboard** list box is displayed. The dashboard you deleted is no longer displayed in the **Show Dashboard** list box.

Procedure

Step 1 Click the **Dashboard** tab.

Step 2 From the **Show Dashboard** list box, select the dashboard you want to delete.

Step 3 On the toolbar, click **Delete Dashboard**.

Step 4 Click **Yes**.

Managing system notifications

You can specify the number of notifications that you want to display on your **System Notification** dashboard item and dismiss system notifications after you read them.

Before you begin

Ensure the **System Notification** dashboard item is added to your dashboard. For more information, see **Creating a custom dashboard**.

Procedure

Step 1 On the System Notification dashboard item header, click the **Settings** icon.

Step 2 From the **Display** list box, select the number of system notifications you want to view.

The options are **5**, **10** (default), **20**, **50**, and **All**.

To view all system notifications logged in the past 24 hours, click **All**. A window is displayed that includes all system notifications. For more information on events, see **Log activity investigation**.

Step 3 To dismiss a system notification, click the **Delete** icon.

Adding search-based dashboard items to the Add Items list

From the **Log Activity** and **Network Activity** tabs, you can add search-based dashboard items to your **Add Items** menu.

About this task

This procedure applies to all search-based dashboard items, including Risk Manager dashboard items. Risk Manager dashboard items are only displayed when IBM Security QRadar Risk Manager has been purchased and licensed, and you have established the connection between the Console and the IBM Security QRadar Risk Manager appliance. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.

Before you begin

To add an event and flow search dashboard item to the **Add Item** menu on the **Dashboard** tab, you must access the **Log Activity** or **Network Activity** tab to create search criteria that specifies that the search results can be displayed on the

Dashboard tab. The search criteria must also specify that the results are grouped on a parameter.

Procedure

Step 1 Choose one of the following options:

- To add a flow search dashboard item, click the **Network Activity** tab.
- To add an event search dashboard item, click the **Log Activity** tab.

Step 2 From the **Search** list box, choose one of the following options:

- To create a new search, select **New Search**.
- To edit a saved search, select **Edit Search**.

Step 3 Configure or edit your search parameters, as required. For more information on flow searches, see **Searching events or flows**.

Ensure you configure the following parameters:

- On the Edit Search pane, select the **Include in my Dashboard** option.
- On the Column Definition pane, select a column and click the **Add Column** icon to move the column to the **Group By** list.

Step 4 Click **Filter**.

The search results are displayed.

Step 5 Click **Save Criteria**. See **Saving search criteria on the Offense tab**.

Step 6 Click **OK**.

Step 7 Verify that your saved search criteria successfully added the event or flow search dashboard item to the **Add Items** list

a Click the **Dashboard** tab.

b Choose one of the following options:

- To verify an event search item, select **Add Item > Log Activity > Event Searches**.
- To verify a flow search item, select **Add Item > Network Activity > Flow Searches**.

The dashboard item should be displayed on the list using the same name as your saved search criteria.

3 OFFENSE MANAGEMENT

QRadar SIEM can correlate events and flows with destination IP addresses located across multiple networks in the same offense. This allows you to effectively investigate each offense in your network. You can navigate the various pages of the **Offenses** tab to investigate event and flow details to determine the unique events and flows that caused the offense.

Offense overview

Using the **Offenses** tab, you can investigate and offenses, source and destination IP addresses, network behaviors, and anomalies on your network. You can also search for offenses based on various criteria.

For more information on searching offenses, see **Offense searches**.

Offense permission considerations

The **Offenses** tab does not use device level user permissions to determine which offenses each user should be able to view; this is determined by network permissions. Therefore, all users can view all offenses regardless of which log source or flow source is associated with the offense. For more information about device level permissions, see the *IBM Security QRadar SIEM Administration Guide*.

Key terms

Using the **Offenses** tab, you can access and analyze the following items:

- **Offenses** - An offense includes multiple events or flows originating from one source, such as a host or log source. The **Offenses** tab displays offenses, which include traffic and vulnerabilities that collaborate and validate the magnitude of an offense. The magnitude of an offense is determined by several tests performed on the offense each time it is re-evaluated. Re-evaluation occurs when events are added to the offense and at scheduled intervals.
- **Source IP Addresses** - A source IP address specifies the device that attempts to breach the security of a component on your network. A source IP address can use various methods of attack, such as reconnaissance or Denial of Service (DoS) attacks, to attempt unauthorized access.
- **Destination IP Addresses** - A destination IP address specifies the network device that a source IP address attempts to access.

Offense retention

On the **Admin** tab, you can configure the offense retention period system settings to remove offenses from the database after a configured period of time. The default offense retention period is 3 days. You must have administrative permission to access the **Admin** tab and configure system settings. When configuring the thresholds, QRadar SIEM adds 5 days to any defined threshold. For more information, see the *IBM Security QRadar SIEM Administration Guide - Configuring System Settings*.

When you close offenses, the closed offenses are removed from the database after the offense retention period has elapsed. If additional events occur for an offense, a new offense is created. If you perform a search that includes closed offenses, the item is displayed in the search results as long as it has not been removed from the database.

Offense monitoring

Using the different views available on the **Offenses** tab, you can monitor offenses to determine what offenses are currently occurring on your network. Offenses are listed with the highest magnitude first. You can locate and view the details of a particular offense, and then take action on the offense, if required.

After you start navigating through the various views, the top of the **Offenses** tab displays the navigation trail to your current view. If you want to return to a previously viewed page, click the page name on the navigation trail.

From the navigation menu on the **Offenses** tab, you can access the following pages:

Table 3-1 Offense tab navigation menu options

Options	Description
My Offenses	Displays all offenses that are assigned to you.
All Offenses	Displays all global offenses on the network.
By Category	Displays all offenses grouped by the high- and low-level category.
By Source IP	Displays all offenses grouped by the source IP addresses that are involved in an offense.
By Destination IP	Displays all offenses grouped by the destination IP addresses that are involved in an offense.
By Network	Displays all offenses grouped by the networks that are involved in an offense.
Rules	Provides access to the Rules page, from which you can view and create custom rules. This option is only displayed if you have the **View Custom Rules** role permission. For more information, see **Rule management**.

Monitoring the All Offenses or My Offenses pages

You can monitor offenses on the All Offenses or My Offenses page. The All Offenses page displays a list of all offenses occurring in your network. The My Offenses page displays a list of offenses that are assigned to you.

About this task

The top of the table displays the details of the offense search parameters, if any, applied to the search results. To clear these search parameters, you can click **Clear Filter**. For more information on searching offenses, see **Offense searches**.

Note: To view a pane on the summary page in greater detail, click the associated toolbar option. For example, if you want to view the details of the source IP addresses, click **Sources**. For more information on the toolbar options, see **Offense tab toolbar functions**.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, select **All Offenses** or **My Offenses**.

Step 3 You can refine the list of offenses using the following options:

- From the **View Offenses** list box, select an option to filter the list of offenses for a specific time frame.
- If required, click the **Clear Filter** link beside each filter that is displayed in the Current Search Parameters pane.

Step 4 Double-click the offense you want to view.

Step 5 On the Offense Summary page, review the offense details. See **Offense parameters**.

Step 6 Perform any necessary actions on the offense. See **Offense management tasks**.

Monitoring offenses grouped by category

You can monitor offenses on the By Category details page, which provides you with a list of offenses grouped on the high-level category.

About this task

Count fields, such as **Event/Flow Count** and **Source Count**, do not consider network permissions of the user.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **By Category**.

Step 3 To view low-level category groups for a particular high-level category, click the arrow icon next to the high-level category name.

Step 4 To view a list of offenses for a low-level category, double-click the low-level category.

Step 5 Double-click the offense you want to view.

Step 6 On the Offense Summary page, review the offense details. See **Offense parameters**.

Step 7 Perform any necessary actions on the offense. See **Offense management tasks**.

Monitoring offenses grouped by source IP

On the Source page, you can monitor offenses grouped by source IP address.

About this task

A source IP address specifies the host that has generated offenses as a result of an attack on your system. All source IP addresses are listed with the highest magnitude first. The list of offenses only displays source IP addresses with active offenses.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **By Source IP**.

Step 3 You can refine the list of offenses using the following options:

- From the **View Offenses** list box, select an option to filter the list of offenses for a specific time frame.
- If required, click the **Clear Filter** link beside each filter that is displayed in the Current Search Parameters pane.

Step 4 Double-click the group you want to view.

Step 5 To view a list of local destination IP addresses for the source IP address, click **Destinations** on the Source page toolbar.

Step 6 To view a list of offenses associated with this source IP address, click **Offenses** on the Source page toolbar.

Step 7 Double-click the offense you want to view.

Step 8 On the Offense Summary page, review the offense details. See **Offense parameters**.

Step 9 Perform any necessary actions on the offense. See **Offense management tasks**.

Monitoring offenses grouped by destination IP

On the Destinations page, you can monitor offenses grouped by local destination IP addresses.

About this task

All destination IP addresses are listed with the highest magnitude first.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **By Destination IP**.

Step 3 You can refine the list of offenses using the following options:

- From the **View Offenses** list box, select an option to filter the list of offenses for a specific time frame.
- If required, click the **Clear Filter** link beside each filter that is displayed in the Current Search Parameters pane.

Step 4 Double-click the destination IP address you want to view.

Step 5 To view a list of offenses associated with this destination IP address, click **Offenses** on the Destination page toolbar.

Step 6 To view a list of source IP addresses associated with this destination IP address, click **Sources** on the Destination page toolbar.

Step 7 Double-click the offense you want to view.

Step 8 On the Offense Summary page, review the offense details. See **Offense parameters**.

Step 9 Perform any necessary actions on the offense. See **Offense management tasks**.

Monitoring offenses grouped by network

On the networks page, you can monitor offenses grouped by network.

About this task

All networks are listed with the highest magnitude first.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **By Network**.

Step 3 Double-click the network you want view.

Step 4 To view a list of source IP addresses associated with this network, click **Sources** on the Network page toolbar.

Step 5 To view a list of destination IP addresses associated with this network, click **Destinations** on the Network page toolbar.

Step 6 To view a list of offenses associated with this network, click **Offenses** on the Network page toolbar.

Step 7 Double-click the offense you want to view.

Step 8 On the Offense Summary page, review the offense details. See **Offense parameters**.

Step 9 Perform any necessary actions on the offense. See **Offense management tasks**.

Offense management tasks

When monitoring offenses, you can perform actions on the offense.

You can perform the following actions:

- Add notes
- Remove offenses

- Protect offenses
- Export offense data to XML or CSV
- Assign offenses to other users
- Send email notifications
- Mark an offense for follow-up
- Hide or close an offense from any offense list

To perform an action on multiple offenses, hold the Control key while you select each offense you want to select. To view offense details on a new page, hold the Control key while you double-click on an offense.

Adding notes

You can add notes to any offense on the **Offenses** tab. Notes can include information you want to capture for the offense, such as a Customer Support ticket number or offense management information.

About this task

Notes can include up to 1996 characters. The note text does not automatically wrap and is not editable.The text is displayed on the tab exactly as entered. For example, if you type the text without hard carriage returns, the note text is displayed on one line in the **Notes** summary and the **Note** column includes a scroll bar.

The **Add Note** option is available on the following locations in an offense summary:

- **Actions** list box on the offense summary toolbar.
- **Add Note** icon on the Last 5 Notes pane.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Navigate to the offense to which you want to add notes.

Step 3 Double-click the offense.

Step 4 From the **Actions** list box, select **Add Note**.

Step 5 Type the note you want to include for this offense.

Step 6 Click **Add Note**.

Result

The note is displayed in the Last 5 Notes pane on the offense summary. A **Notes** icon is displayed in the flag column of the offenses list. If you hover your mouse over the notes indicator, the note for that offense is displayed.

Hiding offenses

To prevent an offense from being displayed in the **Offenses** tab, you can hide the offense.

About this task

After you hide an offense, the offense is no longer displayed in any list (for example, All Offenses) on the **Offenses** tab; however, if you perform a search that includes the hidden offenses, the item is displayed in the search results.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **All Offenses**.

Step 3 Select the offense you want to hide.

Step 4 From the **Actions** list box, select **Hide**.

Step 5 Click **OK**.

Showing hidden offenses

Hidden offenses are not visible on the **Offenses** tab, however, you can show hidden offenses if you want to view them again.

About this task

To show hidden offenses, you must perform a search that includes hidden offenses. The search results include all offenses, including hidden and non-hidden offenses. Offenses are specified as hidden by the **Hidden** icon in the **Flag** column.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **All Offenses**.

Step 3 Search for hidden offenses:

- **a** From the **Search** list box, select **New Search**.
- **b** In the **Exclude option** list on the Search Parameters pane, clear the **Hidden Offenses** check box.
- **c** Click **Search**.

Step 4 Locate and select the hidden offense you want to show.

Step 5 From the **Actions** list box, select **Show**.

Closing offenses

To remove an offense completely from your system, you can close the offense.

About this task

After you close (delete) offenses, the offenses are no longer displayed in any list (for example, All Offenses) on the **Offenses** tab. The closed offenses are removed from the database after the offense retention period has elapsed. The default offense retention period is 3 days. If additional events occur for an offense, a new offense is created. If you perform a search that includes closed offenses, the item is displayed in the search results as long as it has not been removed from the database.

When you close offenses, you must select a reason for closing the offense and you can add a note.The **Notes** field displays the note entered for the previous offense closing. Notes must not exceed 2,000 characters. This note will be displayed in the Notes pane of this offense. If you have the Manage Offense Closing permission, you can add new custom reasons to the **Reason for Closing** list box. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **All Offenses**.

Step 3 Choose one of the following options:

- Select the offense you want to close, and then select **Close** from the **Actions** list box.
- From the **Actions** list box, select **Close Listed**.

Step 4 From the **Reason for Closing** list box, select a reason. The default reason is **non-issue**.

Step 5 Optional. In the **Notes** field, type a note to provide additional information about closing the note.

Step 6 Click **OK**.

Result

After you close offenses, the counts that are displayed on the By Category pane of the **Offenses** tab can take several minutes to reflect the closed offenses.

Protecting offenses

You can prevent offenses from being removed from the database after the retention period has elapsed.

About this task

Offenses are retained for a configurable retention period. The default retention period is 3 days; however, Administrators can customize the retention period. You might have offenses that you want to retain regardless of the retention period. You can prevent these offenses from being removed from the database after the retention period has elapsed. For more information about the Offense Retention Period, see the *IBM Security QRadar SIEM Administration Guide*.

CAUTION: *When the SIM data model is reset using the* ***Hard Clean*** *option, all offenses, including protected offenses, are removed from the database and the disk. You must have administrative privileges to reset the SIM data model. For more information, see the IBM Security QRadar SIEM Administration Guide.*

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **All Offenses**.

Step 3 Choose one of the following options:

- Select the offense you want to protect, and then select **Protect** from the **Actions** list box.
- From the **Actions** list box, select **Protect Listed**.

Step 4 Click **OK**.

Result

The protected offense is indicated by a **Protected** icon in the **Flag** column.

Unprotecting offenses

You can unprotect offenses that have been previously protected from removal after the offense retention period has elapsed.

About this task

To list only protected offenses, you can perform a search that filters for only protected offenses. If you clear the **Protected** check box and ensure all other options are selected under the **Excludes option** list on the Search Parameters pane, only protected offenses are displayed.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **All Offenses**.

Step 3 Optional. Perform a search that displays only protected offenses.

Step 4 Choose one of the following options:

- Select the offense you want to protect, and then select **Unprotect** from the **Actions** list box.
- From the **Actions** list box, select **Unprotect Listed**.

Step 5 Click **OK**.

Exporting offenses

You can export offenses in Extensible Markup Language (XML) or Comma Separated Values (CSV) format.

About this task

If you want to re-use or store your offense data, you can export offenses. For example, you can export offenses to create non-QRadar SIEM-based reports. You could also export offenses as a secondary long-term retention strategy. Customer Support might require you to export offenses for troubleshooting purposes.

The resulting XML or CSV file includes the parameters specified in the Column Definition pane of your search parameters. The length of time required to export your data depends on the number of parameters specified.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **All Offenses**.

Step 3 Select the offense you want to export.

Step 4 Choose one of the following options:

- To export the offenses in XML format, select **Actions > Export to XML** from the **Actions** list box.
- To export the offenses in CSV format, select **Actions > Export to CSV** from the **Actions** list box

Step 5 Choose one of the following options:

- To open the list for immediate viewing, select the **Open with** option and select an application from the list box.
- To save the list, select the **Save to Disk** option.

Step 6 Click **OK**.

Assigning offenses to users

Using the **Offenses** tab, you can assign offenses to QRadar SIEM users for investigation.

About this task

When an offense is assigned to a user, the offense is displayed on the My Offenses page belonging to that user. You must have appropriate privileges to assign offenses to users. For more information about user roles, see the *IBM Security QRadar SIEM Administration Guide*.

You can assign offenses to users from either the **Offenses** tab or Offense Summary pages. This procedure provides instruction on how to assign offenses from the **Offenses** tab.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **All Offenses**.

Step 3 Select the offense you want to assign.

Step 4 From the **Actions** list box, select **Assign**.

Step 5 From the **Username** list box, select the user you want to assign this offense to.

Note: The **Username** list box only displays users who have **Offenses** tab privileges.

Step 6 Click **Save**.

Result

The offense is assigned to the selected user. The **User** icon is displayed in the **Flag** column of the **Offenses** tab to indicate that the offense is assigned. The designated user can see this offense in their My Offenses page.

Sending email notification

You can send an email containing an offense summary to any valid email address.

About this task

The body of the email message includes the following information (if available):

- Source IP address
- Source user name, host name, or asset name
- Total number of sources
- Top five sources by magnitude
- Source networks
- Destination IP address
- Destination user name, host name, or asset name
- Total number of destinations
- Top five destinations by magnitude
- Destination networks
- Total number of events
- Rules that caused the offense or event rule to fire
- Full description of offense or event rule
- Offense ID
- Top five categories
- Start time of offense or time the event generated
- Top five Annotations
- Link to the offense in the QRadar SIEM user interface
- Contributing CRE rules

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Navigate to the offense for which you want to send an email notification.

Step 3 Double-click the offense.

Step 4 From the **Actions** list box, select **Email**.

Step 5 Configure the following parameters.

Parameter	Description
To	Type the email address of the user you want to notify if a change occurs to the selected offense. Separate multiple email addresses with a comma.
From	Type the default originating email address. The default is root@localhost.com.
Email Subject	Type the default subject for the email. The default is Offense ID.
Email Message	Type the standard message you want to accompany the notification email.

Step 6 Click **Send**.

Marking an item for follow-Up

Using the **Offenses** tab, you can mark an offense, source IP address, destination IP address, and network for follow-up. This allows you to track a particular item for further investigation.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Navigate to the offense you want to mark for follow-up.

Step 3 Double-click the offense.

Step 4 From the **Actions** list box, select **Follow up**.

Result

The offense now displays a flag in the **Flags** column, indicating the offense is flagged for follow-up. If you do not see your flagged offense on the offenses list, you can sort the list to display all flagged offenses first. To sort an offense list by flagged offense, double-click the **Flags** column header.

Offense tab toolbar functions

Each page and table on the **Offenses** tab has a toolbar to provide you with the functions required to perform certain actions or to investigate the contributing factors of an offense. The following table provides descriptions for the toolbar functions.

Table 3-2 Offense tab toolbar functions

Function	Description
Add Note	Click **Add Note** to add a new note to an offense. This option is only available on the Last 5 Notes pane of the Offense Summary page.
Actions	The options available on the **Actions** list box varies based on the page, table, or item (such as an offense or source IP address). The **Actions** list box may not display exactly as listed below. From the **Actions** list box, you can choose one of the following actions: • **Follow up** - Select this option to mark an item for further follow-up. See **Marking an item for follow-Up**. • **Hide** - Select this option to hide an offense. For more information about hiding offenses, see **Hiding offenses**. • **Show** - Select this option to show all hidden offenses. For more information about showing offenses, see **Showing hidden offenses**. • **Protect Offense** - Select this option to protect an offense. For more information about protecting offenses, see **Protecting offenses**. • **Close** - Select this option to close an offense. For more information about closing offenses, see **Closing offenses**. • **Close Listed** - Select this option to close listed offense. For more information about closing listed offenses, see **Closing offenses**. • **Email** - Select this option to email an offense summary to one or more recipients. See **Sending email notification**. • **Add Note** - Select this option to add notes to an item. See **Adding notes**. • **Assign** - Select this option to assign an offense to a user. See **Assigning offenses to users**. • **Print** - Select this option to print an offense.

Table 3-2 Offense tab toolbar functions (continued)

Function	Description
Annotations	Click **Annotations** to view all annotations for an offense. • **Annotation** - Specifies the details for the annotation. Annotations are text descriptions that rules can automatically add to offenses as part of the rule response. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide*. • **Time** - Specifies the date and time when the annotation was created. • **Weight** - Specifies the weight of the annotation.
Anomaly	Click **Anomaly** to display the saved search results that caused the anomaly detection rule to generate the offense. ***Note:*** *This button is only displayed if the offense was generated by an anomaly detection rule.*
Categories	Click **Categories** to view category information for the offense. To further investigate the events related to a specific category, you can also right-click a category and select **Events** or **Flows**. Alternatively, you can highlight the category and click the **Events** or **Flows** icon on the List of Event Categories toolbar. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Connections	Click **Connections** to further investigate connections. ***Note:*** *This option is only available if you have purchased and licensed IBM Security QRadar Risk Manager. For more information, see the IBM Security QRadar Risk Manager Users Guide.* When you click the **Connections** icon, the connection search criteria page is displayed on a new page, pre-populated with event search criteria. You can customize the search parameters, if required. Click **Search** to view the connection information.
Destinations	Click **Destinations** to view all local destination IP addresses for an offense, source IP address, or network. ***Note:*** *If the destination IP addresses are remote, a separate page opens providing information for the remote destination IP addresses.*
Display	The Offense Summary page displays many tables of information related to an offense. To locate a table, you can scroll to the table you want to view or select the option from the **Display** list box.
Events	Click **Events** to view all events for an offense. When you click **Events**, the event search results are displayed. For information on searching events, see **Searching events or flows**.

Table 3-2 Offense tab toolbar functions (continued)

Function	Description
Flows	Click **Flows** to further investigate the flows associated with an offense. When you click **Flows**, the flow search results are displayed. See **Searching events or flows**.
Log Sources	Click **Log Sources** to view all log sources for an offense.
Networks	Click **Networks** to view all destination networks for an offense.
Notes	Click **Notes** to view all notes for an offense, source IP address, destination IP address, or network. For more information about notes, see **Adding notes**.
Offenses	Click **Offenses** to view a list of offenses associated with an source IP address, destination IP address, or network.
Print	Click **Print** to print an offense.
Rules	Click **Rules** to view all rules that contributed to an offense. The rule that created the offense is listed first. If you have appropriate permissions to edit a rule, double-click the rule to launch the Edit Rules page. For more information about user roles, see the *IBM Security QRadar SIEM Administration Guide*. If the rule has been deleted, a red icon (x) is displayed beside the rule. If you double-click a deleted rule, a message is displayed to indicate the rule no longer exists.
Save Criteria	After you perform an offense search, click **Save Criteria** to save your search criteria for future use.
Save Layout	By default, the By Category details page is sorted by the Offense Count parameter. If you change the sort order or sort by a different parameter, click **Save Layout** to save the current display as your default view. The next time you log in to the Offenses tab, the saved layout is displayed.
Search	This option is only available on the List of Local Destinations table toolbar. Click **Search** to filter destination IPs for a source IP address. To filter destinations: **1** Click **Search**. **2** Enter values for the following parameters: **Destination Network** - From the list box, select the network you want to filter. **Magnitude** - From the list box, select whether you want to filter for magnitude Equal to, Less than, or Greater than the configured value. **Sort by** - From the list box, select how you want to sort the filter results. **3** Click **Search**.

Table 3-2 Offense tab toolbar functions (continued)

Function	Description
Show Inactive Categories	On the By Category details page, the counts for each category are accumulated from the values in the low-level categories. Low-level categories with associated offenses are displayed with an arrow. You can click the arrow to view the associated low-level categories. If you want to view all categories, click **Show Inactive Categories**.
Sources	Click **Sources** to view all source IP addresses for the offense, destination IP address, or network.
Summary	If you clicked to an option from the **Display** list box, you can click **Summary** to return to the detailed summary view.
Users	Click **Users** to view all users associated with an offense.
View Attack Path	Click **View Attack Path** to further investigate the attack path of an offense. When you click the **View Attack Path** icon, the Current Topology page is displayed on a new page. ***Note:*** *This option is only available if you have purchased and licensed IBM Security QRadar Risk Manager. For more information, see the IBM Security QRadar Risk Manager Users Guide.*
View Topology	Click **View Topology** to further investigate the source of an offense. When you click the **View Topology** icon, the Current Topology page is displayed on a new page. ***Note:*** *This option is only available when IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the IBM Security QRadar Risk Manager Users Guide.*

Offense parameters

The following table provides descriptions of parameters provided on all pages of the **Offenses** tab.

Table 3-3 Offense parameters

Parameter	Location	Description
Annotation	Top 5 Annotations table	Specifies the details for the annotation. Annotations are text descriptions that rules can automatically add to offenses as part of the rule response. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide*.
Anomaly	Last 10 Events (Anomaly Events) table	Select this option to display the saved search results that caused the anomaly detection rule to generate the event.
Anomaly Text	Last 10 Events (Anomaly Events) table	Specifies a description of the anomalous behavior that was detected by the anomaly detection rule.
Anomaly Value	Last 10 Events (Anomaly Events) table	Specifies the value that caused the anomaly detection rule to generate the offense.
Application	Last 10 Flows table	Specifies the application associated with the flow.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Application Name	Offense Source table, if the Offense Type is App ID	Specifies the application associated with the flow that created the offense.
ASN Index	Offense Source table, if the Offense Type is Source ASN or Destination ASN	Specifies the ASN value associated with the flow that created the offense.
Asset Name	Offense Source table, if the Offense Type is Source IP or Destination IP	Specifies the asset name, which you can assign using the Asset Profile function. For more information, see **Asset management**.
Asset Weight	Offense Source table, if the Offense Type is Source IP or Destination IP	Specifies the asset weight, which you can assign using the Asset Profile function. For more information, see **Asset management**.
Assigned to	Offense table	Specifies the user assigned to the offense. If no user is assigned, this field specifies Not assigned. Click **Not assigned** to assign the offense to a user. For more information, see **Assigning offenses to users**.
Category	Last 10 Events table	Specifies the category of the event.
Category Name	By Category Details page	Specifies the high-level category name. For more information about high-level categories, see the *IBM Security QRadar SIEM Administration Guide*.
Chained	• Offense Source table, if the Offense Type is Destination IP • Top 5 Destination IPs table	Specifies whether the destination IP address is chained. A chained destination IP address is associated with other offenses. For example, a destination IP address might become the source IP address for another offense. If the destination IP address is chained, click **Yes** to view the chained offenses.
Creation Date	Last 5 Notes table	Specifies the date and time that the note was created.
Credibility	Offense table	Specifies the credibility of the offense, as determined by the credibility rating from source devices. For example, credibility is increased when multiple offenses report the same event or flow.
Current Search Parameters	• By Source IP Details page • By Destination IP Details page	The top of the table displays the details of the search parameters applied to the search results. To clear these search parameters, click **Clear Filter**. ***Note:*** *This parameter is only displayed after you apply a filter.*

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Description	• All Offenses page • My Offenses page • Offense table • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page • Offense Source table, if the Offense Type is Log Source • Top 5 Log Sources table	Specifies the description of the offense or log source.
Destination IP	• Last 10 Events table • Last 10 Flows table	Specifies the destination IP address of the event or flow.
Destination IP	• Top 5 Destination IPs table • By Source IP - List of Local Destinations page • By Destination IP Details page • By Network - List of Local Destinations page	Specifies the IP address of the destination. If DNS lookups is enabled on the **Admin** tab, you can view the DNS name by pointing your mouse over the IP address. For more information, see the *IBM Security QRadar SIEM Administration Guide.*
Destination IP(s)	Offense table	Specifies the IP addresses and asset name (if available) of the local or remote destinations. Click the link to view additional details.
Destination IPs	• All Offenses page • My Offenses page	Specifies the IP addresses and asset name (if available) of the local or remote destinations. If more than one destination IP address is associated with the offense, this field specifies Multiple and the number of destination IP addresses.
Destination IPs	• By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the IP addresses and asset names (if available) of the destination associated with the offense. If DNS lookups is enabled on the **Admin** tab, you can view the DNS name by pointing your mouse over the IP address or asset name. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
Destination IPs	By Network Details page	Specifies the number of destination IP addresses associated with the network.
Destination Port	Last 10 Flows table	Specifies the destination port of the flow.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Destination(s)	• Top 5 Source IPs table • By Source IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page	Specifies the number of destination IP addresses for the source IP address.
Dst Port	Last 10 Events table	Specifies the destination port of the event.
Duration	Offense table	Specifies the amount of time elapsed since the offense was first detected.
Event Name	• Offense Source table, if the Offense Type is Event Name • Last 10 Events table • Last 10 Events (Anomaly Events) table	Specifies the event name, as identified in the QID map, associated with the event or flow that created the offense. Point your mouse over the event name to view the QID.
Event/Flow Count	By Category Details page	Specifies the number of active events or flow (events or flows that are not closed or hidden) associated with the offense in the category. Offenses only stay active for a period of time if no new events or flows are received. The offenses are still displayed on the **Offenses** tab, but are not counted in this field.
Event/Flow Count	Destination page Network page	Specifies the total number of generated events or flows associated with the destination IP address or network.
Event/Flow Count	Offense table	Specifies the number of events and flows that have occurred for the offense and the number of categories. Click the events link to further investigate the events associated with the offense. When you click the events link, the event search results are displayed. Click the flows link to further investigate the flows associated with the offense. When you click the flows link, the flow search results are displayed. ***Note:*** *If the flow count displays N/A, the offense might have a start date that precedes the date that you upgraded to IBM Security QRadar SIEM 7.1.0 (MR1), therefore, flows cannot be counted. You can, however, click the N/A link to investigate the associated flows in the flow search results.*

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Events	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the number of events for the offense.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Events/Flows	• Offense Source table, if the Offense Type is Source IP, Destination IP, Hostname, Username Source Port or Destination, Event Name, Port, Source MAC Address or Destination MAC Address, Log Source, Source IPv6 or Destination IPv6, Source ASN or Destination ASN, Rule, App ID • Top 5 Source IPs table • By Source IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • Source Details page • Top 5 Destination IPs table • By Source IP - List of Local Destinations page • By Destination IP Details page • By Network - List of Local Destinations page • Top 5 Users table • Top 5 Log Sources table • Top 5 Categories table • By Network Details page • Top 5 Categories table	Specifies the number of events or flows associated with the source IP address, destination IP address, event name, user name, MAC address, log source, host name, port, log source, ASN address, IPv6 address, rule, ASN, Application, network or category. Click the link to view more details.
First event/flow seen on	Source Details page	Specifies the date and time in which the source IP address generated the first event or flow.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Flag	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Indicates the action taken on the offense. The actions are represented by the following icons: • **Flag** - Indicates that the offense is marked for follow-up. This allows you to track a particular item for further investigation. For more information about how to mark an offense for follow-up, see **Marking an item for follow-Up**. • **User** - Indicates that the offense has been assigned to a user. When an offense is assigned to a user, the offense is displayed on the My Offenses page belonging to that user. For more information about assigning offenses to users, see **Assigning offenses to users**. • **Notes** - Indicates that a user has added notes to the offense. Notes can include any information you want to capture for the offense. For example, you could add a note that specifies information that is not automatically included in an offense, such as a Customer Support ticket number or offense management information. For more information about adding notes, see **Adding notes**. • **Protected** - Indicates that the offense is protected. The Protect feature prevents specified offenses from being removed from the database after the retention period has elapsed. For more information about protected offenses, see **Protecting offenses**. • **Inactive Offense** - Indicates that this is an inactive offense. An offense becomes inactive after five days have elapsed since the offense received the last event. Also, all offenses become inactive after upgrading your QRadar SIEM software. An inactive offense cannot become active again. If new events are detected for the offense, a new offense is created and the inactive offense is retained until the offense retention period has elapsed. You can perform the following actions on inactive offenses: protect, flag for follow up, add notes, and assign to users. Point your mouse over the icon to display additional information.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Flag	• By Source IP Details page • By Source IP - List of Local Destinations page • By Destination IP Details page • By Destination IP - List of Sources page • By Network Details page • By Network - List of Sources page • By Network - List of Local Destinations page	Specifies the action taken on the source IP address, destination IP address, or network. For example, if a flag is displayed, the offense is source IP address for follow-up. Point your mouse over the icon to display additional information.
Flows	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the number of flows for the offense. ***Note:*** *If the Flows column displays N/A, the offense might have a start date that precedes the date you upgraded to QRadar SIEM 7.1.0 (MR1).*
Group	• Offense Source table, if the Offense Type is Log Source • Top 5 Log Sources table	Specifies to which group the log source belongs.
Group(s)	Offense Source table, if the Offense Type is Rule	Specifies which rule group the rule belongs to.
High Level Category	Offense Source table, if the Offense Type is Event Name	Specifies the high-level category of the event. For more information about high-level categories, see the *IBM Security QRadar SIEM Administration Guide*.
Host Name	Offense Source table, if the Offense Type is Source IP or Destination IP	Specifies the host name associated with the source or destination IP address. If no host name is identified, this field specifies Unknown.
Host Name	Offense Source table, if the Offense Type is Hostname	Specifies the host name associated with the flow that created the offense.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
ID	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page	Specifies the unique identification number QRadar SIEM assigns to the offense.
IP	• Offense Source table, if the Offense Type is Source IP or Destination IP • Source Details page	Specifies the source IP address associated with the event or flow that created the offense.
IP/DNS Name	Destination page	Specifies the IP address of the destination. If DNS lookups is enabled on the **Admin** tab, you can view the DNS name by pointing your mouse over the IP address or asset name. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
IPv6	Offense Source table, if the Offense Type is Source IPv6 or Destination IPv6	Specifies the IPv6 address associated with the event or flow that created the offense.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Last Event/Flow	• All Offenses page • My Offenses page • By Source IP - List of Local Destinations page • Top 5 Source IPs table • By Source IP Details page • By Network - List of Sources page • Top 5 Destination IPs table • By Destination IP Details page • By Destination IP - List of Sources page • By Network - List of Local Destinations page • Top 5 Categories table	Specifies the elapsed time since the last event or flow was observed for the offense, category, source IP address, or destination IP address.
Last event/flow seen on	Source Details page	Specifies the date and time of the last generated event or flow associated with the source IP address.
Last Event/Flow Time	Offense Source table, if the Offense Type is Log Source	Specifies the date and time the log source was last observed on the system.
Last Known Group	Offense Source table, if the Offense Type is Username, Source MAC Address, Destination MAC Address, or Hostname	Specifies the current group the user, MAC address, or host name belongs to. If no group is currently associated, the value for this field is Unknown. ***Note:*** *This field does not display historical information.*
Last Known Host	Offense Source table, if the Offense Type is Username, Source MAC Address, or Destination MAC Address	Specifies the current host the user or MAC address is associated with. If no host is identified, this field specifies Unknown. ***Note:*** *This field does not display historical information.*
Last Known IP	Offense Source table, if the Offense Type is Username, Source MAC Address, Destination MAC Address, or Hostname	Specifies the current IP address of the user, MAC, or hostname. If no IP address is identified, this field specifies Unknown. ***Note:*** *This field does not display historical information.*
Last Known MAC	Offense Source table, if the Offense Type is Username or Hostname	Specifies the last known MAC address of the user or host name. If no MAC is identified, this field specifies Unknown. ***Note:*** *This field does not display historical information.*

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Last Known Machine	Offense Source table, if the Offense Type is Username, Source MAC Address, Destination MAC Address, or Hostname	Specifies the current machine name associated with the user, MAC address, or host name. If no machine name is identified, this field specifies Unknown. ***Note:*** *This field does not display historical information.*
Last Known Username	Offense Source table, if the Offense Type is Source MAC Address, Destination MAC Address, or Hostname	Specifies the current user of the MAC address or host name. If no MAC address is identified, this field specifies Unknown. ***Note:*** *This field does not display historical information.*
Last Observed	Offense Source table, if the Offense Type is Username, Source MAC Address, Destination MAC Address, or Hostname	Specifies the date and time the user, MAC address, or host name was last observed on the system.
Last Packet Time	Last 10 Flows table	Specifies the date and time the last packet for the flow was sent.
Local Destination Count	Top 5 Categories table By Category Details page	Specifies the number of local destination IP addresses associated with the category.
Local Destination(s)	Source Details page	Specifies the local destination IP addresses associated with the source IP address. To view additional information about the destination IP addresses, click the IP address or term that is displayed. If there are multiple destination IP addresses, the term Multiple is displayed.
Location	• Offense Source table, if the Offense Type is Source IP or Destination IP • Top 5 Source IPs table • By Source IP Details page • Source Details page • By Destination IP - List of Sources page • By Network - List of Sources page	Specifies the network location of the source IP address, or destination IP address. If the location is local, you can click the link to view the networks.
Log Source	Last 10 Events table	Specifies the log source that detected the event.
Log Source Identifier	Offense Source table, if the Offense Type is Log Source	Specifies the host name of the log source.

Table 3-3 Offense parameters (continued)

Parameter	**Location**	**Description**
Log Source Name	Offense Source table, if the Offense Type is Log Source	Specifies the log source name, as identified in the Log Sources table, associated with the event that created the offense. ***Note:*** *The information displayed for log source offenses is derived from the Log Sources page on the **Admin** tab. You must have administrative access to access the **Admin** tab and manage log sources. For more information about log source management, see the IBM Security QRadar Log Sources User Guide*
Log Sources	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the log sources associated with the offense. If more than one log source is associated with the offense, this field specifies Multiple and the number of log sources.
Low Level Category	Offense Source table, if the Offense Type is Event Name	Specifies the low-level category of the event. For more information about low-level categories, see the *IBM Security QRadar SIEM Administration Guide*.
MAC	• Offense Source table, if the Offense Type is Source IP or Destination IP • Top 5 Source IPs table • Top 5 Destination IPs table • By Source IP Details page • By Source IP - List of Local Destinations page • By Destination IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • By Network - List of Local Destinations page	Specifies the MAC address of the source or destination IP address when the offense began. If the MAC address is unknown, this field specifies Unknown.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
MAC Address	Offense Source table, if the Offense Type is Source MAC Address or Destination MAC Address	Specifies the MAC address associated with the event that created the offense. If no MAC address is identified, this field specifies Unknown.
Magnitude	• All Offenses page • My Offenses page • Offense table • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page • Top 5 Categories table • Last 10 Events table • By Network Details page • Network page	Specifies the relative importance of the offense, category, event, or network. The magnitude bar provides a visual representation of all correlated variables. Variables include Relevance, Severity, and Credibility. Point your mouse over the magnitude bar to display values and the calculated magnitude. For more information about relevance, severity, and credibility, see the **Glossary**.
Magnitude	• Offense Source table, if the Offense Type is Source IP or Destination IP • Top 5 Source IPs table • Top 5 Destination IPs table • By Source IP Details page • Source Details page • By Source IP - List of Local Destinations page • Destination page • By Destination IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • By Network - List of Local Destinations page	Specifies the relative importance of the source or destination IP address. The magnitude bar provides a visual representation of the CVSS risk value of the asset associated with the IP address. Point your mouse over the magnitude bar to display the calculated magnitude. For more information about CVSS, see the **Glossary**.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Name	• Top 5 Log Sources table • Top 5 Users table • Top 5 Categories table • Network page	Specifies the name of the log source, user, category, network IP address or name.
Network	By Network Details page	Specifies the name of the network.
Network(s)	Offense table	Specifies the destination network for the offense. If the offense has one destination network, this field displays the network leaf. Click the link to view the network information. If the offense has more than one destination network, the term Multiple is displayed. Click the link to view additional details.
Notes	• Offense Source table, if the Offense Type is Rule • Last 5 Notes table	Specifies the notes for the rule.
Offense Count	By Category Details page	Specifies the number of active offenses in each category. Active offenses are offenses that have not been hidden or closed. If the By Category Details page includes the **Exclude Hidden Offenses** filter, the offense count that is displayed in the **Offense Count** parameter might not be correct. If you want to view the total count in the By Category pane, click **Clear Filter** beside the **Exclude Hidden Offenses** filter on the By Category Details page.
Offense Source	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies information about the source of the offense. The information displayed in the **Offense Source** field depends on the type of offense. For example, if the offense type is Source Port, the **Offense Source** field displays the source port of the event that created the offense.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Offense Type	• All Offenses page • My Offenses page • Offense table • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the type of offense. The Offense Type is determined by the rule that created the offense. For example, if the offense type is log source event, the rule that generated the offense correlates events based on the device that detected the event. Offense types include: • Source IP • Destination IP • Event Name • User Name • Source MAC Address • Destination MAC Address • Log Source • Host Name • Source Port • Destination Port • Source IPv6 • Destination IPv6 • Source ASN • Destination ASN • Rule • App ID The offense type determines what type of information is displayed on the Offense Source Summary pane.
Offense(s)	• Source Details page • Destination page	Specifies the names of the offenses associated with the source or destination IP address. To view additional information about the offense, click the name or term that is displayed. If there are multiple offenses, the term Multiple is displayed.
Offense(s) Launched	Network page	Specifies the offenses launched from the network. If multiple offenses are responsible, this field specifies Multiple and the number of offenses.
Offense(s) Targeted	Network page	Specifies the offenses targeted for the network. If multiple offenses are responsible, this field specifies Multiple and the number of offenses

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Offenses	• Offense Source table, if the Offense Type is Source IP, Destination IP, Event Name, Username, Source MAC Address or Destination MAC Address, Log Source, Hostname, Source Port or Destination Port, Source IPv6 or Destination IPv6, Source ASN or Destination ASN, Rule, App ID • Top 5 Source IPs table • Top 5 Destination IPs table • Top 5 Log Sources table • Top 5 Users table • By Source IP Details page • By Source IP - List of Local Destinations page • By Destination IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • By Network - List of Local Destinations page	Specifies the number of offenses associated with the source IP address, destination IP address, event name, user name, MAC address, log source, host name, port, IPv6 address, ASN, rule, or application. Click the link to view more details.
Offenses Launched	By Network Details page	Specifies the number of offenses originated from the network.
Offenses Targeted	By Network Details page	Specifies the number of offenses targeted for the network.
Port	Offense Source table, if the Offense Type is Source Port or Destination Port	Specifies the port associated with the event or flow that created the offense.
Relevance	Offense table	Specifies the relative importance of the offense.
Response	Offense Source table, if the Offense Type is Rule	Specifies the response type for the rule.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Rule Description	Offense Source table, if the Offense Type is Rule	Specifies the summary of the rule parameters.
Rule Name	Offense Source table, if the Offense Type is Rule	Specifies the name of the rule associated with the event or flow that created the offense. ***Note:*** *The information displayed for rule offenses is derived from the Rules tab. For more information about rules, see the IBM Security QRadar SIEM Administration Guide.*
Rule Type	Offense Source table, if the Offense Type is Rule	Specifies the rule type for the offense.
Severity	• Offense Source table, if the Offense Type is Event Name • Offense table	Specifies the severity of the event or offense. Severity specifies the amount of threat that an offense poses in relation to how prepared the destination IP address is for the attack. This value is directly mapped to the event category that correlates to the offense. For example, a Denial of Service (DoS) attack has a severity of 10, which specifies a severe occurrence.
Source Count	By Category Details page	Specifies the number of source IP addresses associated with offenses in the category. If a source IP address is associated with offenses in five different low-level categories, the source IP address is only counted once.
Source IP	• By Source IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • Top 5 Source IPs table • Last 10 Flows table	Specifies the IP address or host name of the device that attempted to breach the security of a component on your network. If DNS lookups is enabled on the **Admin** tab, you can view the DNS name by pointing your mouse over the IP address. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
Source IP(s)	Offense table	Specifies the IP address or host name of the device that attempted to breach the security of a component on your network. Click the link to view additional details. For more information about source IP addresses, see **Monitoring offenses grouped by source IP**.
Source IPs	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the IP addresses or host name of the device that attempted to breach the security of a component on your network. If more than one source IP address is associated with the offense, this field specifies Multiple and the number of source IP addresses. If DNS lookups is enabled on the **Admin** tab, you can view the DNS name by pointing your mouse over the IP address or asset name. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
Source IPs	By Network Details page	Specifies the number of source IP addresses associated with the network.
Source Port	Last 10 Flows table	Specifies the source port of the flow.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Source(s)	• Top 5 Destination IPs table • By Source IP - List of Local Destinations page • By Destination IP Details page	Specifies the number of source IP addresses for the destination IP address.
Source(s)	• Destination page • Network page	Specifies the source IP addresses of the offense associated with the destination IP address or network. To view additional information about the source IP addresses, click the IP address, asset name, or term that is displayed. If a single source IP address is specified, an IP address and asset name is displayed (if available). You can click the IP address or asset name to view the source IP address details. If there are multiple source IP addresses, this field specifies Multiple and the number of source IP addresses.
Source(s)	By Network - List of Local Destinations page	Specifies the number of source IP addresses associated with the destination IP address.
Start	Offense table	Specifies the date and time the first event or flow occurred for the offense.
Start Date	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the date and time of the first event or flow associated with the offense.
Status	Offense Source table, if the Offense Type is Log Source	Specifies the status of the log source.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Status	Offense table	Displays icons to indicate the status of an offense. Status icons include: • **Inactive Offense** - Indicates that this is an inactive offense. An offense becomes inactive after five days have elapsed since the offense received the last event. Also, all offenses become inactive after upgrading your QRadar SIEM software. An inactive offense cannot become active again. If new events are detected for the offense, a new offense is created and the inactive offense is retained until the offense retention period has elapsed. You can perform the following actions on inactive offenses: protect, flag for follow up, add notes, and assign to users • **Hidden Offense** - Indicates that the offense is hidden from view on the All Offenses page. Hidden offenses are only visible on the All Offenses page if you perform a search for hidden offenses. For more information on hidden offenses, see **Hiding offenses**. • **User** - Indicates that the offense has been assigned to a user. When an offense is assigned to a user, the offense is displayed on the My Offenses page belonging to that user. For more information about assigning offenses to users, see **Assigning offenses to users**. • **Protected** - Indicates that the offense is protected. The Protect feature prevents specified offenses from being removed from the database after the retention period has elapsed. For more information about protected offenses, see **Protecting offenses**. • **Closed Offense** - Indicates that the offense has been closed. For more information about closing offenses, see **Closing offenses**. Point your mouse over the icon to display additional information.
Time	• Last 10 Events table • Last 10 Events (Anomaly Events) table	Specifies the date and time when the first event was detected in the normalized event. This date and time is specified by the device that detected the event.
Time	Top 5 Annotations table	Specifies the date and time that the annotation was created.
Total Bytes	Last 10 Flows table	Specifies the total number of bytes for the flow.
Total Events/Flows	• Top 5 Log Sources table • Top 5 Users table	Specifies the total number of events for the log source or user.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
User	• Offense Source table, if the Offense Type is Source IP or Destination IP, or Username • Top 5 Source IPs table • Top 5 Destination IPs table • By Source IP Details page • By Source IP - List of Local Destinations page • By Destination IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • By Network - List of Local Destinations page	Specifies the user associated with a source IP address or destination IP address. If no user is identified, this field specifies Unknown.
Username	Offense Source table, if the Offense Type is Username	Specifies the user name associated with the event or flow that created the offense. ***Note:*** *If you move your mouse pointer over the* ***Username*** *parameter, the tooltip that is displayed provides the user name associated with the most recent user name information from the* ***Assets*** *tab instead of the username associated with the event or flow that created the offense.*
Username	Last 5 Notes table	Specifies the user who created the note.
Users	• All Offenses page • My Offenses page • By Source IP - List of Offenses page • By Network - List of Offenses page • By Destination IP - List of Offenses page	Specifies the user names associated with the offense. If more than one user name is associated with the offense, this field specifies Multiple and the number of user names. If no user is identified, this field specifies Unknown.
View Offenses	• By Source IP Details page • By Destination IP Details page	Select an option from this list box to filter on the offenses you want to view on this page. You can view all offenses or filter by the offenses based on a time range. From the list box, select the time range you want to filter by.

Table 3-3 Offense parameters (continued)

Parameter	Location	Description
Vulnerabilities	Offense Source table, if the Offense Type is Source IP or Destination IP	Specifies the number of identified vulnerabilities associated with the source or destination IP address. This value also includes the number of active and passive vulnerabilities.
Vulnerabilities	By Destination IP - List of Sources page	Specifies whether a source IP address has vulnerabilities.
Vulnerability	• Top 5 Source IPs table • By Source IP Details page • By Network - List of Sources page • Top 5 Destination IPs table • By Source IP - List of Local Destinations page • By Destination IP Details page • By Network - List of Local Destinations page	Specifies whether the source or destination IP address has vulnerabilities.
Weight	• Top 5 Source IPs table • Top 5 Destination IPs table • By Source IP - List of Local Destinations page • By Source IP Details page • By Destination IP Details page • By Destination IP - List of Sources page • By Network - List of Sources page • By Network - List of Local Destinations page • Top 5 Annotations table	Specifies the weight of the source IP address, destination IP address, or annotation. The weight of an IP address is assigned on the **Assets** tab. For more information, see **Asset management**.

4 LOG ACTIVITY INVESTIGATION

Using the **Log Activity** tab, you can monitor and investigate log activity (events) in real-time or perform advanced searches.

Log Activity tab overview

An event is a record from a log source, such as a firewall or router device, that describes an action on a network or host. The **Log Activity** tab specifies which events are associated with offenses.

You must have permission to view the **Log Activity** tab. For more information on permissions and assigning roles, see the *IBM Security QRadar SIEM Administration Guide*.

Log Activity tab toolbar

Using the toolbar, you can access the following options:

Table 4-1 Log Activity tab toolbar options

Option	Description
Search	Click **Search** to perform advanced searches on events. Options include: • **New Search** - Select this option to create a new event search. • **Edit Search** - Select this option to select and edit an event search. • **Manage Search Results** - Select this option to view and manage search results. For more information about the search feature, see **Data searches**.
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the **Quick Searches** list box only when you have saved search criteria that specifies the **Include in my Quick Searches** option.
Add Filter	Click **Add Filter** to add a filter to the current search results.
Save Criteria	Click **Save Criteria** to save the current search criteria.
Save Results	Click **Save Results** to save the current search results. This option is only displayed after a search is complete. This option is disabled in streaming mode.

Table 4-1 Log Activity tab toolbar options (continued)

Option	Description
Cancel	Click **Cancel** to cancel a search in progress. This option is disabled in streaming mode.
False Positive	Click **False Positive** to open the False Positive Tuning window, which allows you to tune out events that are known to be false positives from creating offenses. For more information about false positives, see the **Glossary**. This option is disabled in streaming mode. For more information about tuning false positives, see **Tuning false positives**.
Rules	The Rules option is only visible if you have permission to view rules. Click **Rules** to configure custom event rules. Options include: • **Rules** - Select this option to view or create a rule. If you only have the permission to view rules, the summary page of the Rules Wizard is displayed. If you have the permission to maintain custom rules, the Rules Wizard is displayed and you can edit the rule. ***Note:*** *The anomaly detection rule options are only visible if you have the* ***Log Activity > Maintain Custom Rules*** *permission.* To enable the anomaly detection rule options (Add Threshold Rule, Add Behavioral Rule, and Add Anomaly Rule), you must save aggregated search criteria because the saved search criteria specifies the required parameters. • **Add Threshold Rule** - Select this option to create a threshold rule. A threshold rule tests event traffic for activity that exceeds a configured threshold. Thresholds can be based on any data collected by QRadar SIEM. For example, if you create a threshold rule indicating that no more than 220 clients can log into the server between 8 am and 5 pm, the rules generate an alert when the 221st client attempts to login. When you select the **Add Threshold Rule** option, the Rules Wizard is displayed, prepopulated with the appropriate options for creating a threshold rule. • **Add Behavioral Rule** - Select this option to create a behavioral rule. A behavioral rule tests event traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, you can create a behavioral rule to compare the average volume of traffic for the last 5 minutes with the average volume of traffic over the last hour. If there is more than a 40% change, the rule generates a response. When you select the **Add Behavioral Rule** option, the Rules Wizard is displayed, prepopulated with the appropriate options for creating a behavioral rule.

Table 4-1 Log Activity tab toolbar options (continued)

Option	Description
	• **Add Anomaly Rule** - Select this option to create an anomaly rule. An anomaly rule tests event traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, if an area of your network that never communicates with Asia starts communicating with hosts in that country, an anomaly rule generates an alert. When you select the **Add Anomaly Rule** option, the Rules Wizard is displayed, prepopulated with the appropriate options for creating an anomaly rule. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*
Actions	Click **Actions** to perform the following actions: • **Show All** - Select this option to remove all filters on search criteria and display all unfiltered events. • **Print** - Select this option to print the events displayed on the page. • **Export to XML > Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See **Exporting events**. • **Export to XML > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete. See **Exporting events**. • **Export to CSV > Visible Columns** - Select this option to export only the columns that are visible on the Log Activity tab. This is the recommended option. See **Exporting events**. • **Export to CSV > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete. See **Exporting events**. • **Delete** - Select this option to delete a search result. See **Managing event and flow search results**. • **Notify** - Select this option to specify that you want a notification emailed to you on completion of the selected searches. This option is only enabled for searches in progress. ***Note:*** *The* ***Print****,* ***Export to XML****, and* ***Export to CSV*** *options are disabled in streaming mode and when viewing partial search results.*

Table 4-1 Log Activity tab toolbar options (continued)

Option	Description
Quick Filter	Type your search criteria in the **Quick Filter** field and click the **Quick Filter** icon or press Enter on the keyboard. All events that match your search criteria are displayed in the events list. A text search is run on the event payload to determine which match your specified criteria. ***Note:*** *When you click the* ***Quick Filter*** *field, a tooltip is displayed, providing information on the appropriate syntax to use for search criteria. For more syntax information, see* **Quick Filter syntax**.

Quick Filter syntax

The Quick Filter feature enables you to search event payloads using a text search string. The Quick Filter functionality is available in the following locations on the user interface:

- **Log Activity toolbar** - On the toolbar, a **Quick Filter** field enables you to type a text search string and click the **Quick Filter** icon to apply your quick filter to the currently displayed list of events.
- **Add Filter dialog box** - From the **Add Filter** dialog box, accessed by clicking the **Add Filter** icon on the **Log Activity** tab, you can select **Quick Filter** as your filter parameter and type a text search string. This enables you to apply your quick filter to the currently displayed list of events or flows. For more information about the Add Filter dialog box, see **Quick Filter syntax**.
- **Event and Flow search pages** - From the event and flow search pages, you can add a Quick Filter to your list of filters to be included in your search criteria. For more information about configuring search criteria, see **Searching events or flows**.

When viewing events in real time (streaming) or last interval mode, you can only type simple words or phrases in the **Quick Filter** field. When viewing events using a time-range, use the following syntax guidelines for typing your text search criteria:

- Search terms can include any plain text that you expect to find in the payload. For example, `Firewall`
- Include multiple terms in double quotes to indicate that you want to search for the exact phrase. For example, `“Firewall deny"`
- Search terms can include single and multiple character wild cards. The search term cannot start with a wild card. For example, `F?rewall` or `F??ew*`
- Group terms using logical expressions, such as AND, OR, and NOT. The syntax is case sensitive and the operators must be upper case to be recognized as logical expressions and not as search terms. For example: `(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`

  When creating search criteria that includes the NOT logical expression, you must include at least one other logical expression type, otherwise, your filter will not return any results. For example: **`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`**

- The following characters must be preceded by a backslash to indicate that the character is part of your search term: + - && || ! () {} [] ^ " ~ * ? : \. For example: **`"%PIX\-5\-304001"`**

Right-click menu options

On the **Log Activity** tab, you can right-click an event to access additional event filter information.

The right-click menu options are:

Table 4-2 Right-click menu options

Option	Description
Filter on	Select this option to filter on the selected event, depending on the selected parameter in the event.
False Positive	Select this option to open the False Positive window, which allows you to tune out events that are known to be false positives from creating offenses. This option is disabled in streaming mode. See **Tuning false positives**.
More options:	Select this option to investigate an IP address or a user name. For more information about investigating an IP address, see **Investigating IP addresses**. For more information about investigating a user name, see **Investigating user names**. ***Note:*** *This option is not displayed in streaming mode.*

Status bar

When streaming events, the status bar displays the average number of results received per second. This is the number of results the Console successfully received from the Event Processors. If this number is greater than 40 results per second, only 40 results are displayed. The remainder is accumulated in the result buffer. To view additional status information, move your mouse pointer over the status bar.

When QRadar SIEM is not streaming events, the status bar displays the number of search results currently displayed on the tab and the amount of time required to process the search results.

Log activity monitoring

By default, the **Log Activity** tab displays events in streaming mode, allowing you to view events in real-time. For more information about streaming mode, see **Viewing streaming events**. You can specify a different time range to filter events using the **View** list box.

If you previously configured saved search criteria as the default, the results of that search are automatically displayed when you access the **Log Activity** tab. For more information about saving search criteria, see **Saving event and flow search criteria**.

Viewing streaming events

Streaming mode enables you to view event data entering your system. This mode provides you with a real-time view of your current event activity by displaying the last 50 events.

About this task

If you apply any filters on the **Log Activity** tab or in your search criteria before enabling streaming mode, the filters are maintained in streaming mode. However, streaming mode does not support searches that include grouped events. If you enable streaming mode on grouped events or grouped search criteria, the **Log Activity** tab displays the normalized events. See **Viewing normalized events**.

When you want to select an event to view details or perform an action, you must pause streaming before you double-click an event. When streaming is paused, the last 1,000 events are displayed.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **View** list box, select **Real Time (streaming)**.

For information on the toolbar options, see **Table 4-1**. For more information about the parameters displayed in streaming mode, see **Table 4-7**.

Step 3 Optional. Pause or play the streaming events. Choose one of the following options:

- To select an event record, click the **Pause** icon to pause streaming.
- To restart streaming mode, click the **Play** icon.

Viewing normalized events

QRadar SIEM collects events in raw format, and then normalizes the events for display on the **Log Activity** tab.

About this task

Normalization involves parsing raw event data and preparing the data to display readable information on the tab. When QRadar SIEM normalizes events, the system normalizes names as well. Therefore, the name that is displayed on the **Log Activity** tab might not match the name that is displayed in the event.

Note: If you have selected a time frame to display, a time series chart is displayed. For more information about using time series charts, see **Time series chart overview**.

The **Log Activity** tab displays the following parameters when you view normalized events:

Table 4-3 Log Activity tab - Default (Normalized) parameters

Parameter	Description
Current Filters	The top of the table displays the details of the filters applied to the search results. To clear these filter values, click **Clear Filter.** ***Note:*** *This parameter is only displayed after you apply a filter.*
View	From this list box, you can select the time range you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to* ***Current Statistics*** *to display or hide the statistics* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistical information.*
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see **Viewing associated offenses**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Offenses icon	Click the **Offenses** icon to view details of the offense associated with this event. For more information, see **Chart management**.
Event Name	Specifies the normalized name of the event.
Log Source	Specifies the log source that sent the event to QRadar SIEM. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.

Table 4-3 Log Activity tab - Default (Normalized) parameters (continued)

Parameter	Description
Event Count	Specifies the total number of events bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are detected within a short period of time.
Time	Specifies the date and time when QRadar SIEM received the event.
Low Level Category	Specifies the low-level category associated with this event. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.
Source IP	Specifies the source IP address of the event.
Source Port	Specifies the source port of the event.
Destination IP	Specifies the destination IP address of the event.
Destination Port	Specifies the destination port of the event.
Username	Specifies the user name associated with this event. User Names are often available in authentication related events. For all other types of events where the user name is not available, this field specifies N/A.
Magnitude	Specifies the magnitude of this event. Variables include credibility, relevance, and severity. Point your mouse over the magnitude bar to display values and the calculated magnitude. For more information about credibility, relevance, and severity, see the **Glossary**.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Display** list box, select **Default (Normalized)**.

Step 3 From the **View** list box, select the time frame you want to display.

Step 4 Click the **Pause** icon to pause streaming.

Step 5 Double-click the event you want to view in greater detail. See **Event details**.

Viewing raw events

You can view raw event data, which is the unparsed event data from the log source.

About this task

When you view raw event data, the **Log Activity** tab provides the following parameters for each event:

Table 4-4 Raw event parameters

Parameter	Description
Current Filters	The top of the table displays the details of the filters applied to the search results. To clear these filter values, click **Clear Filter.** ***Note:*** *This parameter is only displayed after you apply a filter.*
View	From the list box, select the time range you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to* ***Current Statistics*** *to display or hide the statistics.* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistic information.*
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see **Viewing associated offenses**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To displayed charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Offenses icon	Click this icon to view details of the offense associated with this event. For more information, see **Viewing associated offenses**.
Start Time	Specifies the time of the first event, as reported to QRadar SIEM by the log source.

Table 4-4 Raw event parameters (continued)

Parameter	Description
Log Source	Specifies the log source that originated the event. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
Payload	Specifies the original event payload information in UTF-8 format.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Display** list box, select **Raw Events**.

Step 3 From the **View** list box, select the time frame you want to display.

Step 4 Double-click the event you want to view in greater detail. See **Event details**.

Viewing grouped events

Using the **Log Activity** tab, you can view events grouped by various options. From the **Display** list box, you can select the parameter by which you want to group events.

About this task

The **Display** list box is not displayed in streaming mode because streaming mode does not support grouped events. If you entered streaming mode using non-grouped search criteria, this option is displayed.

The Display list box provides the following options:

Table 4-5 Grouped events options

Group option	Description
Low Level Category	Displays a summarized list of events grouped by the low-level category of the event. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Event Name	Displays a summarized list of events grouped by the normalized name of the event.
Destination IP	Displays a summarized list of events grouped by the destination IP address of the event.
Destination Port	Displays a summarized list of events grouped by the destination port address of the event.
Source IP	Displays a summarized list of events grouped by the source IP address of the event.
Custom Rule	Displays a summarized list of events grouped by the associated custom rule.
Username	Displays a summarized list of events grouped by the user name associated with the events.
Log Source	Displays a summarized list of events grouped by the log sources that sent the event to QRadar SIEM.

Table 4-5 Grouped events options (continued)

Group option	Description
High Level Category	Displays a summarized list of events grouped by the high-level category of the event. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Network	Displays a summarized list of events grouped by the network associated with the event.
Source Port	Displays a summarized list of events grouped by the source port address of the event.

After you select an option from the **Display** list box, the column layout of the data depends on the chosen group option. Each row in the events table represents an event group. The **Log Activity** tab provides the following information for each event group:

Table 4-6 Grouped event parameters

Parameter	Description
Grouping By	Specifies the parameter that the search is grouped on.
Current Filters	The top of the table displays the details of the filter applied to the search results. To clear these filter values, click **Clear Filter**.
View	From the list box, select the time range you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to* ***Current Statistics*** *to display or hide the statistics.* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot events, you might be asked to supply current statistic information.*

Table 4-6 Grouped event parameters (continued)

Parameter	**Description**
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the chart from your display. Each chart provides a legend, which is a visual reference to help you associate the chart objects to the parameters they represent. Using the legend feature, you can perform the following actions: • Move your mouse pointer over a legend item to view more information about the parameters it represents. • Right-click the legend item to further investigate the item. For more information about right-click menu options, see **About QRadar SIEM**. • Click a legend item to hide the item in the chart. Click the legend item again to show the hidden item. You can also click the corresponding graph item to hide and show the item. • Click **Legend** if you want to remove the legend from your chart display. ***Note:*** *The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see* **Viewing associated offenses**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Source IP (Unique Count)	Specifies the source IP address associated with this event. If there are multiple IP addresses associated with this event, this field specifies the term Multiple and the number of IP addresses.
Destination IP (Unique Count)	Specifies the destination IP address associated with this event. If there are multiple IP addresses associated with this event, this field specifies the term Multiple and the number of IP addresses.
Destination Port (Unique Count)	Specifies the destination ports associated with this event. If there are multiple ports associated with this event, this field specifies the term Multiple and the number of ports.
Event Name	Specifies the normalized name of the event.
Log Source (Unique Count)	Specifies the log sources that sent the event to QRadar SIEM. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
High Level Category (Unique Count)	Specifies the high-level category of this event. If there are multiple categories associated with this event, this field specifies the term Multiple and the number of categories. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide.*

Table 4-6 Grouped event parameters (continued)

Parameter	Description
Low Level Category (Unique Count)	Specifies the low-level category of this event. If there are multiple categories associated with this event, this field specifies the term Multiple and the number of categories. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Protocol (Unique Count)	Specifies the protocol ID associated with this event. If there are multiple protocols associated with this event, this field specifies the term Multiple and the number of protocol IDs.
Username (Unique Count)	Specifies the user name associated with this event, if available. If there are multiple user names associated with this event, this field specifies the term Multiple and the number of user names.
Magnitude (Maximum)	Specifies the maximum calculated magnitude for grouped events. Variables used to calculate magnitude include credibility, relevance, and severity. For more information about credibility, relevance, and severity, see the **Glossary**.
Event Count (Sum)	Specifies the total number of events bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.
Count	Specifies the total number of normalized events in this event group.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **View** list box, select the time frame you want to display.

Step 3 From the **Display** list box, choose which parameter you want to group events on. See **Table 4-5**.

The events groups are listed. For more information on the event group details. See **Table 4-6**.

Step 4 To view the List of Events page for a group, double-click the event group you want to investigate.

The List of Events page does not retain chart configurations you might have defined on the **Log Activity** tab. For more information about the List of Events page parameters, see **Table 4-3**.

Step 5 To view the details of an event, double-click the event you want to investigate. For more information on event details, see **Table 4-7**.

Event details

You can view a list of event in various modes, including streaming mode or in event groups. In whichever mode you choose to view events, you can locate and view the details of a single event. The event details page provides the following information:

Table 4-7 Event details

Parameter	**Description**
Event Information	
Event Name	Specifies the normalized name of the event.
Low Level Category	Specifies the low-level category of this event. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Event Description	Specifies a description of the event, if available.
Magnitude	Specifies the magnitude of this event. For more information about magnitude, see the **Glossary**.
Relevance	Specifies the relevance of this event. For more information about relevance, see the **Glossary**.
Severity	Specifies the severity of this event. For more information about severity, see the **Glossary**.
Credibility	Specifies the credibility of this event. For more information about credibility, see the **Glossary**.
Username	Specifies the user name associated with this event, if available.
Start Time	Specifies the time of the event was received from the log source.
Storage Time	Specifies the time that the event was stored in the QRadar SIEM database.
Log Source Time	Specifies the system time as reported by the log source in the event payload.
Anomaly Detection Information - This pane is only displayed if this event was generated by an anomaly detection rule. For more information about anomaly detection rules, see the *IBM Security QRadar SIEM Administration Guide*. Click the **Anomaly** icon to view the saved search results that caused the anomaly detection rule to generate this event.	
Rule Description	Specifies the anomaly detection rule that generated this event.
Anomaly Description	Specifies a description of the anomalous behavior that was detected by the anomaly detection rule.
Anomaly Alert Value	Specifies the anomaly alert value.
Source and Destination Information	
Source IP	Specifies the source IP address of the event.
Destination IP	Specifies the destination IP address of the event.
Source Asset Name	Specifies the user-defined asset name of the event source. For more information about assets, see **Asset management**.
Destination Asset Name	Specifies the user-defined asset name of the event destination. For more information about assets, see **Asset management**

Table 4-7 Event details (continued)

Parameter	**Description**
Source Port	Specifies the source port of this event.
Destination Port	Specifies the destination port of this event.
Pre NAT Source IP	For a firewall or another device capable of Network Address Translation (NAT), this parameter specifies the source IP address before the NAT values were applied. NAT translates an IP address in one network to a different IP address in another network.
Pre NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address before the NAT values were applied.
Pre NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port before the NAT values were applied.
Pre NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port before the NAT values were applied.
Post NAT Source IP	For a firewall or another device capable of NAT, this parameter specifies the source IP address after the NAT values were applied.
Post NAT Destination IP	For a firewall or another device capable of NAT, this parameter specifies the destination IP address after the NAT values were applied.
Post NAT Source Port	For a firewall or another device capable of NAT, this parameter specifies the source port after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter specifies the destination port after the NAT values were applied.
IPv6 Source	Specifies the source IPv6 address of the event.
IPv6 Destination	Specifies the destination IPv6 address of the event.
Source MAC	Specifies the source MAC address of the event.
Destination MAC	Specifies the destination MAC address of the event.
Payload Information	
Payload	Specifies the payload content from the event. This field offers three tabs to view the payload: • Universal Transformation Format (UTF) - Click **UTF**. • Hexadecimal - Click **HEX**. • Base64 - Click **Base64**.
Additional Information	
Protocol	Specifies the protocol associated with this event.
QID	Specifies the QID for this event. Each event has a unique QID. For more information about mapping a QID, see **Modifying event mapping**.

Table 4-7 Event details (continued)

Parameter	Description
Log Source	Specifies the log source that sent the event to QRadar SIEM. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events bundled in this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.
Custom Rules	Specifies custom rules that match this event. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*
Custom Rules Partially Matched	Specifies custom rules that partially match this event. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*
Annotations	Specifies the annotation for this event. Annotations are text descriptions that rules can automatically add to events as part of the rule response. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide*.
Identity Information - QRadar SIEM collects identity information, if available, from log source messages. Identity information provides additional details about assets on your network. Log sources only generate identity information if the log message sent to QRadar SIEM contains an IP address and least one of the following items: user name or MAC address. Not all log sources generate identity information. For more information about identity and assets, see **Asset management**.	
Identity Username	Specifies the user name of the asset associated with this event.
Identity IP	Specifies the IP address of the asset associated with this event.
Identity Net Bios Name	Specifies the Network Base Input/Output System (Net Bios) name of the asset associated with this event.
Identity Extended Field	Specifies additional information about the asset associated with this event. The content of this field is user-defined text and depends on the devices on your network that are available to provide identity information. Examples include: physical location of devices, relevant policies, network switch, and port names.
Has Identity (Flag)	Specifies True if QRadar SIEM has collected identify information for the asset associated with this event. For more information about which devices send identity information, see the *IBM Security QRadar DSM Configuration Guide*.
Identity Host Name	Specifies the host name of the asset associated with this event.
Identity MAC	Specifies the MAC address of the asset associated with this event.
Identity Group Name	Specifies the group name of the asset associated with this event.

Event details toolbar

The event details toolbar provides the following functions:

Table 4-8 Event details toolbar

Function	Description
Return to Events List	Click **Return to Event List** to return to the list of events.
Offense	Click **Offense** to display the offenses associated with the event.
Anomaly	Click **Anomaly** to display the saved search results that caused the anomaly detection rule to generate this event. ***Note:*** *This icon is only displayed if this event was generated by an anomaly detection rule.*
Map Event	Click **Map Event** to edit the event mapping. For more information, see **Modifying event mapping**.
False Positive	Click **False Positive** to tune QRadar SIEM to prevent false positive events from generating into offenses.
Extract Property	Click **Extract Property** to create a custom event property from the selected event. For more information, see **Custom event and flow properties**.
Previous	Click **Previous** to view the previous event in the event list.
Next	Click **Next** to view the next event in the event list.
PCAP Data	***Note:*** *This option is only displayed if your QRadar SIEM Console is configured to integrate with the Juniper JunOS Platform DSM. For more information about managing PCAP data, see* **Managing PCAP data***.* From the **PCAP Data** list box, select one of the following options: • **View PCAP Information** - Select this option to view the PCAP information. For more information, see **Viewing PCAP information**. • **Download PCAP File** - Select this option to download the PCAP file to your desktop system. For more information, see **Downloading the PCAP file to your desktop system**.
Print	Click **Print** to print the event details.

Viewing associated offenses

From the **Log Activity** tab, you can view the offense associated with the event.

About this task

If an event matches a rule, an offense can be generated on the **Offenses** tab. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide*. For more information about managing offenses, see **Offense management**.

When you view an offense from the **Log Activity** tab, the offense might not display if the Magistrate has not yet saved the offense associated with the selected event to disk or the offense has been purged from the database. If this occurs, the system notifies you.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Click the **Offense** icon beside the event you want to investigate.

Step 4 View the associated offense.

Modifying event mapping

You can manually map a normalized or raw event to a high-level and low-level category (or QID). This manual action allows QRadar SIEM to map unknown log source events to known QRadar SIEM events so that they can be categorized and processed appropriately.

About this task

For normalization purposes, QRadar SIEM automatically maps events from log sources to high- and low-level categories. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.

When QRadar SIEM receives events from log sources that the system is unable to categorize, QRadar SIEM categorizes these events as unknown. These events occur for several reasons, including:

- **User-defined Events** - Some log sources, such as Snort, allow you to create user-defined events.
- **New Events or Older Events** - Vendor log sources might update their software with maintenance releases to support new events that QRadar SIEM might not support.

Note: The **Map Event** icon is disabled for events when the high-level category is SIM Audit or the log source type is Simple Object Access Protocol (SOAP).

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Double-click the event you want to map.

Step 4 Click **Map Event**.

Step 5 If you know the QID that you want to map to this event, type the QID in the **Enter QID** field. Go to **Step 7**.

Step 6 If you do not know the QID you want to map to this event, you can search for a particular QID:

a Choose one of the following options:

- To search for a QID by category, select the high-level category from the **High-Level Category** list box.
- To search for a QID by category, select the low-level category from the **Low-Level Category** list box.
- To search for a QID by log source type, select a log source type from the **Log Source Type** list box.
- To search for a QID by name, type a name in the **QID/Name** field.

b Click **Search**.

A list of QIDs are displayed.

c Select the QID you want to associate this event with.

Step 7 Click **OK**.

Tuning false positives

You can use the False Positive Tuning function to prevent false positive events from creating offenses. You can tune false positive events from the event list or event details page.

About this task

You must have appropriate permissions for creating customized rules to tune false positives. For more information about roles, see the *IBM Security QRadar SIEM Administration Guide*. For more information about false positives, see the **Glossary**.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Select the event you want to tune.

Step 4 Click **False Positive**.

Step 5 In the Event/Flow Property pane on the False Positive window, select one of the following options:

- Event/Flow(s) with a specific QID of <Event>
- Any Event/Flow(s) with a low-level category of <Event>
- Any Event/Flow(s) with a high-level category of <Event>

Step 6 In the Traffic Direction pane, select one of the following options:

- <Source IP Address> to <Destination IP Address>
- <Source IP Address> to Any Destination
- Any Source to <Destination IP Address>
- Any Source to any Destination

Step 7 Click **Tune**.

Managing PCAP data

If your QRadar SIEM Console is configured to integrate with the Juniper JunOS Platform DSM, QRadar SIEM can receive, process, and store Packet Capture (PCAP) data from a Juniper SRX-Series Services Gateway log source.

For more information about the Juniper JunOS Platform DSM, see the *IBM Security QRadar DSM Configuration Guide*.

Displaying the PCAP data column

The PCAP Data column is not displayed on the **Log Activity** tab by default. When you create search criteria, you must select the **PCAP Data** column in the Column Definition pane.

Before you begin

Before you can display PCAP data on the **Log Activity** tab, the Juniper SRX-Series Services Gateway log source must be configured with the PCAP Syslog Combination protocol. For more information about configuring log source protocols, see the *IBM Security QRadar Log Sources Users Guide*.

About this task

When you perform a search that includes the **PCAP Data** column, an icon is displayed in the **PCAP Data** column of the search results if PCAP data is available for an event. Using the **PCAP** icon, you can view the PCAP data or download the PCAP file to your desktop system.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 From the **Search** list box, select **New Search**.

Step 3 Optional. To search for events that have PCAP data, configure the following search criteria:

- **a** From the first list box, select **PCAP data**.
- **b** From the second list box, select **Equals**.
- **c** From the third list box, select **True**.
- **d** Click **Add Filter**.

Step 4 Configure your column definitions to include the **PCAP Data** column:

- **a** From the **Available Columns** list in the Column Definition pane, click **PCAP Data**.
- **b** Click the **Add Column** icon on the bottom set of icons to move the **PCAP Data** column to the **Columns** list.
- **c** Optional. Click the **Add Column** icon in the top set of icons to move the **PCAP Data** column to the **Group By** list.

Step 5 Click **Filter**.

Step 6 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 7 Double-click the event you want to investigate.

What to do next

For more information about viewing and downloading PCAP data, see the following sections:

- **Viewing PCAP information**
- **Downloading the PCAP file to your desktop system**

Viewing PCAP information

From the **PCAP Data** toolbar menu, you can view the PCAP information or download the PCAP file to your desktop system. You can view a readable version of the data in the PCAP file.

Before you begin

Before you can view a PCAP information, you must perform or select a search that displays the **PCAP Data** column. See **Displaying the PCAP data column**.

About this task

Before PCAP data can be displayed, QRadar SIEM must retrieve the PCAP file for display on the user interface. If the download process takes an extended period of time, the Downloading PCAP Packet Information window is displayed. In most cases, the download process is quick and this window is not displayed.

After the file is retrieved, a pop-up window provides a readable version of the PCAP file. You can read the information displayed on the window, or download the information to your desktop system

Procedure

Step 1 For the event you want to investigate, choose one of the following options:

- Select the event and click the **PCAP** icon.
- Right-click the **PCAP** icon for the event and select **More Options > View PCAP Information**.
- Double-click the event you want to investigate, and then select **PCAP Data > View PCAP Information** from the event details toolbar.

Step 2 If you want to download the information to your desktop system, choose one of the following options:

- Click **Download PCAP File** to download the original PCAP file to be used in an external application.
- Click **Download PCAP Text** to download the PCAP information in .TXT format.

Step 3 Choose one of the following options:

- If you want to open the file for immediate viewing, select the **Open with** option and select an application from the list box.
- If you want to save the list, select the **Save File** option.

Step 4 Click **OK**.

Downloading the PCAP file to your desktop system

You can download the PCAP file to your desktop system for storage or for use in other applications.

Before you begin

Before you can view a PCAP information, you must perform or select a search that displays the **PCAP Data** column. See **Displaying the PCAP data column**.

Procedure

Step 1 For the event you want to investigate, choose one of the following options:

- Select the event and click the **PCAP** icon.
- Right-click the **PCAP** icon for the event and select **More Options > Download PCAP File**.
- Double-click the event you want to investigate, and then select **PCAP Data > Download PCAP File** from the event details toolbar.

Step 2 Choose one of the following options:

- If you want to open the file for immediate viewing, select the **Open with** option and select an application from the list box.
- If you want to save the list, select the **Save File** option.

Step 3 Click **OK**.

Exporting events

You can export events in Extensible Markup Language (XML) or Comma Separated Values (CSV) format. The length of time required to export your data depends on the number of parameters specified.

Procedure

Step 1 Click the **Log Activity** tab.

Step 2 Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.

Step 3 From the **Actions** list box, select one of the following options:

- **Export to XML > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
- **Export to XML > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete.
- **Export to CSV > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
- **Export to CSV > Full Export (All Columns)** - Select this option to export all event parameters. A full export can take an extended period of time to complete.

Step 4 If you want to resume your activities while the export is in progress, click **Notify When Done**.

Result

When the export is complete, you receive notification that the export is complete. If you did not select the **Notify When Done** icon, the status window is displayed.

5 NETWORK ACTIVITY INVESTIGATION

Using the **Network Activity** tab, you can monitor and investigate network activity (flows) in real-time or perform advanced searches.

Network Activity tab overview

You must have permission to view the **Network Activity** tab. For more information on permissions and assigning roles, see the *IBM Security QRadar SIEM Administration Guide*.

The **Network Activity** tab allows you to visually monitor and investigate flow data in real-time, or perform advanced searches to filter the displayed flows. A flow is a communication session between two hosts. You can view flow information to determine how the traffic is communicated, and what was communicated (if the content capture option is enabled). Flow information can also include such details as protocols, Autonomous System Number (ASN) values, or Interface Index (IFIndex) values.

Network Activity tab toolbar

Using the toolbar, you can access the following options:

Table 5-1 Network Activity tab toolbar options

Option	Description
Search	Click **Search** to perform advanced searches on flows. Options include: • **New Search** - Select this option to create a new flow search. • **Edit Search** - Select this option to select and edit a flow search. • **Manage Search Results** - Select this option to view and manage search results. For more information about the search feature, see **Data searches**.
Quick Searches	From this list box, you can run previously saved searches. Options are displayed in the **Quick Searches** list box only when you have saved search criteria that specifies the **Include in my Quick Searches** option.
Add Filter	Click **Add Filter** to add a filter to the current search results.
Save Criteria	Click **Save Criteria** to save the current search criteria.

Table 5-1 Network Activity tab toolbar options (continued)

Option	Description
Save Results	Click **Save Results** to save the current search results. This option is only displayed after a search is complete. This option is disabled in streaming mode.
Cancel	Click **Cancel** to cancel a search in progress. This option is disabled in streaming mode.
False Positive	Click **False Positive** to open the False Positive Tuning window, which allows you to tune out flows that are known to be false positives from creating offenses. For more information about false positives, see the **Glossary**. This option is disabled in streaming mode. See **Exporting flows**.

Table 5-1 Network Activity tab toolbar options (continued)

Option	Description
Rules	The Rules option is only visible if you have permission to view custom rules. Click **Rules** to configure custom flow rules. Options include: • **Rules** - Select this option to view or create a rule. If you only have the permission to view rules, the summary page of the Rules Wizard is displayed. If you have the permission to maintain custom rules, the Rules Wizard is displayed and you can edit the rule. ***Note:*** *The anomaly detection rule options are only visible if you have the* ***Network Activity > Maintain Custom Rules*** *permission.* To enable the anomaly detection rule options (Add Threshold Rule, Add Behavioral Rule, and Add Anomaly Rule), you must save aggregated search criteria because the saved search criteria specifies the required parameters. • **Add Threshold Rule** - Select this option to create a threshold rule. A threshold rule tests flow traffic for activity that exceeds a configured threshold. Thresholds can be based on any data collected by QRadar SIEM. For example, if you create a threshold rule indicating that no more than 220 clients can log into the server between 8 am and 5 pm, the rules generate an alert when the 221st client attempts to login. When you select the **Add Threshold Rule** option, the Rules Wizard is displayed, prepopulated with the appropriate options for creating a threshold rule. • **Add Behavioral Rule** - Select this option to create a behavioral rule. A behavior rule tests flow traffic for volume changes in behavior that occurs in regular seasonal patterns. For example, if a mail server typically communicates with 100 hosts per second in the middle of the night and then suddenly starts communicating with 1,000 hosts a second, a behavioral rule generates an alert. When you select the **Add Behavioral Rule** option, the Rules Wizard is displayed, prepopulated with the appropriate options for creating a behavioral rule. • **Add Anomaly Rule** - Select this option to create an anomaly rule. An anomaly rule tests flow traffic for abnormal activity, such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, you can create an anomaly rule to compare the average volume of traffic for the last 5 minutes with the average volume of traffic over the last hour. If there is more than a 40% change, the rule generates a response.

Table 5-1 Network Activity tab toolbar options (continued)

Option	Description
	When you select the **Add Anomaly Rule** option, the Rules Wizard is displayed, prepopulated with the appropriate options for creating an anomaly rule. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*
Actions	Click **Actions** to perform the following actions: • **Show All** - Select this option to remove all filters on search criteria and display all unfiltered flows. • **Print** - Select this option to print the flows displayed on the page. • **Export to XML** - Select this option to export flows in XML format. See **Exporting flows**. • **Export to CSV** - Select this option to export flows in CSV format. See **Exporting flows**. • **Delete** - Select this option to delete a search result. See **Data searches**. • **Notify** - Select this option to specify that you want a notification emailed to you on completion of the selected searches. This option is only enabled for searches in progress. ***Note:*** *The* ***Print****,* ***Export to XML****, and* ***Export to CSV*** *options are disabled in streaming mode and when viewing partial search results.*
Quick Filter	Type your search criteria in the **Quick Filter** field and click the **Quick Filter** icon or press Enter on the keyboard. All flows that match your search criteria are displayed in the flows list. A text search is run on the event payload to determine which match your specified criteria. ***Note:*** *When you click the* ***Quick Filter*** *field, a tooltip is displayed, providing information on the appropriate syntax to use for search criteria. For more syntax information, see* ***Quick Filter syntax****.*

Quick Filter syntax

The Quick Filter feature enables you to search flow payloads using a text search string. The Quick Filter functionality is available in the following locations on the user interface:

- **Network Activity toolbar** - On the toolbar, a **Quick Filter** field enables you to type a text search string and click the **Quick Filter** icon to apply your quick filter to the currently displayed list of flows.
- **Add Filter dialog box** - From the **Add Filter** dialog box, accessed by clicking the **Add Filter** icon on the **Network Activity** tab, you can select **Quick Filter** as your filter parameter and type a text search string. This enables you to apply your quick filter to the currently displayed list of flows. For more information about the **Add Filter** dialog box, see **Data searches**.

- **Flow search pages** - From the flow search pages, you can add a Quick Filter to your list of filters to be included in your search criteria. For more information about configuring search criteria, see **Data searches**.

When viewing flows in real time (streaming) or last interval mode, you can only type simple words or phrases in the **Quick Filter** field. When viewing flow using a time-range, use the following syntax guidelines for typing your text search criteria:

- Search terms can include any plain text that you expect to find in the payload. For example, `Firewall`
- Include multiple terms in double quotes to indicate that you want to search for the exact phrase. For example, `“Firewall deny"`
- Search terms can include single and multiple character wild cards. The search term cannot start with a wild card. For example, `F?rewall` or `F??ew*`
- Group terms using logical expressions, such as AND, OR, and NOT. The syntax is case sensitive and the operators must be upper case to be recognized as logical expressions and not as search terms. For example: `(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`

  When creating search criteria that includes the NOT logical expression, you must include at least one other logical expression type, otherwise, your filter will not return any results. For example: `(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
- The following characters must be preceded by a backslash to indicate that the character is part of your search term: + - && || ! () {} [] ^ " ~ * ? : \. For example: `"%PIX\-5\-304001"`

Right-click menu options

On the **Network Activity** tab, you can right-click a flow to access additional flow filter criteria.

The right-click menu options are:

Table 5-2 Right-click menu options

Option	Description
Filter on	Select this option to filter on the selected flow, depending on the selected parameter in the flow.
False Positive	Select this option to open the False Positive Tuning window, which allows you to tune out flows that are known to be false positives from creating offenses. This option is disabled in streaming mode. See **Exporting flows**.
More options:	Select this option to investigate an IP address. See **Investigating IP addresses**. ***Note:*** *This option is not displayed in streaming mode.*

Status bar

When streaming flows, the status bar displays the average number of results received per second. This is the number of results the Console successfully received from the Event Processors. If this number is greater than 40 results per second, only 40 results are displayed. The remainder is accumulated in the result buffer. To view additional status information, move your mouse pointer over the status bar.

When QRadar SIEM is not streaming flows, the status bar displays the number of search results currently displayed and the amount of time required to process the search results.

OverFlow records

If you have administrative permissions, you can specify the maximum number of flows you want to send from the QFlow Collector to the Event Processors. All data collected after the configured flow limit has been reached is grouped into one flow record. This flow record is then displayed on the **Network Activity** tab with a source IP address of 127.0.0.4 and a destination IP address of 127.0.0.5. This flow record specifies OverFlow on the **Network Activity** tab.

Network activity monitoring

By default, the **Network Activity** tab displays flows in streaming mode, allowing you to view flows in real-time. For more information about streaming mode, see **Viewing streaming flows**. You can specify a different time range to filter flows using the **View** list box.

If you previously configured a saved search as the default, the results of that search are automatically displayed when you access the **Network Activity** tab. For more information about saving search criteria, see **Saving event and flow search criteria**.

Viewing streaming flows

Streaming mode enables you to view flow data entering your system. This mode provides you with a real-time view of your current flow activity by displaying the last 50 flows.

About this task

If you apply any filters on the **Network Activity** tab or in your search criteria before enabling streaming mode, the filters are maintained in streaming mode. However, streaming mode does not support searches that include grouped flows. If you enable streaming mode on grouped flows or grouped search criteria, the **Network Activity** tab displays the normalized flows. See **Viewing normalized flows**.

When you want to select a flow to view details or perform an action, you must pause streaming before you double-click an event. When streaming is paused, the last 1,000 flows are displayed.

Procedure

Step 1 Click the **Network Activity** tab.

Step 2 From the **View** list box, select **Real Time (streaming)**.

For information on the toolbar options, see **Table 5-1**. For more information about the parameters displayed in streaming mode, see **Table 5-3**.

Step 3 Optional. Pause or play the streaming flows. Choose one of the following options:

- To select an event record, click the **Pause** icon to pause streaming.
- To restart streaming mode, click the **Play** icon.

Viewing normalized flows

QRadar SIEM collects flow data, and then normalizes the flow data for display on the **Network Activity** tab.

About this task

Normalization involves preparing flow data to display readable information on the tab.

Note: If you have selected a time frame to display, a time series chart is displayed. For more information about using the time series charts, see **Time series chart overview**.

The **Network Activity** tab displays the following parameters when you view normalized flows:

Table 5-3 Network Activity tab parameters

Parameter	Description
Current Filters	The top of the table displays the details of the filters applied to the search results. To clear these filter values, click **Clear Filter**. ***Note:*** *This parameter is only displayed after you apply a filter.*
View	From the list box, you can select the time range you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to* ***Current Statistics*** *to display or hide the statistics.* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot flows, you might be asked to supply current statistical information.*

Table 5-3 Network Activity tab parameters (continued)

Parameter	Description
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the charts from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see **Configuring charts**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Offense icon	Click the **Offenses** icon to view details of the offense associated with this flow.
Flow Type	Specifies the flow type. Flow types are measured by the ratio of incoming activity to outgoing activity. Flow types include: • **Standard Flow** - Bidirectional traffic • **Type A** - Single-to-Many (unidirectional), for example, a single host performing a network scan. • **Type B** - Many-to-Single (unidirectional), for example, a Distributed DoS (DDoS) attack. • **Type C** - Single-to-Single (unidirectional), for example, a host to host port scan.
First Packet Time	Specifies the date and time that QRadar SIEM received the flow.
Storage time	Specifies the time the flow was stored in the QRadar SIEM database.
Source IP	Specifies the source IP address of the flow.
Source Port	Specifies the source port of the flow.
Destination IP	Specifies the destination IP address of the flow.
Destination Port	Specifies the destination port of the flow.
Source Bytes	Specifies the number of bytes sent from the source host.
Destination Bytes	Specifies the number of bytes sent from the destination host.
Total Bytes	Specifies the total number of bytes associated with the flow.
Source Packets	Specifies the total number of packets sent from the source host.
Destination Packets	Specifies the total number of packets sent from the destination host.
Total Packets	Specifies the total number of packets associated with the flow.
Protocol	Specifies the protocol associated with the flow.
Application	Specifies the detected application of the flow. For more information about application detection, see the *IBM Security QRadar Application Configuration Guide*.

Table 5-3 Network Activity tab parameters (continued)

Parameter	Description
ICMP Type/Code	Specifies the Internet Control Message Protocol (ICMP) type and code, if applicable. If the flow has ICMP type and code information in a known format, this field displays as `Type <A>, Code <B>`, where `<A>` and `<B>` are the numeric values of the type and code.
Source Flags	Specifies the Transmission Control Protocol (TCP) flags detected in the source packet, if applicable.
Destination Flags	Specifies the TCP flags detected in the destination packet, if applicable.
Source QoS	Specifies the Quality of Service (QoS) service level for the flow. QoS enables a network to provide various levels of service for flows. QoS provides the following basic service levels: • **Best Effort** - This service level does not guarantee delivery. The delivery of the flow is considered best effort. • **Differentiated Service** - Certain flows are granted priority over other flows. This priority is granted by classification of traffic. • **Guaranteed Service** - This service level guarantees the reservation of network resources for certain flows.
Destination QoS	Specifies the QoS level of service for the destination flow.
Flow Source	Specifies the system that detected the flow. For more information about flow sources, see the *IBM Security QRadar SIEM Administration Guide*.
Flow Interface	Specifies the interface that received the flow.
Source If Index	Specifies the source Interface Index (IFIndex) number.
Destination If Index	Specifies the destination IFIndex number.
Source ASN	Specifies the source Autonomous System Number (ASN) value.
Destination ASN	Specifies the destination ASN value.

Procedure

Step 1 Click the **Network Activity** tab.

Step 2 From the **Display** list box, select **Default (Normalized)**.

Step 3 From the **View** list box, select the time frame you want to display.

Step 4 Click the **Pause** icon to pause streaming.

Step 5 Double-click the flow you want to view in greater detail. See **Flow details**.

Viewing grouped flows

Using the **Network Activity** tab, you can view flows grouped by various options. From the **Display** list box, you can select the parameter by which you want to group flows.

About this task

The **Display** list box is not displayed in streaming mode because streaming mode does not support grouped flows. If you entered streaming mode using non-grouped search criteria, this option is displayed.

The Display list box provides the following options:

Table 5-4 Grouped flow options

Group Option	Description
Unioned Flows	Displays several flows in one uninterrupted pattern across several intervals, in a single record. For example, if a flow is five minutes long, the unioned flow displays as a single flow five minutes long. Without the unioned flow, the flow displays as five flows: one flow for each minute. Unioned flows display a summarized list of flows grouped by unioned flow information.
Source or Destination IP	Displays a summarized list of flows grouped by the IP address associated with the flow.
Source IP	Displays a summarized list of flows grouped by the source IP address of the flow.
Destination IP	Displays a summarized list of flows grouped by the destination IP address of the flow.
Source Port	Displays a summarized list of flows grouped by the source port of the flow.
Destination Port	Displays a summarized list of flows grouped by the destination port of the flow.
Source Network	Displays a summarized list of flows grouped by the source network of the flow.
Destination Network	Displays a summarized list of flows grouped by the destination network of the flow.
Application	Displays a summarized list of flows grouped by the application that originated the flow.
Geographic	Displays a summarized list of flows grouped by geographic location.
Protocol	Displays a summarized list of flows grouped by the protocol associated with the flow.
Flow Bias	Displays a summarized list of flows grouped by the flow direction.
ICMP Type	Displays a summarized list of flows grouped by the ICMP type of the flow.

After you select an option from the **Display** list box, the column layout of the data depends on the chosen group option. Each row in the flows table represents an flow group. The **Network Activity** tab provides the following information for each flow group:

Table 5-5 Grouped flow parameters

Parameter	Description
Grouping By	Specifies the parameter that the search is grouped on.
Current Filters	The top of the table displays the details of the filter applied to the search results. To clear these filter values, click **Clear Filter**.
View	From the list box, select the time range you want to filter for.
Current Statistics	When not in Real Time (streaming) or Last Minute (auto refresh) mode, current statistics are displayed, including: ***Note:*** *Click the arrow next to **Current Statistics** to display or hide the statistics.* • **Total Results** - Specifies the total number of results that matched your search criteria. • **Data Files Searched** - Specifies the total number of data files searched during the specified time span. • **Compressed Data Files Searched** - Specifies the total number of compressed data files searched within the specified time span. • **Index File Count** - Specifies the total number of index files searched during the specified time span. • **Duration** - Specifies the duration of the search. ***Note:*** *Current Statistics are useful for troubleshooting. When you contact Customer Support to troubleshoot flows, you might be asked to supply current statistical information.*
Charts	Displays configurable charts representing the records matched by the time interval and grouping option. Click **Hide Charts** if you want to remove the graph from your display. The charts are only displayed after you select a time frame of Last Interval (auto refresh) or above, and a grouping option to display. For more information about configuring charts, see **Configuring charts**. ***Note:*** *If you use Mozilla Firefox as your browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.*
Source IP (Unique Count)	Specifies the source IP address of the flow.
Destination IP (Unique Count)	Specifies the destination IP address of the flow. If there are multiple destination IP addresses associated with this flow, this field specifies the term Multiple and the number of IP addresses.
Source Port (Unique Count)	Displays the source port of the flow.

Table 5-5 Grouped flow parameters (continued)

Parameter	Description
Destination Port (Unique Count)	Specifies the destination port of the flow. If there are multiple destination ports associated with this flow, this field specifies the term Multiple and the number of ports.
Source Network (Unique Count)	Specifies the source network of the flow. If there are multiple source networks associated with this flow, this field specifies the term Multiple and the number of networks.
Destination Network (Unique Count)	Specifies the destination network of the flow. If there are multiple destination networks associated with this flow, this field specifies the term Multiple and the number of networks.
Application (Unique Count)	Specifies the detected application of the flows. If there are multiple applications associated with this flow, this field specifies the term Multiple and the number of applications.
Source Bytes (Sum)	Specifies the number of bytes from the source.
Destination Bytes (Sum)	Specifies the number of bytes from the destination.
Total Bytes (Sum)	Specifies the total number of bytes associated with the flow.
Source Packets (Sum)	Specifies the number of packets from the source.
Destination Packets (Sum)	Specifies the number of packets from the destination.
Total Packets (Sum)	Specifies the total number of packets associated with the flow.
Count	Specifies the number of flows sent or received.

Procedure

Step 1 Click the **Network Activity** tab.

Step 2 From the **View** list box, select the time frame you want to display.

Step 3 From the **Display** list box, choose which parameter you want to group flows on. See **Table 5-4**.

The flow groups are listed. For more information on the flow group details. See **Table 5-6**.

Step 4 To view the List of Flows page for a group, double-click the flow group you want to investigate.

The List of Flows page does not retain chart configurations you might have defined on the **Network Activity** tab. For more information about the List of Flows parameters, see **Table 5-3**.

Step 5 To view the details of a flow, double-click the flow you want to investigate. For more information about the flow details page, see **Table 5-6**.

Flow details

You can view a list of flows in various modes, including streaming mode or in flow groups. In whichever mode you choose to view flows, you can locate and view the details of a single flow. The flow details page provides the following information:

Table 5-6 Flow details

Parameter	Description
Flow Information	
Protocol	Specifies the protocol associated with this flow. For more information about protocols, see the *IBM Security QRadar Application Configuration Guide*.
Application	Specifies the detected application of the flow. For more information about application detection, see the *IBM Security QRadar Application Configuration Guide*.
Magnitude	Specifies the magnitude of this flow. For more information about magnitude, see the **Glossary**.
Relevance	Specifies the relevance of this flow. For more information about relevance, see the **Glossary**.
Severity	Specifies the severity of this flow. For more information about severity, see the **Glossary**.
Credibility	Specifies the credibility of this flow. For more information about credibility, see the **Glossary**.
First Packet Time	Specifies the start time of the flow, as reported to QRadar SIEM by the flow source. For more information about flow sources, see the *IBM Security QRadar SIEM Administration Guide*.
Last Packet Time	Specifies the end time of the flow, as reported to QRadar SIEM by the flow source. For more information about flow sources, see the *IBM Security QRadar SIEM Administration Guide*.
Storage Time	Specifies the time the flow was stored in the QRadar SIEM database.
Event Name	Specifies the normalized name of the flow.
Low Level Category	Specifies the low-level category of this flow. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Event Description	Specifies a description of the flow, if available.
Source and Destination Information	
Source IP	Specifies the source IP address of the flow.
Destination IP	Specifies the destination IP address of the flow.
Source Asset Name	Specifies the source asset name of the flow. For more information about assets, see **Asset management**.
Destination Asset Name	Specifies the destination asset name of the flow. For more information about assets, see **Asset management**.
IPv6 Source	Specifies the source IPv6 address of the flow.
IPv6 Destination	Specifies the destination IPv6 address of the flow.

Table 5-6 Flow details (continued)

Parameter	Description
Source Port	Specifies the source port of the flow.
Destination Port	Specifies the destination port of the flow.
Source QoS	Specifies the QoS level of service for the source flow.
Destination QoS	Specifies the QoS level of service for the destination flow.
Source ASN	Specifies the source ASN number. ***Note:*** *If this flow has duplicate records from multiple flow sources, the corresponding source ASN numbers are listed.*
Destination ASN	Specifies the destination ASN number. ***Note:*** *If this flow has duplicate records from multiple flow sources, the corresponding destination ASN numbers are listed.*
Source If Index	Specifies the source IFIndex number. ***Note:*** *If this flow has duplicate records from multiple flow sources, the corresponding source IFIndex numbers are listed.*
Destination If Index	Specifies the destination IFIndex number. ***Note:*** *If this flow has duplicate records from multiple flow sources, the corresponding source IFIndex numbers are listed.*
Source Payload	Specifies the packet and byte count for the source payload.
Destination Payload	Specifies the packet and byte count for the destination payload.
Payload Information	
Source Payload	Specifies source payload content from the flow. This field offers three formats to view the payload: • Universal Transformation Format (UTF) - Click **UTF**. • Hexidecimal - Click **HEX**. • Base64 - Click **Base64**. ***Note:*** *If your flow source is Netflow v9 or IPFIX, unparsed fields from these sources might be displayed in the* ***Source Payload*** *field. The format of the unparsed field is <name>=<value>. For example,* ***MIN_TTL=x****.*
Destination Payload	Specifies destination payload content from the flow. This field offers three formats to view the payload: • Universal Transformation Format (UTF) - Click **UTF**. • Hexidecimal - Click **HEX**. • Base64 - Click **Base64**.

Table 5-6 Flow details (continued)

Parameter	Description
Additional Information	
Flow Type	Specifies the flow type. Flow types are measured by the ratio of incoming activity to outgoing activity. Flow types include: • **Standard** - Bidirectional traffic • **Type A** - Single-to-Many (unidirectional) • **Type B** - Many-to-Single (unidirectional) • **Type C** - Single-to-Single (unidirectional)
Flow Direction	Specifies the direction of the flow. Flow directions include: • **L2L** - Internal traffic from a local network to another local network. • **L2R** - Internal traffic from a local network to a remote network. • **R2L** - Internal traffic from a remote network to a local network. • **R2R** - Internal traffic from a remote network to another remote network.
Custom Rules	Specifies custom rules that match this flow. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*
Custom Rules Partially Matched	Specifies custom rules that partially match to this flow. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*
Flow Source/Interface	Specifies the flow source name of the system that detected the flow. ***Note:*** *If this flow has duplicate records from multiple flow sources, the corresponding flow sources are listed.*
Annotations	Specifies the annotation or notes for this flow. Annotations are text descriptions that rules can automatically add to flows as part of the rule response. For more information about rules, see the *IBM Security QRadar SIEM Administration Guide.*

Flow details toolbar

The flow details toolbar provides the following functions:

Table 5-7 Flow details toolbar

Function	Description
Return to Results	Click **Return to Results** to return to the list of flows.
Offense	Click **Offense** to display the offenses that the flow was correlated to.
Extract Property	Click **Extract Property** to create a custom flow property from the selected flow. For more information, see **Custom event and flow properties**.

Table 5-7 Flow details toolbar (continued)

Function	Description
False Positive	Click **False Positive** to open the False Positive Tuning window, which allows you to tune out flows that are known to be false positives from creating offenses. This option is disabled in streaming mode. See **Exporting flows**.
Previous	Click **Previous** to view the previous flow in the event list.
Next	Click **Next** to view the next flow in the event list.
Print	Click **Print** to print the flow details.

Tuning false positives

You can use the False Positive Tuning function to prevent false positive flows from creating offenses. You can tune false positive flows from the flow list or flow details page.

About this task

You must have appropriate permissions for creating customized rules to tune false positives. For more information about roles, see the *IBM Security QRadar SIEM Administration Guide*. For more information about false positives, see the **Glossary**.

Procedure

Step 1 Click the **Network Activity** tab.

Step 2 Optional. If you are viewing flows in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Select the flow you want to tune.

Step 4 Click **False Positive**.

Step 5 In the Event/Flow Property pane on the False Positive window, select one of the following options:

- Event/Flow(s) with a specific QID of <Event>
- Any Event/Flow(s) with a low-level category of <Event>
- Any Event/Flow(s) with a high-level category of <Event>

Step 6 In the Traffic Direction pane, select one of the following options:

- <Source IP Address> to <Destination IP Address>
- <Source IP Address> to Any Destination
- Any Source to <Destination IP Address>
- Any Source to any Destination

Step 7 Click **Tune**.

Note: You can tune false positive flows from the summary or details page.

Exporting flows

You can export flows in Extensible Markup Language (XML) or Comma Separated Values (CSV) format. The length of time required to export your data depends on the number of parameters specified.

Procedure

Step 1 Click the **Network Activity** tab.

Step 2 Optional. If you are viewing flows in streaming mode, click the **Pause** icon to pause streaming.

Step 3 From the **Actions** list box, select one of the following options:

- **Export to XML > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
- **Export to XML > Full Export (All Columns)** - Select this option to export all flow parameters. A full export can take an extended period of time to complete.
- **Export to CSV > Visible Columns** - Select this option to export only the columns that are visible on the **Log Activity** tab. This is the recommended option.
- **Export to CSV > Full Export (All Columns)** - Select this option to export all flow parameters. A full export can take an extended period of time to complete.

Step 4 If you want to resume your activities, click **Notify When Done**.

Result

When the export is complete, you receive notification that the export is complete. If you did not select the **Notify When Done** icon, the status window is displayed.

6 CHART MANAGEMENT

Using the charts on the **Log Activity** and **Network Activity** tabs, you can view your data using various chart configuration options.

Charts overview

If you select a time frame or a grouping option to view your data on the **Log Activity** and **Network Activity** tabs, charts display above the event or flow list. Charts do not display while in streaming mode.

You can configure a chart to select what data you want to plot. You can configure charts independently of each other to display your search results from different perspectives.

Chart types include:

- **Bar Chart** - Displays data in a bar chart. This option is only available for grouped events.
- **Pie Chart** - Displays data in a pie chart. This option is only available for grouped events.
- **Table** - Displays data in a table. This option is only available for grouped events.
- **Time Series** - Displays an interactive line chart representing the records matched by a specified time interval. For information on configuring time series search criteria, see **Time series chart overview**.

After you configure a chart, your chart configurations are retained when you:

- Change your view using the **Display** list box.
- Apply a filter.
- Save your search criteria.

Your chart configurations are not retained when you:

- Start a new search.
- Access a quick search.

- View grouped results in a branch window.
- Save your search results.

Note: If you use the Mozilla Firefox web browser and an ad blocker browser extension is installed, charts do not display. To display charts, you must remove the ad blocker browser extension. For more information, see your browser documentation.

Time series chart overview

Time series charts are graphical representations of your log or network activity over time. Peaks and valleys displayed in the charts depict high and low volume activity. Time series charts are useful for short-term and long-term trending of data. Using time series charts, you can access, navigate, and investigate log or network activity from various views and perspectives.

Note: You must have the appropriate role permissions to manage and view time series charts. For more information about role permissions, see the *IBM Security QRadar SIEM Administration Guide*.

To display time series charts, you must create and save a search that includes time series and grouping options. QRadar SIEM supports up to 100 saved time series searches. QRadar SIEM includes default time series saved searches, which you can access from the list of available searches on the event or flow search page. You can easily identify saved time series searches on the **Quick Searches** menu, because the search name is appended with the time range specified in the search criteria.

If your search parameters match a previously saved search for column definition and grouping options, a time series chart might automatically display for your search results. If a time series chart does not automatically display for your unsaved search criteria, no previously saved search criteria exists to match your search parameters. If this occurs, you must enable time series data capture and save your search criteria.

You can magnify and scan a time line on a time series chart to investigate log or network activity. The following table provides functions you can use to view time series charts:

Table 6-1 Time series charts functions

Function	Description
View data in greater detail	Using the zoom feature, you can investigate smaller time segments of event traffic. • Move your mouse pointer over the chart, and then use your mouse wheel to magnify the chart (roll the mouse wheel up). • Highlight the area of the chart you want to magnify. When you release your mouse button, the chart displays a smaller time segment. Now you can click and drag the chart to scan the chart. When you magnify a time series chart, the chart refreshes to display a smaller time segment.
View a larger time span of data	Using the zoom feature, you can investigate larger time segments or return to the maximum time range. You can expand a time range using one of the following options: • Click **Zoom Reset** at the top left corner of the chart. • Move your mouse pointer over the chart, and then use your mouse wheel to expand the view (roll the mouse wheel down).
Scan the chart	When you have magnified a time series chart, you can click and drag the chart left or right to scan the time line.

Chart legends

Each chart provides a legend, which is a visual reference to help you associate the chart objects to the parameters they represent.

Using the legend feature, you can perform the following actions:

- Move your mouse pointer over a legend item or the legend color block to view more information about the parameters it represents.
- Right-click the legend item to further investigate the item. For more information about right-click menu options, see **About QRadar SIEM**.
- Click a pie or bar chart legend item to hide the item in the chart. Click the legend item again to show the hidden item. You can also click the corresponding graph item to hide and show the item.
- Click **Legend**, or the arrow beside it, if you want to remove the legend from your chart display.

Configuring charts

You can use configuration options to change the chart type, the object type you want to chart, and the number of objects represented on the chart. For time series charts, you can also select a time range and enable time series data capture.

About this task

QRadar SIEM can accumulate data so that when you perform a time series search, a cache of data is available to display data for the previous time period. After you enable time series data capture for a selected parameter, an asterisk (*) is displayed next to the parameter in the **Value to Graph** list box.

Before you begin

Charts are not displayed when you view events or flows in Real Time (streaming) mode. To display charts, you must access the **Log Activity** or **Network Activity** tab, and choose one of the following options:

- Select options from the **View** and **Display** list boxes, and then click **Save Criteria** on the toolbar. See **Saving event and flow search criteria**.
- On the toolbar, select a saved search from the **Quick Search** list box.
- Perform a grouped search, and then click **Save Criteria** on the toolbar. See **Searching events or flows** and **Saving event and flow search criteria**.

If you plan to configure a time series chart, ensure that the saved search criteria is grouped and specifies a time range.

Procedure

Step 1 Click the **Log Activity** or **Network Activity** tab.

Step 2 In the Charts pane, click the **Configure** icon.

Step 3 Configure values the following parameters:.

Parameters	Description
Value to Graph	From the list box, select the object type that you want to graph on the Y axis of the chart. Options include all normalized and custom event or flow parameters included in your search parameters.
Display Top	From the list box, select the number of objects you want to view in the chart. The default is 10. Charting any more than 10 items might cause your chart data to be unreadable.
Chart Type	From the list box, select the chart type you want to view. If your bar, pie, or table chart is based on saved search criteria with a time range of more than 1 hour, you must click **Update Details** to update the chart and populate the event details.
Capture Time Series Data	Select this check box if you want to enable time series data capture. When you select this check box, the chart feature begins accumulating data for time series charts. By default, this option is disabled. This option is only available on Time Series charts.

Parameters	**Description**
Time Range	From the list box, select the time range you want to view. This option is only available on Time Series charts.

Step 4 If you selected the **Time Series** chart option and enabled the **Capture Time Series Data** option, click **Save Criteria** on the toolbar.

Step 5 To view the list of events or flows if your time range is greater than 1 hour, click **Update Details**.

7 DATA SEARCHES

On the **Log Activity**, **Network Activity**, and **Offenses** tabs, you can search events, flows, and offenses using specific criteria. You can create a new search or load a previously saved set of search criteria. You can select, organize, and group the columns of data to be displayed in search results.

Event and flow Searches

You can perform searches on the **Log Activity** and **Network Activity** tabs. After you perform a search, you can save the search criteria and the search results.

Searching events or flows

On the **Log Activity** and **Network Activity** tabs, you can search for events and flows that match your search criteria.

About this task

When you perform a search, QRadar SIEM searches the entire database for events or flows that match your criteria. This process might take an extended period of time depending on the size of your database.

The **Quick Filter** search parameter in the Search Parameters pane allows you to search for events or flows that match your text string in the event payload. For more information about how to use the **Quick Filter** parameter, see **Quick Filter syntax** (events) or **Quick Filter syntax** (flows).

The following table describes the search options you can use to search event and flow data:

Table 7-1 Event and flow search options

Options	Description
Group	This list box allows you to select an event search group or flow Search Group to view in the **Available Saved Searches** list.
Type Saved Search or Select from List	This field allows you to type the name of a saved search or a keyword to filter the **Available Saved Searches** list.
Available Saved Searches	This list displays all available searches, unless you apply a filter to the list using the **Group or Type Saved Search** or **Select from List** options. You can select a saved search on this list to display or edit.

Table 7-1 Event and flow search options

Options	**Description**
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Include in my Quick Searches	This check box allows you to include this search in your **Quick Search** menu, which is located on the **Log Activity** tab and **Network Activity** toolbars. For more information about the **Quick Search** menu, see **Log activity investigation** or **Network activity investigation**.
Include in my Dashboard	This check box allows you to include the data from your saved search on the **Dashboard** tab. For more information on the **Dashboard** tab, see **Dashboard management**. ***Note:*** *This parameter is only displayed if the search is grouped.*
Set as Default	This check box allows you to set this search as your default search when you access the **Log Activity** or **Network Activity** tab.
Share with Everyone	This check box allows you to share this search with all other users.
Real Time (streaming)	This option allows you to display event or flow results in streaming mode. For more information on streaming mode, see **Viewing streaming events**. ***Note:*** *When Real Time (streaming) is enabled, you are unable to group your search results. If you select any grouping option in the Column Definition pane, an error message opens.*
Last Interval (auto refresh)	This option allows you the search results to display in auto-refresh mode. In auto-refresh mode, the **Log Activity** and **Network Activity** tabs refresh at one minute intervals to display the most recent information.
Recent	This option allows you to select a predefined time range for your search. After you select this option, you must select a time range option from the list box.
Specific Interval	This option allows you to select a custom time range for your search. After you select this option, you must select the date and time range from the **Start Time** and **End Time** calendars.

Table 7-1 Event and flow search options

Options	Description
Data Accumulation	This pane is only displayed when you load a saved search. Enabling unique counts on accumulated data that is shared with many other saved searches and reports may decrease system performance. When you load a saved search, this pane displays the following options: • If no data is accumulating for this saved search, the following information message is displayed: `Data is not being accumulated for this search`. • If data is accumulating for this saved search, the following options are displayed: **columns** - When you click or hover your mouse over this link, a list of the columns that are accumulating data opens. **Enable Unique Counts/Disable Unique Counts** - This link allows you to enable or disable the search results to display unique event and flow counts instead of average counts over time. After you click the **Enable Unique Counts** link, a dialog box opens and indicates which saved searches and reports share the accumulated data.
Current Filters	This list displays the filters applied to this search. The options to add a filter are located above **Current Filters** list.
Save results when the search is complete	This check box allows you to save and name the search results.
Display	This list allows you to select a predefined column set to display in the search results.
Type Column or Select from List	You can use field to filter the columns that are listed in the **Available Columns** list. You can type the name of the column you want to locate or type a keyword to display a list of column names that include that keyword. For example, type **Device** to display a list of columns that include Device in the column name.
Available Columns	This list displays available columns. Columns that are currently in use for this saved search are highlighted and displayed in the **Columns** list.
Add and remove column icons (top set)	The top set of icons allows you to customize the **Group By** list. • **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** icon. • **Remove Column** - Select one or more columns from the **Group By** list and click the **Remove Column** icon.

Table 7-1 Event and flow search options

Options	Description
Add and remove column icons (bottom set)	The bottom set of icon allows you to customize the **Columns** list. • **Add Column** - Select one or more columns from the **Available Columns** list and click the **Add Column** icon. • **Remove Column** - Select one or more columns from the **Columns** list and click the **Remove Column** icon.
Group By	This list specifies the columns on which the saved search groups the results. You can further customize the **Group By** list using the following options: • **Move Up** - Select a column and move it up through the priority list using the **Move Up** icon. • **Move Down** - Select a column and move it down through the priority list using the **Move Down** icon. The priority list specifies in which order the results are grouped. The search results are grouped by the first column in the **Group By** list and then grouped by the next column on the list.
Columns	Specifies columns chosen for the search. You can select more columns from the **Available Columns** list. You can further customize the **Columns** list by using the following options: • **Move Up** - Select a column and move it up through the priority list using the **Move Up** icon. • **Move Down** - Select a column and move it down through the priority list using the **Move Down** icon. If the column type is numeric or time-based and there is an entry in the **Group By** list, the column includes a list box to allow you to choose how you want to group the column. If the column type is group, the column includes a list box to allow you to choose how many levels you want to include for the group.
Order By	From the first list box, select the column by which you want to sort the search results. Then, from the second list box, select the order you want to display for the search results. Options include **Descending** and **Ascending**.

Procedure

Step 1 Choose one of the following options:

- To search events, click the **Log Activity** tab.
- To search flows, click the **Network Activity** tab.

Step 2 From the **Search** list box, select **New Search**.

Step 3 Choose one of the following options:

- To load a previously saved search, go to **Step 4**.
- To create a new search, go to **Step 5**.

Step 4 Select a previously saved search:

a Choose one of the following options:

- From the **Available Saved Searches** list, select the saved search you want to load.
- In the **Type Saved Search or Select from List** field, type the name of the search you want to load.

b Click **Load**.

c In the Edit Search pane, select the options you want for this search. See **Table 7-1**.

Step 5 In the Time Range pane, select the options for the time range you want to capture for this search. See **Table 7-1**.

Step 6 Optional. In the Data Accumulation pane, enable unique counts:

a Click **Enable Unique Counts**.

b On the Warning window, read the warning message and click **Continue**. For more information on enabling unique counts, see **Table 7-1**.

Step 7 In the Search Parameters pane, define your search criteria:

a From the first list box, select a parameter you want to search for. For example, Device, Source Port, or Event Name.

b From the second list box, select the modifier you want to use for the search.

c In the entry field, type specific information related to your search parameter.

d Click **Add Filter**.

e Repeat steps **a** through **d** for each filter you want to add to the search criteria.

Step 8 Optional. To automatically save the search results when the search is complete, select the **Save results when search is complete** check box, and then type a name for the saved search.

Step 9 In the Column Definition pane, define the columns and column layout you want to use to view the results:

a From the **Display** list box, select the preconfigured column set to associate with this search.

b Click the arrow next to **Advanced View Definition** to display advanced search parameters.

c Customize the columns to display in the search results. See **Table 7-1**.

Step 10 Click **Filter**.

Result

When you generate a search that displays on the **Log Activity** or **Network Activity** tab before the search has collected all results, the partial results page is displayed. If the search is not complete, the **In Progress (<percent>% Complete)** status is displayed in the top right corner.

While viewing partial search results, the search engine works in the background to complete the search and refreshes the partial results to update your view.

When the search is complete, the **Completed** status is displayed in the top right corner.

Saving event and flow search criteria

On the **Log Activity** and **Network Activity** tabs, you can save configured search criteria so that you can re-use the criteria and use the saved search criteria in other QRadar SIEM components, such as reports. Saved search criteria does not expire.

About this task

If you specify a time range for your search, QRadar SIEM appends your search name with the specified time range. For example, a saved search named Exploits by Source with a time range of Last 5 minutes becomes Exploits by Source - Last 5 minutes.

If you change a column set in a previously saved search, and then save the search criteria using the same name, previous accumulations for time series charts are lost.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 Perform a search. See **Searching events or flows**.

The search results are displayed.

Step 3 Click **Save Criteria**.

Step 4 Enter values for the parameters:

Parameter	Description
Search Name	Type the unique name you want to assign to this search criteria.
Assign Search to Group(s)	Select the check box for the group you want to assign this saved search. If you do not select a group, this saved search is assigned to the **Other** group by default. For more information, see **Managing search groups**.
Manage Groups	Click **Manage Groups** to manage search groups. For more information, see **Managing search groups**.

Parameter	Description
Timespan options:	Choose one of the following options: • **Real Time (streaming)** - Select this option to filter your search results while in streaming mode. For more information about streaming mode, see **Viewing streaming events** or **Viewing streaming flows**. • **Last Interval (auto refresh)** - Select this option to filter your search results while in auto-refresh mode. The **Log Activity** and **Network Activity** tabs refreshes at one minute intervals to display the most recent information. • **Recent** - Select this option and, from this list box, select the time range you want to filter for. • **Specific Interval** - Select this option and, from the calendar, select the date and time range you want to filter for.
Include in my Quick Searches	Select this check box to include this search in your **Quick Search** list box, which is located on the **Log Activity** and **Network Activity** toolbars.
Include in my Dashboard	Select this check box to include the data from your saved search on the **Dashboard** tab. For more information about the **Dashboard** tab, see **Dashboard management**. ***Note:*** *This parameter is only displayed if the search is grouped.*
Set as Default	Select this check box to set this search as your default search when you access the **Log Activity** or **Network Activity** tab.
Share with Everyone	Select this check box to share these search requirements with all other QRadar SIEM users.

Step 5 Click **OK**.

Offense searches

You can search offenses using specific criteria to display offenses that match the search criteria in a results list. You can create a new search or load a previously saved set of search criteria.

Searching offenses on the My Offenses and All Offenses pages

On the **My Offenses** and **All Offenses** pages of the **Offense** tab, you can search for offenses that match your criteria.

About this task

The following table describes the search options you can use to search offense data on the My Offenses and All Offenses pages:

Table 7-2 My Offenses and All Offenses page search options

Options	Description
Group	This list box allows you to select an offense Search Group to view in the **Available Saved Searches** list.

Table 7-2 My Offenses and All Offenses page search options

Options	Description
Type Saved Search or Select from List	This field allows you to type the name of a saved search or a keyword to filter the **Available Saved Searches** list.
Available Saved Searches	This list displays all available searches, unless you apply a filter to the list using the **Group or Type Saved Search** or **Select from List** options. You can select a saved search on this list to display or edit.
All Offenses	This option allows you to search all offenses regardless of time range.
Recent	This option allows you to select a pre-defined time range you want to filter for. After you select this option, you must select a time range option from the list box.
Specific Interval	This option allows you to configure a custom time range for your search. After you select this option, you must select one of the following options. • **Start Date between** - Select this check box to search offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search. • **Last Event/Flow between** - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Offense Id	In this field, you can type the Offense ID you want to search for.
Description	In this field, you can type the description you want to search for.
Assigned to user	From this list box, you can select the user name you want to search for.
Direction	From this list box, you can select the offense direction you want to search for. Options include: • Local to Local • Local to Remote • Remote to Local • Remote to Remote • Local to Remote or Local • Remote to Remote or Local
Source IP	In this field, you can type the source IP address or CIDR range you want to search for.
Destination IP	In this field, you can type the destination IP address or CIDR range you want to search for.

Table 7-2 My Offenses and All Offenses page search options

Options	Description
Magnitude	From this list box, you can specify a magnitude and then select to display only offenses with a magnitude that is equal to, less than, or greater than the configured value. The range is 0 to 10.
Severity	From this list box, you can specify a severity and then select to display only offenses with a severity that is equal to, less than, or greater than the configured value. The range is 0 to 10.
Credibility	From this list box, you can specify a credibility and then select to display only offenses with a credibility that is equal to, less than, or greater than the configured value. The range is 0 to 10.
Relevance	From this list box, you can specify a relevance and then select to display only offenses with a relevance that is equal to, less than, or greater than the configured value. The range is 0 to 10.
Contains Username	In this field, you can type a regular expression (regex) statement to search for offenses containing a specific user name. When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.
Source Network	From this list box, you can select the source network you want to search for.
Destination Network	From this list box, you can select the destination network you want to search for.
High Level Category	From this list box, you can select the high-level category you want to search for. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Low Level Category	From this list box, you can select the low-level category you want to search for. For more information about categories, see the *IBM Security QRadar SIEM Administration Guide*.
Exclude	The options in this pane allow you to exclude offenses from the search results. The options include: • Active Offenses • Hidden Offenses • Closed Offenses • Inactive offenses • Protected Offense
Close by User	This parameter is only displayed when the **Closed Offenses** check box is cleared in the Exclude pane. From this list box, you can select the user name you want to search closed offenses for or select **Any** to displayed all closed offenses.
Reason For Closing	This parameter is only displayed when the **Closed Offenses** check box is cleared in the Exclude pane. From this list box, you can select a reason you want to search closed offenses for or select **Any** to displayed all closed offenses.

Table 7-2 My Offenses and All Offenses page search options

Options	Description
Events	From this list box, you can specify an event count and then select to display only offenses with an event count that is equal to, less than, or greater than the configured value.
Flows	From this list box, you can specify a flow count and then select to display only offenses with a flow count that is equal to, less than, or greater than the configured value.
Total Events/Flows	From this list box, you can specify a total event and flow count and then select to display only offenses with a total event and flow count that is equal to, less than, or greater than the configured value.
Destinations	From this list box, you can specify a destination IP address count and then select to display only offenses with a destination IP address count that is equal to, less than, or greater than the configured value.
Log Source Group	From this list box, you can select a log source group that contains the log source you want to search for. The **Log Source** list box displays all log sources assigned to the selected log source group.
Log Source	From this list box, you can select the log source you want to search for.
Rule Group	From this list box, you can select a rule group that contains the contributing rule you want to search for. The **Rule** list box displays all rules assigned to the selected rule group.
Rule	From this list box, you can select the contributing rule you want to search for.
Offense Type	From this list box, you can select an offense type you want to search for. For more information on the options in the **Offense Type** list box, see Table 7-3.

The following table describes the options available in the Offense Type list box:

Table 7-3 Offense type options

Offense types	Description
Any	This option searches all offense sources.
Source IP	To search for offenses with a specific source IP address, you can select this option, and then type the source IP address you want to search for.
Destination IP	To search for offenses with a specific destination IP address, you can select this option, and then type the destination IP address you want to search for.

Table 7-3 Offense type options (continued)

Offense types	Description
Event Name	To search for offenses with a specific event name, you can click the **Browse** icon to open the Event Browser and select the event name (QID) you want to search for. You can search for a particular QID using one of the following options: • To search for a QID by category, select the **Browse by Category** check box and select the high- or low-level category from the list boxes. • To search for a QID by log source type, select the **Browse by Log Source Type** check box and select a log source type from the **Log Source Type** list box. • To search for a QID by name, select the QID Search check box and type a name in the **QID/Name** field.
Username	To search for offenses with a specific username, you can select this option, and then type the user name you want to search for.
Source MAC Address	To search for offenses with a specific source MAC address, you can select this option, and then type the source MAC address you want to search for.
Destination MAC Address	To search for offenses with a specific destination MAC address, you can select this option, and then type the destination MAC address you want to search for.
Log Source	From the **Log Source Group** list box, you can select the log source group that contains the log source you want to search for. The **Log Source** list box displays all log sources assigned to the selected log source group. From the **Log Source** list box, select the log source you want to search for.
Host Name	To search for offenses with a specific host name, you can select this option, and then type the host name you want to search for.
Source Port	To search for offenses with a specific source port, you can select this option, and then type the source port you want to search for.
Destination Port	To search for offenses with a specific destination port, you can select this option, and then type the destination port you want to search for.
Source IPv6	To search for offenses with a specific source IPv6 address, you can select this option, and then type the source IPv6 address you want to search for.
Destination IPv6	To search for offenses with a specific destination IPv6 address, you can select this option, and then type the destination IPv6 address you want to search for.
Source ASN	To search for offenses with a specific Source ASN, you can select the source ASN from the **Source ASN** list box.
Destination ASN	To search for offenses with a specific destination ASN, you can select the destination ASN from the **Destination ASN** list box.

Table 7-3 Offense type options (continued)

Offense types	Description
Rule	To search for offenses associated with a specific rule, you can select the rule group that contains the rule you want to search from the **Rule Group** list box. The **Rule Group** list box displays all rules assigned to the selected rule group. From the **Rule** list box, you select the rule you want to search for.
App ID	To search for offenses with a application ID, you can select the application ID from the **App ID** list box.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 From the **Search** list box, select **New Search**.

Step 3 Choose one of the following options:

- To load a previously saved search, go to **Step 4**.
- To create a new search, go to **Step 7**.

Step 4 Select a previously saved search using one of the following options:

- From the **Available Saved Searches** list, select the saved search you want to load.
- In the **Type Saved Search or Select from List** field, type the name of the search you want to load.

Step 5 Click **Load**.

After you load the saved search, the Edit Search pane is displayed.

Step 6 Optional. Select the **Set as Default** check box to set this search as your default search.

If you set this search as your default search, the search automatically performs and displays results each time you access the **Offenses** tab.

Step 7 On the Time Range pane, select an option for the time range you want to capture for this search. See **Table 7-2**.

Step 8 On the Search Parameters pane, define your specific search criteria. See **Table 7-2**.

Step 9 On the Offense Source pane, specify the offense type and offense source you want to search:

a From the list box, select the offense type you want to search for.

When you select an offense type, corresponding search parameters are displayed.

b Type your search parameters. See **Table 7-3**.

Step 10 In the Column Definition pane, define the order in which you want to sort the results:

a From the first list box, select the column by which you want to sort the search results.

b From the second list box, select the order you want to display for the search results. Options include **Descending** and **Ascending**.

Step 11 Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Source IP page

This topic provides the procedure for how to search offenses on the **By Source IP** page of the **Offense** tab.

About this task

The following table describes the search options you can use to search offense data on the By Source IP page:

Table 7-4 By Source IP page search options

Options	Description
All Offenses	You can select this option to search all source IP addresses regardless of time range.
Recent	You can select this option and, from this list box, select the time range you want to search for.
Specific Interval	To specify an interval to search for, you can select the Specific Interval option and then select one of the following options: • **Start Date between** - Select this check box to search source IP addresses associated with offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search for. • **Last Event/Flow between** - Select this check box to search source IP addresses associated with offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search for.
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Source IP	In this field, you can type the source IP address or CIDR range you want to search for.
Magnitude	From this list box, you can specify a magnitude and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value. The range is 0 to 10.
VA Risk	From this list box, you can specify a VA risk and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value. The range is 0 to 10.

Table 7-4 By Source IP page search options

Options	Description
Events/Flows	From this list box, you can specify an event or flow count and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
Exclude	You can select the check boxes for the offenses you want to exclude from the search results. The options include: • Active Offenses • Hidden Offenses • Closed Offenses • Inactive offenses • Protected Offense

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **By Source IP**.

Step 3 From the **Search** list box, select **New Search**.

Step 4 On the Time Range pane, select an option for the time range you want to capture for this search. See **Table 7-4**.

Step 5 On the Search Parameters pane, define your specific search criteria. See **Table 7-4**.

Step 6 On the Column Definition pane, define the order in which you want to sort the results:

a From the first list box, select the column by which you want to sort the search results.

b From the second list box, select the order you want to display for the search results. Options include **Descending** and **Ascending**.

Step 7 Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Destination IP page

On the **By Destination IP** page of the **Offense** tab, you can search offenses grouped by the destination IP address.

About this task

The following table describes the search options you can use to search offenses on the By Destination IP page:

Table 7-5 By Destination IP page search options

Options	Description
All Offenses	You can select this option to search all destination IP addresses regardless of time range.
Recent	You can select this option and, From this list box, select the time range you want to search for.
Specific Interval	To specify a particular interval to search for, you can select the Specific Interval option, and then select one of the following options: • **Start Date between** - Select this check box to search destination IP addresses associated with offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search. • **Last Event/Flow between** - Select this check box to search destination IP addresses associated with offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.
Search	The **Search** icon is available in multiple panes on the search page. You can click **Search** when you are finished configuring the search and want to view the results.
Destination IP	You can type the destination IP address or CIDR range you want to search for.
Magnitude	From this list box, you can specify a magnitude, and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
VA Risk	From this list box, you can specify a VA risk, and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value. The range is 0 to 10.
Events/Flows	From this list box, you can specify an event or flow count magnitude, and then select display only offenses with an event or flow count that is equal to, less than, or greater than the configured value.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **By Destination IP**.

Step 3 From the **Search** list box, select **New Search**.

Step 4 On the Time Range pane, select an option for the time range you want to capture for this search. See Table 7-5.

Step 5 On the Search Parameters pane, define your specific search criteria. See Table 7-5.

Step 6 On the Column Definition pane, define the order in which you want to sort the results:

a From the first list box, select the column by which you want to sort the search results.

b From the second list box, select the order in which you want to display the search results. Options include **Descending** and **Ascending**.

Step 7 Click **Search**.

What to do next

Saving search criteria on the Offense tab

Searching offenses on the By Networks page

On the **By Network** page of the **Offense** tab, you can search offenses grouped by the associated networks.

About this task

The following table describes the search options you can use to search offense data on the By Network page:

Table 7-6 By Network page search options

Options	Description
Network	From this list box, you can select the network you want to search for.
Magnitude	From this list box, you can specify a magnitude, and then select display only offenses with a magnitude that is equal to, less than, or greater than the configured value.
VA Risk	From this list box, you can specify a VA risk, and then select display only offenses with a VA risk that is equal to, less than, or greater than the configured value.
Event/Flows	From this list box, you can specify an event or flow count, and then select display only offenses with an event or flow count that is equal to, less than, or greater than the configured value.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Click **By Networks**.

Step 3 From the **Search** list box, select **New Search**.

Step 4 On the Search Parameters pane, define your specific search criteria. See Table 7-6.

Step 5 On the Column Definition pane, define the order in which you want to sort the results:

a From the first list box, select the column by which you want to sort the search results.

b From the second list box, select the order in which you want to display the search results. Options include **Descending** and **Ascending**.

Step 6 Click **Search**.

What to do next

Saving search criteria on the Offense tab

Saving search criteria on the Offense tab

On the **Offenses** tab, you can save configured search criteria so that you can re-use the criteria for future searches. Saved search criteria does not expire.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Perform a search. See Offense searches.

The search results are displayed.

Step 3 Click **Save Criteria**.

Step 4 Enter values for the following parameters:

Parameter	**Description**
Search Name	Type a name you want to assign to this search criteria.
Assign Search to Group(s)	Select the check box for the groups to which you want to assign this saved search. If you do not select a group, this saved search is assigned to the Other group by default.
Manage Groups	Click **Manage Groups** to manage search groups. See Managing search groups.
Timespan options:	Choose one of the following options: • **All Offenses** - Select this option to search all offenses regardless of time range. • **Recent** - Select the option and, from this list box, select the time range you want to search for. • **Specific Interval** - To specify a particular interval to search for, select the **Specific Interval** option, and then select one of the following options: **Start Date between** - Select this check box to search offenses that started during a certain time period. After you select this check box, use the list boxes to select the dates you want to search for. **Last Event/Flow between** - Select this check box to search offenses for which the last detected event occurred within a certain time period. After you select this check box, use the list boxes to select the dates you want to search.
Set as Default	Select this check box to set this search as your default search.

Step 5 Click **OK**.

Deleting search criteria

If saved search criteria is no longer required, you can delete the search criteria.

About this task

When you delete a saved search, QRadar SIEM objects that are associated with the saved search might no longer function. Reports and anomaly detection rules are QRadar SIEM objects that use saved search criteria. After you delete a saved search, edit the associated objects to ensure they continue to function.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 From the **Search** list box, select **New Search** or **Edit Search**.

Step 3 In the Saved Searches pane, select a saved search from the **Available Saved Searches** list box.

Step 4 Click **Delete**.

If the saved search criteria is not associated with other QRadar SIEM objects, a confirmation window is displayed. See **Step 5**.

If the saved search criteria is associated with other QRadar SIEM objects, the Delete Saved Search window is displayed. The window lists all QRadar SIEM objects that are associated with the saved search you want to delete. Note the associated objects. See **Step 6**.

Step 5 Click **OK**.

Step 6 Choose one of the following options:

- Click **OK** to proceed. The saved search is now deleted.
- Click **Cancel** to close the Delete Saved Search window.

What to do next

If the saved search criteria was associated with other QRadar SIEM objects, access the associated objects you noted and edit the objects to remove or replace the association with the deleted saved search.

Performing a sub-search

The sub-search feature allows you to perform searches within a set of previously completed search results. The sub-search function allows you to refine your search results without requiring you to search the database again.

About this task

This feature is not available for grouped searches, searches in progress, or in streaming mode.

Before you begin

When defining a search that you want to use as a base for sub-searching, make sure that Real Time (streaming) option is disabled and the search is not grouped.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 Perform a search. See **Searching events or flows**.

Step 3 When your search is complete, add another filter:

a Click **Add Filter**.

b From the first list box, select a parameter you want to search for.

c From the second list box, select the modifier you want to use for the search. The list of modifiers that are available depends on the attribute selected in the first list.

d In the entry field, type specific information related to your search.

e Click **Add Filter**.

Result

The Original Filter pane specifies the original filters applied to the base search. The Current Filter pane specifies the filters applied to the sub-search. You can clear sub-search filters without restarting the base search. Click the **Clear Filter** link next to the filter you want to clear. If you clear a filter from the Original Filter pane, the base search is relaunched.

If you delete the base search criteria for saved sub-search criteria, you still have access to saved sub-search criteria. If you add a filter, the sub-search searches the entire database since the search function no longer bases the search on a previously searched data set

What to do next

Saving event and flow search criteria

Managing event and flow search results

You can initiate multiple event and flow searches, and then navigate to other tabs to perform other tasks while your searches complete in the background. You can configure a search to send you an email notification when the search is complete. At any time while a search is in progress, you can return to the **Log Activity** or **Network Activity** tabs to view partial or complete search results.

Saving search results

After you perform an event or flow search, you can save the search results.

About this task

If you perform a search and do not explicitly save the search results, the search results are available on Manage Search Windows for 24 hours and then are automatically deleted.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 Perform a search. See **Searching events or flows**.

Step 3 Click **Save Results**.

Step 4 On the Save Search Result window, type a unique name for the search results.

Step 5 Click **OK**.

Viewing managed search results

Using the Manage Search Results page, you can view partial or complete search results.

About this task

Saved search results retain chart configurations from the associated search criteria, however, if the search result is based on search criteria that has been deleted, the default charts (bar and pie) are displayed.

The Manage Search Results page provides the following parameters:

Table 7-7 Manage Search Results page parameters

Parameter	Description
Flags	Indicates that an email notification is pending for when the search is complete.
User	Specifies the name of the user who started the search.
Name	Specifies the name of the search, if the search has been saved. For more information about saving a search, see **Saving search results**.
Started On	Specifies the date and time the search was started.
Ended On	Specifies the date and time the search ended.
Duration	Specifies the amount of time the search took to complete. If the search is currently in progress, the **Duration** parameter specifies how long the search has been processing to date. If the search was canceled, the **Duration** parameter specifies the period of time the search was processing before it was canceled.
Expires On	Specifies the date and time an unsaved search result will expire. The saved search retention figure is configured in the system settings. For more information about configuring system settings, see the *IBM Security QRadar SIEM Administration Guide*.

Table 7-7 Manage Search Results page parameters (continued)

Parameter	Description
Status	Specifies the status of the search. The statuses are: • **Queued** - Specifies that the search is queued to start. • **<percent>% Complete** - Specifies the progress of the search in terms of percentage complete. You can click the link to view partial results. • **Sorting** - Specifies that the search has finished collecting results and is currently preparing the results for viewing. • **Canceled** - Specifies that the search has been canceled. You can click the link to view the results that were collected before the cancellation. • **Completed** - Specifies that the search is complete. You can click the link to view the results. See **Log activity monitoring** or **Network activity monitoring**.
Size	Specifies the file size of the search result set.

The Manage Search Results window toolbar provides the following functions:

Table 7-8 Manage Search Results toolbar

Function	Description
New Search	Click **New Search** to create a new search. When you click this icon, the search page is displayed. See **Searching events or flows**.
Save Results	Click **Save Results** to save the selected search results. See **Saving search results**.
Cancel	Click **Cancel** to cancel the selected search result that are in progress or are queued to start. See **Canceling a search**.
Delete	Click **Delete** to delete the selected search result. See **Deleting a search result**.
Notify	Click **Notify** to enable email notification when the selected search is complete.
View	From this list box, you can select which search results you want to list on the Search Results page. The options are: • Saved Search Results • All Search Results • Canceled/Erroneous Searches • Searches in Progress

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 From the Search menu, select **Manage Search Results**.

Step 3 View the list of search results. See Table 7-7.

What to do next

Canceling a search

Deleting a search result

Canceling a search

While a search is queued or in progress, you can cancel the search on the Manage Search Results page.

About this task

If the search is in progress when you cancel it, the results that were accumulated until the cancellation are maintained.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 From the Search menu, select **Manage Search Results**.

Step 3 Select the queued or in progress search result you want to cancel.

Step 4 Click **Cancel**.

Step 5 Click **Yes**.

Deleting a search result

If a search result is no longer required, you can delete the search result from the Manage Search Results page.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 From the Search menu, select **Manage Search Results**.

Step 3 Select the search result you want to delete.

Step 4 Click **Delete**.

Step 5 Click **Yes**.

Managing search groups

Using the Search Groups window, you can create and manage event, flow, and offense search groups. These groups allow you to easily locate saved search criteria on the **Log Activity**, **Network Activity**, and **Offenses** tabs, and in the Report Wizard.

Viewing search groups

QRadar SIEM provides a default set of groups and subgroups, which you can view on the Event Search Group, Flow Search Group, or Offense Search Group windows.

About this task

All saved searches that are not assigned to a group are located in the **Other** group.

The Event Search Group, Flow Search Group, and Offense Search Group windows display the following parameters for each group:

Table 7-9 Search Group window parameters

Parameter	Description
Name	Specifies the name of the search group.
User	Specifies the name of the user that created the search group.
Description	Specifies the description of the search group.
Date Modified	Specifies the date the search group was modified.

The Event Search Group, Flow Search Group, and Offense Search Group window toolbars provide the following functions:

Table 7-10 Search Group window toolbar functions

Function	Description
New Group	To create a new search group, you can click **New Group**. See **Creating a new search group**.
Edit	To edit an existing search group, you can click **Edit**. See **Editing a search group**.
Copy	To copy a saved search to another search group, you can click **Copy**. See **Copying a saved search to another groupe**.
Remove	To remove a search group or a saved search from a search group, select the item you want to remove, and then click **Remove**. See **Removing a group or a saved search from a group**.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.
- Click the **Offenses** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 View the search groups. See **Table 7-9**.

What to do next

Creating a new search group

Editing a search group

Copying a saved search to another group

Removing a group or a saved search from a group

Creating a new search group

On the Event Search Group, Flow Search Group, and Offense Group Search windows, you can create a new search group.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.
- Click the **Offenses** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Select the folder for the group under which you want to create the new group.

Step 5 Click **New Group**.

Step 6 In the **Name** field, type a unique name for the new group.

Step 7 Optional. In the **Description** field, type a description.

Step 8 Click **OK**.

Editing a search group

You can edit the **Name** and **Description** fields of a search group.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.
- Click the **Offenses** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Select the group you want edit.

Step 5 Click **Edit**.

Step 6 Edit the parameters:

- Type a new name in the **Name** field.
- Type a new description in the **Description** field.

Step 7 Click **OK**.

Copying a saved search to another group

You can copy a saved search to another group. You can copy the saved search to more than one group.

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.
- Click the **Offenses** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Select the saved search you want to copy.

Step 5 Click **Copy**.

Step 6 On the Item Groups window, select the check box for the group you want to copy the saved search to.

Step 7 Click **Assign Groups**.

Removing a group or a saved search from a group

You can use the Remove icon to remove a search from a group or remove a search group.

About this task

When you remove a saved search from a group, the saved search is not deleted from your system. The saved search is removed from the group and automatically moved to the **Other** group.

You cannot remove the following groups from your system:

- Event Search Groups
- Flow Search Groups
- Offense Search Groups
- Other

Procedure

Step 1 Choose one of the following options:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.
- Click the **Offenses** tab.

Step 2 Select **Search > Edit Search**.

Step 3 Click **Manage Groups**.

Step 4 Choose one of the following options:

- Select the saved search you want to remove from the group.

- Select the group you want to remove.

Step 5 Click **Remove**.

Step 6 Click **OK**.

8 CUSTOM EVENT AND FLOW PROPERTIES

Custom event and flow properties allow you to search, view, and report on information within logs that QRadar SIEM does not typically normalize and display.

Custom property overview

You can create custom event and flow properties from several locations on the **Log Activity** or **Network Activity** tabs:

- **Event details** - You can select an event from the **Log Activity** tab to create a custom event property derived from its payload.
- **Flow details** - You can select a flow rom the **Network Activity** tab to create a custom flow property derived from its payload.
- **Search page** - You can create and edit a custom event or property from the Search page. When you create a new custom property from the Search page, the property is not derived from any particular event or flow; therefore, the Custom Property Definition window does not prepopulate. You can copy and paste payload information from another source.

Required permissions

To create custom properties, you must have the **User Defined Event Properties** or the **User Defined Flow Properties** permission. If you have Administrative permissions, you can also create and modify custom properties from the **Admin** tab. Click **Admin > Data Sources > Custom Event Properties** or **Admin > Data Sources > Custom Flow Properties**. Check with your administrator to ensure you have the correct permissions. For more information regarding permissions, see the *IBM Security QRadar SIEM Administration Guide*.

Custom property types

When you create a custom property, you can choose to create one of the following custom property type:

- **Regex** - Using regular expression (Regex) statements, you can extract unnormalized data from event or flow payloads.

  For example, QRadar SIEM reports on all users who make user permission changes on an Oracle server. QRadar SIEM provides a list of users and the number of times they made a change to the permission of another account. However, QRadar SIEM typically cannot display the actual user account or permission that was changed. You can create a custom property to extract this information from the logs, and then use the property in searches and reports.

Use of this feature requires advanced knowledge of regular expressions (regex). Regex defines the field that you want to become the custom property. After you enter a regex statement, you can validate it against the payload. When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.

A custom property can be associated with multiple regular expressions. When an event or flow is parsed, each regex pattern is tested on the event or flow until a regex pattern matches the payload. The first regex pattern to match the event or flow payload determines the data to be extracted.

- **Calculated** - Using calculation-based custom properties, you can perform calculations on existing numeric event or flow properties to produce a calculated property. For example, you can create a property that displays a percentage by dividing one numeric property by another numeric property.

Custom property management

You can create, edit, copy, and delete custom properties.

Creating a regex-based custom property

You can create a regex-based customer property to match event or flow payloads to a regular expression.

About this task

When you configure a regex-based custom property, the Custom Event Property or Custom Flow Property windows provide the following parameters:

Table 8-1 Custom property definition window parameters (regex)

Parameter	Description
Test Field	Specifies the payload that was extracted from the unnormalized event or flow.
Property Definition	
Existing Property	To select an existing property, select this option, and then select a previously saved property name from the list box.
New Property	To create a new property, select this option, and then type a unique name for this custom property. The new property name cannot be the name of a normalized property, such as *Username*, *Source IP*, or *Destination IP*.
Optimize parsing for rules, reports, and searches	To parse and store the property the first time QRadar SIEM receives the event or flow, select the check box. When you select the check box, the property does not require additional parsing for reporting, searching, or rule testing. If you clear this check box, the property is parsed each time a report, search, or rule test is performed. By default, this option is disabled.

Table 8-1 Custom property definition window parameters (regex) (continued)

Parameter	Description
Field Type	From the list box, select the field type. The field type determines how the custom property is displayed in QRadar SIEM and which options are available for aggregation. The field type options are: • Alpha-Numeric • Numeric • IP • Port The default is Alpha-Numeric.
Description	Type a description of this custom property.
Property Expression Definition	
Log Source Type	From the list box, select the type of log source to which this custom event property applies. This parameter is only displayed on the Custom Event Property Definition window.
Log Source	From the list box, select the log source to which this custom event property applies. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources. This parameter is only displayed on the Custom Event Property Definition window.
Event Name	To specify an event name to which this custom property applies, select this option. Click **Browse** to access the Event Browser and select the QRadar SIEM Identifier (QID) for the event name you want applied to this custom property. By default, this option is enabled.
Category	To specify a low-level category to which this custom property applies, select this option. To select a low-level category: **1** From the **High Level Category** list box, select the high-level category. The **Low Level Category** list updates to include only the low-level categories associated with the selected high-level category. **2** From the **Low Level Category** list box, select the low-level category to which this custom property applies.

Table 8-1 Custom property definition window parameters (regex) (continued)

Parameter	Description
RegEx	Type the regular expression you want to use for extracting the data from the payload. Regular expressions are case-sensitive. Sample regular expressions: • email: `(.+@[^\.].*\.[a-z]{2,}$)` • URL: `(http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\S*)?$)` • Domain Name: `(http[s]?://(.+?)["/?:])` • Floating Point Number: `([-+]?\d*\.?\d*$)` • Integer: `([-+]?\d*$)` • IP Address: `(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)` For example: To match a log that resembles: `SEVERITY=43` Construct the following Regular Expression: `SEVERITY=([-+]?\d*$)` ***Note:*** *Capture groups must be enclosed in parenthesis.*
Capture Group	Type the capture group you want to use if the regex contains more than one capture group. Capture groups treat multiple characters as a single unit. In a capture group, characters are grouped inside a set of parentheses.
Test	Click **Test** to test the regular expression against the payload.
Enabled	Select this check box to enable this custom property. If you clear the check box, this custom property does not display in search filters or column lists and the property is not parsed from payloads. The default is Enabled.

Procedure

Step 1 Choose one of the following:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 Optional. If you are viewing events or flows in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Double-click the event or flow you want to base the custom property on.

Step 4 Click **Extract Property**.

Step 5 In the Property Type Selection pane, select the **Regex Based** option.

Step 6 Configure the custom property parameters. See Table 8-1.

Step 7 Click **Test** to test the regular expression against the payload.

Step 8 Click **Save**.

Results

The custom property is now displayed as an option in the list of available columns on the search page. To include a custom property in an events or flows list, you must select the custom property from the list of available columns when creating a search.

Creating a calculation-based custom property

You can create a calculation-based customer property to match event or flow payloads to a regular expression.

About this task

When you configure a calculation-based custom property, the Custom Event Property or Custom Flow Property windows provide the following parameters:

Table 8-2 Custom property definition window parameters (calculation)

Parameter	Description
Property Definition	
Property Name	Type a unique name for this custom property. The new property name cannot be the name of a normalized property, such as *Username*, *Source IP*, or *Destination IP*.
Description	Type a description of this custom property.
Property Calculation Definition	
Property 1	From the list box, select the first property you want to use in your calculation. Options include all numeric normalized and numeric custom properties. You can also specify a specific numeric value. From the **Property 1** list box, select the **User Defined** option. The **Numeric Property** parameter is displayed. Type a specific numeric value.
Operator	From the list box, select the operator you want to apply to the selected properties in the calculation. Options include: • Add • Subtract • Multiply • Divide
Property 2	From the list box, select the second property you want to use in your calculation. Options include all numeric normalized and numeric custom properties. You can also specify a specific numeric value. From the **Property 1** list box, select the **User Defined** option. The **Numeric Property** parameter is displayed. Type a specific numeric value.

Table 8-2 Custom property definition window parameters (calculation) (continued)

Parameter	Description
Enabled	Select this check box to enable this custom property. If you clear the check box, this custom property does not display in event or flow search filters or column lists and the event or flow property is not parsed from payloads. The default is Enabled.

Procedure

Step 1 Choose one of the following:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 Optional. If you are viewing events or flows in streaming mode, click the **Pause** icon to pause streaming.

Step 3 Double-click the event or flow you want to base the custom property on.

Step 4 Click **Extract Property**.

Step 5 In the Property Type Selection pane, select the **Calculation Based** option.

Step 6 Configure the custom property parameters. See **Table 8-2**.

Step 7 Click **Save**.

Results

The custom property is now displayed as an option in the list of available columns on the search page. To include a custom property in an events or flows list, you must select the custom property from the list of available columns when creating a search.

Modifying a custom property

Using the Custom Event Properties or Custom Flow Properties window, you can modify a custom property.

About this task

The Custom Event Properties and Custom Flow Properties windows provide the following information:

Table 8-3 Custom properties window columns

Column	Description
Property Name	Specifies a unique name for this custom property.
Type	Specifies the type for this custom property. Options include: • **Regex** - A regex-based custom property matches event or flow payloads to a regular expression. See **Creating a regex-based custom property** • **Calculated** - A calculation-based custom property performs a calculation on event or flow properties. See **Creating a calculation-based custom property**.

Table 8-3 Custom properties window columns (continued)

Column	Description
Property Description	Specifies a description for this custom property.
Log Source Type	Specifies the name of the log source type to which this custom property applies. This column is only displayed on the Custom Event Properties window.
Log Source	Specifies the log source to which this custom property applies. If there are multiple log sources associated with this event or flow, this field specifies the term Multiple and the number of log sources. This column is only displayed on the Custom Event Properties window.
Expression	Specifies the expression for this custom property. The expression depends on the custom property type: • For a regex-based custom property, this parameter specifies the regular expression you want to use for extracting the data from the payload. • For a calculation-based custom property, this parameter specifies the calculation you want to use to create the custom property value.
Username	Specifies the name of the user who created this custom property.
Enabled	Specifies whether this custom property is enabled. This field specifies either True or False.
Creation Date	Specifies the date this custom property was created.
Modification Date	Specifies the last time this custom property was modified.

The Custom Event Property and Custom Flow Property toolbars provide the following functions:

Table 8-4 Custom property toolbar options

Option	Description
Add	Click **Add** to add a new custom property. See **Creating a regex-based custom property** or **Creating a calculation-based custom property**.
Edit	Click **Edit** to edit the selected custom property. See **Modifying a custom property**.
Copy	Click **Copy** to copy selected custom properties.
Delete	Click **Delete** to delete selected custom properties.
Enable/Disable	Click **Enable/Disable** to enable or disable the selected custom properties for parsing and viewing in the search filters or column lists.

Procedure

Step 1 Choose one of the following:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 From the **Search** list box, select **Edit Search**.

Step 3 Click **Manage Custom Properties**.

Step 4 Select the custom property you want to edit and click **Edit**.

Step 5 Edit the necessary parameters. See **Table 8-1**.

Step 6 Optional. If you edited the regular expression, click **Test** to test the regular expression against the payload.

Step 7 Click **Save**.

Copying a custom property

To create a new custom property that is based an existing custom property, you can copy the existing custom property, and then modify the parameters.

Procedure

Step 1 Choose one of the following:

- Click the **Log Activity** tab.
- Click the **Network Activity** tab.

Step 2 From the **Search** list box, select **Edit Search**.

Step 3 Click **Manage Custom Properties**.

Step 4 Select the custom property you want to copy and click **Copy**.

Step 5 Select the **New Property** option and type a new property name.

Step 6 Edit the necessary parameters. See **Table 8-1**.

Step 7 If you edited the regular expression, click **Test** to test the regular expression against the payload.

Step 8 Click **Save**.

Deleting a custom property

You can delete any custom property, provided the custom property is not associated with another custom property.

About this task

If you attempt to delete a custom property associated with another custom property, an error message is displayed to provide the name of the associated custom property.

Procedure

Step 1 Choose one of the following:

- Click the **Log Activity** tab.

- Click the **Network Activity** tab.

Step 2 From the **Search** list box, select **Edit Search**.

Step 3 Click **Manage Custom Properties**.

Step 4 Select the custom property you want to delete and click **Delete**.

Step 5 Click **Yes**.

9 RULE MANAGEMENT

From the **Log Activity**, **Network Activity**, and **Offenses** tabs, you can view and maintain rules. This topic applies to users who have the **View Custom Rules** or **Maintain Custom Rules** user role permissions.

Rule permission considerations

You can view and manage rules for areas of the network that you can access if the you have the following user role permissions:

- View Custom Rules
- Maintain Custom Rules

To create anomaly detection rules, you must have the appropriate **Maintain Custom Rule** permission for tab on which you want create the rule. For example, to be able to create an anomaly detection rule on the Log Activity tab, you must have the **Log Activity > Maintain Custom Rule**.

For more information about user role permissions, see the *IBM Security QRadar SIEM Administration Guide*.

Rules overview

Rules perform tests on events, flows, or offenses, and if all the conditions of a test are met, the rule generates a response. For a complete list of default rules, see the *IBM Security QRadar SIEM Administration Guide*.

The tests in each rule can also reference other building blocks and rules. You are not required to create rules in any specific order because the system checks for dependencies each time a new rule is added, edited, or deleted. If a rule that is referenced by another rule is deleted or disabled, a warning is displayed and no action is taken.

Rule categories

The two rule categories are:

- **Custom Rules** - Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network.
- **Anomaly Detection Rules** - Anomaly detection rules perform tests on the results of saved flow or event searches as a means to detect when unusual traffic patterns occur in your network.

Rule types

Custom rules include the following rule types:

- **Event Rule** - An event rule performs tests on events as they are processed in real-time by the Event Processor. You can create an event rule to detect a single event (within certain properties) or event sequences. For example, if you want to monitor your network for unsuccessful login attempts, access multiple hosts, or a reconnaissance event followed by an exploit, you can create an event rule. It is common for event rules to create offenses as a response.
- **Flow Rule** - A flow rule performs tests on flows as they are processed in real-time by the QFlow Collector. You can create a flow rule to detect a single flow (within certain properties) or flow sequences. It is common for flow rules to create offenses as a response.
- **Common Rule** - A common rule performs tests on fields that are common to both event and flow records. For example, you can create a common rule to detect events and flows that have a specific source IP address. It is common for common rules to create offenses as a response.
- **Offense Rule** - An offense rule processes offenses only when changes are made to the offense, such as, when new events are added or the system scheduled the offense for reassessment. It is common for offense rules to email a notification as a response.

Anomaly detection rules perform tests on the results of saved flow or event searches as a means to detect when unusual traffic patterns occur in your network. This rule category includes the following rule types:

- **Anomaly** - An anomaly rule tests event and flow traffic for abnormal activity such as the existence of new or unknown traffic, which is traffic that suddenly ceases or a percentage change in the amount of time an object is active. For example, you can create an anomaly rule to compare the average volume of traffic for the last 5 minutes with the average volume of traffic over the last hour. If there is more than a 40% change, the rule generates a response.
- **Threshold** - A threshold rule tests event and flow traffic for activity that is less than, equal to, or greater than a configured threshold, or within a specified range. Thresholds can be based on any data collected by QRadar SIEM. For example, you can create a threshold rule specifying that no more than 220 clients can log into the server between 8 am and 5 pm. The threshold rule generates an alert when the 221st client attempts to login.
- **Behavioral** - A behavioral rule tests event and flow traffic for volume changes in behavior that occurs in regular seasonal patterns. For example, if a mail server typically communicates with 100 hosts per second in the middle of the night and then suddenly starts communicating with 1,000 hosts a second, a behavioral rule generates an alert.

Rule conditions

Each rule might contain the following components:

- **Functions** - With functions, you can use building blocks and other rules to create a multi-event, multi-flow, or multi-offense function. You can connect rules using functions that support Boolean operators, such as OR and AND. For example, if you want to connect event rules, you can use the **when an event matches any|all of the following rules** function. For a complete list of functions, see **Rule tests**.

- **Building blocks** - A building block is a rule without a response and is used as a common variable in multiple rules or to build complex rules or logic that you want to use in other rules. You can save a group of tests as building blocks for use with other functions. Building blocks allow you to re-use specific rule tests in other rules. For example, you can save a building block that includes the IP addresses of all mail servers in your network and then use that building block to exclude those mail servers from another rule. The default building blocks are provided as guidelines, which should be reviewed and edited based on the needs of your network. For a complete list of building blocks, see the *IBM Security QRadar SIEM Administration Guide*.
- **Tests** - You can run tests on the property of an event, flow, or offense, such as source IP address, severity of event, or rate analysis. For a complete list of tests, see **Rule tests**.

Rule responses

When rule conditions are met, a rule can generate one or more of the following responses:

- Create an offense.
- Send an email.
- Generate system notifications using the Dashboard feature.
- Add data to reference sets. For more information on reference sets, see the *IBM Security QRadar SIEM Administration Guide*.
- Add data to reference data collections that can be used in rule tests. Before you can configure a rule to send data to a reference data collection, you must create the reference data collection using the Command Line Interface (CLI). For more information on how to create and use reference data collections, see *IBM Security QRadar Reference Data Collections* technical note.

  Using this option, you can add data to the following data collection types:

  - **Reference Map** - In a Reference Map, data is stored in records that map a key to a value. For example, to correlate user activity on your network, you can create a reference map that uses the **Username** parameter as a key and the user’s global ID as a value.
  - **Reference Map of Sets** - In a Reference Map of Sets, data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, you can create a Map of Sets that uses a custom event property for Patent ID as the key and the **Username** parameter as the value to populate a list of authorized users.
  - **Reference Map of Maps** - In a Reference Map of Maps, data is stored in records that map one key to another key, which is then mapped to single value. For example, to test for network bandwidth violations, you can create a Map of Maps that uses the **Source IP** parameter as the first key, the

Application parameter as the second key, and the **Total Bytes** parameter as the value.

- Generate a response to an external system, including the following server types:
    - **Local Syslog** - Syslog is a standard that allows you to store event, flow, and offense information in a software-independent log file. Using the Rules wizard, you can configure rules to generate a syslog file.
    - **Forwarding Destinations** - A rule can forward raw log data received from log sources and normalized event data to one or more vendor systems, such as ticketing or alerting systems.
    - **Simple Network Management Protocol (SNMP)** - The SNMP protocol enables QRadar SIEM to send event, flow, and offense notifications to another host to be stored. Using the Rules wizard, you can configure rules to generate a response that sends SNMP traps to the configured host.
    - **Interface For Metadata Access Points (IF-MAP)** - The Interface For Metadata Access Points (IF-MAP) rule response enables the rule to publish alert and offense data derived from events, flows, and offense data on an IF-MAP server.

Viewing rules

You can view the details of a rule, including the tests, building blocks, and responses.

Before you begin

Depending on your user role permissions, you can access the rules page from the **Offenses**, **Log Activity**, or **Network Activity** tab. For more information on user role permissions, see the *IBM Security QRadar SIEM Administration Guide*.

About this task

The Rules page displays a list of rules with their associated parameters. For more information on the parameters displayed for each rule listed on the Rules page, see **Table 9-1**.

To locate the rule you want to open and view the details of, you can use the **Group** list box or **Search Rules** field on the toolbar. For more information on the Rules page toolbar, see **Table 9-2**.

Procedure

Step 1 Choose one of the following options:

- Click the **Offenses** tab, and then click **Rules** on the navigation menu.
- Click the **Log Activity** tab, and then select **Rules** from the **Rules** list box on the toolbar.
- Click the **Network Activity** tab, and then select **Rules** from the **Rules** list box on the toolbar.

Step 2 From the **Display** list box, select **Rules**.

Step 3 Double-click the rule you want to view.

Step 4 Review the rule details.

Results

If you have the **View Custom Rules** permission, but do not have the **Maintain Custom Rules** permission, the Rule Summary page is displayed and the rule cannot be edited.

If you have the **Maintain Custom Rules** permission, the Rule Test Stack Editor page is displayed. You can review and edit the rule details. See **Editing a rule**.

Creating a custom rule

QRadar SIEM provides default rules, however, you can create new rules to meet the needs of your deployment.

About this task

To create a new rule, you must have the **Offenses > Maintain Custom Rules** permission.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Actions** list box, select one of the following options:

- New Event Rule
- New Flow Rule
- New Common Rule
- New Offense Rule

Step 4 Read the introductory text on the Rule Wizard. Click **Next**.

You are prompted to choose the source from which you want this rule to apply. The default is the rule type you selected in **Step 3**. You only need to choose a source on this page if you want to change your selection.

Step 5 Click **Next** to view the Rule Test Stack Editor page.

Step 6 In the **enter rule name here** field in the Rule pane, type a unique name you want to assign to this rule.

Step 7 From the list box, select whether you want to test the rule locally or globally:

- **Local** - The rule is tested on the local Event Processor and not shared with the system. The default is Local.
- **Global** - The rule is shared and tested by any Event Processor on the system. Global rules send events and flows to the central Event Processor, which might decrease performance on the central Event Processor.

Step 8 Add one or more tests to a rule:

a Optional. To filter the options in the **Test Group** list box, type the text you want to filter for in the **Type to filter** field.

b From the **Test Group** list box, select the type of test you want to add to this rule.

c For each test you want to add to the rule, select the **+** sign beside the test.

d Optional. To identify a test as excluded test, click **and** at the beginning of the test in the Rule pane. The **and** is displayed as **and not**.

e Click the underlined configurable parameters to customize the variables of the test.

f From the dialog box, select values for the variable, and then click **Submit**.

Step 9 To export the configured rule as a building block to use with other rules:

a Click **Export as Building Block**.

b Type a unique name for this building block.

c Click **Save**.

Step 10 On the Groups pane, select the check boxes of the groups to which you want to assign this rule.

Step 11 In the **Notes** field, type a note that you want to include for this rule. Click **Next**.

Step 12 On the Rule Responses page, configure the responses you want this rule to generate. Choose one of the following options:

- To configure responses for an Event Rule, Flow Rule, or Common Rule, see Table 9-3.
- To configure responses for an Offense Rule, see Table 9-4.

Step 13 Click **Next**.

Step 14 Review the Rule Summary page to ensure the settings are correct. Make any changes if necessary, and then click **Finish**.

Creating an anomaly detection rule

The Anomaly Detection Rule wizard allows you to create rules that apply time range criteria using Data and Time tests.

Before you begin

To create a new anomaly detection rule, you must meet the following requirements:

- Have the Maintain Custom Rules permission.
- Perform a grouped search.

The anomaly detection options are only displayed after you perform a grouped search and save the search criteria.

About this task

You must have the appropriate role permission to be able to create an anomaly detection rule:

- To create anomaly detection rules on the **Log Activity** tab, you must have the **Log Activity > Maintain Custom Rules** role permission
- To create anomaly detection rules on the **Log Activity** tab, you must have the **Network > Maintain Custom Rules** role permission

Anomaly detection rules use all grouping and filter criteria from the saved search criteria the rule is based on, but do not use any time ranges from the search criteria.

When you create an anomaly detection rule, the rule is populated with a default test stack. You can edit the default tests or add tests to the test stack. At least one Accumulated Property test must be included in the test stack.

By default, the **Test the [Selected Accumulated Property] value of each [group] separately** option is selected on the Rule Test Stack Editor page. This causes an anomaly detection rule to test the selected accumulated property for each event or flow group separately. For example, if the selected accumulated value is **UniqueCount(sourceIP)**, the rule tests each unique source IP address for each event/flow group.

This **Test the [Selected Accumulated Property] value of each [group] separately** option is dynamic. The **[Selected Accumulated Property]** value depends on what option you select for the **this accumulated property** test field of the default test stack. The **[group]** value depends on the grouping options specified in the saved search criteria. If multiple grouping options are included, the text might be truncated. Move your mouse pointer over the text to view all groups.

Procedure

Step 1 Click the **Log Activity** or **Network Activity** tab.

Step 2 Perform a search.

Step 3 From the **Rules** menu, select the rule type you want to create. Options include:

- Add Anomaly Rule
- Add Threshold Rule
- Add Behavioral Rule

The Rule wizard is displayed.

Step 4 Read the introductory text. Click **Next**.

You are prompted to choose the source from which you want this rule to apply. The default is the rule type you selected in **Step 3**. You only need to choose a source on this page if you want to change your selection.

Step 5 Click **Next** to view the Rule Test Stack Editor page.

Step 6 In the **enter rule name here** field, type a unique name you want to assign to this rule.

Step 7 To add a test to a rule:

a Optional. To filter the options in the **Test Group** list box, type the text you want to filter for in the **Type to filter** field.

b From the **Test Group** list box, select the type of test you want to add to this rule.

c For each test you want to add to the rule, select the **+** sign beside the test.

d Optional. To identify a test as excluded test, click **and** at the beginning of the test in the Rule pane. The **and** is displayed as **and not**.

e Click the underlined configurable parameters to customize the variables of the test.

f From the dialog box, select values for the variable, and then click **Submit**.

Step 8 Optional. To test the total selected accumulated properties for each event/flow group, clear the **Test the [Selected Accumulated Property] value of each [group] separately** check box.

Step 9 In the groups pane, select the check boxes of the groups you want to assign this rule to. For more information about grouping rules, see **Rule group management**.

Step 10 In the **Notes** field, type any notes you want to include for this rule. Click **Next**.

Step 11 On the Rule Responses page, configure the responses you want this rule to generate. See **Table 9-5**.

Step 12 Click **Next**.

Step 13 Review the configured rule. Click **Finish**.

Rule management tasks

You can manage custom and anomaly rules. You can enable and disable rules, as required. You can also edit, copy, or delete a rule.

Note: The anomaly detection functionality on the **Log Activity** and **Network Activity** tabs only allows you to create anomaly detection rules. To manage default and previously created anomaly detection rules, you must use the Rules page on the **Offenses** tab.

Enabling/disabling rules

When tuning your system, you can enable or disable the appropriate rules to ensure that your system generates meaningful offenses for your environment.

About this task

You must have the **Offenses > Maintain Custom Rules** role permission to be able to enable or disable a rule.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box on the Rules page, select **Rules**.

Step 4 Select the rule you want to enable or disable.

Step 5 From the **Actions** list box, select **Enable/Disable**.

Editing a rule

You can edit a rule to change the rule name, rule type, tests, or responses.

About this task

You must have the **Offenses > Maintain Custom Rules** role permission to be able to edit a rule.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box on the Rules page, select **Rules**.

Step 4 Double-click the rule you want to edit.

Step 5 From the **Actions** list box, select **Open**.

Step 6 Optional. If you want to change the rule type, click **Back** and select a new rule type.

Step 7 On the Rule Test Stack Editor page, edit the parameters. See **Table 9-1**.

Step 8 Click **Next**.

Step 9 On the Rule Response page, edit the parameters:

- See **Table 9-3** for event, flow, or common rule responses.
- See **Table 9-4** for offense rule responses.
- See **Table 9-5** for anomaly detection rule responses.

Step 10 Click **Next**.

Step 11 Review the edited rule. Click **Finish**.

Copying a rule

To create a new rule, you can copy an existing rule, enter a new name for the rule, and then customize the parameters in the new rule as required.

About this task

You must have the **Offenses > Maintain Custom Rules** role permission to be able to copy a rule.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box, select **Rules**.

Step 4 Select the rule you want to duplicate.

Step 5 From the **Actions** list box, select **Duplicate**.

Step 6 In the **Enter name for the copied rule** field, type a name for the new rule. Click **OK**.

Deleting a rule

QRadar SIEM allows you to delete a rule from your system.

About this task

You must have the **Offenses > Maintain Custom Rules** role permission to be able to delete a rule.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box, select **Rules**.

Step 4 Select the rule you want to delete.

Step 5 From the **Actions** list box, select **Delete**.

Rule group management

If you are an administrator, you are able to create, edit, and delete groups of rules. Categorizing your rules or building blocks into groups allows you to efficiently view and track your rules. For example, you can view all rules related to compliance.

As you create new rules, you can assign the rule to an existing group. For information on assigning a group using the rule wizard, see **Creating a custom rule** or **Creating an anomaly detection rule**.

Viewing a rule group

On the Rules page, you can filter the rules or building blocks to view only the rules or building blocks belonging to a specific group.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box, select whether you want to view rules or building blocks.

Step 4 From the **Filter** list box, select the group category you want to view.

Result

The list of items assigned to that group displays.

Creating a group

The Rules page provides default rule groups, however, you can create a new group.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Click **Groups**.

Step 4 From the navigation tree, select the group under which you want to create a new group.

Step 5 Click **New Group**.

Step 6 Enter values for the following parameters:

- **Name** - Type a unique name to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 Optional. To change the location of the new group, click the new group and drag the folder to the new location in your navigation tree.

Step 9 Close the Group window.

Assigning an item to a group

You can assign a selected rule or building block to a group.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Select the rule or building block you want to assign to a group.

Step 4 From the **Actions** list box, select **Assign Groups**.

Step 5 Select the group you want to assign the rule or building block to.

Step 6 Click **Assign Groups**.

Step 7 Close the Choose Groups window.

Editing a group

You can edit a group to change the name or description.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Click **Groups**.

Step 4 From the navigation tree, select the group you want to edit.

Step 5 Click **Edit**.

Step 6 Update values for the following parameters:

- **Name** - Type a unique name to assign to the new group. The name can be up to 255 characters in length.
- **Description** - Type a description you want to assign to this group. The description can be up to 255 characters in length.

Step 7 Click **OK**.

Step 8 Optional. To change the location of the group, click the new group and drag the folder to the new location in your navigation tree.

Step 9 Close the Group window.

Copying an item to another group

Using the groups functionality, you can copy a rule or building block from one group to other groups.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Click **Groups**.

Step 4 From the navigation tree, select the rule or building block you want to copy to another group.

Step 5 Click **Copy**.

Step 6 Select the check box for the group you want to copy the rule or building block to.

Step 7 Click **Copy**.

Step 8 Close the Group window.

Deleting an item from a group

You can delete an item from a group. When you delete an item from a group, the rule or building block is only deleted from group; it remains available on the Rules page.

Procedure

Step 1 Click the **Offense** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Click **Groups**.

Step 4 Using the navigation tree, navigate to and select the item you want to delete.

Step 5 Click **Remove**.

Step 6 Click **OK**.

Step 7 Close the Group window.

Deleting a group

You can delete a group. When you delete a group, the rules or building blocks of that group remain available on the Rules page.

Procedure

Step 1 Click the **Offense** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Click **Groups**.

Step 4 Using the navigation tree, navigate to and select the group you want to delete.

Step 5 Click **Remove**.

Step 6 Click **OK**.

Step 7 Close the Group window.

Editing building blocks

QRadar SIEM includes a set of default building blocks, which you can edit to match the needs of your deployment.

About this task

A building block is a re-usable rule test stack that you can include as a component in other rules.

For example, you can edit the BB:HostDefinition: Mail Servers building block to identify all mail servers in your deployment. Then, you can configure any rule to exclude your mail servers from the rule tests.

For more information about the default building blocks, see the *IBM Security QRadar SIEM Administration Guide*.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box, select **Building Blocks**.

Step 4 Double-click the building block you want to edit.

Step 5 Update the building block, as necessary. Click **Next**.

Step 6 Continue through the wizard. For more information, see **Creating a custom rule**.

Step 7 Click **Finish**.

Rules page parameters

The list of deployed rules provides the following information for each rule:

Table 9-1 Rules page parameters

Parameter	Description
Rule Name	Displays the name of the rule.
Group	Displays the group to which this rule is assigned. For more information about groups, see **Rule group management**.
Rule Category	Displays the rule category for the rule. Options include: • Custom Rule • Anomaly Detection Rule

Table 9-1 Rules page parameters (continued)

Parameter	Description
Rule Type	Displays the rule type. Rule types include: • Event • Flow • Common • Offense • Anomaly • Threshold • Behavioral For more information about the rule types, see **Rule types**.
Enabled	Indicates whether the rule is enabled or disabled. For more information about enabling and disabling rules, see **Enabling/disabling rules**.
Response	Displays the rule response, if any. Rule responses include: • Dispatch New Event • Email • Log • Notification • SNMP • Reference Set • Reference Data • IF-MAP Response For more information about rule responses, see **Rule responses**.
Event/Flow Count	Displays the number of events or flows associated with this rule when the rule contributes to an offense.
Offense Count	Displays the number of offenses generated by this rule.
Origin	Displays whether this rule is a default rule (System) or a custom rule (User).
Creation Date	Specifies the date and time this rule was created.
Modification Date	Specifies the date and time this rule was modified.

Rules page toolbar

The Rules page toolbar provides the following functions:

Table 9-2 Rules page toolbar function

Function	Description
Display	From the list box, select whether you want to display rules or building blocks in the rules list.

Table 9-2 Rules page toolbar function (continued)

Function	Description
Group	From the list box, select which rule group you want to be displayed in the rules list.
Groups	Click **Groups** to manage rule groups. For more information about grouping rules, see **Rule group management**.
Actions	Click **Actions** and select one of the following options: • **New Event Rule** - Select this option to create a new event rule. See **Creating a custom rule**. • **New Flow Rule** - Select this option to create a new flow rule. See **Creating a custom rule**. • **New Common Rule** - Select this option to create a new common rule. See **Creating a custom rule**. • **New Offense Rule** - Select this option to create a new offense rule. See **Creating a custom rule**. • **Enable/Disable** - Select this option to enable or disable selected rules. See **Enabling/disabling rules**. • **Duplicate** - Select this option to copy a selected rule. See **Copying a rule**. • **Edit** - Select this option to edit a selected rule. See **Editing a rule**. • **Delete** - Select this option to delete a selected rule. See **Deleting a rule**. • **Assign Groups** - Select this option to assign selected rules to rule groups. See **Assigning an item to a group**.
Revert Rule	Click **Revert Rule** to revert a modified system rule to the default value. When you click **Revert Rule**, a confirmation window is displayed. When you revert a rule, any previous modifications are permanently removed. ***Note:*** *To both revert the rule and maintain a modified version, duplicate the rule and use the* ***Revert Rule*** *option on the modified rule.*

Table 9-2 Rules page toolbar function (continued)

Function	Description
Search Rules	Type your search criteria in the **Search Rules** field and click the **Search Rules** icon or press Enter on the keyboard. All rules that match your search criteria are displayed in the rules list. The following parameters are searched for a match with your search criteria: • Rule Name • Rule (description) • Notes • Response The Search Rule feature attempts to locate a direct text string match. If no match is found, the Search Rule feature then attempts a regular expression (regex) match.

Rule Response page parameters

Table 9-3 provides the Rule Response page parameters if the rule type is Event Rule, Flow Rule, or Common.

Table 9-3 Event/Flow/Common Rule Response page parameters

Parameter	Description
Severity	Select this check box if you want this rule to set or adjust severity. When selected, you can use the list boxes to configure the appropriate severity level. For more information about severity, see the **Glossary**.
Credibility	Select this check box if you want this rule to set or adjust credibility. When selected, you can use the list boxes to configure the appropriate credibility level. For more information about credibility, see the **Glossary**.
Relevance	Select this check box if you want this rule to set or adjust relevance. When selected, you can use the list boxes to configure the appropriate relevance level. For more information about relevance, see the **Glossary**.

Table 9-3 Event/Flow/Common Rule Response page parameters (continued)

Parameter	Description
Ensure the detected event is part of an offense	Select this check box if you want the event to be forwarded to the Magistrate component. If no offense exists on the **Offenses** tab, a new offense is created. If an offense exists, this event is added to the offense. When you select this check box, the following options are displayed: • **Index offense based on** - From the list box, select the parameter on which you want to index the offense. The default is Source IPv6. For event rules, options include destination IP, destination IPv6, destination MAC address, destination port, event name, host name, log source, rule, source IP, source IPv6, source MAC address, source port, or user name. For flow rules, options include App ID, destination ASN, destination IP, destination IP Identity, destination port, event name, rule, source ASN, source IP, source IP identity, or source Port. For common rules, options include destination IP, destination IP identity, destination port, rule, source IP, source IP identity and source port. • **Annotate this offense** - Select this check box to add an annotation to this offense and type the annotation. • **Include detected events by <index> from this point forward, for second(s), in the offense** - Select this check box and type the number of seconds you want to include detected events by <index> on the **Offenses** tab. This field specifies the parameter on which the offense is indexed. The default is Source IP.
Annotate event	Select this check box if you want to add an annotation to this event and type the annotation you want to add to the event.
Drop the detected event	Select this check box to force an event, which is normally sent to the Magistrate component, to be sent to the Ariel database for reporting or searching. This event does not display on the **Offenses** tab.
Rule Response	
Dispatch New Event	Select this check box to dispatch a new event in addition to the original event or flow, which will be processed like all other events in the system. The **Dispatch New Event** parameters are displayed when you select this check box. By default, the check box is clear.
Event Name	Type a unique name for the event you want to be displayed on the **Offenses** tab.
Event Description	Type a description for the event. The description is displayed in the Annotations pane of the event details.

Table 9-3 Event/Flow/Common Rule Response page parameters (continued)

Parameter	Description
Severity	From the list box, select the severity for the event. The range is 0 (lowest) to 10 (highest) and the default is 0. The Severity is displayed in the Annotation pane of the event details. For more information about severity, see the **Glossary**.
Credibility	From the list box, select the credibility of the event. The range is 0 (lowest) to 10 (highest) and the default is 10. Credibility is displayed in the Annotation pane of the event details. For more information about credibility, see the **Glossary**.
Relevance	From the list box, select the relevance of the event. The range is 0 (lowest) to 10 (highest) and the default is 10. Relevance is displayed in the Annotations pane of the event details. For more information about relevance, see the **Glossary**.
High-Level Category	From the list box, select the high-level event category you want this rule to use when processing events. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.
Low-Level Category	From the list box, select the low-level event category you want this rule to use when processing events. For more information about event categories, see *IBM Security QRadar SIEM Administration Guide*.
Annotate this offense	Select this check box to add an annotation to this offense and type the annotation.

Table 9-3 Event/Flow/Common Rule Response page parameters (continued)

Parameter	Description
Ensure the dispatched event is part of an offense	Select this check box if you want, as a result of this rule, the event forwarded to the Magistrate component. If no offense has been created on the **Offenses** tab, a new offense is created. If an offense exists, this event is added. When you select this check box, the following options are displayed: • **Index offense based on** - From the list box, select the parameter on which you want to index the offense. The default is Source IP. For event rules, options include destination IP, destination IPv6, destination MAC address, destination port, event name, host name, log source, rule, source IP, source IPv6, source MAC address, source port, or user name. For flow rules, options include App ID, destination ASN, destination IP, destination IP Identity, destination port, event name, rule, source ASN, source IP, source IP identity, or source Port. For common rules, options include destination IP, destination IP identity, destination port, rule, source IP, source IP identity and source port. • **Include detected events by <index> from this point forward, for second(s), in the offense** - Select this check box and type the number of seconds you want to include detected events by <index> on the **Offenses** tab. This field specifies the parameter on which the offense is indexed. The default is Source IP. • **Offense Naming** - Select one of the following options: **This information should contribute to the name of the associated offense(s)** - Select this option if you want the Event Name information to contribute to the name of the offense. **This information should set or replace the name of the associated offense(s)** - Select this option if you want the configured Event Name to be the name of the offense. **This information should not contribute to the naming of the associated offense(s)** - Select this option if you do not want the Event Name information to contribute to the name of the offense. This is the default.
Email	Select this check box to display the email options. By default, the check box is clear.
Enter email addresses to notify	Type the email address to send notification if this rule generates. Separate multiple email addresses using a comma.

Table 9-3 Event/Flow/Common Rule Response page parameters (continued)

Parameter	Description
SNMP Trap	This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. For more information about configuring system settings, see the *IBM Security QRadar SIEM Administration Guide*. ▶ Select this check box to enable this rule to send an SNMP notification (trap). The SNMP trap output includes system time, the trap OID, and the notification data, as defined by the Q1 Labs MIB. For more information about the Q1 Labs MIB, see the *IBM Security QRadar SIEM Administration Guide*. For example, the SNMP notification might resemble: `"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Offense description"`
Send to Local SysLog	Select this check box if you want to log the event or flow locally. By default, this check box is clear. For example, the syslog output might resemble: `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description`
Send to Forwarding Destinations	This check box is only displayed for Event rules. Select this check box if you want to log the event or flow on a forwarding destination. A forwarding destination is a vendor system, such as SIEM, ticketing, or alerting systems. When you select this check box, a list of forwarding destinations is displayed. Select the check box for the forwarding destination you want to send this event or flow to. To add, edit, or delete a forwarding destination, click the **Manage Destinations** link. For more information about configuring forwarding destinations, see the *IBM Security QRadar SIEM Administration Guide*.
Notify	Select this check box if you want events that generate as a result of this rule to be displayed in the System Notifications item on the Dashboard tab. For more information about the Dashboard tab, see **Dashboard management**. ***Note:*** *If you enable notifications, configure the* ***Response Limiter*** *parameter.*

Table 9-3 Event/Flow/Common Rule Response page parameters (continued)

Parameter	Description
Add to Reference Set	Select this check box if you want events generated as a result of this rule to add data to a reference set. To add data to a reference set: **1** Using the first list box, select the data you want to add. Options include all normalized or custom data. **2** Using the second list box, select the reference set to which you want to add the specified data. The **Add to Reference Set** rule response provides the following functions: • **Refresh** - Click **Refresh** to refresh the first list box to ensure that the list is current. • **Configure Reference Sets** - Click **Configure Reference Sets** to configure the reference set. This option is only available if you have administrative permissions. For more information on managing reference sets, see the *IBM Security QRadar SIEM Administration Guide*.
Add to Reference Data	Before you can use this rule response, you must create the reference data collection using the Command Line Interface (CLI). For more information on how to create and use reference data collections, see *IBM Security QRadar Reference Data Collections Technical Note*. Select this check box if you want events generated as a result of this rule to add to a reference data collection. After you select the check box, select one of the following options: • **Add to a Reference Map** - Select this option to send data to a collection of single key/multiple value pairs. You must select the key and value for the data record, and then select the reference map you want to add the data record to. • **Add to a Reference Map of Sets** - Select this option to send data to a collection of key/single value pairs. You must select the key and the value for the data record, and then select the reference map of sets you want to add the data record to. • **Add to a Reference Map of Maps** - Select this option to send data to a collection of multiple key/single value pairs. You must select a key for the first map, a key for the second map, and then the value for the data record. You must also select the reference map of maps you want to add the data record to.
Publish on the IF-MAP Server	If the IF-MAP parameters are configured and deployed in the system settings, select this option to publish the event information on the IF-MAP server. For more information about configuring the IF-MAP parameters, see the *IBM Security QRadar SIEM Administration Guide*.
Response Limiter	Select this check box and use the list boxes to configure the frequency in which you want this rule to respond.

Table 9-3 Event/Flow/Common Rule Response page parameters (continued)

Parameter	Description
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

Table 9-4 provides the Rule Response page parameters if the rule type is Offense.

Table 9-4 Offense Rule Response page parameters

Parameter	Description
Rule Action	
Name/Annotate the detected offense	Select this check box to display Name options.
New Offense Name	Type the name you want to assign to the offense.
Offense Annotation	Type the offense annotation you want to be displayed on the **Offenses** tab.
Offense Name	Select one of the following options: • **This information should contribute to the name of the offense** - Select this option if you want the Event Name information to contribute to the name of the offense. • **This information should set or replace the name of the offense** - Select this option if you want the configured Event Name to be the name of the offense.
Rule Response	
Email	Select this check box to display the email options. By default, the check box is clear.
Enter email address to notify	Type the email address to send the notification if the event generates. Separate multiple email addresses using a comma.

Table 9-4 Offense Rule Response page parameters (continued)

Parameter	Description
SNMP Trap	This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. For more information about configuring system settings, see the *IBM Security QRadar SIEM Administration Guide*. ▶ Select this check box to enable this rule to send an SNMP notification (trap). For an offense rule, the SNMP trap output includes system time, the trap OID, and the notification data, as defined by the Q1 Labs MIB. For more information about the Q1 Labs MIB, see the *IBM Security QRadar SIEM Administration Guide*. For example, the SNMP notification might resemble: `"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Offense description"`
Send to Local SysLog	Select this check box if you want to log the event or flow locally. By default, this check box is clear. For example, the syslog output might resemble: `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description`
Send to Forwarding Destinations	Select this check box if you want to log the event or flow on a forwarding destination. A forwarding destination is a vendor system, such as SIEM, ticketing, or alerting systems. When you select this check box, a list of forwarding destinations is displayed. Select the check box for the forwarding destination you want to send this event or flow to. To add, edit, or delete a forwarding destination, click the **Manage Destinations** link. For more information about configuring forwarding destinations, see the *IBM Security QRadar SIEM Administration Guide*.
Publish on the IF-MAP Server	If the IF-MAP parameters are configured and deployed in the system settings, select this option to publish the offense information on the IF-MAP server. For more information about configuring the IF-MAP parameters, see the *IBM Security QRadar SIEM Administration Guide*.
Response Limiter	Select this check box and use the list boxes to configure the frequency with which you want this rule to respond.
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

The following table provides the Rule Response page parameters if the rule type is Anomaly.

Table 9-5 Anomaly Detection Rule Response page parameters

Parameter	Description
Rule Response	
Dispatch New Event	Specifies that this rule dispatches a new event in addition to the original event or flow, which is processed like all other events in the system. By default, this check box is selected and cannot be cleared.
Event Name	Type the unique name of the event you want to be displayed on the **Offenses** tab.
Event Description	Type a description for the event. The description is displayed in the Annotations pane of the event details.
Offense Naming	Select one of the following options: • **This information should contribute to the name of the associated offense(s)** - Select this option if you want the Event Name information to contribute to the name of the offense. • **This information should set or replace the name of the associated offense(s)** - Select this option if you want the configured Event Name to be the name of the offense. • **This information should not contribute to the naming of the associated offense(s)** - Select this option if you do not want the Event Name information to contribute to the name of the offense. This is the default.
Severity	Using the list boxes, select the severity for the event. The range is 0 (lowest) to 10 (highest) and the default is 5. The Severity is displayed in the Annotations pane of the event details. For more information about severity, see the **Glossary**.
Credibility	Using the list boxes, select the credibility of the event. The range is 0 (lowest) to 10 (highest) and the default is 5. Credibility is displayed in the Annotations pane of the event details. For more information about credibility, see the **Glossary**.
Relevance	Using the list boxes, select the relevance of the event. The range is 0 (lowest) to 10 (highest) and the default is 5. Relevance is displayed in the Annotations pane of the event details. For more information about relevance, see the **Glossary**.
High Level Category	From the list box, select the high-level event category you want this rule to use when processing events. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.
Low Level Category	From the list box, select the low-level event category you want this rule to use when processing events. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.

Table 9-5 Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
Annotate this offense	Select this check box to add an annotation to this offense and type the annotation.
Ensure the dispatched event is part of an offense	As a result of this rule, the event is forwarded to the Magistrate component. If an offense exists, this event will be added. If no offense has been created on the **Offenses** tab, a new offense is created. This parameter is enabled by default. The following options are displayed: • **Index offense based on** - Specifies that the new offense is based on event name. This parameter is enabled by default. • **Include detected events by Event Name from this point forward, for second(s), in the offense** - Select this check box and type the number of seconds you want to include detected events or flows from the source on the **Offenses** tab.
Email	Select this check box to display the email options. By default, the check box is clear.
Enter email address to notify	Type the email address to send notification if this rule generates. Separate multiple email addresses using a comma.
SNMP Trap	This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. For more information about configuring system settings, see the *IBM Security QRadar SIEM Administration Guide*. ▶ Select this check box to enable this rule to send an SNMP notification (trap). The SNMP trap output includes system time, the trap OID, and the notification data, as defined by the Q1 Labs MIB. For more information about the Q1 Labs MIB, see the *IBM Security QRadar SIEM Administration Guide*. For example, the SNMP notification might resemble: `"Wed Sep 28 12:20:57 GMT 2005, QRADAR Custom Rule Engine Notification - Rule 'SNMPTRAPTest' Fired. 172.16.20.98:0 -> 172.16.60.75:0 1, Event Name: ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited, QID: 1000156, Category: 1014, Notes: Offense description"`
Notify	Select this check box if you want events that generate as a result of this rule to be displayed in the System Notifications item in the Dashboard tab. For more information about the Dashboard tab, see **Dashboard management**. ***Note:*** *If you enable notifications, configure the* ***Response Limiter*** *parameter.*

Table 9-5 Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
Send to Local SysLog	Select this check box if you want to log the event or flow locally. By default, the check box is clear. For example, the syslog output might resemble: `Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description`
Add to Reference Set	Select this check box if you want events generated as a result of this rule to add data to a reference set. To add data to a reference set: **1** Using the first list box, select the data you want to add. Options include all normalized or custom data. **2** Using the second list box, select the reference set to which you want to add the specified data. The **Add to Reference Set** rule response provides the following functions: • **Refresh** - Click **Refresh** to refresh the first list box to ensure that the list is current. • **Configure Reference Sets** - Click **Configure Reference Sets** to configure the reference set. This option is only available if you have administrative permissions. For more information on managing reference sets, see the *IBM Security QRadar SIEM Administration Guide*.
Add to Reference Data	Before you can use this rule response, you must create the reference data collection using the Command Line Interface (CLI). For more information on how to create and use reference data collections, see *IBM Security QRadar Reference Data Collections Technical Note*. Select this check box if you want events generated as a result of this rule to add to a reference data collection. After you select the check box, select one of the following options: • **Add to a Reference Map** - Select this option to send data to a collection of single key/multiple value pairs. You must select the key and value for the data record, and then select the reference map you want to add the data record to. • **Add to a Reference Map of Sets** - Select this option to send data to a collection of key/single value pairs. You must select the key and the value for the data record, and then select the reference map of sets you want to add the data record to. • **Add to a Reference Map of Maps** - Select this option to send data to a collection of multiple key/single value pairs. You must select a key for the first map, a key for the second map, and then the value for the data record. You must also select the reference map of maps you want to add the data record to.

Table 9-5 Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
Publish on the IF-MAP Server	If the IF-MAP parameters are configured and deployed in the system settings, select this option to publish the offense information on the IF-MAP server. For more information about configuring the IF-MAP parameters, see the *IBM Security QRadar SIEM Administration Guide*.
Response Limiter	Select this check box and use the list boxes to configure the frequency with which you want this rule to respond.
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

10 ASSET MANAGEMENT

QRadar SIEM automatically discovers assets (servers and hosts) on your network, based on passive flow data and vulnerability data, to create asset profiles. Using the **Assets** tab, you can manage assets on your network.

Assets tab overview

Asset profiles provide information about each known asset in your network, including what services are running on each asset. Asset profile information is used for correlation purposes to help reduce false positives. For example, if a source attempts to exploit a specific service running on an asset, QRadar SIEM can determine if the asset is vulnerable to this attack by correlating the attack to the asset profile.

Using the **Assets** tab, you can:

- Search for specific assets.
- View all the learned assets.
- View identity information for learned assets.
- Manually add asset profiles.
- Edit asset profiles for manually added or discovered assets.
- Tune false positive vulnerabilities.
- Print or export asset profiles.

Asset profiles are only populated if you have flow data or vulnerability assessment (VA) scans configured. For flow data to populate asset profiles, bidirectional flows are required. For more information about VA, see the *IBM Security QRadar Vulnerability Assessment Guide*. For more information about flow sources, see the *IBM Security QRadar SIEM Administration Guide*.

Vulnerability details

Third-party scanners identify and report discovered vulnerabilities to QRadar SIEM using external references, such as the Open Source Vulnerability Database (OSVDB) and National Vulnerability Database (NVDB). Examples of third-party scanners include QualysGuard and nCircle ip360. The OSVDB assigns a unique reference identifier (OSVDB ID) to each vulnerability. Additionally, external data references can identify vulnerabilities with an ID. Examples of external data reference IDs include Common Vulnerability and Exposures (CVE) ID or Bugtraq ID.

For more information on scanners and vulnerability assessment, see the *IBM Security QRadar SIEM Vulnerability Assessment Guide*.

Asset searches

The search feature allows you to search host profiles, assets, and identity information. Identity information provides additional details about log sources on your network, including DNS information, user logins, and MAC addresses.

Using the asset search feature, you can search for assets by external data references to determine if known vulnerabilities exist in your deployment.

For example:

You receive a notification that CVE ID: CVE-2010-000 is being actively exploited in the field. To verify if any hosts in your deployment are vulnerable to this exploit, you can type the `CVE-2010-000` in the **CVE ID** search parameter to view a list of all hosts that are vulnerable to that specific CVE ID.

Note: For more information about OSVDB, see *http://osvdb.org/*. For more information about NVDB, see *http://nvd.nist.gov/*.

Investigating asset profiles

When you access the **Assets** tab, the Asset Profile Search is displayed. You must configure search parameters to display the asset profiles you want to investigate.

About this task

The **Search** icon is available below each pane on the Asset Profile Search page. After you have specified your search criteria and do not require additional search criteria from the remaining panes, you can click the **Search** icon.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the Asset Profile Search page, define the criteria for what assets you want to list. Choose one of the following options:

- To list all asset profiles in your deployment, click **Show All**.
- To list a defined set of assets, define your search criteria. See **Table 10-2**.

Step 3 Optional. To view additional information about an asset, move your mouse over the IP address for the asset you want to investigate.

Step 4 To view the Asset Profile page for the asset, double-click the asset. See **Table 10-4**.

Step 5 Optional. To further investigate associated data, click a toolbar function on the Asset Profile pane. For descriptions of the toolbar functions, see **Table 10-8**.

Step 6 Optional. To edit parameters directly from the Asset Profile page, make the necessary changes and click **Save Changes**.

Step 7 To view the Research Vulnerability Details window for the asset, choose one of the following options:

- In the Ports and Vulnerabilities pane, double-click the row for the vulnerability you want to view.
- In the Ports and Vulnerabilities pane, click the link in the **Name** parameter for the vulnerability you want to view.

  See **Review Vulnerability Details window parameters**.

Asset profile management tasks

Using the **Assets** tab, you can add, edit, delete, import, and export asset profiles.

Adding an asset profile

QRadar SIEM automatically discovers and adds asset profiles; therefore, adding an asset profile is typically not necessary. However, you may be required to manually add a profile.

About this task

When you add an asset profile, you must configure the following parameters:

Table 10-1 Add Asset Profile page parameters

Parameter	Description
IP	Type the IP address or CIDR range of the asset.
Asset Name	Type the name of the asset. This parameter is case sensitive. The maximum length is 255 characters.
Description	Type a description of the asset. The maximum length is 255 characters.
Asset Weight	From the list box, type the asset weight you want to assign to this asset. The range is 0 to 10. The default is 0.
Business Owner	Type the name of business owner of the asset. An example of a business owner is a department manager. The maximum length is 255 characters.
Business Owner Contact Info	Type the contact information for the business owner. The maximum length is 255 characters.
Technical Owner	Type the technical owner of the asset. An example of a business owner is the IT manager or director. The maximum length is 255 characters.
Technical Owner Contact Info	Type the contact information for the technical owner. The maximum length is 255 characters.
Location	Type the physical location of the asset. The maximum length is 255 characters.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 Click **Add Asset**.

Step 4 Enter values for the parameters. See Table 10-1.

Step 5 Click **Save**.

What to do next

After you add an asset profile, you can edit the profile to configure additional asset profile parameters, such as operating system and business owner information. See Editing an asset.

Editing an asset

You can edit an automatically discovered or manually added asset profile.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 On the Asset Profile Search page, define the criteria for what assets you want to list. Choose one of the following options:

- To list all asset profiles in your deployment, click **Show All**.
- To list a defined set of assets, define your search criteria. See Table 10-2.

Step 4 From the list of assets, select the asset you want to edit.

Step 5 Click **Edit Asset**.

Step 6 Edit the parameters. See Table 10-6.

Step 7 Click **Save Changes**.

Deleting assets

You can delete specific assets or all listed asset profiles.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 On the Asset Profile Search page, define the criteria for what assets you want to list. Choose one of the following options:

- To list all asset profiles in your deployment, click **Show All**.
- To list a defined set of assets, define your search criteria. See Table 10-2.

Step 4 Choose one of the following options:

- Select the asset you want to delete, and then select **Delete Asset** from the **Actions** list box.
- From the **Actions** list box, select **Delete Listed**.

Step 5 Click **OK**.

Importing asset profiles

You can import asset profile information into QRadar SIEM.

Before you begin

The imported file must be a CSV file in the following format:

```
ip,name,weight,description
```

Where:

- **IP** - Specifies any valid IP address in the dotted decimal format. For example: 192.168.5.34.
- **Name** - Specifies the name of this asset up to 255 characters in length. Commas are not valid in this field and invalidates the import process. For example: WebServer01 is correct.
- **Weight** - Specifies a number from 0 to 10, which indicates the importance of this asset on your network. A value of 0 denotes low importance and 10 is very high.
- **Description** - Specifies a textual description for this asset up to 255 characters in length. This value is optional.

For example, the following entries might be included in a CSV file:

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

The import process merges the imported asset profiles with the asset profile information you have currently stored in the system.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 From the **Actions** list box, select **Import Assets**.

Step 4 Click **Browse** to locate and select the CSV file you want to import.

Step 5 Click **Import Assets** to begin the import process.

Result

If an error occurs during the import process, no assets are imported.

Exporting assets

You can export listed asset profiles to an Extended Markup Language (XML) or Comma-Separated Value (CSV) file.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Asset Profiles**.

Step 3 On the Asset Profile Search page, define the criteria for what assets you want to list. Choose one of the following options:

- To list all asset profiles in your deployment, click **Show All**.
- To list a defined set of assets, define your search criteria. See Table 10-2.

Step 4 From the **Actions** list box, select one of the following options:

- Export to XML
- Export to CSV

A status window provides the status of the export process.

Step 5 Optional. If you want to use other tabs and pages in QRadar SIEM while the export is in progress, click the **Notify When Done** link.

When the export is complete, the File Download window is displayed.

Step 6 On the File Download window, choose one of the following options:

- **Open** - Select this option to open the export results in your choice of browser.
- **Save** - Select this option to save the results to your desktop.

Step 7 Click **OK**.

Assets tab parameters and toolbars

This topic includes tables that describe the parameters and toolbars displayed on each page of the **Assets** tab.

Asset Profile Search page parameters and toolbar functions

The following table describes the Asset Profile Search page parameters:

Table 10-2 Asset Profile Search parameters

Parameter	Description
Asset Properties	
IP	Type the IP address or CIDR range of the assets you want to search for.
MAC	Type the MAC address of the asset you want to search for.
Host Name	Type the host name of the asset you want to search for. This search field is case insensitive and accepts any symbol characters.
Machine Name	Type the machine name of the asset you want to search for. This search field is case insensitive and accepts any symbol characters.
Username	Type the user of the assets you want to search for. This search field is case insensitive and accepts any symbol characters.
User Group	Type the user group of the assets you want to search for. This search field is case insensitive and accepts any symbol characters.

Table 10-2 Asset Profile Search parameters (continued)

Parameter	Description
Extra Data	Type the text you want to search for. The content of this field is user-defined text and depends on the devices on your network that are available to provide identity data. Examples include: physical location of devices, relevant policies, or network switch and port names.
Asset Name	Type the name of the assets you want to search for. This search field is case insensitive and accepts any symbol characters.
Description	Type the description of the assets you want to search for.
Port	Type the ports (TCP or UDP) or port ranges of the assets you want to search for. You can enter multiple ports, separated by commas. For example, 80, 8080, or 6000 to 7000.
Risk Level	From the list box, select less than, equal to, or greater than the specified risk level. Then type the risk level of the assets you want to search for. The range is 0 to 10.
Network	From the list box, select the network of the assets you want to search.
Asset Weight	Type the asset weight of the assets you want to search for. From the list box, select whether you want to search for less than, equal to, or greater than the specified asset weight. Then type the asset weight you want to search for. The range is 0 to 10. The asset weight allows QRadar SIEM to appropriately prioritize offenses against high valued assets.
Show only hosts with vulnerabilities	Select this check box if you want only to display only assets with vulnerabilities in the search results.
Operating System	Type the operating system of the assets you want to search for. For example, Red Hat Linux®.
Service Vendor	Type the service vendor of the assets you want to search for. For example, RedHat inc.
Service Version	Type the service version of the assets you want to search for. For example, 7.1.
Extended Asset Properties	
Business Owner	Type the business owner of the assets you want to search for. An example of a business owner is a department manager.
Business Owner Contact Info	Type the business owner contact information of the assets you want to search for.
Technical Owner	Type the technical owner of the assets you want to search for. An example of a technical owner is an IT manager or director.
Technical Owner Contact Info	Type the technical owner contact information of the assets you want to search for.
Location	Type the physical location of the assets you want to search for.
Vulnerability Attributes	

Table 10-2 Asset Profile Search parameters (continued)

Parameter	Description
Extra Data	Type the text you want to search for. The content of this field is user-defined text and depends on the devices on your network that are available to provide identity data. Examples include: physical location of devices, relevant policies, or network switch and port names.
Asset Name	Type the name of the assets you want to search for. This search field is case insensitive and accepts any symbol characters.
Description	Type the description of the assets you want to search for.
Port	Type the ports (TCP or UDP) or port ranges of the assets you want to search for. You can enter multiple ports, separated by commas. For example, 80, 8080, or 6000 to 7000.
Risk Level	From the list box, select less than, equal to, or greater than the specified risk level. Then type the risk level of the assets you want to search for. The range is 0 to 10.
Network	From the list box, select the network of the assets you want to search.
Asset Weight	Type the asset weight of the assets you want to search for. From the list box, select whether you want to search for less than, equal to, or greater than the specified asset weight. Then type the asset weight you want to search for. The range is 0 to 10. The asset weight allows QRadar SIEM to appropriately prioritize offenses against high valued assets.
Show only hosts with vulnerabilities	Select this check box if you want only to display only assets with vulnerabilities in the search results.
Operating System	Type the operating system of the assets you want to search for. For example, Red Hat Linux®.
Service Vendor	Type the service vendor of the assets you want to search for. For example, RedHat inc.
Service Version	Type the service version of the assets you want to search for. For example, 7.1.
Extended Asset Properties	
Business Owner	Type the business owner of the assets you want to search for. An example of a business owner is a department manager.
Business Owner Contact Info	Type the business owner contact information of the assets you want to search for.
Technical Owner	Type the technical owner of the assets you want to search for. An example of a technical owner is an IT manager or director.
Technical Owner Contact Info	Type the technical owner contact information of the assets you want to search for.
Location	Type the physical location of the assets you want to search for.
Vulnerability Attributes	

Table 10-2 Asset Profile Search parameters (continued)

Parameter	Description
OSVDB ID	Type the vulnerability identifier, as defined on the OSVDB, of the assets you want to search for. You can type multiple OSVDB IDs, separated by commas.
Bugtraq ID	Type the Bugtraq ID you want to search for. For example, 1234.
CERT	Type Computer Emergency Response Team (CERT) advisory number you want to search for. For example, CA-2001-01.
CERT VU	Type the CERT vulnerability note (VU) number you want to search for. For example, 619982.
CIAC Advisory	Type the Computer Incident Advisory Capability (CIAC) advisory number you want to search for. For example, O-084.
CVE ID	Type the CVE ID you want to search for. For example, 2004-0001.
DISA IAVA	Type the Defense Information System Agency (DISA) Information Assurance Vulnerability Alert (IAVA) number you want to search for. For example, 2008-A-<nnnn>, where <nnnn> is a numeric identifier.
Exploit Database	Type the Exploit Database ID you want to search for.
FrSIRT Advisory	Type the French Security Incident Response Team (FrSIRT) Advisory ID you want to search for.
Generic Exploit URL	Type the Generic Exploit URL you want to search for. ***Note:*** *Typically the Generic Exploit URL links to exploit script/code or a detailed text file that explains how to exploit a specific vulnerability.*
Generic Informational URL	Type the Generic Informational URL you want to search for. ***Note:*** *The Generic Information URL links to information about a type or class of vulnerability. For example, this attribute can contain a link to a white paper on DDoS attacks.*
IBM APPSCAN	Type the IBM AppScan identifier you want to search for. For example, security-check-applicationtestscriptdetected.
ISS X-Force ID	Type the Internet Security System (ISS) X-Force ID you want to search for. For example, 1234.
Keyword	Type the keyword you want use to search all fields in the OSVDB.
Mail List Post	Type the URL for the Mail List Post ID you want to search for.
Metasploit ID	Type the Metasploit ID you want to search for.
Microsoft Knowledge Base Article	Type the Microsoft® Knowledge Base Article ID you want to search for. For example, KB958644.
Microsoft Security Bulletin	Type the Microsoft Security ID you want to search for. For example, MS04-004.
Milw0rm	Type the Milw0rm ID you want to search for. For example, 6824.
Nessus Script ID	Type the URL for the Nessus Script ID you want to search for. For example, 10123.

Table 10-2 Asset Profile Search parameters (continued)

Parameter	Description
News Article	Type the URL for the News Article ID you want to search for. ***Note:*** *The News Article ID references mainstream news articles about specific vulnerabilities.*
Niko Item ID	Type the Niko Item ID you want to search for.
OVAL ID	Type the Open Vulnerability and Assessment Language (OVAL) ID you want to search for. For example, 5863.
Other Advisory URL	Type the Other Advisory URL you want to search for.
Other Solution URL	Type the Other Solution URL you want to search for.
Packet Storm	Type the Packet Storm reference you want to search for.
RedHat RHSA	Type the RedHat Security Alert (RHSA) ID you want to search for. For example, RHSA-2004:065-05.
Related OSVDB ID	Type the related OSVDB ID you want to search for. IDs are cross-referenced in the OSVDB. Typically OSVDB IDs are cross-referenced if the source of the information is the same.
SCIP VulDB ID	Type the Secure Communications Interoperability Protocol (SCIP) Vulnerability Database (VulDB) ID you want to search for.
Secunia Advisory ID	Type the Secunia Advisory ID you want to search for. For example: 10123.
Security Tracker	Type the Security Tracker ID you want to search for. For example, 1009695.
Snort Signature ID	Type the Snort Signature ID you want to search for. For example, 1324.
Tenable PVS	Type the Tenable Passive Vulnerability Scanner (PVS) ID you want to search for.
US-CERT Cyber Security Alert	Type the US-CERT Cyber Security Alert ID you want to search for. For example, TA06-333A.
VUPEN Advisory	Type the VUPEN Security ID you want to search for.
Vender Specific Advisory URL	Type the Vender Specific Advisory URL you want to search for.
Vendor Specific News/Changelog Entry	Type the URL of the Vendor Specific New/Changelog Entry you want to search for.
Vendor Specific Solution URL	Type the Vendor Specific Solution URL you want to search for.
Vendor URL	Type the Vendor URL you want to search for.

The Asset Profile Search toolbar provides the following options:

Table 10-3 Assets tab toolbar

Options	Description
Add Asset	Click **Add Asset** to add an asset profile. See **Adding an asset profile**.
Actions	Click **Actions** to import assets. See **Importing asset profiles**. ***Note:*** *The Actions menu is available only if you have administrative privileges. For more information, see the IBM Security QRadar SIEM Administration Guide.*

Asset Profiles page parameters and toolbar functions

The Asset Profiles page provides the following information on each asset:

Table 10-4 Asset Profile page parameters

Parameter	Description
IP Address	Specifies the IP address of the asset.
MAC	Specifies the last known MAC address of the asset.
Name	Specifies the name, host name, or machine name of the asset. If unknown, this field is blank.
User	Specifies the last known user of the asset. If unknown, this field is blank.
Group	Specifies the last known user group of the asset. If unknown, this field is blank.
Network	Specifies the network in which the asset belongs.
Weight	Specifies the asset weight of the asset.
Risk Level	Specifies the risk level of the asset.
Vulnerabilities	Specifies the number of identified vulnerabilities associated with this asset. This value also includes the number of active and passive vulnerabilities.
Last Seen	Specifies the last date and time the asset was seen. If the asset was manually entered but never actively or passively seen, the column indicates Never.

The Asset Profiles page toolbar provides the following functions:

Table 10-5 Asset Profiles page toolbar functions

Function	Description
Modify Search	Click **Modify Search** to return to the Assets Search page to modify your search criteria. See **Investigating asset profiles**.
Add Asset	Click **Add Asset** to add an asset profile. See **Adding an asset profile**.
Edit Asset	Click **Edit Asset** to edit an asset profile. This option is enabled only if you have selected an asset profile from the results list. See **Editing an asset**.

Table 10-5 Asset Profiles page toolbar functions (continued)

Function	Description
Actions	Click **Actions** to perform the following actions: • **Delete Asset** - Select this option to delete the selected asset profiles. See **Deleting assets**. • **Delete Listed** - Select this option to delete all asset profiles listed in the results list. See **Deleting assets**. • **Import Assets** - Select this option to import assets. See **Importing asset profiles**. • **Export to XML** - Select this option to export asset profiles in XML format. See **Exporting assets**. • **Export to CSV** - Select this option to export asset profiles in CSV format. See **Exporting assets**. ***Note:*** *The **Actions** menu is available only if you have administrative privileges. For more information, see the IBM Security QRadar SIEM Administration Guide.*
Print	Click **Print** to print the asset profiles displayed on the page.

Asset Profile page parameters and toolbar functions

The Asset Profile page provides the following information:

Table 10-6 Asset Profile page parameters

Parameter	Description
Name	Specifies the name of the asset.
Description	Specifies a description for this asset.
IP Address	Specifies the IP address of the asset.
Network	Specifies the network in which the asset belongs.
Host Name (DNS Name)	Specifies the IP address or DNS name of the asset, if known.
Risk Level	Specifies the risk level (0 to 10) for the asset where 0 is the lowest and 10 is the highest. This is a weighted value against all other hosts in your deployment.
Operating System	Specifies the operating system running on the asset. ***Note:*** *You can edit this parameter directly if the **Override** parameter is specified as **Override Until the Next Scan** or **Override Forever**. From the list box, select the operating system name.*
Vendor	Specifies the operating system vendor name of the asset, as detected by the VA scanner or manually entered. ***Note:*** *You can edit this parameter directly if the **Override** parameter is specified as **Override Until the Next Scan** or **Override Forever**. From the list box, select the operating system vendor name.*

Table 10-6 Asset Profile page parameters (continued)

Parameter	Description
Version	Specifies the version of the operating system. ***Note:*** *You can edit this parameter if the* ***Override*** *parameter is specified as* ***Override Until the Next Scan*** *or* ***Override Forever****. From the list box, select the operating system version.*
Override	The **Override** parameter specifies the method by which operating system information (Operating System, Vender, and Version parameters) is derived. From the list box, select one of the following options: • **Detected By a Scanner** - Select this option to specify that the scanner provides operating system information. • **Override Until the Next Scan** - Select this option to specify that the scanner provides operating system information and the information can be temporarily edited. If you edit the operating system parameters, the scanner restores the information at its next scan. This is the default. • **Override Forever** - Select this option to specify that you want to manually enter operating system information and disable the scanner from updating the information.
Asset Weight	Specifies the level of importance associated with this asset. The range is 0 (Not Important) to 10 (Very Important).
MAC	Specifies the last known MAC address of the asset.
Machine Name	Specifies the last known machine name of the asset.
Username	Specifies the last known user of the asset.
Extra Data	Specifies any extended information based on an event.
Host Name	Specifies the last known host name of the asset.
User Group	Specifies the last known user group of the asset.
Business Owner	Specifies the name of business owner of the asset. An example of a technical owner is a department manager.
Business Owner Contact Info	Specifies the contact information for the business owner.
Technical Owner	Specifies the technical owner of the asset. An example of a technical owner is an IT manager or director.
Technical Owner Contact Info	Specifies the contact information of the technical owner.
Location	Specifies the physical location of the asset.

The Asset Profile page toolbar provides the following functions:

Table 10-7 Asset Profile page toolbar

Function	Description
Return to Asset List	Click **Return to Asset List** to return to the assets search results page.

Table 10-7 Asset Profile page toolbar (continued)

Function	Description
Modify Search	Click **Modify Search** to return to the Assets Search page to modify your search criteria. See **Investigating asset profiles**.
Print	Click **Print** to print the asset profiles displayed on the page.

The Asset Profile pane on the Asset Profile page provides the following functions:

Table 10-8 Asset Profile pane toolbar functions

Options	Description
View by Network	If this asset is associated with an offense, this option allows you to view the list of networks associated with this asset. When you click **View By Network**, the List of Networks window is displayed. See **Monitoring offenses grouped by network**.
View Source Summary	If this asset is the source of an offense, this option allows you to view source summary information. When you click **View Source Summary**, the List of Offenses window is displayed. See **Monitoring offenses grouped by source IP**.
View Destination Summary	If this asset is the destination of an offense, this option allows you to view destination summary information. When you click **View Destination Summary**, the List of Destinations window is displayed. See **Monitoring offenses grouped by destination IP**.

Table 10-8 Asset Profile pane toolbar functions (continued)

Options	Description
History	Click **History** to view event history information for this asset. When you click the **History** icon, the Event Search window is displayed, pre-populated with the following event search criteria: • **Time Range** - Recent (Last 24 Hours) • **Search Parameters** - Specifies the following filters to be applied to the search results: - Identity is true - Identity IP is the IP address of the asset • **Column Definition** - Specifies the following columns to be displayed in the search results: - Event name - Log Source - Start Time - Identity User Name - Identity MAC - Identity Host Name - Identity Net Bios Name - Identity Group Name You can customize the search parameters, if required. Click **Search** to view the event history information. For more information about searching events, see **Data searches**.
Applications	Click **Applications** to view application information for this asset. When you click the **Applications** icon, the Flow Search window is displayed, pre-populated with the following event search criteria: • **Time Range** - Recent (Last 24 Hours) • **Search Parameters** - Specifies the following filter to be applied to the search results: Source or Destination IP is the IP address of the asset. • **Column Definition** - Specifies the **Application Group** column to be displayed in the search results. You can customize the search parameters, if required. Click **Search** to view the application information. For more information about searching flows, see **Data searches**.
Search Connections	Click **Search Connections** to search for connections. The Connection Search window is displayed. ***Note:*** *This option only is displayed when the IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the IBM Security QRadar Risk Manager Users Guide.*

Table 10-8 Asset Profile pane toolbar functions (continued)

Options	Description
View Topology	Click **View Topology** to further investigate the asset. The Current Topology window is displayed. ***Note:*** *This option is only available when the IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the IBM Security QRadar Risk Manager Users Guide.*

The Ports and Vulnerabilities pane of the Asset Profile page displays the following information:

Table 10-9 Ports and Vulnerabilities pane parameters

Parameter	Description
Vuln ID	Specifies the ID of the vulnerability. The Vuln ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Port	Specifies the port number for the services discovered on the asset.
Service	Specifies the services discovered on the asset.
Name	Specifies the name of the vulnerability. ▶ Click the link to display the Research Vulnerability Details window. For more information on the Research Vulnerability Details window, see **Review Vulnerability Details window parameters**
Description	Specifies a description of the detected vulnerability. This value is only available if your system integrates VA tools.
Risk/Severity	Specifies the risk level (0 to 10) for the vulnerability.
Last Seen	Specifies the date and time that the service was last detected on the asset either passively or actively.
First Seen	Specifies the date and time when the service was first detected on the asset either passively or actively.
False Positive Tuning	Click **False Positive Tuning** to remove selected vulnerabilities from the list. ***Note:*** *This option is only available if you have one of the following user permissions: Admin or Remove Vulnerabilities.For more information, see the IBM Security QRadar SIEM Administration Guide.*

Review Vulnerability Details window parameters

The Research Vulnerability Details window provides the following details:

Table 10-10 Research Vulnerabilities Details window details

Parameter	Description
Vuln ID	Specifies the ID of the vulnerability. The Vuln ID is a unique identifier that is generated by Vulnerability Information System (VIS).
Published Date	Specifies the date on which the vulnerability details were published on the OSVDB.
Name	Specifies the name of the vulnerability.
CVE	Specifies the CVE identifier for the vulnerability. CVE identifiers are provided by the NVDB. ▶ Click the link to obtain more information. When you click the link, the NVDB website is displayed in a new browser window.
OSVDB	Specifies the OSVDB identifier for the vulnerability. ▶ Click the link to obtain more information. When you click the link, the OSVDB website is displayed in a new browser window.
CVSS Score	Specifies the Common Vulnerability Scoring System (CVSS) score of the vulnerability. A CVSS score is an assessment metric for the severity of a vulnerability. You can use CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities. For more information on CVSS, see *http://www.first.org/cvss/*.
Description	Specifies a description of the detected vulnerability. This value is only available when your system integrates VA tools.
Concern	Specifies the effects the vulnerability can have on your network.
Solution	Follow the instructions provided to resolve the vulnerability.

Table 10-10 Research Vulnerabilities Details window details

Parameter	Description
IPS/IDS Mitigation	Displays information on the Intrusion Prevention System/Intrusion Detection System (IPS/IDS) device associated with this vulnerability. The IPS/IDS Mitigation table displays the following information: • **QID** - Specifies the QID associated with this vulnerability. A QID assigns a unique identifier, high-level, and lower-level category to a single event from an external device. • **Device Type** - Specifies the device type associated with the QID. • **Signature** - Specifies the signature issued from the IPS/IDS device.
Reference	Displays a list of external references, including: • **Reference Type** - Specifies the type of reference listed, such an advisory URL or mail post list. • **URL** - Specifies the URL that you can click to view the reference. ▶ Click the link to obtain more information. When you click the link, the external resource is displayed in a new browser window.
Products	Displays a list of products that are associated with this vulnerability. • **Vendor** - Specifies the vendor of the product. • **Product** - Specifies the product name. • **Version** - Specifies the version number of the product.

11 REPORTS MANAGEMENT

You can use the **Reports** tab to create, edit, distribute, and manage reports.

The **Reports** tab provides you with:

- Detailed reporting options required to satisfy various regulatory standards, such as PCI compliance.
- Flexibility in layout and content.

Reports tab overview

You can create your own custom reports in QRadar SIEM or use a default reports. You can customize and rebrand default reports and distribute these to other QRadar SIEM users.

The **Reports** tab might require an extended period of time to refresh if your system includes a large number of reports.

Note: If you are running Microsoft® Exchange Server 5.5, unavailable font characters might be displayed in the subject line of emailed reports. To resolve this, download and install Service Pack 4 of Microsoft Exchange Server 5.5. For more information, contact Microsoft support.

Timezone considerations

To ensure that the Reports feature uses the correct date and time for reporting data, your QRadar SIEM session must be synchronized with your timezone. During the installation and setup of QRadar SIEM, the time zone is configured. Check with your administrator to ensure your QRadar SIEM session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports created by other QRadar SIEM users. Non-administrative users can only view reports they created or reports which are shared by other users.

Reports tab parameters

The **Reports** tab displays a list of default and custom reports. From the **Reports** tab, you can view statistical information about the reports template, perform actions on the report templates, view the generated reports, delete generated content.

The **Reports** tab provides the following information:

Table 11-1 Reports tab parameters

Parameters	Description
Flag Column	If an error occurred, causing the report generation to fail, the **Error** icon is displayed in this column.
Report Name	Specifies the report name.
Group	Specifies the group to which this report belongs.
Schedule	Specifies the frequency with which the report is generated. Reports that specify an interval schedule, when enabled, are automatically generated according to the specified interval. If a report does not specify an interval schedule, you must manually generate the report. See **Manually generating a report**.
Next Run Time	Specifies the duration of time, in hours and minutes, until the next report is generated.
Last Modification	Specifies the last date this report was modified.
Owner	Specifies the QRadar SIEM user that owns the report.
Author	Specifies the QRadar SIEM user that created the report.
Generated Reports	From this list box, select the date stamp of the generated report you want to view. When you select the date stamp, the **Format** parameter displays the available formats for the generated reports. See **Viewing generated reports**. If no reports have been generated, **None** is displayed.
Formats	Specifies the report formats of the currently selected report in the **Generated Reports** column. Click the icon for the format you want to view. Report formats include: • **PDF** - Portable Document Format • **HTML** - Hyper Text Markup Language format • **RTF** - Rich Text Format • **XML** - Extensible Markup Language (only available for tables) • **XLS** - Microsoft® Excel format (only available for tables)

You can point your mouse over any report to preview a report summary in a tooltip. The summary specifies the report configuration and the type of content the report generates.

Report tab sort order

By default, reports are sorted by the **Last Modification** column. On the Reports navigation menu, reports are sorted by interval schedule. To filter the report to only display reports of a specific frequency, click the arrow beside the **Report** menu item on the navigation menu and select the group (frequency) folder.

Reports tab toolbar

You can use the toolbar to perform a number of actions on reports. The following table identifies and describes the Reports toolbar options.

Table 11-2 Reports tab toolbar options

Option	Description
Group	From the list box, select the group you want to view. The group is displayed with the assigned reports. For more information, see **Report groups**.
Manage Groups	Click **Manage Groups** to manage report groups. Using the Manage Groups feature, you can organize your reports into functional groups. For more information, see **Report groups**.
Actions	Click **Actions** to perform the following actions: • **Create** - Select this option to create a new report. For more information, see **Editing a report**. • **Edit** - Select this option to edit the selected report. You can also double-click a report to edit the content. • **Duplicate** - Select this option to duplicate or rename the selected report. For more information, see **Duplicating a report**. • **Assign Groups** - Select this option to assign the selected report to a report group. For more information, see **Report groups**. • **Share** - Select this option to share the selected report with other users. You must have administrative privileges to share reports. For more information, see **Sharing a report**. • **Toggle Scheduling** - Select this option to toggle the selected report to the Active or Inactive state. • **Run Report** - Select this option to generate the selected report. For more information, see **Manually generating a report**. To generate multiple reports, hold the Control key and click on the reports you want to generate. • **Run Report on Raw Data** - Select this option to generate the selected report using raw data. This option is useful when you want to generate a report before the required accumulated data is available. For example, if you want to run a weekly report before a full week has elapsed since you created the report, you can generate the report using this option. • **Delete Report** - Select this option to delete the selected report. To delete multiple reports, hold the Control key and click on the reports you want to delete. • **Delete Generated Content** - Select this option to delete all generated content for the selected rows. To delete multiple generated reports, hold the Control key and click on the generate reports you want to delete.

Table 11-2 Reports tab toolbar options (continued)

Option	Description
Hide Inactive Reports	Select this check box to hide inactive report templates. The **Reports** tab automatically refreshes and displays only active reports. Clear the check box to show the hidden inactive reports.
Search Reports	Type your search criteria in the **Search Reports** field and click the **Search Reports** icon. A search is run on the following parameters to determine which match your specified criteria: • Report Title • Report Description • Report Groups • Report Author User Name

Status bar

The status bar displays the number of search results (**Displaying 1 of 10 items**) currently displayed and the amount of time (**Elapsed time:**) required to process the search results.

Report layout

A report can consist of several data elements and can represent network and security data in a variety of styles, such as tables, line charts, pie charts, and bar charts.

When you select the layout of a report, consider the type of report you want to create. For example, do not choose a small chart container for graph content that displays a large number of objects. Each graph includes a legend and a list of networks from which the content is derived; choose a large enough container to hold the data. To preview how each chart displays a data, see **Graph types**.

Chart types

When you create a report, you must choose a chart type for each chart you want to include in your report. The chart type determines how the generated report presents data and network objects. You can chart data with several characteristics and create the charts in a single generated report.

QRadar SIEM includes the following chart types:

- **None** - When you select the **None** option, the container is displayed empty in the report. This option might be useful for creating white space in your report. If you select the None option for any container, no further configuration is required for that container.
- **Asset Vulnerabilities** - You can use the Asset Vulnerabilities chart to view vulnerability data for each defined asset in your deployment. You can generate Asset Vulnerability charts when vulnerabilities have been detected by a VA scan. For more information, see the *IBM Security QRadar Managing Vulnerability Assessment Guide.*

- **Connections** -The Connections option is only displayed when the IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.
- **Device Rules** - The Device Rules option is only displayed when the IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.
- **Device Unused Objects** -The Device Unused Objects option is only displayed when the IBM Security QRadar Risk Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager Users Guide*.
- **Events/Logs** - You can use the Event/Logs chart to view event information. You can base your charts on data from saved searches from the **Log Activity** tab. This allows you to customize the data that you want to display in the generated report. You can configure the chart to plot data over a configurable period of time. This functionality helps you to detect event trends.

  For more information about saved searches, see **Data searches**.
- **Flows** - You can use the Flows chart to view flow information. You can base your charts on data from saved searches from the **Network Activity** tab. This allows you to customize the data that you want to display in the generated report. You can use saved searches to configure the chart to plot flow data over a configurable period of time. This functionality helps you to detect flow trends.

  For more information about saved searches, see **Data searches**.
- **Top Destination IPs** - The Top Destination IPs chart displays the top destination IPs in the network locations you select.
- **Top Offenses** - The Top Offenses chart displays the TopN offenses that occur at present time for the network locations you select.
- **Top Source IPs** -The Top Source IPs chart displays and sorts the top offense sources (IP addresses) that attack your network or business assets.

For more information on these chart types, see **Chart container parameters**.

Graph types

Each chart type supports a variety of graph types you can use to display data. The network configuration files determine the colors the charts use to depict network traffic. Each IP address is depicted using a unique color.

The following table provides examples of how QRadar SIEM charts network and security data:

Table 11-3 Graph types

Graph Type	Availability
Line Graph	Available with the following chart types: • Events/Logs • Flows • Connections
Stacked Line Graph	Available with the following chart types: • Events/Logs • Flows • Connections
Bar Graph	Available with the following chart types: • Events/Logs • Flows • Asset Vulnerabilities • Connections
Horizontal Bar Graph	Available with the following chart types: • Top Source IPs • Top Offenses • Top Destination IPs
Stacked Bar Graph	Available with the following chart types: • Events/Logs • Flows • Connections
Pie Graph	Available with the following chart type: • Events/Logs • Flows • Asset Vulnerabilities • Connections

Table 11-3 Graph types (continued)

Graph Type	Availability
Table Graph	Available with the following charts: • Event/Logs • Flows • Top Source IPs • Top Offenses • Top Destination IPs • Connections To display content in a table, you must design the report with a full page width container.
Aggregate Table	Available with the Asset Vulnerabilities chart. To display content in a table, you must design the report with a full page width container.

Creating custom reports

On the **Reports** tab, you can access the Report Wizard to create a new report.

About this task

The Report Wizard provides a step-by-step guide on how to design, schedule, and generate reports. The wizard uses the following key elements to help you create a report:

- **Layout** - Position and size of each container
- **Container** - Placeholder for the featured content
- **Content** - Definition of the chart that is placed in the container

After creating a report that generates weekly or monthly, the scheduled time must have elapsed before the generated report returns results. For a scheduled report, you must wait the scheduled time period for the results to build. For example, a weekly search requires 7 days to build the data. This search does not return results before 7 days has elapsed.

When you specify the output format for the report, consider that the file size of generated reports can be one to two megabytes, depending on the selected output format. PDF format is smaller in size and does not consume a large quantity of disk storage space.

Procedure

Step 1 Click the **Reports** tab.

Step 2 From the **Actions** list box, select **Create**.

Step 3 On the Welcome to the Report Wizard change, click **Next** to move to the next page of the Report Wizard.

Step 4 Select one of the following scheduling options:

Option	**Description**
Manually	Generates a report once. This is the default setting; however, you can generate this report as often as required.
Hourly	Schedules the report to generate at the end of each hour using the data from the previous hour. If you choose the Hourly option, further configuration is required. From the list boxes, select a time frame to begin and end the reporting cycle. A report is generated for each hour within this time frame. Time is available in half-hour increments. The default is 1:00 a.m for both the **From** and **To** fields.
Daily	Schedules the report to generate daily using the data from the previous day. For each chart on a report, you can select the previous 24 hours of the day, or select a specific time frame from the previous day. If you choose the **Daily** option, further configuration is required. Select the check box beside each day you want to generate a report. Also, you can use the list box to select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly	Schedules the report to generate weekly using the data from the previous week. If you choose the **Weekly** option, further configuration is required. Select the day you want to generate the report. The default is Monday. From the list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Monthly	Schedules the report to generate monthly using the data from the previous month. If you choose the **Monthly** option, further configuration is required. From the list box, select the date you want to generate the report. The default is the first day of the month. Also, use the list box to select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

Step 5 In the Allow this report to generate manually pane, select one of the following options and then click **Next**:

- **Yes** - Enables manual generation of this report.
- **No** - Disables manual generation of this report.

Step 6 Configure the layout of your report:

a From the **Orientation** list box, select the page orientation: Portrait or Landscape. The default is Landscape.

b Select one of the six layout options displayed on the Report Wizard.

c Click **Next** to move to the next page of the Report Wizard.

Step 7 Specify values for the following parameters:

- **Report Title** - Type a report title. The title can be up to 100 characters in length. Do not use special characters.
- **Logo** - From the list box, select a logo. For more information about branding your report, see **Branding reports**.

Step 8 Configure each container in the report:

a From the **Chart Type** list box, select a chart type. See **Chart types**.

b On the Container Details - <chart_type> window, configure the chart parameters. For detailed information about configuring your chart, see **Chart container parameters**.

c Click **Save Container Details**.

The Wizard returns to the Specify Report Contents page, enabling you to configure the other containers in your report.

d If required, repeat steps **a** to **c** for all containers.

e Click **Next** to move to the next page of the Report Wizard.

Step 9 Preview the Layout Preview page, and then click **Next** to move to the next step of the Report Wizard.

Step 10 Select the check boxes for the report formats you want to generate, and then click **Next**.

Options include the following report formats:

- **PDF** - Portable Document Format
- **HTML** - Hyper Text Markup Language format
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (only available for tables)
- **XLS** - Microsoft® Excel format

Step 11 Select the distribution channels for your report, and then click **Next**. Options include the following distribution channels:

Option	**Description**
Report Console	Select this check box to send the generated report to the **Reports** tab. This is the default distribution channel.
Select the users that should be able to view the generated report.	This option is only displayed after you select the **Report Console** check box. From the list of users, select the QRadar SIEM users you want to grant permission to view the generated reports. ***Note:*** *You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the IBM Security QRadar SIEM Administration Guide.*

Option	Description
Select all users	This option is only displayed after you select the **Report Console** check box. Select this check box if you want to grant permission to all QRadar SIEM users to view the generated reports. ***Note:*** *You must have appropriate network permissions to share the generated report with other users. For more information about permissions, see the IBM Security QRadar SIEM Administration Guide.*
Email	Select this check box if you want to distribute the generated report using email.
Enter the report distribution email address(es)	This option is only displayed after you select the **Email** check box. Type the email address for each generated report recipient; separate a list of email addresses with commas. The maximum characters for this parameter is 255. ***Note:*** *Email recipients receive this email from no_reply_reports@qradar.*
Include Report as attachment (non-HTML only)	This option is only displayed after you select the **Email** check box. Select this check box to send the generated report as an attachment.
Include link to Report Console	This option is only displayed after you select the **Email** check box. Select this check box to include a link the Report Console in the email.

Step 12 On the Finishing Up page, enter values for the following parameters:

Parameter	Description
Report Description	Type a description for this report. The description is displayed on the Report Summary page and in the generated report distribution email.
Groups	Select the groups to which you want to assign this report. For more information about groups, see **Report groups**.
Would you like to run the report now?	Select this check box if you want to generate the report when the wizard is complete. By default, the check box is selected.

Step 13 Click **Next** to view the report summary.

Step 14 On the Report Summary page, select the tabs available on the summary report to preview your report configuration.

Step 15 Click **Finish**.

Result

The report immediately generates. If you cleared the **Would you like to run the report now?** check box on the final page of the wizard, the report is saved and generates at the scheduled time.

The report title is the default title for the generated report. If you re-configure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Report management tasks

Using the Reports tab and the Reports Wizard, you can manage your reports. You can edit, duplicate, share, and brand reports. You can also delete generated reports.

Editing a report

Using the Report Wizard, you can edit any default or custom report to change.

About this task

QRadar SIEM provides a significant number of default reports that you can use or customize. The default **Reports** tab displays the list of reports. Each report captures and displays the existing data.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Double-click the report you want to customize.

Step 3 On the Report Wizard, change the parameters to customize the report to generate the content you require. For more information on how to use the Report Wizard, see **Creating custom reports**.

Step 4 Click **Finish**.

Result

If you re-configure a report to enter a new report title, the report is saved as a new report with the new name; however, the original report remains the same.

Viewing generated reports

On the **Reports** tab, an icon is displayed in the **Formats** column if a report has generated content. You can click the icon to view the report.

About this task

When a report has generated content, the **Generated Reports** column displays a list box. The list box displays all generated content, organized by the time-stamp of the report. The most recent reports are displayed at the top of the list. If a report has no generated content, the **None** value is displayed in the **Generated Reports** column.

Icons representing the report format of the generated report are displayed in the **Formats** column. Reports can be generated in the following formats:

- **PDF** - Portable Document Format

- **HTML** - Hyper Text Markup Language format
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language (only available for tables)
- **XLS** - Microsoft® Excel format

The XML and XLS formats are available only for reports that use a single chart table format (portrait or landscape).

You can view only the reports to which you have been given access from the QRadar SIEM administrator. Administrative users can access all reports.

If you use the Mozilla Firefox web browser and you select the RTF report format, the Mozilla Firefox web browser launches a new browser window. This new window launch is the result of the Mozilla Firefox web browser configuration and does not affect QRadar SIEM. You can close the window and continue with your QRadar SIEM session.

Procedure

Step 1 Click the **Reports** tab.

Step 2 From the list box in the **Generated Reports** column, select the time-stamp of report you want to view.

Step 3 Click the icon for the format you want to view.

Result

The report opens in the selected format.

Deleting generated content

When you delete generated content, all reports that have generated from the report template are deleted, but the report template is retained.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the reports for which you want to delete the generated content.

Step 3 From the **Actions** list box, click **Delete Generated Content**.

Result

All generated content for the selected report is deleted.

Manually generating a report

A report can be configured to generate automatically, however, you can manually generate a report at any time.

About this task

While a report generates, the **Next Run Time** column displays one of the three following messages:

- **Generating** - The report is generating.

- **Queued (*position in the queue*)** - The report is queued for generation. The message indicates the position the report is in the queue. For example, 1 of 3.
- **(*x* hour(s) *x* min(s) *y* sec(s))** - The report is scheduled to run. The message is a count-down timer that specifies when the report will run next.

You can select the **Refresh** icon to refresh the view, including the information in the **Next Run Time** column.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to generate.

Step 3 Click **Run Report**.

What to do next

After the report generates, you can view the generated report from the **Generated Reports** column. See **Viewing generated reports**.

Duplicating a report

To create a report that closely resembles an existing report, you can duplicate the report you want to model, and then customize it.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to duplicate.

Step 3 From the **Actions** list box, click **Duplicate**.

Step 4 Type a new name, without spaces, for the report.

Step 5 Click **OK**.

The new report is displayed in the reports list.

What to do next

You can customize the duplicated report. See **Editing a report**.

Sharing a report

You can share reports with other users. When you share a report, you provide a copy of the selected report to another user to edit or schedule.

About this task

Any updates that the user makes to a shared report does not affect the original version of the report.

You must have administrative privileges to share reports. Also, for a new user to view and access reports, an administrative user must share all the necessary reports with the new user.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the reports you want to share.

Step 3 From the **Actions** list box, click **Share**.

Step 4 From the list of users, select the users with whom you want to share this report.

If no users with appropriate access are available, a message is displayed.

Step 5 Click **Share**.

Branding reports

To brand reports, you can import logos and specific images. To brand reports with custom logos, you must upload and configure the logos before you begin using the Report Wizard.

Before you begin

Ensure that the graphic you want to use is 144 x 50 pixels with a white background.

To make sure your browser displays the new logo, clear your browser cache.

About this task

Report branding is beneficial for your enterprise if you support more than one logo. When you upload an image to QRadar SIEM, the image is automatically saved as a Portable Network Graphic (PNG).

When you upload a new image and set the image as your default, the new default image is not applied to reports that have been previously generated. Updating the logo on previously generated reports requires you to manually generate new content from the report.

If you upload an image that is larger in length than the report header can support, the image automatically resizes to fit the header; this is approximately 50 pixels in height.

Procedure

Step 1 Click the **Reports** tab.

Step 2 On the navigation menu, click **Branding**.

Step 3 Click **Browse** to browse the files located on your system.

Step 4 Select the file that contains the logo you want to upload.

Step 5 Click **Open**.

Step 6 Click **Upload Image** to upload the image to QRadar SIEM.

Step 7 Select the logo you want to use as the default and click **Set Default Image**.

Report groups

On the **Reports** tab, you can sort the list of reports into functional groups. If you categorize reports into groups, you can efficiently organize and find reports. For example, you can view all reports related to Payment Card Industry Data Security Standard (PCIDSS) compliance.

By default, the **Reports** tab displays the list of all reports, however, you can categorize reports into groups such as:

- Compliance
- Executive
- Log Sources
- Network Management
- Security
- VoIP
- Other

When you create a new report, you can assign the report to an existing group or create a new group. You must have administrative access to create, edit, or delete groups. For more information about user roles, see the *IBM Security QRadar SIEM Administration Guide*.

Creating a group

QRadar SIEM includes default report groups, however, you can also add groups.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 Using the navigation tree, select the group under which you want to create a new group.

Step 4 Click **New Group**.

Step 5 Enter values for the following parameters:

- **Name** - Type the name for the new group. The name can be up to 255 characters in length.
- **Description** - Type a description for this group. The description can be up to 255 characters in length. This field is optional.

Step 6 Click **OK**.

Step 7 To change the location of the new group, click the new group and drag the folder to the new location on the navigation tree.

Step 8 Close the Report Groups window.

Editing a group

You can edit a report group to change the name or description.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 From the navigation tree, select the group you want to edit.

Step 4 Click **Edit**.

Step 5 Update values for the parameters, as necessary:

- **Name** - Type the name for the new group. The name can be up to 255 characters in length.
- **Description** - Type a description for this group. The description can be up to 255 characters in length. This field is optional.

Step 6 Click **OK**.

Step 7 Close the Report Groups window.

Assigning a report to a group

Using the **Assign Groups** option, you can assign a report to a another group.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Select the report you want to assign to a group.

Step 3 From the **Actions** list box, select **Assign Groups**.

Step 4 From the **Item Groups** list, select the check box of the group you want to assign to this report.

Step 5 Click **Assign Groups**.

Copying a report to another group

Using the **Copy** icon, you can copy a report to one or more report groups.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 From the navigation tree, select the report you want to copy.

Step 4 Click **Copy**.

Step 5 Select the group or groups to which you want to copy the report.

Step 6 Click **Assign Groups**.

Step 7 Close the Report Groups window.

Removing a report from a group

Using the **Remove** icon, you can remove a report from a group.

About this task

When you remove a report from a group, the report still exists on the **Reports** tab. The report is not removed from your system.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Click **Manage Groups**.

Step 3 From the navigation tree, navigate to the folder that contains the report you want to remove.

Step 4 From the list of groups, select the report you want to remove.

Step 5 Click **Remove**.

Step 6 Click **OK**.

Step 7 Close the Report Groups window.

Chart container parameters

The chart type determines how the generated report presents data and network objects. You can chart data with several characteristics and create the charts in a single generated report.

Asset Vulnerabilities chart container parameters

The following table describes the Asset Vulnerabilities chart container parameters:

Table 11-4 Asset Vulnerabilities chart container parameters

Parameter	Description
Container Details - Assets	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Assets to Top	From the list box, select how many assets you want to include in this report.

Table 11-4 Asset Vulnerabilities chart container parameters (continued)

Parameter	Description
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Aggregate Table** - Displays the data in an aggregated table, which is a table that contains sub-tables (sub-reports). When you select this option, you must configure the sub-report details. The **Table** option is only available for the full page width container. • **Bar** - Displays the data in a bar chart. When you select this option, the report does not include sub-report data. This is the default. This graph type requires the saved search to be a grouped search. • **Pie** - Displays the data in a pie chart. When you select this option, the report does not include sub-report data. This graph type requires the saved search to be a grouped search. To view examples of each graph charts data type, see **Graph types**.
Order Assets By	Select the type of data on which you want the chart to be ordered. Options include: • **Asset Weight** - Orders the data by the asset weight defined in the asset profile. • **CVSS Risk** - Orders the data by the Common Vulnerability Scoring System (CVSS) risk level. For more information about CVSS, see *http://www.first.org/cvss/*. • **Vulnerability Count** - Orders the data by the vulnerability count of the assets.
Sub-Report Details	
Sub-report	Specifies the type of information that displays in the sub-report.
Order Sub-report By	Select the parameter by which you want to organize the sub-report data. The options include: • Risk (Base Score) • OSVDB ID • OSVDB Title • Last Modified Date • Disclosure Date • Discovery Date For more information about the Open Source Vulnerability Database (OSVDB), see *http://osvdb.org/*.
Limit Sub-report to Top	From the list box, select how many vulnerabilities you want to include in this sub-report.
Graph Content	

Table 11-4 Asset Vulnerabilities chart container parameters (continued)

Parameter	Description
Vulnerabilities	To specify the vulnerabilities you want to report: **1** Click **Browse**. **2** From the **Search by** list box, select the vulnerability attribute you want to search by. Options include CVE ID, Bugtraq ID, OSVDB ID, and OSVDB Title. For more information about vulnerability attributes, see **Asset management**. **3** From the **Search Results** list, select the vulnerabilities you want to report. Click **Add**. **4** Click **Submit**.
IP Address	Type the IP address, CIDR, or a comma-delimited list of IP addresses you want to report. Partial CIDRs are permitted.
Networks	From the navigation tree, select one or more networks from which to gather chart data.

Event/Logs chart container parameters

The following table describes the Events/Logs chart container parameters:

Table 11-5 Event/Logs chart container parameters

Parameter	Description
Container Details - Events/Logs	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Events/Logs to Top	From the list box, select the number of events/logs to be displayed in the generated report.
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Bar** - Displays the data in a bar chart. This is the default graph type. This graph type requires the saved search to be a grouped search. • **Line** - Displays the data in a line chart. • **Pie** - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search. • **Stacked Bar** - Displays the data in a stacked bar chart. • **Stacked Line** - Displays the data in a stacked line chart. • **Table** - Displays the data in table format. The **Table** option is only available for the full page width container only. To view examples of each graph charts data type, see **Graph types**.

Table 11-5 Event/Logs chart container parameters (continued)

Parameter	Description
Manual Scheduling	The Manual Scheduling pane is displayed only if you selected the **Manually** scheduling option in the Report Wizard. Using the Manual Scheduling options, you can create a manual schedule that can run a report over a custom defined period of time, with the option to only include data from the hours and days that you select. For example, you can schedule a report to run from October 1 to October 31, only including data generated during your business hours, such as Monday to Friday, 8 AM to 9 PM. To create a manual schedule: **1** From the **From** list box, type the start date you want for the report, or select the date using the **Calender** icon. The default is the current date. **2** From the list boxes, select the start time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **3** From the **To** list box, type the end date you want for the report, or select the date using the **Calender** icon. The default is the current date. **4** From the list boxes, select the end time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **5** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.

Table 11-5 Event/Logs chart container parameters (continued)

Parameter	Description
Hourly Scheduling	The Hourly Scheduling pane is displayed only if you selected the **Hourly** scheduling option in the Report Wizard. ▶ From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* Hourly Scheduling automatically graphs all data from the previous hour.
Daily Scheduling	The Daily Scheduling pane is displayed only if you selected the **Daily** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous day (24 hours)** • **Data of previous day from** - From the list boxes, select the period of time you want for the generated report. Time is available in half-hour increments. The default is 1:00 a.m. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.*

Table 11-5 Event/Logs chart container parameters (continued)

Parameter	Description
Weekly Scheduling	The Weekly Scheduling pane is displayed only if you selected the **Weekly** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous week** • **All Data from previous week from** - From the list boxes, select the period of time you want for the generated report. The default is Sunday. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the* ***Timezone*** *parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as* ***GMT -5.00 America/New_York****, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.

Table 11-5 Event/Logs chart container parameters (continued)

Parameter	Description
Monthly Scheduling	The Monthly Scheduling pane is displayed only if you selected the **Monthly** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous month** • **Data from previous month from the** - From the list boxes, select the period of time you want for the generated report. The default is 1st to 31st. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the event search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.
Graph Content	
Group	From the list box, select a saved search group to display the saved searches belonging to that group in the **Available Saved Searches** list box.
Type Saved Search or Select from List	To refine the **Available Saved Searches** list, type the name of the search you want to locate in the **Type Saved Search or Select from List** field. You can also type a keyword to display a list of searches that include that keyword. For example, type `Firewall` to display a list of all searches that include Firewall in the search name.
Available Saved Searches	Provides a list of available saved searches. By default, all available saved searches are displayed, however, you can filter the list by selecting a group from the **Group** list box or typing the name of a known saved search in the **Type Saved Search or Select from List** field.

Table 11-5 Event/Logs chart container parameters (continued)

Parameter	Description
Create New Event Search	Click **Create New Event Search** to create a new search. For more information about how to create an event search, see **Log activity investigation**.

Flows chart container parameters

The following table describes the Flows chart container parameters:

Table 11-6 Flows chart container details

Parameter	Description
Container Details - Flows	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Flows to Top	From the list box, select the number of flows to be displayed in the generated report.
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Bar** - Displays the data in a bar chart. This is the default graph type. This graph type requires the saved search to be a grouped search. • **Line** - Displays the data in a line chart. • **Pie** - Displays the data in a pie chart. This graph type requires the saved search to be a grouped search. • **Stacked Bar** - Displays the data in a stacked bar chart. • **Stacked Line** - Displays the data in a stacked line chart. • **Table** - Displays the data in table format. To view examples of each graph charts data type, see **Graph types**.

Table 11-6 Flows chart container details (continued)

Parameter	Description
Manual Scheduling	The Manual Scheduling pane is displayed only if you selected the **Manually** scheduling option in the Report Wizard. Using the Manual Scheduling options, you can create a manual schedule that can run a report over a custom defined period of time, with the option to only include data from the hours and days that you select. For example, you can schedule a report to run from October 1 to October 31, only including data generated during your business hours, such as Monday to Friday, 8 AM to 9 PM. To create a manual schedule: **1** From the **From** list box, type the start date you want for the report, or select the date using the **Calender** icon. The default is the current date. **2** From the list boxes, select the start time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **3** From the **To** list box, type the end date you want for the report, or select the date using the **Calender** icon. The default is the current date. **4** From the list boxes, select the end time you want for the report. Time is available in half-hour increments. The default is 1:00 a.m. **5** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the* ***Timezone*** *parameter, consider the location of the Event Processors associated with the flow search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as* ***GMT -5.00 America/New_York****, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.

Table 11-6 Flows chart container details (continued)

Parameter	Description
Hourly Scheduling	The Hourly Scheduling pane is displayed only if you selected the **Hourly** scheduling option in the Report Wizard. ▶ From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the* ***Timezone*** *parameter, consider the location of the Event Processors associated with the flow search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as* ***GMT -5.00 America/New_York****, the data from Europe reports the time zone incorrectly.* Hourly Scheduling automatically graphs all data from the previous hour.
Daily Scheduling	The Daily Scheduling pane is displayed only if you selected the **Daily** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous day (24 hours)** • **Data of previous day from** - From the list boxes, select the period of time you want for the generated report. Time is available in half-hour increments. The default is 1:00 a.m. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the* ***Timezone*** *parameter, consider the location of the Event Processors associated with the flow search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as* ***GMT -5.00 America/New_York****, the data from Europe reports the time zone incorrectly.*

Table 11-6 Flows chart container details (continued)

Parameter	Description
Weekly Scheduling	The Weekly Scheduling pane is displayed only if you selected the **Weekly** scheduling option in the Report Wizard. **1** Choose one of the following options: • All data from previous week • **All Data from previous week from** - From the list boxes, select the period of time you want for the generated report. The default is Sunday. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the flow search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.

Table 11-6 Flows chart container details (continued)

Parameter	Description
Monthly Scheduling	The Monthly Scheduling pane is displayed only if you selected the **Monthly** scheduling option in the Report Wizard. **1** Choose one of the following options: • **All data from previous month** • **Data from previous month from the** - From the list boxes, select the period of time you want for the generated report. The default is 1st to 31st. **2** From the **Timezone** list box, select the time zone you want to use for your report. ***Note:*** *When configuring the **Timezone** parameter, consider the location of the Event Processors associated with the flow search used to gather data for some of the reported data. If the report uses data from multiple Event Processors spanning multiple time zones, the configured time zone might be incorrect. For example, if your report is associated to data collected from Event Processors in North America and Europe, and you configure the time zone as **GMT -5.00 America/New_York**, the data from Europe reports the time zone incorrectly.* To further refine your schedule: **1** Select the **Targeted Data Selection** check box. More options are displayed. **2** Select the **Only hours from** check box, and then using the list boxes, select the time range you want for your report. For example, you can select only hours from 8:00 AM to 5:00 PM. **3** Select the check box for each day of the week you want to schedule your report for.
Graph Content	
Group	From the list box, select a saved search group to display the saved searches belonging to that group in the **Available Saved Searches** list box.
Type Saved Search or Select from List	To refine the **Available Saved Searches** list, type the name of the search you want to locate in the **Type Saved Search or Select from List** field. You can also type a keyword to display a list of searches that include that keyword. For example, type **`Firewall`** to display a list of all searches that include Firewall in the search name.
Available Saved Searches	Provides a list of available saved searches. By default, all available saved searches are displayed, however, you can filter the list by selecting a group from the **Group** list box or typing the name of a known saved search in the **Type Saved Search or Select from List** field.

Table 11-6 Flows chart container details (continued)

Parameter	Description
Create New Flow Search	Click **Create New Flow Search** to create a new search. For more information about creating a flow search, see **Network activity investigation**.

Top Source IPs chart container parameters

The following table describes the Top Source IPs chart container parameters:

Table 11-7 Top Source IPs chart container parameters

Parameter	Description
Container Details - Top Source IPs	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Top Source IPs to	From the list box, select the number of source IPs to be displayed in the generated report.
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Table** - Displays the data in table format (with full-width container only). • **Horizontal Bar** - Displays the data in a bar chart.
Order Results By	From the list box, select how the data is sorted on the graph. Options include: • Asset Weight • Risk • Magnitude
Graph Content	
Networks	From the navigation tree, select one or more networks from which to gather chart data.

Top Offenses chart container parameters

The following table describes the Top Offenses chart container parameters:

Table 11-8 Top Offenses chart container parameters

Parameter	Description
Container Details - Top Offenses	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Top Offenses To	From the list box, select the number of offenses to include on the graphs. The default is 10.

Table 11-8 Top Offenses chart container parameters (continued)

Parameter	Description
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Table** - Displays the data in table format (full-width container only). • **Horizontal Bar** -Displays the data in a bar chart.
Order Results By:	From the list box, select how the data is sorted on the graph. Options include: • Severity • Magnitude • Relevance • Credibility
Graph Content - Parameter Based	
Parameter Based	Select this option if you want to include a parameter-based Top Offenses chart in your report. When this option is selected, the **Include**, **Offenses Category**, and **Networks** parameters are displayed.
Include	This option is only displayed if the **Parameter Based** option is selected. Select the check box beside the option you want to include in the generated report. The options are: • Active Offenses • Inactive Offenses • Hidden Offenses • Closed Offenses The **Active Offenses** and **Inactive Offenses** options are selected by default. If you clear all check boxes, no restrictions are applied to the generated report; therefore, the generated report includes all offenses.
Offenses Category	This option is only displayed if the **Parameter Based** option is selected. From the **High Level Category** list box, select the high-level category you want to include in the generated report. From the **Low Level Category** list box, select a low-level category you want to include in the generated report. For more information about high- and low-level categories, see the *IBM Security QRadar SIEM Administration Guide*.
Networks	This option is only displayed if the **Parameter Based** option is selected. From the navigation tree, select one or more networks from which to gather chart data.

Table 11-8 Top Offenses chart container parameters (continued)

Parameter	Description
Graph Content - Saved Search Based	
Saved Search Based	Select this option if you want to include a saved search-based Top Offenses chart in your report. When this option is selected, the **Group, Type Saved Search or Select from List, and Available Saved Searches** parameters are displayed.
Group	From the list box, select a saved search group to display the saved searches belonging to that group in the **Available Saved Searches** list box.
Type Saved Search or Select from List	To refine the **Available Saved Searches** list, type the name of the search you want to locate in the **Type Saved Search or Select from List** field. You can also type a keyword to display a list of searches that include that keyword. For example, type `Firewall` to display a list of all searches that include Firewall in the search name.
Available Saved Searches	Provides a list of available saved searches. By default, all available saved searches are displayed, however, you can filter the list by selecting a group from the **Group** list box or typing the name of a known saved search in the **Type Saved Search or Select from List** field.

Top Destination IPs chart container parameters

The following table describes the Top Destination IPs chart container parameters:

Table 11-9 Top Destination IPs chart container parameters

Parameter	Description
Container Details - Top Destination IPs	
Chart Title	Type a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Type a title to a maximum of 100 characters.
Limit Top Destination IPs to	From the list box, select the number of destination IPs to be displayed in the generated report.
Graph Type	From the list box, select the type of graph to display on the generated report. Options include: • **Table** - Displays the data in table format (full-width container only). • **Horizontal Bar** - Displays the data in a bar chart.
Order Results By	From the list box, select how the data is displayed on the graph. Options include: • Asset Weight • Risk Level • Magnitude

Table 11-9 Top Destination IPs chart container parameters (continued)

Parameter	Description
Graph content	
Networks	From the navigation tree, select one or more networks from which to gather chart data.

A RULE TESTS

You can run tests on the property of an event, flow, or offense, such as source IP address, severity of event, or rate analysis.

Event rule tests

This section provides information on the event rule tests you can apply to the rules, including:

- **Host profile tests**
- **IP/Port tests**
- **Event property tests**
- **Common property tests**
- **Log source tests**
- **Function - Sequence tests**
- **Function - Counter tests**
- **Function - Simple tests**
- **Date/Time tests**
- **Network Property tests**
- **Function - Negative tests**

Host profile tests The host profile tests include:

Table A-1 Event Rule: Host Profile Tests

Test	Description	Default Test Name	Parameters
Host Profile Port	Valid when the port is open on the configured local source or destination. You can also specify if the status of the port is detected using one of the following methods: • **Active** - QRadar SIEM actively searches for the configured port through scanning or vulnerability assessment. • **Passive** - QRadar SIEM passively monitors the network recording hosts previously detected.	when the local **source** host destination port is open **either actively or passively seen**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **actively seen | passively seen | either actively or passively seen** - Specify if you want this test to consider active scanning, passive scanning, or both. The default is either **actively or passively seen**.
Host Existence	Valid when the local source or destination host is known to exist through active or passive scanning. You can also specify if the status of the host is detected using one of the following methods: • **Active** - QRadar SIEM actively searches for the configured host through scanning or vulnerability assessment. • **Passive** - QRadar SIEM passively monitors the network recording hosts previously detected.	when the local **source** host exists **either actively or passively seen**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination host. The default is **source**. • **actively seen | passively seen | either actively or passively seen** - Specify if you want this test to consider active scanning, passive scanning, or both. The default is **either actively or passively seen**.

Table A-1 Event Rule: Host Profile Tests (continued)

Test	Description	Default Test Name	Parameters
Host Profile Age	Valid when the local source or destination host profile age is greater than the configured value within the configured time intervals.	when the local **source** host profile age is **greater than this number of time intervals**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination host. The default is **source**. • **greater than | less than** - Specify if you want this test to consider values greater than or less than the profile host age. • **this number of** - Specify the number of time intervals you want this test to consider. • **time intervals** - Specify whether you want this test to consider minutes or hours.
Host Port Age	Valid when the local source or destination port profile age is greater than or less than a configured amount of time.	when the local **source** host profile port age is **greater than this number of time intervals**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **greater than | less than** - Specify if you want this test to consider values greater than or less than the profile port age. The default is **greater than**. • **this number of** - Specify the number of time intervals you want this test to consider. • **time intervals** - Specify whether you want this test to consider minutes or hours.
Asset Weight	Valid when the specified asset has an assigned weight greater than or less than the configured value.	when the **destination** asset has a weight **greater than this weight**	Configure the following parameters: • **source | destination** - Specify if want this test to consider the source or destination asset. The default is **destination**. • **greater than | less than | equal to** - Specify if you want the value to be greater than, less than, or equal to the configured value. • **this weight** - Specify the weight you want this test to consider.

Table A-1 Event Rule: Host Profile Tests (continued)

Test	Description	Default Test Name	Parameters
Host Vulnerable to Event	Valid when the specified host port is vulnerable to the current event.	when the **destination** is vulnerable to **current** exploit on **any** port	Configure the following parameters: • **destination | source | local host | remote host** - Specify if want this test to consider a destination, source, local host, or remote host. The default is **destination**. • **current | any** - Specify if you want this test to consider the current or any exploit. The default is **current**. • **any | current** - Specify if you want this test to consider any or the current port. The default is **any**.
OSVDB IDs	Valid when an IP address (source, destination, or any) is vulnerable to the configured Open Source Vulnerability Database (OSVDB) IDs.	when the **source IP** is vulnerable to one of the following **OSVDB IDs**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. The default is **source IP**. • **OSVDB IDs** - Specify any OSVDB IDs that you want this test to consider. For more information regarding OSVDB IDs, see *http://osvdb.org/*.

IP/Port tests The IP/Port tests include:

Table A-2 Event Rule: IP / Port Test Group

Test	Description	Default Test Name	Parameters
Source Port	Valid when the source port of the event is one of the configured source ports.	when the source port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Destination Port	Valid when the destination port of the event is one of the configured destination ports.	when the destination port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Local Port	Valid when the local port of the event is one of the configured local ports.	when the local port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Remote Port	Valid when the remote port of the event is one of the configured remote ports.	when the remote port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.

Table A-2 Event Rule: IP / Port Test Group (continued)

Test	Description	Default Test Name	Parameters
Source IP Address	Valid when the source IP address of the event is one of the configured IP addresses.	when the source IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Destination IP Address	Valid when the destination IP address of the event is one of the configured IP addresses.	when the destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Local IP Address	Valid when the local IP address of the event is one of the configured IP addresses.	when the local IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Remote IP Address	Valid when the remote IP address of the event is one of the configured IP addresses.	when the remote IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
IP Address	Valid when the source or destination IP address of the event is one of the configured IP addresses.	when either the source or destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Source or Destination Port	Valid when either the source or destination port is one of the configured ports.	when the source or destination port is any of **these ports**	**these ports** - Specify the ports you want this test to consider.

Event property tests The event property test group includes:

Table A-3 Event Rule: Event Property Tests

Test	Description	Default Test Name	Parameters
Local Network Object	Valid when the event occurs in the specified network.	when the **destination** network is **one of the following networks**	Configure the following parameters: • **source | destination** - Specify if you want this test to consider the source or destination IP address of the event. • **one of the following networks** - Specify the areas of the network you want this test to apply to.
IP Protocol	Valid when the IP protocol of the event is one of the configured protocols.	when the IP protocol is one of the following **protocols**	**protocols** - Specify the protocols you want to add to this test.
Event Payload Search	Each event contains a copy of the original unnormalized event. This test is valid when the entered search string is included anywhere in the event payload.	when the Event Payload contains **this string**	**this string** - Specify the text string you want to include for this test.

Table A-3 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
QID of Event	A QID is a unique identifier for events. This test is valid when the event identifier is a configured QID.	when the event QID is one of the following **QIDs**	**QIDs** - Use one of the following options to locate QIDs: • Select the Browse By Category option and from the list boxes, select the high and low-level category QIDs you want to locate. • Select the QID Search option and enter the QID or name you want to locate. Click **Search**.
Event Context	Event Context is the relationship between the source IP address and destination IP address of the event. For example, a local source IP address to a remote destination IP address. Valid if the event context is one of the following options: • Local to Local • Local to Remote • Remote to Local • Remote to Remote	when the event context is **this context**	**this context** - Specify the context you want this test to consider. The options are: • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Event Category	Valid when the event category is the same as the configured category, for example, Denial of Service (DoS) attack.	when the event category for the event is one of the following **categories**	**categories** - Specify the event category you want this test to consider. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.
Severity	Valid when the event severity is greater than, less than, or equal to the configured value.	when the event severity is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the severity is greater than, less than, or equal to the configured value. • **5** - Specify the index, which is a value from 0 to 10. The default is **5**.
Credibility	Valid when the event credibility is greater than, less than, or equal to the configured value.	when the event credibility is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the credibility is greater than, less than, or equal to the configured value. • **5** - Specify the index, which is a value from 0 to 10. The default is **5**.

Table A-3 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
Relevance	Valid when the event relevance is greater than, less than, or equal to the configured value.	when the event relevance is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the relevance is greater than, less than, or equal to the configured value. • **5** - Specify the index, which is a value from 0 to 10. The default is **5**.
Source Location	Valid when the source IP address of the event is either local or remote.	when the source is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic.
Destination Location	Valid when the destination IP address of the event is either local or remote.	when the destination is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic.
Rate Analysis	QRadar SIEM monitors event rates of all source IP addresses/QIDs and destination IP addresses/QIDs and marks events that exhibit abnormal rate behavior. Valid when the event has been marked for rate analysis.	when the event has been marked with rate analysis	N/A
Geographic Location	Valid when the source IP address matches the configured geographic location.	when the source is located in this **geographic region**	**geographic location** - Select a geographic location.

Table A-3 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
False Positive Tuning	When you tune false positive events on the **Log Activity** tab, the resulting tuning values are displayed in this test. If you want to remove a false positive tuning, you can edit this test to remove the necessary tuning values.	when the false positive signature matches one of the following **signatures**	**signatures** - Specify the false positive signature you want this test to consider. Enter the signature in the following format: <CAT|QID|ANY>:<value>:<source IP>:<dest IP> Where: <CAT|QID|ANY> - Specify whether you want this false positive signature to consider a category (CAT), Q1 Labs Identifier (QID), or any value. <value> - Specify the value for the <CAT|QID|ANY> parameter. For example, if you specified QID, you must specify the QID value. <source IP> - Specify the source IP address you want this false positive signature to consider. <dest IP> - Specify the destination IP address you want this false positive signature to consider.
Regex	Valid when the configured MAC address, user name, host name, or operating system is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.*	when the **username** matches the following **regex**	Configure the following parameters: • **MAC | source MAC | destination MAC | username | source username | destination username | event username | hostname | source hostname | dest hostname | OS | source OS | dest OS | event payload** - Specify the value you want to associate with this test. The default is **username**. • **regex** - Specify the regex string you want this test to consider.

Table A-3 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
IPv6	Valid when the source or destination IPv6 address is the configured IP address.	when the **source IP(v6)** is one of the following **IPv6 addresses**	Configure the following parameters: • **source IP(v6) | destination IP(v6)** - Specify whether you want this test to consider the source or destination IPv6 address. • **IP(v6) addresses** - Specify the IPv6 addresses you want this test to consider.
Reference Set	Valid when any or all configured event properties are contained in any or all configured reference sets.	when **any** of **these event properties** are contained in **any** of **these reference set(s)**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider.
Reference Map	Valid when any or all event properties in a configured key/value pair are contained within any or all configured reference maps.	when **any** of **these event properties** is the key and **any** of **these event properties** is the value in **any** of **these reference maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider. • **these reference maps** - Specify the reference maps you want this test to consider.
Reference Map of Sets	Valid when any or all event properties in a configured key/value pair are contained within any or all configured reference map of sets.	when **any** of **these event properties** is the key and **any** of **these event properties** is the value in **any** of **these reference map of sets**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider. • **these reference map of sets** - Specify the reference map of sets you want this test to consider.

Table A-3 Event Rule: Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
Reference Map of Maps	Valid when any or all event properties in a configured primary and secondary key/value pair are contained within any or all configured reference map of maps.	when **any** of **these event properties** is the key of the first map and **any** of **these event properties** is the key of the second map and **any** of **these properties** is the value in any of **these reference map of maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these event properties** - Specify the event properties you want this test to consider. • **these reference map of maps** - Specify the reference map of maps you want this test to consider.
Search Filter	Valid when the event matches the specified search filter.	when the event matches **this search filter**	**this search filter** - Specify the search filter you want this test to consider.

Common property tests The common property test group includes:

Table A-4 Event Rule: Common Property Tests

Test	Description	Default Test Name	Parameters
CVSS Risk (Host)	Valid when the specified host has a CVSS risk value that matches the configured value.	when the **destination** host has a CVSS risk value of **greater than this amount**	Configure the following parameters: • **source | destination | either** - Specify whether the test considers the source or destination host of the event. • **greater than | less than | equal to** - Specify if you want the CVSS risk value to be greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
CVSS Risk (Port)	Valid when the specified port has a CVSS risk value that matches the configured value.	when the **destination** port has a CVSS risk value of **greater than this amount**	• **source | destination | either** - Specify whether the test considers the source or destination port of the event. • **greater than | less than | equal to** - Specify if you want the threat level to be greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
Custom Rule Engines	Valid when the event is processed by the specified Custom Rule Engines.	when the event is processed by one of **these** Custom Rule Engines	**these** - Specify the Custom Rule Engine you want this test to consider.
Regex	Valid when the configured property is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.*	when any of **these properties** match the following **regex**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom flow and event properties. • **regex** - Specify the regex string you want this test to consider.

Table A-4 Event Rule: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
Hexadecimal	Valid when the configured property is associated with particular hexadecimal values.	when any of **these properties** contain any of **these hexadecimal values**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom flow and event properties. • **these hexadecimal values** - Specify the hexadecimal values you want this test to consider.

Log source tests The log source tests include:

Table A-5 Event Rule: Log Source Tests

Test	Description	Default Test Name	Parameters
Source Log Sources	Valid when one of the configured log sources is the source of the event.	when the event(s) were detected by one or more of **these log sources**	**these log sources** - Specify the log sources that you want this test to detect.
Log Source Type	Valid when one of the configured log source types is the source of the event.	when the event(s) were detected by one or more of **these log source types**	**these log source types** - Specify the log sources that you want this test to detect.
Inactive Log Sources	Valid when one of the configured log sources has not generated an event in the configured time.	when the event(s) have not been detected by one or more of **these log sources** for **this many** seconds	Configure the following parameters: **these log sources** - Specify the log sources that you want this test to detect. **this many** - Specify the number of time intervals you want this test to consider.
Log Source Groups	Valid when an event is detected by the configured log source groups.	when the event(s) were detected by one or more of **these log source groups**	**these log source groups** - Specify the groups you want this rule to consider.

Function - Sequence tests The function - sequence tests include:

Table A-6 Event Rule: Functions - Sequence Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	You can use saved building blocks or other rules to populate this test. This function allows you to detect a specific sequence of selected rules involving a source and destination within a configured time period.	when all of these **rules, in|in any** order, from **the same|any source IP** to **the same|any destination IP,** over **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **username | source IP | source port | destination IP | destination port | QID | event ID | log source | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | username | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks or other rules to populate this test. You can use this function to detect a number of specified rules, in sequence, involving a source and destination within a configured time interval.	when at least **this number** of these **rules, in|in any** order, from **the same|any source IP** to **the same|any destination IP**, over **this many seconds**	Configure the following parameters: • **this number** - Specify the number of rules you want this function to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | username | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider.
Multi-Event Sequence Function Between Hosts	Allows you to detect a sequence of selected rules involving the same source and destination hosts within the configured time interval. You can also use saved building blocks and other rules to populate this test.	when this sequence of **rules**, involving the same source and destination hosts in **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	Allows you to detect a number of specific rules for a specific IP address or port followed by a number of specific rules for a specific port or IP address. You can also use building blocks or existing rules to populate this test.	when at least **this many** of these **rules, in|in any** order, with the same **username** followed by at least **this many** of these **rules in| in any** order **to/from** the same **destination IP** from the previous sequence, within **this many minutes**	Configure the following parameters: • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify if you want this test to consider rules in a specific order. • **username | source IP | source port | destination IP | destination port** - Specify whether you want this test to consider the user name, source IP, source port, destination IP, or destination port. The default is **username**. • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify if you want this test to consider rules in a specific order. • **to | from** - Specify the direction you want this test to consider. • **username | source IP | source port | destination IP | destination port** - Specify whether you want this test to consider the user name, source IP, source port, destination IP, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this rule to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect a number of specific rules with the same event properties and different event properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Event Property Function	Allows you to detect a configured number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties, and different event properties within the configured time interval after a series of specific rules.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Rule Function	Allows you to detect when specific rules occur a configured number of times in a configured time interval and after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties in a configured time interval and after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties and different event properties in a configured time interval after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties and different event properties in a configured time interval after a series of specific rules occur.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties in a configured time interval after a series of specific rules occur with the same event properties.	when at least **this many** events are seen with the same **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-6 Event Rule: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties and different event properties in a configured time interval after a series of specific rules occur with the same event properties.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Function - Counter tests

The function - counter tests include:

Table A-7 Event Rule: Functions - Counters Group

Test	Description	Default Test Name	Parameters
Multi-Event Counter Function	Allows you to test the number of events from configured conditions, such as, source IP address. You can also use building blocks and other rules to populate this test.	when a(n) **source IP** matches **more than|exactly this many** of these **rules** across **more than|exactly this many destination IP,** over **this many minutes**	Configure the following parameters: • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Specify the source you want this test to consider. The default is **source IP**. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of rules. • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source above. • **this many** - Specify the number of IP addresses, ports, QIDs, events, log sources, or categories you want this test to consider. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time value you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-7 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	Allows you to detect a series of rules for a specific IP address or port followed by a series of specific rules for a specific port or IP address. You can also use building blocks or existing rules to populate this test.	when any of these **rules** with the same **source IP** more than **this many** times, across **more than| exactly this many destination IP** within **this many minutes**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **username | source IP | source port | destination IP | destination port | QID | event ID | log sources | category** - Specify the source you want this test to consider. The default is **source IP**. • **this many** - Specify the number of times the configured rules must match the test. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source option. • **this many** - Specify the number you want this test to consider, depending on the option you configured in the source IP parameter. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time interval you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-7 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Username Function	Allows you to detect multiple updates to user names on a single host.	when the **username** changes more than **this many** times within **this many hours** on a single host.	Configure the following parameters: • **MAC | username | hostname** - Specify if you want this test to consider user name, MAC address, or host name. The default is **username**. • **this many** - Specify the number of changes you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **hours**.
Event Property Function	Allows you to detect a series of events with the same event properties within the configured time interval. For example, you can use this test to detect when 100 events with the same source IP address occurs within 5 minutes.	when at least **this many** events are seen with the same **event properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table A-7 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect a series of events with the same event properties and different event properties within the configured time interval. For example, you can use this test to detect when 100 events with the same source IP address and different destination IP address occurs within 5 minutes.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Rule Function	Allows you to detect a number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table A-7 Event Rule: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect a number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Event Property Function	Allows you to detect a number of specific rules with the same event properties and different event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Function - Simple tests

The function - simple tests include:

Table A-8 Event Rule: Functions - Simple Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks and other rules to populate this test. The event has to match either all or any of the selected rules. If you want to create an OR statement for this rule test, specify the **any** parameter.	when an event matches **any|all** of the following **rules**	Configure the following parameters: • **any | all** - Specify either **any** or **all** of the configured rules that should apply to this test. • **rules** - Specify the rules you want this test to consider.

Date/Time tests

The date and time tests include:

Table A-9 Event Rule: Date/Time Tests

Test	Description	Default Test Name	Parameters
Event Day	Valid when the event occurs on the configured day of the month.	when the event(s) occur **on** the **selected** day of the month	Configure the following parameters: • **on | after | before** - Specify if you want this test to consider on, after, or before the configured day. The default is **on**. • **selected** - Specify the day of the month you want this test to consider.
Event Week	Valid when the event occurs on the configured days of the week.	when the event(s) occur on any of **these days of the week**	**these days of the week** - Specify the days of the week you want this test to consider.
Event Time	Valid when the event occurs at, before, or after the configured time.	when the event(s) occur **after this time**	Configure the following parameters: • **after | before | at** - Specify if you want this test to consider after, before, or at the configured time. The default is **after**. • **this time** - Specify the time you want this test to consider.

Network Property tests The network property test group includes:

Table A-10 Event Rule: Network Property Tests

Test	Description	Default Test Name	Parameters
Local Networks	Valid when the event occurs in the specified network.	when the local network is **one of the following networks**	**one of the following networks** - Specify the areas of the network you want this test to apply to.
Remote Networks	Valid when an IP address is part of any or all of the configured remote network locations.	when the **source IP** is a part of any of the following **remote network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. • **remote network locations** - Specify the network locations you want this test to consider.
Remote Services Networks	Valid when an IP address is part of any or all of the configured remote services network locations.	when the **source IP** is a part of any of the following **remote services network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. • **remote services network locations** - Specify the services network locations you want this test to consider.
Geographic Networks	Valid when an IP address is part of any or all of the configured geographic network locations.	when the **Source IP** is a part of any of the following **geographic network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. • **geographic network locations** - Specify the network locations you want this test to consider.

Function - Negative tests

The function - negative tests include:

Table A-11 Event Rule: Functions - Negative Group

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when none of the specified rules in a configured time interval after a series of specific rules occur with the same event properties.	when none of **these rules** match in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.
Rule Function	Allows you to detect when none of the specified rules in a configured time interval after a series of specific rules occur.	when none of **these rules** match in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Flow rule tests

This section provides information on the flow rule tests you can apply to the rules, including:

- **Host Profile tests**
- **IP/Port tests**
- **Flow Property tests**
- **Common Property tests**
- **Function - Sequence tests**
- **Function - Counters tests**

- Function - Simple tests
- Date/Time tests
- Network Property tests
- Function - Negative tests

Host Profile tests The host profile tests include:

Table A-12 Flow Rules: Host Profile Tests

Test	Description	Default Test Name	Parameters
Host Profile Port	Valid when the port is open on the configured local source or destination. You can also specify if the status of the port is detected using one of the following methods: • **Active** - QRadar SIEM actively searches for the configured port through scanning or vulnerability assessment. • **Passive** - QRadar SIEM passively monitors the network recording hosts previously detected.	when the local **source** host destination port is open **either actively or passively seen**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **actively seen | passively seen | either actively or passively seen** - Specify if you want this test to consider active scanning, passive scanning, or both. The default is **either actively or passively seen**.
Host Existence	Valid when the local source or destination host is known to exist through active or passive scanning. You can also specify if the status of the host is detected using one of the following methods: • **Active** - QRadar SIEM actively searches for the configured port through scanning or vulnerability assessment. • **Passive** - QRadar SIEM passively monitors the network recording hosts previously detected.	when the local **source** host exists **either actively or passively seen**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **actively seen | passively seen | either actively or passively seen** - Specify if you want this test to consider active scanning, passive scanning, or both. The default is **either actively or passively seen**.

Table A-12 Flow Rules: Host Profile Tests (continued)

Test	Description	Default Test Name	Parameters
Host Profile Age	Valid when the local source or destination host profile age is greater than the configured value within the configured time intervals.	when the local **source** host profile age is **greater than this number of time intervals**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination host. The default is **source**. • **greater than | less than** - Specify if you want this test to consider values greater than or less than the profile host age. • **this number of** - Specify the number of time intervals you want this test to consider. • **time intervals** - Specify whether you want this test to consider minutes or hours.
Host Port Age	Valid when the local source or destination port profile age is greater than or less than a configured amount of time.	when the local **source** host profile port age is **greater than this number of time intervals**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **greater than | less than** - Specify if you want this test to consider values greater than or less than the profile port age. The default is **greater than**. • **this number of** - Specify the number of time intervals you want this test to consider. • **time intervals** - Specify whether you want this test to consider minutes or hours.
Asset Weight	Valid when the device being attacked (destination) or the host that is the attacker (source) has an assigned weight greater than or less than the configured value.	when the **destination** asset has a weight **greater than this weight**	Configure the following parameters: • **source | destination** - Specify if want this test to consider the source or destination asset. The default is **destination**. • **greater than | less than | equal to** - Specify if you want the value to be greater than, less than, or equal to the configured value. • **this weight** - Specify the weight you want this test to consider.

Table A-12 Flow Rules: Host Profile Tests (continued)

Test	Description	Default Test Name	Parameters
OSVDB IDs	Valid when an IP address (source, destination, or any) is vulnerable to the configured Open Source Vulnerability Database (OSVDB) IDs.	when the **source IP** is vulnerable to one of the following **OSVDB IDs**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. The default is **source IP**. • **OSVDB IDs** - Specify any OSVDB IDs that you want this test to consider. For more information regarding OSVDB IDs, see *http://osvdb.org/*.

IP/Port tests The IP/Port tests include:

Table A-13 Flow Rules: IP / Port Test Group

Test	Description	Default Test Name	Parameters
Source Port	Valid when the source port of the flow is one of the configured source ports.	when the source port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Destination Port	Valid when the destination port of the flow is one of the configured destination ports.	when the destination port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Local Port	Valid when the local port of the flow is one of the configured local ports.	when the local port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Remote Port	Valid when the remote port of the flow is one of the configured remote ports.	when the remote port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Source IP Address	Valid when the source IP address of the flow is one of the configured IP addresses.	when the source IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Destination IP Address	Valid when the destination IP address of the flow is one of the configured IP addresses.	when the destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Local IP Address	Valid when the local IP address of the flow is one of the configured IP addresses.	when the local IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Remote IP Address	Valid when the remote IP address of the flow is one of the configured IP addresses.	when the remote IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.

Table A-13 Flow Rules: IP / Port Test Group (continued)

Test	Description	Default Test Name	Parameters
IP Address	Valid when the source or destination IP address of the flow is one of the configured IP addresses.	when either the source or destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Source or Destination Port	Valid when either the source or destination port is one of the configured ports.	when the source or destination port is any of **these ports**	**these ports** - Specify the ports you want this test to consider.

Flow Property tests The flow property test group includes:

Table A-14 Flow Rules: Flow Property Tests

Test	Description	Default Test Name	Parameters
IP Protocol	Valid when the IP protocol of the flow is one of the configured protocols.	when the IP protocol is one of the following **protocols**	**protocols** - Specify the protocols you want to add to this test.
Flow Context	Flow Context is the relationship between the source IP address and destination IP address of the flow. For example, a local source IP address to a remote destination IP address. Valid if the flow context is one of the following options: • Local to Local • Local to Remote • Remote to Local • Remote to Remote	when the flow context is **this context**	**this context** - Specify the context you want this test to consider. The options are: • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Valid when the source IP address of the flow is either local or remote.	when the source is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic. The default is **remote**.
Destination Location	Valid when the destination IP address of the flow is either local or remote.	when the destination is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic. The default is **remote**.
Geographic Location	Valid when the source IP address matches the configured geographic location.	when the source is located in this **geographic region**	**geographic location** - Select a geographic location.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	Description	Default Test Name	Parameters
Regex	Valid when the configured MAC address, user name, host name, or operating system is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java™ programming language. For more information, you can refer to regex tutorials available on the web.*	when the **username** matches the following **regex**	Configure the following parameters: • **hostname | source hostname |destination hostname | source payload | destination payload** - Specify the value you want to associate with this test. The default is **username**. • **regex** - Specify the regex string you want this test to consider.
IPv6	Valid when the source or destination IPv6 address is the configured IP address.	when the **source IP(v6)** is one of the following **IP(v6) addresses**	Configure the following parameters: • **source IP(v6) | destination IP(v6)** - Specify whether you want this test to consider the source or destination IPv6 address. • **IP(v6) addresses** - Specify the IPv6 addresses you want this test to consider.
Reference Set	Valid when any or all configured flow properties are contained in any or all configured reference sets.	when **any** of **these flow properties** are contained in **any** of **these reference set(s**)	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these flow properties** - Specify the flow properties you want this test to consider. • **any | all** - Specify if you want this test to consider **any** or **all** of the configured reference sets. • **these reference set(s)** - Specify the reference sets you want this test to consider.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	Description	Default Test Name	Parameters
Reference Map	Valid when any or all flow properties in a configured key/value pair are contained within any or all configured reference maps.	when **any** of **these flow properties** is the key and **any** of **these flow properties** is the value in **any** of **these reference maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured flow properties. • **these flow properties** - Specify the flow properties you want this test to consider. • **these reference maps** - Specify the reference maps you want this test to consider.
Reference Map of Sets	Valid when any or all flow properties in a configured key/value pair are contained within any or all configured reference sets.	when **any** of **these flow properties** is the key and **any** of **these flow properties** is the value in **any** of **these reference map of sets**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured flow properties. • **these flow properties** - Specify the flow properties you want this test to consider. • **these reference map of sets** - Specify the reference map of sets you want this test to consider.
Reference Map of Maps	Valid when any or all flow properties in a configured primary and secondary key/value pair are contained within any or all configured reference map of maps.	when **any** of **these flow properties** is the key of the first map and **any** of **these flow properties** is the key of the second map and **any** of **these flow properties** is the value in any of **these reference map of maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured flow properties. • **these flow properties** - Specify the flow properties you want this test to consider. • **these reference map of maps** - Specify the reference map of maps you want this test to consider.
Flow Bias	Valid when flow direction matches the configured flow bias.	when the flow bias is any of the following **bias**	**inbound | outbound | mostly inbound | mostly outbound | balanced** - Specify the flow bias you want this test to consider. The default is **inbound**.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	Description	Default Test Name	Parameters
Byte / Packet Count	Valid when the number of bytes or packets matches the configured amount.	when the **source bytes** is **greater than this amount**	Configure the following parameters: • **source | destination | local | remote** - Specify whether you want this test to consider the source, destination, local or remote bytes or packets. The default is **source**. • **bytes | packets** - Specify whether you want this test to consider bytes or packets. The default is **bytes**. • **greater than | less than | equal to** - Specify whether the number of bytes or packets is greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
Host Count	Valid when the number of hosts matches the configured amount.	When the number of **source** hosts **is greater than this amount**.	Configure the following parameters: • **source | destination | local | remote** - Specify whether you want this test to consider the source, destination, local or remote hosts. The default is **source**. • **greater than | less than | equal to** - Specify whether the number of hosts is greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
Packet Rate	Valid when the packet rate matches the configured amount.	when the **source** packet rate is **greater than value** packets/second	Configure the following parameters: • **source | destination | local | remote** - Specify whether you want this test to consider the source, destination, local or remote packet rate. The default is **source**. • **greater than | less than | equal to** - Specify whether the packet rate is greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	**Description**	**Default Test Name**	**Parameters**
Flow Duration	Valid when the flow duration matches the configured time interval.	when flow duration is **greater than value seconds**	Configure the following parameters: • **greater than | less than | equal to** - Specify whether the flow duration is greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Flow Payload Search	Each flow contains a copy of the original unnormalized event. This test is valid when the entered search string is included anywhere in the flow payload.	when the **source** payload **matches the regex string**	Configure the following parameters: • source | destination | local | remote - Specify whether you want this test to consider the source, destination, local or remote payload. The default is **source**. • matches the regex | matches the hexadecimal - Specify whether you want to match a regex or hexadecimal string. The default is **regex**. • **string** - Specify the text string you want to include for this test.
Flow Source Name	Valid when the flow source name matches the configured values.	when the name of the flow source is one of **these sources**	**these sources** - Specify the flow source names you want this test to consider.
Flow Interface	Valid when the flow interface matches the configured values.	when the flow interface is one of **these interfaces**	**these interfaces** - Specify the flow interface you want this test to consider.
Flow Type	Valid when the flow type matches the configured value.	when the flow type is one of **these flow types**	**these flow types** - Specify the flow type you want this test to consider.
Byte/Packet Ratio	Valid when the byte/packet ratio matches the configured value.	when the **source** byte/packet ratio is **greater than value** bytes/packet	Configure the following parameters: • source | destination | local | remote - Specify whether you want this test to consider the source, destination, local or remote byte/packet ratio. The default is **source**. • **greater than | less than | equal to** - Specify whether the flow duration is greater than, less than, or equal to the configured value. • value - Specify the ratio you want this test to consider.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	Description	Default Test Name	Parameters
ICMP Type	Valid when the Internet Control Message Protocol (ICMP) type matches the configured values.	when the ICMP type is any of **these types**	**these types** - Specify the ICMP types you want this test to consider.
ICMP Code	Valid when the ICMP code matches the configured values.	when the ICMP code is any of **these codes**	**these codes** - Specify the ICMP codes you want this test to consider.
DSCP	Valid when the differentiated services code point (DSCP) matches the configured values.	when the **destination** DSCP is any of **these values**	Configure the following parameters: • source | destination | local | remote | either - Specify whether you want this test to consider the source, destination, local, remote, or either DSCP. The default is **destination**. • **these values** - Specify the DSCP values you want this test to consider.
IP Precedence	Valid when the IP precedence matches the configured values	when the **destination** IP precedence is any of **these values**	Configure the following parameters: • source | destination | local | remote | either - Specify whether you want this test to consider the source, destination, local, remote, or either DSCP. The default is **destination**. • **these values** - Specify the IP precedence values you want this test to consider.
Packet Ratio	Valid when the configured packet ratio matches the configured value. This test allows you to specify the values in the packet ratio.	when the **source**/**destination** packet ratio is **greater than this value**	Configure the following parameters: • source | destination | local | remote - Specify which direction you want this test to consider as the preceding value in the ratio. The default is **source**. • **greater than | less than | equal to** - Specify whether the packet ratio is greater than, less than, or equal to the configured value. • value - Specify the ratio you want this test to consider.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	Description	Default Test Name	Parameters
TCP Flags	Valid when the TCP flags match the configured values.	when the **destination** TCP flags **are exactly these flags**	Configure the following parameters: • source | destination | local | remote - Specify whether you want this test to consider the source, destination, local, or remote, TCP flags. The default is **destination**. • **are exactly | includes all of | includes any of** - Specify whether you want this test to consider exactly, all of, or any of the configured TCP flags. The default is **are exactly**. • **these flags** - Specify the TCP flags you want this test to consider.
IF Index	Valid when the IF Index matches the configured values	when the list of **input** IF (interface) indexes includes **all** of **these values**	Configure the following parameters: • **input | output | either** - Specify which direction you want this test to consider. The default is **input**. • **all | any** - Specify whether you want this test to consider all or any configured IF Index values. • **these values** - Specify the IF Indexes you want this test to consider.
TCP Flag Combination	Valid when the TCP flags match the configured flag combinations.	When the **destination** TCP flags are any of **these flag combinations**	Configure the following parameters: • source | destination | local | remote - Specify whether you want this test to consider the source, destination, local, or remote, TCP flags. The default is **destination**. • **these flag combinations** - Specify the flag combinations you want this test to consider. Separate flags with commas.
Search Filter	Valid when the flow matches the specified search filter.	when the flow matches **this search filter**	**this search filter** - Specify the search filter you want this test to consider.

Table A-14 Flow Rules: Flow Property Tests (continued)

Test	Description	Default Test Name	Parameters
Flow Payload	Valid when the specified side of the flow has or does not have a payload.	when **the destination** side of the flow **has** payload data	Configure the following parameters: • **the source | the destination | the local | the remote | either** - Specify whether you want this test to consider the source, destination, local, remote, or either side of the flow. The default is **destination**. • **has | has not** - Specify whether you want this test to consider flows that have a payload or does not have a payload.

Common Property tests

The date and time tests include:

Table A-15 Flow Rules: Common Property Tests

Test	Description	Default Test Name	Parameters
CVSS Risk (Host)	Valid when the specified host has a CVSS risk value that matches the configured value.	when the **destination** host has a CVSS risk value of **greater than this amount**	Configure the following parameters: • **source | destination | either** - Specify whether the test considers the source or destination host of the flow. • **greater than | less than | equal to** - Specify if you want the CVSS risk value to be greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
CVSS Risk (Port)	Valid when the specified port has a CVSS risk value that matches the configured value.	when the **destination** port has a CVSS risk value of **greater than this amount**	• **source | destination | either** - Specify whether the test considers the source or destination port of the flow. • **greater than | less than | equal to** - Specify if you want the threat level to be greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
Custom Rule Engine	Valid when the flow is processed by the specified custom rule engine.	when the flow is processed by one of **these** Custom Rule Engines	**these** - Specify the Custom Rule Engine ID numbers you want this test to consider.

Table A-15 Flow Rules: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
Regex	Valid when the configured property is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java*^{TM} *programming language. For more information, you can refer to regex tutorials available on the web.*	when **these properties** match the following **regex**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom flow and event properties. • **regex** - Specify the regex string you want this test to consider.
Hexadecimal	Valid when the configured property is associated with particular hexadecimal values.	when any of **these properties** contain any of **these hexadecimal values**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom flow and event properties. • **these hexadecimal values** - Specify the hexadecimal values you want this test to consider.

Function - Sequence tests The function - sequence tests include:

Table A-16 Flow Rules: Functions Sequence Group

Test	Description	Default Test Name	Parameters
Multi-Rule Flow Function	Allows you to use saved building blocks or other rules to populate this test. This function allows you to detect a specific sequence of selected rules involving a source and destination within a configured time period.	when all of these **rules, in|in any** order, from **the same|any source IP** to **the same|any destination IP,** over **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is the **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Flow Function	Allows you to use saved building blocks or other rules to populate this test. You can use this function to detect a number of specified rules, in sequence, involving a source and destination within a configured time interval.	when at least **this number** of these **rules, in|in any** order, **from the same| any source IP** to **the same|any destination IP**, over **this many seconds**	Configure the following parameters: • **this number** - Specify the number of rules you want this function to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider.
Multi-Flow Sequence Function Between Hosts	Allows you to detect a sequence of selected rules involving the same source and destination hosts within the configured time interval. You can also use saved building blocks and other rules to populate this test.	when this sequence of **rules**, involving the same source and destination hosts in **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect a number of specific rules with the same flow properties and different flow properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Flow Property Function	Allows you to detect a configured number of specific rules with the same flow properties within the configured time interval.	when **these rules** match at least **this many** times with the same **flow properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when specific rules occur a configured number of times with the same flow properties and different flow properties within the configured time interval after a series of specific rules.	when **these rules** match at least **this many** times with the same **flow properties** and different **flow properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Rule Function	Allows you to detect when specific rules occur a configured number of times in a configured time interval after a series of specific rules occur with the same flow properties.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match with the same **flow properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when specific rules occur a configured number of times with the same flow properties in a configured time interval after a series of specific rules occur with the same flow properties.	when **these rules** match at least **this many** times with the same **flow properties** in **this many minutes** after **these rules** match with the same **flow properties**	Configure the following parameters: • **these** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these** - Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when specific rules occur a configured number of times with the same flow properties and different flow properties in a configured time interval after a series of specific rules occur with the same flow properties.	when **these rules** match at least **this many** times with the same **flow properties** and different **flow properties** in **this many minutes** after **these rules** match with the same **flow properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when a specific number of flows occur with the same flow properties and different flow properties in a configured time interval after a series of specific rules occur.	when at least **this many** flows are seen with the same **flow properties** and different **flow properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **this many** - Specify the number of flows you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Flow Property Function	Allows you to detect when a specific number of flows occur with the same flow properties in a configured time interval after a series of specific rules occur with the same flow properties.	when at least **this many** flows are seen with the same **flow properties** in **this many minutes** after **these rules** match with the same **flow properties**	Configure the following parameters: • **this many** - Specify the number of flows you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Table A-16 Flow Rules: Functions Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when a specific number of flows occur with the same flow properties and different flow properties in a configured time interval after a series of specific rules occur with the same flow properties.	when at least **this many** flows are seen with the same **flow properties** and different **flow properties** in **this many minutes** after **these rules** match with the same **flow properties**	Configure the following parameters: • **this many** - Specify the number of flows you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules**- Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Function - Counters tests The functions - counters tests include:

Table A-17 Flow Rules: Functions - Counters Group

Test	Description	Default Test Name	Parameters
Multi-Flow Counter Function	Allows you to test the number of flows from configured conditions, such as, source IP address. You can also use building blocks and other rules to populate this test.	when a(n) **source IP** matches **more than|exactly this many** of these **rules** across **more than|exactly this many destination IP,** over **this many minutes**	Configure the following parameters: • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **more than |exactly** - Specify if you want this test to consider more than or exactly the number of rules. • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source above. • **this many** - Specify the number of IP addresses, ports, or user names you want this test to consider. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time value you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-17 Flow Rules: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	Allows you to detect a series of rules for a specific IP address or port followed by a series of specific rules for a specific port or IP address. You can also use building blocks or existing rules to populate this test.	when any of these **rules** with the same **source IP** more than **this many** times, across **more than| exactly this many destination IP** within **this many minutes**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **this many** - Specify the number of times the configured rules must match the test. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source option. • **this many** - Specify the number you want this test to consider, depending on the option you configured in the **source IP** parameter. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time interval you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-17 Flow Rules: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect a series of events with the same flow properties within the configured time interval. For example, you can use this test to detect when 100 flows with the same source IP address occurs within 5 minutes.	when at least **this many** flows are seen with the same **flow properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of flows you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Flow Property Function	Allows you to detect a series of events with the same flow properties and different flow properties within the configured time interval. For example, you can use this test to detect when 100 flows with the same source IP address and different destination IP address occurs within 5 minutes.	when at least **this many** flows are seen with the same **flow properties** and different **flow properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of flows you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table A-17 Flow Rules: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect a number of specific rules with the same flow properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Flow Property Function	Allows you to detect a number of specific rules with the same flow properties within the configured time interval.	when **these rules** match at least **this many** times with the same **flow properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table A-17 Flow Rules: Functions - Counters Group (continued)

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect a number of specific rules with the same flow properties and different flow properties within the configured time interval.	when **these rules** match at least **this many** times with the same **flow properties** and different **flow properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Function - Simple tests

The function - simple tests include:

Table A-18 Flow Rules: Functions - Simple Group

Test	Description	Default Test Name	Parameters
Multi-Rule Flow Function	Allows you to use saved building blocks and other rules to populate this test. The flow has to match either all or any of the selected rules. If you want to create an OR statement for this rule test, specify the **any** parameter.	when a flow matches **any|all** of the following **rules**	Configure the following parameters: • **any | all** - Specify either **any** or **all** of the configured rules that should apply to this test. • **rules** - Specify the rules you want this test to consider.

Date/Time tests The date and time tests include:

Table A-19 Flow Rules: Date/Time Tests

Test	Description	Default Test Name	Parameters
Flow Day	Valid when the flow occurs on the configured day of the month.	when the flow(s) occur **on** the **selected** day of the month	Configure the following parameters: • **on | after | before** - Specify if you want this test to consider on, after, or before the configured day. The default is **on**. • **selected** - Specify the day of the month you want this test to consider.
Flow Week	Valid when the flow occurs on the configured days of the week.	when the flow(s) occur on any of **these days of the week**	**these days of the week** - Specify the days of the week you want this test to consider.
Flow Time	Valid when the flow occurs at, before, or after the configured time.	when the flow(s) occur **after this time**	Configure the following parameters: • **after | before | at** - Specify if you want this test to consider after, before, or at the configured time. The default is **after**. • **this time** - Specify the time you want this test to consider.

Network Property tests The network property test group includes:

Table A-20 Flow Rules: Network Property Tests

Test	Description	Default Test Name	Parameters
Local Network Object	Valid when the flow occurs in the specified network.	when the local network is **one of the following networks**	**one of the following networks** - Specify the areas of the network you want this test to apply to.
Remote Networks	Valid when an IP address is part of any or all of the configured remote network locations.	when the **source IP** is a part of any of the following **remote network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. The default is **source IP**. • **remote network locations** - Specify the network locations you want this test to consider.

Table A-20 Flow Rules: Network Property Tests (continued)

Test	Description	Default Test Name	Parameters
Remote Services Networks	Valid when an IP address is part of any or all of the configured remote services network locations.	when the **source IP** is a part of any of the following **remote services network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. The default is **source IP**. • **remote services network locations** - Specify the services network locations you want this test to consider.
Geographic Networks	Valid when an IP address is part of any or all of the configured geographic network locations.	when the **source IP** is a part of any of the following **geographic network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. The default is **source IP**. • **geographic network locations** - Specify the network locations you want this test to consider.

Function - Negative tests

The function - negative tests include:

Table A-21 Flow Rules: Functions - Negative Group

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when none of the specified rules occur in a configured time interval after a series of specific rules occur with the same flow properties.	when none of **these rules** match in **this many minutes** after **these rules** match with the same **flow properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Table A-21 Flow Rules: Functions - Negative Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect when none of the specified rules occur in a configured time interval after a series of specific rules occur.	when none of **these rules** match in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Common rule tests

This section provides information on the common rule tests you can apply to both event and flow records, including:

- **Host Profile tests**
- **IP/Port tests**
- **Common Property tests**
- **Functions - Sequence tests**
- **Function - Counter tests**
- **Function - Simple tests**
- **Date/Time tests**
- **Network Property tests**
- **Functions Negative tests**

Host Profile tests The host profile tests include:

Table A-22 Common Rule: Host Profile Tests

Test	Description	Default Test Name	Parameters
Host Profile Port	Valid when the port is open on the configured local source or destination. You can also specify if the status of the port is detected using one of the following methods: • **Active** - QRadar SIEM actively searches for the configured port through scanning or vulnerability assessment. • **Passive** - QRadar SIEM passively monitors the network recording hosts previously detected.	when the local **source** host destination port is open **either actively or passively seen**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **actively seen | passively seen | either actively or passively seen** - Specify if you want this test to consider active scanning, passive scanning, or both. The default is **either actively or passively seen**.
Host Existence	Valid when the local source or destination host is known to exist through active or passive scanning. You can also specify if the status of the host is detected using one of the following methods: • **Active** - QRadar SIEM actively searches for the configured port through scanning or vulnerability assessment. • **Passive** - QRadar SIEM passively monitors the network recording hosts previously detected.	when the local **source** host exists **either actively or passively seen**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **actively seen | passively seen | either actively or passively seen** - Specify if you want this test to consider active scanning, passive scanning, or both. The default is **either actively or passively seen**.

Table A-22 Common Rule: Host Profile Tests (continued)

Test	Description	Default Test Name	Parameters
Host Profile Age	Valid when the local source or destination host profile age is greater than the configured value within the configured time intervals.	when the local **source** host profile age is **greater than this number of time intervals**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **greater than | less than** - Specify if you want this test to consider values greater than or less than the profile port age. • **this number of** - Specify the number of time intervals you want this test to consider. • **time intervals** - Specify whether you want this test to consider minutes or hours.
Host Port Age	Valid when the local source or destination host port profile age is greater than or less than a configured amount of time.	when the local **source** host profile port age is **greater than this number of time intervals**	Configure the following parameters: • **source | destination** - Specify if you want this test to apply to the source or destination port. The default is **source**. • **greater than | less than** - Specify if you want this test to consider values greater than or less than the profile port age. The default is **greater than**. • **this number of** - Specify the number of time intervals you want this test to consider. • **time intervals** - Specify whether you want this test to consider minutes or hours.
Asset Weight	Valid when the device being attacked (destination) or the host is that attacker (source) has an assigned weight greater than or less than the configured value.	when the **destination** asset has a weight **greater than this weight**	Configure the following parameters: • **source | destination** - Specify if want this test to consider the source or destination asset. The default is **destination**. • **greater than | less than | equal to** - Specify if you want the value to be greater than, less than, or equal to the configured value. • **this weight** - Specify the weight you want this test to consider.

Table A-22 Common Rule: Host Profile Tests (continued)

Test	Description	Default Test Name	Parameters
OSVDB IDs	Valid when an IP address (source, destination, or any) is vulnerable to the configured Open Source Vulnerability Database (OSVDB) IDs.	when the **source IP** is vulnerable to one of the following **OSVDB IDs**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. The default is **source IP**. • **OSVDB IDs** - Specify any OSVDB IDs that you want this test to consider. For more information regarding OSVDB IDs, see *http://osvdb.org/*.

IP/Port tests The IP/Port tests include:

Table A-23 Common Rule: IP / Port Test Group

Test	Description	Default Test Name	Parameters
Source Port	Valid when the source port of the event or flow is one of the configured source ports.	when the source port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Destination Port	Valid when the destination port of the event or flow is one of the configured destination ports.	when the destination port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Local Port	Valid when the local port of the event or flow is one of the configured local ports.	when the local port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Remote Port	Valid when the remote port of the event or flow is one of the configured remote ports.	when the remote port is one of the following **ports**	**ports** - Specify the ports you want this test to consider.
Source IP Address	Valid when the source IP address of the event or flow is one of the configured IP addresses.	when the source IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Destination IP Address	Valid when the destination IP address of the event or flow is one of the configured IP addresses.	when the destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Local IP Address	Valid when the local IP address of the event or flow is one of the configured IP addresses.	when the local IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.

Table A-23 Common Rule: IP / Port Test Group (continued)

Test	Description	Default Test Name	Parameters
Remote IP Address	Valid when the remote IP address of the event or flow is one of the configured IP addresses.	when the remote IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
IP Address	Valid when the source or destination IP address of the event or flow is one of the configured IP addresses.	when either the source or destination IP is one of the following **IP addresses**	**IP addresses** - Specify the IP addresses you want this test to consider.
Source or Destination Port	Valid when either the source or destination port is one of the configured ports.	when the source or destination port is any of **these ports**	**these ports** - Specify the ports you want this test to consider.

Common Property tests

The common property tests include:

Table A-24 Common Rules: Common Property Tests

Test	Description	Default Test Name	Parameters
IP Protocol	Valid when the IP protocol of the event or flow is one of the configured protocols.	when the IP protocol is one of the following **protocols**	**protocols** - Specify the protocols you want to add to this test.
Payload Search	This test is valid when the entered search string is included anywhere in the event or flow source or destination payload.	when the Flow Source or Destination Payload contains **this string**	**this string** - Specify the text string you want to include for this test.
Context	Context is the relationship between the source and destination of the event or flow. For example, a local source to a remote destination. Valid if the context is one of the following options: • Local to Local • Local to Remote • Remote to Local • Remote to Remote	when the context is **this context**	**this context** - Specify the context you want this test to consider. The options are: • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Valid when the source is either local or remote.	when the source is local or **remote {default: Remote}**	**local | remote** - Specify if you want the source to be local or remote. The default is **remote**
Destination Location	Valid when the destination IP address of the event or flow is either local or remote.	when the destination is **local or remote {default: remote}**	**local | remote** - Specify either local or remote traffic.

Table A-24 Common Rules: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
Geographic Location	Valid when the source IP address matches the configured geographic location.	when the source is located in this **geographic region**	**geographic location** - Select a geographic location.
Regex	Valid when the configured MAC address, user name, host name, or operating system is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.*	when the **username** matches the following **regex**	Configure the following parameters: • **hostname | source hostname |destination hostname | source payload | destination payload** - Specify the value you want to associate with this test. The default is **username**. • **regex** - Specify the regex string you want this test to consider.
IPv6	Valid when the source or destination IPv6 address is the configured IP address.	when the **source IP(v6)** is one of the following **IPv6 addresses**	Configure the following parameters: • **source IP(v6) | destination IP(v6)** - Specify whether you want this test to consider the source or destination IPv6 address. • **IP(v6) addresses** - Specify the IPv6 addresses you want this test to consider.
Reference Set	Valid when any or all configured event or flow properties are contained in any or all configured reference sets.	when **any** of **these properties** are contained in **any** of **these reference set(s)**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured event properties. • **these properties** - Specify the event or flow properties you want this test to consider. • **any | all** - Specify if you want this test to consider **any** or **all** of the configured reference sets. • **these reference set(s)** - Specify the reference sets you want this test to consider.

Table A-24 Common Rules: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
Reference Map	Valid when any or all event or flow properties in a configured key/value pair are contained within any or all configured reference maps.	when **any** of **these properties** is the key and **any** of **these properties** is the value in **any** of **these reference maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured common event and flow properties. • **these properties** - Specify the common event and flow properties you want this test to consider. • **these reference maps** - Specify the reference maps you want this test to consider.
Reference Map of Sets	Valid when any or all event or flow properties in a configured key/value pair are contained within any or all configured reference map of sets.	when **any** of **these properties** is the key and **any** of **these properties** is the value in **any** of **these reference map of sets**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured common event and flow properties. • **these properties** - Specify the common event and flow properties you want this test to consider. • **these reference map of sets** - Specify the reference map of sets you want this test to consider.
Reference Map of Maps	Valid when any or all event or flow properties in a configured primary and secondary key/value pair are contained within any or all configured reference map of maps.	when **any** of **these properties** is the key of the first map and **any** of **these properties** is the key of the second map and **any** of **these properties** is the value in any of **these reference map of maps**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the configured common event and flow properties. • **these properties** - Specify the common event and flow properties you want this test to consider. • **these reference map of maps** - Specify the reference map of maps you want this test to consider.

Table A-24 Common Rules: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
CVSS Risk (Host)	Valid when the specified host has a CVSS risk value that matches the configured value.	when the **destination** host has a CVSS risk value of **greater than this amount**	Configure the following parameters: • **source | destination | either** - Specify whether the test considers the source or destination host of the flow. • **greater than | less than | equal to** - Specify if you want the CVSS risk value to be greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
CVSS Risk (Port)	Valid when the specified port has a CVSS risk value that matches the configured value.	when the **destination** port has a CVSS risk value of **greater than this amount**	• **source | destination | either** - Specify whether the test considers the source or destination port of the flow. • **greater than | less than | equal to** - Specify if you want the threat level to be greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**.
Search Filter	Valid when the event or flow matches the specified search filter.	when the event or flow matches **this search filter**	**this search filter** - Specify the search filter you want this test to consider.
Regex	Valid when the configured property is associated with a particular regular expressions (regex) string. ***Note:*** *This test assumes knowledge of regular expressions (regex). When you define custom regex patterns, adhere to regex rules as defined by the Java^{TM} programming language. For more information, you can refer to regex tutorials available on the web.*	when **these properties** match the following **regex**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom flow and event properties. • **regex** - Specify the regex string you want this test to consider.
Custom Rule Engines	Valid when the event or flow is processed by the specified Custom Rule Engines.	when the event or flow is processed by one of **these** Custom Rule Engines	**these** - Specify the Custom Rule Engine you want this test to consider.

Table A-24 Common Rules: Common Property Tests (continued)

Test	Description	Default Test Name	Parameters
Hexadecimal	Valid when the configured property is associated with particular hexadecimal values.	when any of **these properties** contain any of **these hexadecimal values**	Configure the following parameters: • **these properties** - Specify the value you want to associate with this test. Options include all normalized, and custom flow and event properties. • **these hexadecimal values** - Specify the hexadecimal values you want this test to consider.

Functions - Sequence tests The functions - sequence tests include:

Table A-25 Common: Functions - Sequence Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks or other rules to populate this test. This function allows you to detect a specific sequence of selected rules involving a source and destination within a configured time period.	when all of these **rules, in|in any** order, from **the same|any source IP** to **the same|any destination IP,** over **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks or other rules to populate this test. You can use this function to detect a number of specified rules, in sequence, involving a source and destination within a configured time interval.	when at least **this number** of these **rules, in|in any** order, **from the same| any source IP** to **the same|any destination IP**, over **this many seconds**	Configure the following parameters: • **this number** - Specify the number of rules you want this function to consider. • **rules** - Specify the rules you want this test to consider. • **in | in any** - Specify whether you want this test to consider **in** or **in any** order. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured sources. • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **the same | any** - Specify if you want this test to consider the **same** or **any** of the configured destinations. • **destination IP | destination port** - Specify whether you want this test to consider a destination IP address, user name, or destination port. The default is **destination IP**. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.
Multi-Event Sequence Function Between Hosts	Allows you to detect a sequence of selected rules involving the same source and destination hosts within the configured time interval. You can also use saved building blocks and other rules to populate this test.	when this sequence of **rules**, involving the same source and destination hosts in **this many seconds**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **seconds**.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect a number of specific rules with the same event properties and different event properties within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Event Property Function	Allows you to detect a configured number of specific rules with the same event properties occur within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties and different event properties occur within the configured time interval after a series of specific rules.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Select the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Rule Function	Allows you to detect when specific rules occur a configured number of times in a configured time interval after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties in a configured time interval after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when specific rules occur a configured number of times with the same event properties and different event properties in a configured time interval after a series of specific rules occur with the same event properties.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties and different event properties in a configured time interval after a series of specific rules occur.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties in a configured time interval after a series of specific rules occur with the same event properties.	when at least **this many** events are seen with the same **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Table A-25 Common: Functions - Sequence Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect when a specific number of events occur with the same event properties and different event properties in a configured time interval after a series of specific rules occur with the same event properties.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes** after **these rules** match with the same **event properties**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties.

Function - Counter tests The function - counter tests include:

Table A-26 Common Rules: Functions - Counter Test Group

Test	Description	Default Test Name	Parameters
Multi-Event Counter Function	Allows you to test the number of events or flows from configured conditions, such as, source IP address. You can also use building blocks and other rules to populate this test.	when a(n) **source IP** matches **more than|exactly this many** of these **rules** across **more than|exactly this many destination IP,** over **this many minutes**	Configure the following parameters: • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of rules. • **this many** - Specify the number of rules you want this test to consider. • **rules** - Specify the rules you want this test to consider. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source above. • **this many** - Specify the number of IP addresses, ports, QIDs, events, log sources, or categories you want this test to consider. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time value you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-26 Common Rules: Functions - Counter Test Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	Allows you to detect a series of rules for a specific IP address or port followed by a series of specific rules for a specific port or IP address. You can also use building blocks or existing rules to populate this test.	when any of these **rules** with the same **source IP** more than **this many** times, across **more than| exactly this many destination IP** within **this many minutes**	Configure the following parameters: • **rules** - Specify the rules you want this test to consider. • **source IP | source port | destination IP | destination port | QID | category** - Specify the source you want this test to consider. The default is **source IP**. • **this many** - Specify the number of times the configured rules must match the test. • **more than | exactly** - Specify if you want this test to consider more than or exactly the number of destination IP addresses, destination ports, QIDs, log source event IDs, or log sources that you selected in the source option. • **this many** - Specify the number you want this test to consider, depending on the option you configured in the **source IP** parameter. • **username | destination IP | source IP | source port | destination port | QID | event ID | log sources | category** - Specify the destination you want this test to consider. The default is **destination IP**. • **this many** - Specify the time interval you want to assign to this test. • **seconds | minutes | hours | days** - Specify the time interval you want this rule to consider. The default is **minutes**.

Table A-26 Common Rules: Functions - Counter Test Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect a series of events with the same event properties within the configured time interval. For example, you can use this test to detect when 100 events with the same source IP address occurs within 5 minutes.	when at least **this many** events are seen with the same **event properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Event Property Function	Allows you to detect a series of events with the same event properties and different event properties within the configured time interval. For example, you can use this test to detect when 100 events with the same source IP address and different destination IP address occurs within 5 minutes.	when at least **this many** events are seen with the same **event properties** and different **event properties** in **this many minutes**	Configure the following parameters: • **this many** - Specify the number of events you want this test to consider. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table A-26 Common Rules: Functions - Counter Test Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect when a number of specific rules with the same event properties occur within the configured time interval.	when **these rules** match at least **this many** times in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.
Event Property Function	Allows you to detect a number of specific rules with the same event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Table A-26 Common Rules: Functions - Counter Test Group (continued)

Test	Description	Default Test Name	Parameters
Event Property Function	Allows you to detect a number of specific rules with the same event properties and different event properties within the configured time interval.	when **these rules** match at least **this many** times with the same **event properties** and different **event properties** in **this many minutes**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of times the configured rules must match the test. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **event properties** - Specify the event properties you want this test to consider. Options include all normalized and custom event properties. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**.

Function - Simple tests

The function - simple tests include:

Table A-27 Common Rules: Functions - Simple Test Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks and other rules to populate this test. The event has to match either all or any of the selected rules. If you want to create an OR statement for this rule test, specify the **any** parameter.	when a flow or an event matches **any|all** of the following **rules**	Configure the following parameters: • **any | all** - Specify either **any** or **all** of the configured rules that should apply to this test. • **rules** - Specify the rules you want this test to consider.

Date/Time tests The date and time tests include:

Table A-28 Common Rule: Date/Time Tests

Test	Description	Default Test Name	Parameters
Event/Flow Day	Valid when the event or flow occurs on the configured day of the month.	when the flow(s) or event(s) occur **on** the **selected** day of the month	Configure the following parameters: • **on | after | before** - Specify if you want this test to consider on, after, or before the configured day. The default is **on**. • **selected** - Specify the day of the month you want this test to consider.
Event/Flow Week	Valid when the event or flow occurs on the configured days of the week.	when the flow(s) or event(s) occur on any of **these days of the week**	**these days of the week** - Specify the days of the week you want this test to consider.
Event/Flow Time	Valid when the event or flow occurs at, before, or after the configured time.	when the flow(s) or event(s) occur **after this time**	Configure the following parameters: • **after | before | at** - Specify if you want this test to consider after, before, or at the configured time. The default is **after**. • **this time** - Specify the time you want this test to consider.

Network Property tests The network property test group includes:

Table A-29 Common Rule: Network Property Tests

Test	Description	Default Test Name	Parameters
Local Network Object	Valid when the event occurs in the specified network.	when the local network is **one of the following networks**	**one of the following networks** - Specify the areas of the network you want this test to apply to.
Remote Networks	Valid when an IP address is part of any or all of the configured remote network locations.	when the **source IP** is part of any of the following **remote network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. • **remote network locations** - Specify the network locations you want this test to consider.

Table A-29 Common Rule: Network Property Tests (continued)

Test	Description	Default Test Name	Parameters
Remote Services Networks	Valid when an IP address is part of any or all of the configured remote services network locations.	when the **source IP** is a part of any of the following **remote services network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. • **remote services network locations** - Specify the remote services network locations you want this test to consider.
Geographic Networks	Valid when an IP address is part of any or all of the configured geographic network locations.	when the **Source IP** is a part of any of the following **geographic network locations**	Configure the following parameters: • **source IP | destination IP | any IP** - Specify if you want this test to consider the source IP address, destination IP address, or any IP address. • **geographic network locations** - Specify the geographic network locations you want this test to consider.

Functions Negative tests

The functions negative tests include:

Table A-30 Common Rules: Functions - Negative Test Group

Test	Description	Default Test Name	Parameters
Flow Property Function	Allows you to detect when none of the specified rules occur in a configured time interval after a series of specific rules occur with the same flow properties.	when none of **these rules** match in **this many minutes** after **these** match with the same **flow properties**	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these** - Specify the rules you want this test to consider. • **flow properties** - Specify the flow properties you want this test to consider. Options include all normalized and custom flow properties.

Table A-30 Common Rules: Functions - Negative Test Group (continued)

Test	Description	Default Test Name	Parameters
Rule Function	Allows you to detect when none of the specified rules occur in a configured time interval after a series of specific rules occur.	when none of **these rules** match in **this many minutes** after **these rules** match	Configure the following parameters: • **these rules** - Specify the rules you want this test to consider. • **this many** - Specify the number of time intervals you want this test to consider. • **seconds | minutes | hours | days** - Specify the time interval you want this test to consider. The default is **minutes**. • **these rules** - Specify the rules you want this test to consider.

Offense rule tests

This section provides information on the tests you can apply to the offense rules, including:

- **IP/Port tests**
- **Function tests**
- **Date/Time tests**
- **Log source tests**
- **Offense Property tests**

IP/Port tests

The IP/Port tests include:

Table A-31 Offense Rules: IP/Port Test Group

Test	Description	Default Test Name	Parameters
Offense Index	Valid when the source IP address is one of the configured IP addresses.	when the offense is indexed by one of the following **IP addresses**.	**IP addresses** - Specify the IP addresses you want this test to consider. You can enter multiple entries using a comma-separated list.
Destination IP Address	Valid when the destination list is any of the configured IP addresses.	when the destination list includes **any** of the following **IP addresses**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** of the listed destinations. The default is **any**. • **IP addresses** - Specify the IP addresses you want this test to consider. You can enter multiple entries using a comma-separated list.

Function tests The function tests include:

Table A-32 Offense Rules: Offense Function Group

Test	Description	Default Test Name	Parameters
Multi-Rule Offense Function	Allows you to use saved building blocks and other rules to populate this test. The offense has to match either all or any of the selected rules. If you want to create an OR statement for this rule test, specify the **any** parameter.	when the offense matches **any** of the following **offense rules**.	Configure the following parameters: • **any | all** - Specify either **any** or **all** of the configured rules that should apply to this test. The default is **any**. • **offense rules** - Specify the rules you want this test to consider.

Date/Time tests The date and time tests include:

Table A-33 Offense Rules: Date/Time Tests

Test	Description	Default Test Name	Parameters
Offense Day	Valid when the offense occurs on the configured day of the month.	when the offense(s) occur **on** the **selected** day of the month	Configure the following parameters: • **on | after | before** - Specify if you want this rule to consider on, after, or before the selected date. The default is **on**. • **selected** - Specify the date you want this test to consider.
Offense Week	Valid when the offense occurs on the configured day of the week.	when the offense(s) occur **on these days of the week**	Configure the following parameters: • **on | after | before** - Specify if you want this rule to consider on, after, or before the selected day. The default is **on**. • **these days of the week** - Specify the days you want this test to consider.
Offense Time	Valid when the offense occurs after, before, or on the configured time.	when the offense(s) occur **after this time**	Configure the following parameters: • **on | after | before** - Specify if you want this test to consider after, before, or at a specified time. The default is **after**. • **this time** - Specify the time you want this test to consider.

Log Source tests

The log source tests include:

Table A-34 Offense Rules: Log Source Tests

Test	Description	Default Test Name	Parameters
Log Source Types	Valid when one of the configured log source types is the source of the offense.	when the log source type(s) that detected the offense is one of the following **log source types**	**log source types** - Specify the log source types that you want this test to detect.
Number of Log Source Type	Valid when the number of log source types is greater than the configured value.	when the number of log source types that detected the offense is **greater than this number**	Configure the following parameters: • **greater than | equal to** - Specify if you want the threat level to be greater than or equal to the configured value. • **this number** - Specify the number of log source types that you want this test to consider.

Offense Property tests

The offense property tests include:

Table A-35 Offense Rules: Offense Property Tests

Test	Description	Default Test Name	Parameters
Network Object	Valid when the network is affected by any or all of the configured networks.	when the networks affected are **any** of **the following networks**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** networks. The default is **any**. • **the following networks** - Specify the networks you want this test to consider.
Offense Category	Valid when the event category is any or all of the configured event categories.	when the categories of the offense includes **any** of the following **list of categories**	Configure the following parameters: • **any | all** - Specify if you want this test to consider **any** or **all** categories. The default is **any**. • **list of categories** - Specify the categories you want this test to consider. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.

Table A-35 Offense Rules: Offense Property Tests (continued)

Test	Description	Default Test Name	Parameters
Severity	Valid when the severity is greater than, less than, or equal to the configured value.	when the offense severity is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify if you want the offense severity to be greater than, less than, or equal to the configured value. • **5** - Specify the value you want this test to consider. The default is **5**.
Credibility	Valid when the credibility is greater than, less than, or equal to the configured value.	when the offense credibility is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify if you want the offense credibility to be greater than, less than, or equal to the configured value. • **5** - Specify the value you want this test to consider.
Relevance	Valid when the relevance is greater than, less than, or equal to the configured value.	when the offense relevance is **greater than 5 {default}**	Configure the following parameters: • **greater than | less than | equal to** - Specify if you want the offense relevance to be greater than, less than, or equal to the configured value. • **5** - Specify the value you want this test to consider.
Offense Context	Offense Context is the relationship between the source and destination of the offense. For example, a local attacker to a remote target. Valid if the offense context is one of the following options: • Local to Local • Local to Remote • Remote to Local • Remote to Remote	when the offense context is **this context**	**this context** - Specify the context you want this test to consider. The options are: • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Source Location	Valid when the source is either local or remote.	when the source is local or **local or remote {default: Remote}**	**local | remote** - Specify if you want the source to be local or remote. The default is **remote**.
Destination Location	Valid when the destination is either local or remote.	when the destination list includes **local or remote IP addresses {default: remote}**	**locate IPs | remote IPs** - Specify if you want the target to be local or remote. The default is **remote IPs**.

Table A-35 Offense Rules: Offense Property Tests (continued)

Test	Description	Default Test Name	Parameters
Destination Count in an Offense	Valid when the number of destinations for an offense is greater than, less than, or equal to the configured value.	when the number of destinations under attack is **greater than this number**	Configure the following parameters: • **greater than | equal to** - Specify if you want the number of destinations to be greater than or equal to the configured value. • **this number** - Specify the value you want this test to consider.
Event Count in an Offense	Valid when the number of events for an offense is greater than, less than, or equal to the configured value.	when the number of events making up the offense is **greater than this number**	Configure the following parameters: • **greater than | less than | equal to** - Specify if you want the event count to be greater than, less than, or equal to the configured value. • **this number** - Specify the value you want this test to consider.
Flow Count in an Offense	Valid when the number of flows for an offense is greater than, less than, or equal to the configured value.	when the number of flows making up the offense is **greater than this number**	Configure the following parameters: • **greater than | less than | equal to** - Specify if you want the flow count to be greater than, less than, or equal to the configured value. • **this number** - Specify the value you want this test to consider.
Total Event/Flow Count in an Offense	Valid when the total number of events and flows for an offense is greater than, less than, or equal to the configured value.	when the number of events and flows making up the offense is **greater than this number**	Configure the following parameters: • **greater than | less than | equal to** - Specify if you want the event and flow count to be greater than, less than, or equal to the configured value. • **this number** - Specify the value you want this test to consider.
Category Count in an Offense	Valid when the number of event categories for an offense is greater than, less than, or equal to the configured value.	when the number of categories involved in the offense is **greater than this number**	Configure the following parameters: • **greater than | equal to** - Specify if you want the number of categories to be greater than or equal to the configured value. • **this number** - Specify the value you want this test to consider. For more information about event categories, see the *IBM Security QRadar SIEM Administration Guide*.
Offense ID	Valid when the Offense ID is the configured value.	when the offense ID is **this ID**	**this ID** - Specify the offense ID you want this test to consider.

Table A-35 Offense Rules: Offense Property Tests (continued)

Test	Description	Default Test Name	Parameters
Offense Creation	Valid when a new offense is created.	when a new offense is created	
Offense Change	Valid when the configured offense property has increased above the configured value.	when the offense **property** has increased by at least **this percent**	Configure the following parameters: • **Magnitude | Severity | Credibility | Relevance| Destination count | Source count | Category count | Annotation count | Event count** - Specify the property you want this test to consider.The default is **Magnitude**. • **this** - Specify the percent or unit value you want this test to consider. • **percent | unit(s)** - Specify if you want this test to consider percentage or units.

Anomaly detection rule tests

This section provides information on the tests you can apply to the anomaly detection rules, including:

- **Anomaly rule tests**
- **Behavioral rule tests**
- **Threshold rule tests**

Anomaly rule tests

This section provides information on the anomaly rule tests you can apply to the rules, including:

- **Anomaly tests**
- **Time threshold tests**

Anomaly tests

The anomaly test group includes:

Table A-36 Anomaly Rules: Anomaly Tests

Test	Description	Default Test Name	Parameters
Anomaly	Valid when the accumulated property has increased or decreased by the specified percentage over a short period of time when compared against the specified larger period time. For example, if your average destination bytes for the last 24 hours is 100,000,000 bytes out for each minute and then over a 5 minute period, the average bytes out increases by 40%, this test is valid. ***Note:*** *The Accumulator sends data to the Anomaly Detection Rule engine in one minute intervals. For more information about the accumulator, see the IBM Security QRadar SIEM Administration Guide.*	when the average value (per interval) of **this accumulated property** over the last **1 min** is at least **percentage**% different from the average value (per interval of the same property over the last **1 min**	Configure the following parameters: • **this accumulated property** - Specify the accumulated property you want this test to consider. • **1 min** - Specify the time interval you want this test to consider. The default is **1 min**. • **40** - Specify the percentage you want this test to consider. The default is **40**. • **1 min** - Specify the time interval this tests used to compare the interval length. The default is **1 min.**
Minimum Value	Valid when the tested value for the accumulated interval exceeds the configured value.	when accumulation intervals are only considered if the tested value for that interval exceeds **some value**	**some value** - Specify the value you want to consider for the configured accumulation interval.

Time threshold tests

The time threshold test group includes:

Table A-37 Anomaly Rules: Time Threshold Tests

Test	Description	Default Test Name	Parameters
Date Range	Valid when anomalous activity is detected within the specified date range.	when the date is between **this date** and **this date**	Configure the following parameters: • **this date** - Specify the start date for your date range. • **this date** - Specify the end date for your date range.
Day of the Week	Valid when anomalous activity is detected on the specified day of the week.	when the day of the week is any of **these selected days**	**these selected days** - Specify the days you want this test to consider.

Table A-37 Anomaly Rules: Time Threshold Tests (continued)

Test	Description	Default Test Name	Parameters
Time Range	Valid when anomalous activity is detected within the specified time range.	when the time of day is between **this time** and **this time**	Configure the following parameters: • **this time** - Specify the start time for your date range. • **this time** - Specify the end date for your date range.

Behavioral rule tests

This section provides information on the behavioral rule tests you can apply to the rules, including:

- **Behavioral tests**
- **Time threshold tests**

Behavioral tests

The behavioral test group includes:

Table A-38 Behavioral Rules: Behavioral Tests

Test	Description	Default Test Name	Parameters
Accumulated Property	Specifies which accumulated property this rule considers.	when **this accumulated property** is the tested property	**this accumulated property** - Specify the accumulated property you want this test to consider.
Current Traffic Level	Valid when the current traffic level represents specified seasonal change in data over the time period specified in the Season Length test. For example, the current traffic level test can compare current data with data from the same time period yesterday.	when the importance of the current traffic level (on a scale of 0 to 100) is **importance** compared to learned traffic trends and behavior	**70** - Specify the level of importance, on a scale of 0 to 100, you want this test to consider. The default is **70**.
Current Traffic Trend	Valid when the current traffic trend represents the specified seasonal effect in data for each time interval. For example, the current traffic trend test can test for when data increases the same amount from week 2 to week 3 as it did from week 1 to week 2.	when the importance of the current traffic trend (on a scale of 0 to 100) is **importance** compared to learned traffic trends and behavior	**30** - Specify the level of importance, on a scale of 0 to 100, you want this test to consider. The default is **30**.

Table A-38 Behavioral Rules: Behavioral Tests (continued)

Test	Description	Default Test Name	Parameters
Current Traffic Behavior	Valid when the current traffic behavior changes in data for each time interval. For example, the current traffic behavior test can test for data changes when comparing this minute to the minute before.	when the importance of the current traffic behavior (on a scale of 0 to 100) is **importance** compared to learned traffic trends and behavior	**30** - Specify the level of importance, on a scale of 0 to 100, you want this test to consider. The default is **30**.
Deviation	Valid when accumulated property deviates from the predicted traffic pattern.	when the actual field value deviates by a margin of at least **deviation**% of the extrapolated (predicted field value).	**50** - Specify the percentage of deviation you want this test to consider. The default is **50**.
Season Length	Valid when the season length represents the time interval you want to test. Typically, for network traffic, you can set the season length as a week. When monitoring traffic from automated systems, set the season length as day.	when the season length is **season**	**a day | a week | a month** - Specify the season length you want this test to consider.
Minimum Value	Valid when the tested value for the accumulated interval exceeds the configured value.	when accumulation intervals are only considered if the tested value for that interval exceeds **0**	**0** - Specify the value you want to consider for the configured accumulation interval.

Time threshold tests

The time threshold test group includes:

Table A-39 Behavioral Rules: Time Threshold Tests

Test	Description	Default Test Name	Parameters
Date Range	Valid when anomalous activity is detected within the specified date range.	when the date is between **this date** and **this date**	Configure the following parameters: • **this date** - Specify the start date for your date range. • **this date** - Specify the end date for your date range.
Day of the Week	Valid when anomalous activity is detected on the specified day of the week.	when the day of the week is any of **these selected days**	**these selected days** - Specify the days you want this test to consider.
Time Range	Valid when anomalous activity is detected within the specified time range.	when the time of day is between **this time** and **this time**	Configure the following parameters: • **this time** - Specify the start time for your date range. • **this time** - Specify the end date for your date range.

This section provides information on the threshold rule tests you can apply to the rules, including:

- Field threshold tests
- Time threshold tests

Field threshold tests

The field threshold test group includes:

Table A-40 Threshold Rules: Field Threshold Tests

Test	Description	Default Test Name	Parameters
Threshold Value	Valid when the accumulated property is greater than, less than, or equal to specified value. You can specify the interval, in minutes, you want to accumulate the property.	when **this accumulated property** is **greater than this value** (accumulated in **1 min** intervals)	• **this accumulated property** - Specify the accumulated property you want this test to consider. • **greater than | less than | equal to** - Specify whether the accumulate property value is greater than, less than, or equal to the configured value. • **0** - Specify the value you want this test to consider. The default is **0**. • **1 min** - Specify the interval, in minutes, you want to accumulate the property. The default is **1 min**.
Threshold Range	Valid when the accumulated property is within a specified range. You can specify the interval, in minutes, you want to accumulate the property.	when **this accumulated property** is between **this value** and **this value** (accumulated in **1 min** intervals)	• **this accumulated property** - Specify the accumulated property you want this test to consider. • **0** - Specify the value you want this test to consider as the start of the range. The default is **0**. • **0** - Specify the value you want this test to consider as the end of the range. The default is **0**. • **1 min** - Specify the interval, in minutes, you want to accumulate the property. The default is **1 min**.

Time threshold tests

The time threshold test group includes:

Table A-41 Threshold Rules: Time Threshold Tests

Test	Description	Default Test Name	Parameters
Date Range	Valid when anomalous activity is detected within the specified date range.	when the date is between **this date** and **this date**	Configure the following parameters: • **this date** - Specify the start date for your date range. • **this date** - Specify the end date for your date range.

Table A-41 Threshold Rules: Time Threshold Tests (continued)

Test	Description	Default Test Name	Parameters
Day of the Week	Valid when anomalous activity is detected on the specified day of the week.	when the day of the week is any of **these selected days**	**these selected days** - Specify the days you want this test to consider.
Time Range	Valid when anomalous activity is detected within the specified time range.	when the time of day is between **this time** and **this time**	Configure the following parameters: • **this time** - Specify the start time for your date range. • **this time** - Specify the end date for your date range.

B Glossary

active system In a High Availability (HA) cluster, the active system is the system with all services running. Either the primary or secondary HA host can be the active host. If the secondary HA host is the active host, failover has occurred.

accumulator The accumulator resides on the host that contains an Event Processor to assist with analyzing flows, events, reporting, writing database data, and alerting a DSM.

Address Resolution Protocol (ARP) A protocol for mapping an Internet Protocol (IP) address to a physical host address recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet LAN, however, addresses for attached devices are 48 bits long.

anomaly A deviation from expected behavior of the network.

application signature A unique set of characteristics or properties, derived by the examination of packet payload, used to identify a specific application.

ARP See Address Resolution Protocol.

ARP Redirect ARP allows a host to determine the address of other devices on the LAN or VLAN. A host can use ARP to identify the default gateway (router) or path off to the VLAN. ARP Redirect allows QRadar SIEM to notify a host if a problem exists with sending traffic to a system. This renders the host and network unusable until the user intervenes.

ASN See Autonomous System Number.

Autonomous System Number An autonomous system is a collection of IP networks that all adhere to the same specific and clearly defined routing policy. An Autonomous System Number (ASN) is a unique ID number assigned to each autonomous system.

behavior Indicates the normal manner in which the system or network functions or operates.

branding A reporting option that enables a QRadar SIEM user to upload custom logos for customized reports.

CIDR See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)

Addressing scheme for the Internet, which allocates and species Internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.

client

The host that originates communication.

Cluster Virtual IP address

The Cluster Virtual IP address is the IP address used to communicate with an HA cluster. When you configure HA, the IP address of the primary HA host becomes the Cluster Virtual IP address. If the primary HA host fails, the Cluster Virtual IP address will be assumed by the secondary HA host.

coalescing interval

The interval for coalescing (bundling) events is 10 seconds, beginning with the first event that does not match any currently coalescing events. Within the interval, the first three matching events are released immediately to the Event Processor and the fourth and subsequent events are coalesced such that the payload and other features are kept from the fourth event. Each arrival of a matching event during the interval increments the event count of the fourth event. At the end of the interval, the coalesced event is released to the Event Processor and the next interval begins for matching events. If no matching events arrive during this interval, the process restarts. Otherwise, the coalescing continues with all events counted and released in 10 second intervals.

Common Vulnerability Scoring System (CVSS)

A CVSS score is an metric for assessing the severity of a vulnerability. QRadar SIEM uses CVSS scores to measure how much concern a vulnerability warrants in comparison to other vulnerabilities.

Console

Web interface for QRadar SIEM. QRadar SIEM is accessed from a standard web browser (Internet Explorer 7.0/8.0 or Mozilla Firefox 3.6 and above). When you access the system, a prompt is displayed for a user name and password, which must be configured in advance by the QRadar SIEM administrator.

content capture

QFlow Collectors capture a configurable amount of payload and store the data in the flow logs. You can view this data using the **Network Activity** tab.

credibility

Indicates the integrity of an event or offense as determined by the credibility rating that is configured in the log source. Credibility increases as the multiple sources report the same event.

database leaf objects

The end point objects in a hierarchy. At each point in the hierarchy above this point there is a parent object that contains the aggregate values of all of the leaf objects below.

datapoint

Any point on the QRadar SIEM charts where data is extracted.

DHCP

See Dynamic Host Configuration Protocol.

Device Support Module (DSM)

Device Support Modules (DSMs) allows you to integrate QRadar SIEM with log sources.

DNS
See Domain Name System.

DSM
See Device Support Module (DSM).

Domain Name System (DNS)
An online, distributed database used to map human-readable machine names into an IP address for resolving machine names to IP addresses.

duplicate flow
When multiple QFlow Collectors detect the same flow, this is referred to as a duplicate flow. However, in this event, the QFlow Collector drops the flow as a duplicate so the Event Processor only receives one report on the flow.

Dynamic Host Configuration Protocol (DHCP)
A protocol that allows dynamic assignment of IP addresses to customer premise equipment.

encryption
Encryption provides greater security for all QRadar SIEM traffic between managed hosts. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host to provide protected access to the servers.

event
Record from a device that describes an action on a network or host.

Event Collector
Collects security events and flows from various types of devices in your network. The Event Collector gathers events and flows from local, remote, and device sources. The Event Collector then normalizes the events and flows, and sends the information to the Event Processor.

Event Processor
Processes events collected from one or more Event Collectors. The events are bundled once again to conserve network usage. When received, the Event Processor correlates the information from QRadar SIEM and distributed to the appropriate area, depending on the type of event.

false positive
When an event is tuned as false positive, the event no longer contributes to custom rules, therefore, offenses do not generate based on the false positive event. The event is still stored in the database and contributes to reports.

flow
Communication session between two hosts. Describes how traffic is communicated, what was communicated (if content capture option has been selected), and includes such details as when, who, how much, protocols, priorities, or options.

flow data
Specific properties of a flow including: IP addresses, ports, protocol, bytes, packets, flags, direction, application ID, and payload data (optional).

flow logs
Record of flows that enables the system to understand the context of a particular transmission over the network. Flows are stored in flow logs.

flow sources

Source of flows that the QFlow Collector receives. Using the deployment editor, you can add internal and external flow sources from either the System or Event Views in the deployment editor.

forwarding destination

QRadar SIEM allows you to forward raw log data received from log sources and QRadar SIEM-normalized event data to one or more vendor systems, such as ticketing or alerting systems. On the QRadar SIEM user interface, these vendor systems are called forwarding destinations.

Fully Qualified Domain Name (FQDN)

The portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to.

Fully Qualified Network Name (FQNN)

Full path name of a certain point in the network hierarchy. For example, Company A hierarchy has a department object that contains a marketing object. Therefore, the FQNN is CompanyA.Department.Marketing.

FQDN

See Fully Qualified Domain Name.

FQNN

See Fully Qualified Network Name.

gateway

A device that communicates with two protocols and translates services between them.

HA

See High Availability.

HA cluster

An HA cluster consists of a primary HA host and a secondary HA host that behaves as a standby for the primary.

Hash-Based Message Authentication Code (HMAC)

A cryptographic code that uses a cryptic hash function and a secret key.

High Availability

The High Availability (HA) feature ensures availability of QRadar SIEM data in the event of a hardware or network failure. An HA cluster consists of a primary host and a secondary host that acts as a standby for the primary. The secondary host maintains the same data as the primary host by one of two methods: data replication or shared external storage. At regular intervals, every 10 seconds by default, the secondary host sends a heartbeat ping to the primary host to detect hardware and network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host.

HMAC

See Hash-based Message Authentication Code (HMAC).

Host Context

Monitors all QRadar SIEM components to ensure that each component is operating as expected.

ICMP

See Internet Control Message Protocol.

identity QRadar SIEM collects identity information, if available, from log source messages. Identity information provides additional details about assets on your network. Log sources only generate identity information if the log message sent to QRadar SIEM contains an IP address and at least one of the following items: user name or MAC address. Not all log sources generate identity information.

IDS See Intrusion Detection System.

Internet Control Message Protocol (ICMP) An Internet network-layer protocol between a host and gateway.

Internet Protocol (IP) The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.

Internet Service Provider (ISP) An Internet Service Provider (ISP) provides users access to the Internet and other related services.

interval The default time period in the system. Affects the update intervals of the graphs and how much time each flow log file contains.

Intrusion Detection System (IDS) An application or device that identifies suspicious activity on the network.

Intrusion Prevention System (IPS) Application that reacts to network intrusions.

IP See Internet Protocol.

IP Multicast IP Multicast reduces traffic on a network by delivering a single stream of information to multiple users at one time.

IP network A group of IP routers that route IP datagrams. These routers are sometimes referred to as Internet gateways. Users access the IP network from a host. Each network in the Internet includes some combination of hosts and IP routers.

IPS See Intrusion Prevention System.

item A Dashboard option that creates a customized portal that displays any permissible view for monitoring purposes.

L2L See Local To Local.

L2R See Local To Remote.

LAN See Local Area Network.

LDAP See Lightweight Directory Access Protocol.

leaves Children or objects which are part of a parent group.

Lightweight Directory Access Protocol (LDAP) A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access to a directory server.

Local Area Network (LAN) A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

Local To Local (L2L) Internal traffic from one local network to another local network.

Local To Remote (L2R) Internal traffic from a local network to a remote network.

log source Log sources are external event log sources such as security equipment (for example, firewalls and IDSs) and network equipment (for example, switches and routers).

Magistrate Provides the core processing components of the SIEM option. The Magistrate provides reports, alerts, and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules to create an offense.

magnitude Specifies the relative importance of the offense and is a weighted value calculated from the Relevance, Severity, and Credibility. The magnitude bar on the **Offenses** tab and Dashboard provides a visual representation of all correlated variables of the offense, source, destination, or network. The magnitude of an offense is determined by several tests that performed on an offense every time it has been scheduled for re-evaluation, typically because events have been added or the minimum time for scheduling has occurred.

NAT See Network Address Translation (NAT).

NetFlow A proprietary accounting technology developed by Cisco Systems® Inc. that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a NetFlow collector. You can configure QRadar SIEM to accept NDE's and thus become a NetFlow collector.

Network Address Translation (NAT) NAT translates an IP address in one network to a different IP address in another network.

network hierarchy Contains each component of your network, and identifies which objects belong within other objects. The accuracy and completeness of this hierarchy is essential to traffic analysis functions. The network hierarchy provides for storage of flow logs, databases, and TopN files.

network layer Layer 3 in the Open System Interconnection (OSI) architecture; the layer that establishes a path between open systems.

network objects Components of your network hierarchy. You can add layers to the hierarchy by adding additional network objects and associating them to already defined objects. (Objects that contain other objects are called groups.)

network weight The numeric value applied to each network that signifies the importance of the network. The network weight is user defined.

offense A message sent or event generated in response to a monitored condition. For example, an offense informs you if a policy has been breached or the network is under attack.

Off-site Source An off-site device that forwards normalized data to an Event Collector. You can configure an off-site source to receive flows or events and allow the data to be encrypted before forwarding.

Off-site Target An off-site device that receives event or flow data. An off-site target can only receive data from an Event Collector.

Open Systems Interconnection (OSI) A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.

OSI See Open Systems Interconnection.

Packeteer Packeteer devices collect, aggregate, and store network performance data. When you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to QRadar SIEM.

payload data The actual application data, excluding any header or administrative information, contained in an IP flow.

primary HA host In an HA cluster, the primary HA host is the host to which you want to add HA protection. You can configure HA for any system (Console or non-Console) in your deployment. When you configure HA, the IP address of the primary HA host becomes the Cluster Virtual IP address; therefore, you must configure a new IP address for the primary host.

OSVDB Open Source Vulnerability Database (OSVDB) is an open source database created for and by the network security community. The database provides technical information on network security vulnerabilities.

protocol A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It might still require an authorization exchange with a policy module or external policy server before admission.

QFlow Collector Collects data from devices and various live or recorded data feeds, such as, network taps, span/mirror ports, NetFlow, and QRadar SIEM flow logs.

QID QRadar SIEM Identifier. A mapping of a single event of an external device to a Q1 Labs unique identifier.

R2L See Remote To Local.

R2R See Remote To Remote.

refresh timer The **Dashboard**, **Log Activity**, and **Network Activity** tabs feature a dynamic status bar that displays the amount of time until QRadar SIEM automatically refreshes the current network activity data; built-in refresh can be manually refreshed at any time.

relevance Relevance determines the impact on your network of an event, category, or offense. For example, if a certain port is open, the relevance is high.

Remote To Local (R2L) External traffic from a remote network to a local network.

Remote To Remote (R2R) External traffic from a remote network to another remote network.

reports A function that creates executive or operational level charting representations of network activity based on time, sources, offenses, security, and events.

report interval A configurable time interval at which the Event Processor must send all captured event and flow data to the Console.

routing rules Collection of conditions and consequent routing that are performed when event data matches each rule.

rule Collection of conditions and consequent actions. You can configure rules that allow QRadar SIEM to capture and respond to specific event sequences. The rules allow you to detect specific, specialized events and forward notifications to either the **Offenses** tab or log file, or email a user.

secondary HA host In an HA cluster, the secondary HA host is the standby for the primary host. If the primary HA host fails, the secondary HA host automatically assumes all responsibilities of the primary HA host.

severity Indicates the amount of threat a source poses in relation to how prepared the destination is for the attack. This value is mapped to an event category in the QID map that is correlated to the offense.

Simple Network Management Protocol (SNMP) A network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.

Simple Object Access Protocol (SOAP) A protocol that allows a program running in one kind of operating system to communicate with a program in the same or another kind of an operating system.

SNMP See Simple Network Management Protocol.

SOAP See Simple Object Access Protocol.

standby system In an HA cluster, the standby system is the host that is acting as standby for the active system. Only the secondary HA host can be the standby system. The standby system has no services running. If disk replication is enabled, the standby system is replicating data from the active system. If the active system fails, the standby system automatically assumes the active role.

subnet A network subdivided into networks or subnets. When subnetting is used, the host portion of the IP address is divided into a subnet number and a host number. Hosts and routers identify the bits used for the network and subnet number through the use of a subnet mask.

subnet mask A bit mask that is logically ANDed with the destination IP address of an IP packet to determine the network address. A router routes packets using the network address.

sub-search Allows you to perform searches within a set of completed search results. The sub-search function allows you to refine your search results without requiring you to search the database again.

superflows Multiple flows with the same properties are combined into one flow to increase processing by reducing storage.

System Time The right corner of the user interface displays System time, which is the time on the QRadar SIEM Console. This is the time that determines the time of events and offenses.

System View Allows you to assign software components, such as a QFlow Collector, to systems (managed hosts) in your deployment. The System View includes all managed hosts in your deployment. A managed host is a system in your deployment that has QRadar SIEM software installed.

TACACS Terminal Access Controller Access Control System (TACACS) is an authentication protocol that allows remote server access to forward a user logon password to an authentication server to determine whether access can be allowed to a given system. TACACS+ uses TCP.

TCP See Transmission Control Protocol.

TCP flags A type of marker that can be added to a packet to alert the system of abnormal activity. Only a few specific combinations of flags are valid and typical, in normal traffic. Abnormal combinations of flags often indicate an attack or an abnormal network condition.

TCP resets For TCP-based applications, QRadar SIEM can issue a TCP reset to either the client or server in a conversation. This stops the communications between the client and the server.

Time Series A chart type that graphs data based on time. This chart focuses on the networks or IP address data information from the selected networks.

TopN Displays the top *N* networks or IP address information for the data you are viewing. For example, using the chart feature, you can display the top five networks generating traffic in the U.S.

Transmission Control Protocol (TCP) A reliable stream service that operates at the transport-layer Internet protocol, which ensures successful end-to-end delivery of data packets without error.

violation Includes a violation of corporate policy.

Whois Allows you to look up information about registered Internet names and numbers.

C NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service might be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right might be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM might make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM might use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices might vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

INDEX