IBM Security QRadar
Version 7.2.6

Users Guide

Note

Before using this information and the product that it supports, read the information in "Notices" on page 239.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

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.

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. What's new for users in QRadar V7.2.6

IBM Security QRadar V7.2.6 introduces optimized indexing, new CRE test that compares properties, licensing improvements, and more.

Optimized indexes that speed search performance

In previous releases, indexes were created for each 1-minute interval. Now, with Super Indexes in QRadar V7.2.6, the index data structure is optimized and a single super index is created at the end of each hour. For multi-hour searches in particular, QRadar now scans the index more optimally, resulting in an up to 10x performance increase for Indicator of Compromise (IOC) type searches. Some examples of IOC type searches are searches on IP address, domain and host name. All new data that is received by QRadar is automatically indexed in the new format.

Only the index of new data received is optimized. For more information about improving the performance of historical data, see the Optimizing your Ariel indexes in 7.2.6 technote (http://www.ibm.com/support/docview.wss?uid=swg21968002).

New CRE tests

A new custom rule engine (CRE) test is available to compare one property against another, including custom properties.

You can now compare a source IP address against a destination IP address. You can compare a user name against a custom property. ⓘ Learn more...

Use AQL WHERE clause grammar to build complex comparisons in the custom rules engine (CRE). You can use AND/OR logic, reference container lookups and asset model queries. You type only the conditions when you build your WHERE clause. ⓘ Learn more...

License enhancements

QRadar V7.2.6 changes the way that events affect your license. In previous releases, all events that were generated by QRadar, such as EPS notifications, system notificaitons, and internally generated logs, were counted against your license. Now, the following internal events do not count toward your license:

- system notifications
- custom rule engine (CRE)
- audit
- ADE
- asset profiler
- results from scheduled searches
- health metrics
- QRadar Risk Manager questions, simulations and internal logging.

Only events that are generated on devices on the customer premise count toward your license. Also, 60% of events that you drop by using routing rules are credited back, up to a maximum of 2000 events per second (EPS).

Viewing reference sets in rules and search results

You now have more access to data. Reference set information was previously unavailable to you if you didn't have Administrator privileges. Administrators can now grant access to you so that you can view reference sets in search results, and in common rules. You can now include reference sets in searches and common rules. You can view lists of reference sets, the contents of reference sets, and can export reference sets. Learn more...

Quick Filter in the right-click menu

The right-click menus now include a Quick Filter option for events and flows. Use the Quick Filter criteria to pivot data during your investigations. You can search on items that match, or don't match your selection. After you add the match/not match filter, more search criteria become available in the right-click menu.

Learn more...

Improved query workflow to provide faster access to data

QRadar improves the way that you interact with data and also lets you quickly expand the time before and after an offense occurred. Use the options for time series charts on the Network and Log activity tabs to quickly change the displayed time period, without leaving the activity view. For example, if you are investigating an offense that occurred on an endpoint at 4:30 PM on Tuesday, you can drill into the events from the offense itself. You can look at what happened a few minutes before or later the time span that you are looking at without having to open the **Edit Search** page. You can specify a time period, down to the minute, or expand a time period from the drop-down list. Learn more...

Historical correlation enhancements

IBM Security QRadar V7.2.6 introduces better visibility into threats and management of historical correlation profiles and results:

Increased visibility of real threats

In IBM Security QRadar V7.2.5, historical offenses were created for any rule that was triggered during a historical correlation run. In V7.2.6, historical offenses are created only when the triggered rule specifies that an offense must be created for the detected event.

Improved auditing

Audit records are created each time a historical correlation profile is run or canceled. This change provides you with improved monitoring and increased visibility to see which users are running or canceling historical correlation runs.

New offense search capabilities

You can now search for offenses that were created from a selected historical correlation profile. You can also exclude historical correlation results from saved searches. With these new search parameters, you can separate historical correlation offenses from real-time offenses for reporting.

Improved historical correlation profile management

Depending on the volume of historical data that you are processing and the criteria that you specify, you might find that the correlation takes a long time to complete. You can now cancel historical correlation profiles that are running or queued to run.

You can sort and filter columns in the Historical Correlation window to easily find the information that you are looking for.

When you view the run history for a profile, you can quickly see the number of offenses that were created by a run. With a single-click, you drill down on the historical correlation catalogs to see the list of events or flows that matched the profile criteria.

Learn more...

New AQL string and statistical functions

Use the following Ariel Query Language (AQL) functions in advanced searches when you want to find the position of a string or replace a string in a regular expression:

Function	**Description**
strpos	Returns the position of string inside another string.
regex_replace	Replaces a string by using a regex as the search condition.
first	Returns the first instances of the specified column.
last	Returns the last instances of the specified column.
stddev	Returns the sample standard deviation.
stddevp	Returns the population standard deviation.

For more information, see the Supported Functions section in the *IBM Security QRadar Ariel Query Language Guide*.

Chapter 2. 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.

Default license key

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

Security exceptions and certificates

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.

Navigate the web-based application

When you use QRadar SIEM, use the navigation options available in the QRadar SIEM user interface instead of your web browser **Back** button.

Capabilities in your security intelligence product

IBM Security QRadar product documentation describes functionality such as offenses, flows, assets, and historical correlation, that might not be available in all QRadar products. Depending on the product that you are using, some documented features might not be available in your deployment. Review the capabilities for each product to guide you to the information that you need.

IBM Security QRadar SIEM includes the full range of security intelligence capabilities for on-premises deployments. QRadar SIEM consolidates log source event data from device endpoints and applications that are distributed throughout your network, and performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives.

Use IBM Security Intelligence on Cloud to collect, analyze, archive, and store large volumes of network and security event logs in a hosted environment. Analyze your data to provide visibility into developing threats, and meet your compliance monitoring and reporting requirements while lowering your total cost of ownership.

Use IBM Security QRadar Log Manager to collect, analyze, archive, and store large volumes of network and security event logs. QRadar Log Manager analyzes data to provide visibility into developing threats, and it can help you to meet compliance monitoring and reporting requirements.

When you are looking for help, use the following table, which lists the capabilities of the products:

Table 1. Comparison of QRadar capabilities

Capability	**QRadar SIEM**	**IBM Security Intelligence on Cloud**	**IBM Security QRadar Log Manager**
Supports hosted deployments	No	Yes	No
Customizable dashboards	Yes	Yes	Yes
Custom rules engine	Yes	Yes	Yes
Manage network and security events	Yes	Yes	Yes
Manage host and application logs	Yes	Yes	Yes
Threshold-based alerts	Yes	Yes	Yes
Compliance templates	Yes	Yes	Yes
Data archiving	Yes	Yes	Yes
IBM Security X-Force® Threat Intelligence IP reputation feed integration	Yes	Yes	Yes
WinCollect stand alone deployments	Yes	Yes	Yes
WinCollect managed deployments	Yes	No	Yes
QRadar Vulnerability Manager integration	Yes	No	Yes
Network activity monitoring	Yes	No	No
Asset profiling	Yes	Yes	No [1]
Offenses management	Yes	Yes	No
Network flow capture and analysis	Yes	No	No
Historical correlation	Yes	Yes	No
QRadar Risk Manager integration	Yes	No	No
QRadar Incident Forensics integration	Yes	No	No
[1] QRadar Log Manager only tracks asset data if QRadar Vulnerability Manager is installed.			

Supported web browsers

For the features in IBM Security QRadar products to work properly, you must use a supported web browser.

When you access the QRadar system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 2. Supported web browsers for QRadar products

Web browser	**Supported versions**
Mozilla Firefox	38.0 Extended Support Release

Table 2. Supported web browsers for QRadar products (continued)

Web browser	Supported versions
32-bit Microsoft Internet Explorer, with document mode and browser mode enabled	10.0 11.0
Google Chrome	Version 46

Enabling document mode and browser mode in Internet Explorer

If you use Microsoft Internet Explorer to access IBM Security QRadar products, you must enable browser mode and document mode.

Procedure

1. In your Internet Explorer web browser, press F12 to open the Developer Tools window.
2. Click **Browser Mode** and select the version of your web browser.
3. Click **Document Mode**, and select the **Internet Explorer standards** for your Internet Explorer release.

IBM Security QRadar login

IBM Security QRadar is a web-based application. QRadar uses default login information for the URL, user name, and password.

Use the information in the following table when you log in to your IBM Security QRadar console.

Table 3. Default login information for QRadar

Login information	Default
URL	https://<IP Address>, where <IP Address> is the IP address of the QRadar console. To log in to QRadar in an IPv6 or mixed environment, wrap the IP address in square brackets: `https://[<IP Address>]`
User name	admin
Password	The password that is assigned to QRadar during the installation process.
License key	A default license key provides you access to the system for 5 weeks.

RESTful API

Use the representational state transfer (REST) application programming interface (API) to make HTTPS queries and integrate IBM Security QRadar with other solutions.

Access and user role permissions

You must have administrative user role permissions in QRadar to access and use RESTful APIs. For more information about how to manage user role permissions, see the *Administration Guide*.

Access to the REST API technical documentation user interface

The API user interface provides descriptions and capabilities for the following REST API interfaces:

Table 4. REST API interfaces

REST API	Description
`/api/ariel`	Query databases, searches, search IDs, and search results.
`/api/asset_model`	Returns a list of all assets in the model. You can also list all available asset property types and saved searches, and update an asset.
`/api/auth`	Log out and invalidate the current session.
`/api/help`	Returns a list of API capabilities.
`/api/siem`	Returns a list of all offenses.
`/api/qvm`	Review and manage QRadar Vulnerability Manager data.
`/api/reference_data`	View and manage reference data collections.
`/api/qvm`	Retrieves assets, vulnerabilities, networks, open services, networks, and filters. You can also create or update remediation tickets.
`/api/scanner`	View, create, or start a remote scan that is related to a scan profile.

The REST API technical documentation interface provides a framework that you can use to gather the required code that you need to implement QRadar functions into other products.

1. Enter the following URL in your web browser to access the technical documentation interface: `https://`*`ConsoleIPaddress`*`/api_doc`.
2. Click the header for the API that you want to access, for example, **/ariel**.
3. Click the subhead for the endpoint that you want to access, for example, **/databases**.
4. Click the Experimental or Provisional sub header.

   Note:

   The API endpoints are annotated as either *experimental* or *stable*.

   Experimental
   Indicates that the API endpoint might not be fully tested and might change or be removed in the future without any notice.

   Stable Indicates that the API endpoint is fully tested and supported.
5. Click **Try it out** to receive properly formatted HTTPS responses.

6. Review and gather the information that you need to implement in your third-party solution.

QRadar API forum and code samples

The API forum provides more information about the REST API, including the answers to frequently asked questions and annotated code samples that you can use in a test environment. For more information, see API forum (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca).

User interface tabs

Functionality is divided into tabs. The **Dashboard** tab is displayed when you log in.

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.

The **Dashboard** tab provides a workspace environment that supports multiple dashboards on which you can display your views of network security, activity, or data that QRadar collects. Five default dashboards are available. Each dashboard contains items that provide summary and detailed information about offenses that occur on your network. You can also create a custom dashboard to allow 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 will allow you to view offenses that occur on your network, which you can locate by 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 will allow you to investigate event logs being sent to QRadar in real-time, perform powerful searches, and view log activity by using configurable time-series charts.

The **Log Activity** tab will allow you to perform in-depth investigations on event data.

For more information, see Log Activity investigation.

Network activity tab

Use the **Network Activity** tab to investigate flows that are sent in real-time, perform powerful searches, and view network activity by using configurable time-series charts.

A flow is a communication session between two hosts. Viewing flow information will allow 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 automatically discovers assets, servers, and hosts, operating on your network.

Automatic discovery is based on passive flow data and vulnerability data, allowing QRadar 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, an attack tries to use a specific service that is running on a specific asset. In this situation, QRadar can determine whether 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 will allow you to create, distribute, and manage reports for any data within QRadar.

The Reports feature will allow 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 preinstalled report templates that are included with QRadar.

The **Reports** tab also will allow you to brand your reports with customized logos. This customization 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 that is collected by configuration data from network and security device, such as firewalls, routers, switches, or IPSs, vulnerability feeds, and vendor security sources. This data is used to identify security, policy, and compliance risks within your network security infrastructure and the probability of those risks that are being exploited.

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

Admin tab

Administrators use the Admin tab to configure and manage the users, systems, networks, plug-ins, and components. Users with administration privileges can access the **Admin** tab.

The administration tools that administrators can access in the **Admin** tab are described in Table 1.

Table 5. Administration management tools available in QRadar

Admin tool	Description
System Configuration	Configure system and user management options.
Data Sources	Configure log sources, flow sources, and vulnerability options.
Remote Networks and Services Configuration	Configure remote networks and services groups.
Deployment Editor	Manage the individual components of your QRadar deployment.

All configuration updates that 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.

QRadar common procedures

Various controls on the QRadar user interface are common to most user interface tabs.

Information about these common procedures is described in the following sections.

Viewing messages

The **Messages** menu, which is on the upper 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 that is based on each notification message type and select the **Notify** check box in the **Custom Rules Wizard**.

About this task

The **Messages** menu indicates how many unread system notifications you have in your system. This indicator increments the number until you close 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 close a system notification from the **Messages** window, the system notification is removed from all system notification displays.

For more information about Dashboard system notifications, see System Notifications item.

The **Messages** window provides the following functions:

Table 6. Functions available in the Messages window

Function	Description
All	Click **All** to view all system notifications. This option is the default, therefore, you click **All** only if you 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.
Information	Click **Information** to view only the system notifications that have a severity level of information.
Dismiss All	Click **Dismiss All** to close all system notifications from your system. If you filtered the list of system notifications by 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 Warnings** • **Dismiss All Info**
View All	Click **View All** to view the system notification events in the **Log Activity** tab. If you filtered the list of system notifications by 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 close the system notification from your system.

Procedure

1. Log in to QRadar .
2. On the upper right corner of the user interface, click **Messages**.
3. On the **Messages** window, view the system notification details.
4. Optional. To refine the list of system notifications, click one of the following options:
   - **Errors**
   - **Warnings**
   - **Information**
5. Optional. To close system notifications, choose of the following options:

Option	**Description**
Dismiss All	Click to close all system notifications.
Dismiss	Click the **Dismiss** icon next to the system notification that you want to close.

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

Sorting results

You sort the results in tables by clicking a column heading. An arrow at the top of the column indicates the direction of the sort.

Procedure

1. Log in to QRadar.
2. Click the column header once to sort the table in descending order; twice to sort the table in ascending order.

Refreshing and pausing the user interface

You can manually refresh, pause, and play the data that is displayed on tabs.

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, which is on the upper 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 that the current display is paused.

Procedure

1. Log in to QRadar.
2. Click the tab that you want to view.
3. Choose one of the following options:

Option	Description
Refresh	Click **Refresh**, on the right corner of the tab, to refresh the tab.
Pause	Click to pause the display on the tab.
Play	Click to restart the timer after the timer is paused.

Investigating IP addresses

You can use several methods to investigate information about IP addresses on the Dashboard, Log Activity, and Network Activity tabs.

Procedure

1. Log in to QRadar.
2. Click the tab that you want to view.
3. Move your mouse pointer over an IP address to view the location of the IP address.
4. Right-click the IP address or asset name and select one of the following options:

Table 7. IP addresses information

Option	Description
Navigate > **View by Network**	Displays the networks that are associated with the selected IP address.
Navigate > **View Source Summary**	Displays the offenses that are associated with the selected source IP address.
Navigate > **View Destination Summary**	Displays the offenses that are associated with the selected destination IP address.
Information > **DNS Lookup**	Searches for DNS entries that are 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.

Table 7. IP addresses information (continued)

Option	Description
Information > **Asset Profile**	Displays asset profile information. This option is displayed if IBM Security QRadar Vulnerability Manager is purchased and licensed. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*. This menu option is available if QRadar 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**	Searches for events that are associated with this IP address.
Information > **Search Flows**	Searches for flows that are associated with this IP address.
Information > **Search Connections**	Searches for connections that are associated with this IP address. This option is only displayed if you purchased IBM Security QRadar Risk Manager and connected QRadar and the IBM Security QRadar Risk Manager appliance. For more information, see the *IBM Security QRadar Risk Manager User Guide*.
Information > **Switch Port Lookup**	Determines the switch port on a Cisco IOS device for this IP address. This option applies only to switches that are discovered by using the **Discover Devices** option on the **Risks** tab. **Note:** This menu option isn't available in QRadar Log Manager
Information > **View Topology**	Displays the **Risks** tab, which depicts the layer 3 topology of your network. This option is available if you purchased IBM Security QRadar Risk Manager and connected QRadar and the IBM Security QRadar Risk Manager appliance. appliance.
Run Vulnerability Scan	Select the **Run Vulnerability Scan** option to scan an IBM Security QRadar Vulnerability Manager scan on this IP address. This option is only displayed when IBM Security QRadar Vulnerability Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*.

Investigate user names

You can right-click a user name to access more menu options. Use these options to view more information about the user name or IP address.

You can investigate user names when IBM Security QRadar Vulnerability Manager is purchased and licensed. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*.

When you right-click a user name, you can choose the following menu options.

Table 8. Menu options for user name investigation

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

For more information about customizing the right-click menu, see the *Administration Guide* for your product.

System time

The right corner of the QRadar user interface displays system time, which is the time on the console.

The console time synchronizes QRadar systems within the QRadar deployment. The console time is used to determine what time events were received from other devices for correct time synchronization correlation.

In a distributed deployment, the console might be 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 to specify a time range.

When you apply time-based filters and searches on the **Log Activity** tab, you must use the console system time to specify a time range.

Updating user preferences

You can set your user preference, such as locale, in the main IBM Security QRadar SIEM user interface.

Procedure

1. To access your user information, click **Preferences**.
2. Update your preferences.

Option	Description
Username	Displays your user name. You cannot edit this field.

Option	Description
Password	QRadar user passwords are stored as a salted SHA-256 string. The password must meet the following criteria: • Minimum of 6 characters • Maximum of 255 characters • Contain at least 1 special character • Contain 1 uppercase character
Password (Confirm)	Password confirmation
Email Address	The email address must meet the following requirements: • Minimum of 10 characters • Maximum of 255 characters
Locale	QRadar is available in the following languages: English, Simplified Chinese, Traditional Chinese, Japanese, Korean, French, German, Italian, Spanish, Russian, and Portuguese (Brazil). If you choose a different language, the user interface displays in English. Other associated cultural conventions, such as, character type, collation, format of date and time, currency unit are used.
Enable Popup Notifications	Select this check box if you want to enable pop-up system notifications to be displayed on your user interface.

Related concepts:

"Quick filter search options" on page 162
Search event and flow payloads by typing a text search string that uses simple words or phrases.

Access online help

You can access the QRadar Online Help through the main QRadar user interface.

To access the Online Help, click **Help** > **Help Contents**.

Resize columns

You can resize the columns on several tabs in QRadar.

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 work in Microsoft Internet Explorer, Version 7.0 web browsers when tabs are displaying records in streaming mode.

Page size

Users with administrative privileges can configure the maximum number of results that display in the tables on various tabs in QRadar.

Chapter 3. Dashboard management

The **Dashboard** tab is the default view when you log in.

It provides a workspace environment that supports multiple dashboards on which you can display your views of network security, activity, or data that is collected.

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

Use the Dashboard tab to monitor your security event behavior.

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

Default dashboards

Use the default dashboard to customize your items into functional views. These functional views focus on specific areas of your network.

The **Dashboard** tab provides five default dashboards that are focused on security, network activity, application activity, system monitoring, and compliance.

Each dashboard displays a default that is set of dashboard items. The dashboard items act as starting point to navigate to more detailed data. The following table defines the default dashboards.

Custom dashboards

You can customize your dashboards. The content that is displayed on the **Dashboard** tab is user-specific. Changes that are made within a QRadar 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. 255 dashboards per user is the maximum; 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 that are 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 that are 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.

Customize your dashboard

You can add several dashboard items to your default or custom dashboards.

You can customize your dashboards to display and organize the dashboards items that meet your network security requirements.

There are 5 default dashboards, which you can access from the **Show Dashboard** list box on the **Dashboard** tab. If you previously viewed a dashboard and returned to the **Dashboard** tab, the last dashboard you viewed is displayed.

Flow search

You can display a custom dashboard item that is 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.

Default saved search criteria is available and 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, see 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 configuring charts, see Configuring charts.

Time series charts are interactive. Using the time series charts, you can magnify and scan through a timeline to investigate network activity.

Offenses

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 about hidden or closed events, see Offense management.

The following table describes the Offense items:

Table 9. Offense items

Dashboard items	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 to 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 to the offense name to view detailed information for the IP address.

Table 9. Offense items (continued)

Dashboard items	**Description**
My Offenses	The **My Offenses** item displays 5 of the most recent offenses that are assigned to you. The offenses are identified with a magnitude bar to inform you of the importance of the offense. Point to 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 to 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 to the IP address to view detailed information for the IP
Categories	The **Top Categories Types** item displays the top 5 categories that are associated with the highest number of offenses.

Log activity

The **Log Activity** dashboard items will 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.

Table 10. Log activity items

Dashboard item	Description
Event Searches	You can display a custom dashboard item that is 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 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. 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 that are grouped by severity. This item will allow you to see the number of events that are received by the level of severity 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 5 log sources that sent events to QRadar within the last 5 minutes. The number of events that are sent from the specified log source is indicated in the pie chart. This item will allow 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

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

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 that are 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 that are 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 that are detected within the last 24 hours and the number of modified offenses within the last 24 hours.

Risk Monitoring Dashboard

You use the **Risk Monitoring** dashboard to monitor policy risk and policy risk change for assets, policies and policy groups.

By default, the **Risk Monitoring** dashboard displays **Risk** and **Risk Change** items that monitor the policy risk score for assets in the High Vulnerabilities, Medium Vulnerabilities, and Low Vulnerabilities policy groups, as well as compliance pass rates and historical changes in policy risk score in the CIS policy group.

The Risk Monitoring dashboard items do not display any results unless IBM Security QRadar Risk Manager is licensed. For more information, see QRadar Risk Manager Users Guide.

To view the default **Risk Monitoring** dashboard, select **Show Dashboard** > **Risk Monitoring** on the **Dashboard** tab.

Related tasks:

"Monitoring policy compliance"
Create a dashboard item that shows policy compliance pass rates and policy risk score for selected assets, policies, and policies groups.

"Monitoring risk change" on page 25
Create a dashboard item that shows policy risk change for selected assets, policies, and policies groups on a daily, weekly, and monthly basis.

Monitoring policy compliance

Create a dashboard item that shows policy compliance pass rates and policy risk score for selected assets, policies, and policies groups.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.

3. Type a name and description for your policy compliance dashboard.
4. Click **OK**.
5. On the toolbar, select **Add Item** > **Risk Manager** > **Risk**.

   Risk Manager dashboard items are displayed only when IBM Security QRadar Risk Manager is licensed.
6. On the header of the new dashboard item, click the yellow **Settings** icon.
7. Use the **Chart Type**, **Display Top**, and **Sort** lists to configure the chart.
8. From the **Group** list, select the group that you want to monitor. For more information, see the table in step 9.

   When you select the **Asset** option, a link to the **Risks** > **Policy Management** > **By Asset** page appears at the bottom of the **Risk** dashboard item. The **By Asset** page displays more detailed information about all results that are returned for the selected **Policy Group**. For more information on a specific asset, select **Table** from **Chart Type** list and click the link in the **Asset** column to view details about the asset in the **By Asset** page.

   When you select the **Policy** option, a link to the **Risks** > **Policy Management** > **By Policy** page appears at the bottom of the **Risk** dashboard item. The **By Policy** page displays more detailed information about all results that are returned for the selected **Policy Group**. For more information on a specific policy, select **Table** from **Chart Type** list and click the link in the **Policy** column to view details about the policy in the **By Policy** page.
9. From the **Graph** list, select the graph type that you want to use. For more information, see the following table:

Group	Asset Passed Percentage	Policy Checks Passed Percentage	Policy Group Passed Percentage	Policy Risk Score
All	Returns the average asset percentage pass rate across assets, policies, and the policy group.	Returns the average policy check percentage pass rate across assets, policies, and the policy group.	Returns the average policy group pass rate across all assets, policies, and the policy group.	Returns the average policy risk score across all assets, policies, and the policy group.
Asset	Returns whether an asset passes asset compliance (100%=passed, 0%=failed). Use this setting to show which assets associated with a Policy Group pass compliance.	Returns percentage of policy checks that an asset passes. Use this setting to show the percentage of policy checks that passed for each asset that is associated with the Policy Group.	Returns the percentage of policy subgroups that are associated with the asset that pass compliance.	Returns the sum of all importance factor values for policy questions that are associated with each asset. Use this setting to view the policy risk for each asset that is associated with a selected policy group.

Group	Asset Passed Percentage	Policy Checks Passed Percentage	Policy Group Passed Percentage	Policy Risk Score
Policy	Returns whether all the assets associated with each policy in a Policy group pass compliance. Use this setting to monitor whether all the assets associated with each policy in a Policy Group pass or not.	Returns percentage of policy checks that pass per policy in the policy group. Use this setting to monitor how many policy checks are failing per policy.	Returns the percentage of policy subgroups of which the policy is a part that pass compliance.	Returns the importance factor values for each policy question in the Policy group. Use this setting to view the importance factor for each policy in a policy group.
Policy Group	Returns the percentage of assets that pass compliance for the selected Policy Group as a whole.	Returns the percentage of policy checks that pass per policy for the policy group as a whole.	Returns the percentage of policy subgroups within the Policy Group that pass compliance.	Returns the sum of all importance factor values for all policy questions in the Policy group.

10. From the **Policy Group** list, select the policy groups that you want to monitor.
11. Click **Save**.

Monitoring risk change

Create a dashboard item that shows policy risk change for selected assets, policies, and policies groups on a daily, weekly, and monthly basis.

About this task

Use this dashboard item to compare changes in the Policy Risk Score, Policies Checks, and Policies values for a policy group over time.

The **Risk Change** dashboard item uses arrows to indicate where policy risk for selected values that increased, decreased, or stayed the same over a chosen time period:

- The number beneath the red arrow indicates the values that show an increased risk.
- The number beneath the gray arrows indicates the values where there is no change in risk.
- The number beneath the green arrow indicates the values that show a decreased risk.

Procedure

1. Click the **Dashboard** tab.
2. On the toolbar, click **New Dashboard**.
3. Type a name and description for your historical policy compliance dashboard.
4. Click **OK**.
5. On the toolbar, select **Add Item** > **Risk Manager** > **Risk Change**.

   Risk Manager Dashboard items are displayed only when IBM Security QRadar Risk Manager is licensed.

6. On the header of the new dashboard item, click the yellow **Settings** icon.
7. From the **Policy Group** list, select the policy groups that you want to monitor.
8. Select an option from the **Value To Compare** list:
   - If you want to see the cumulative changes in importance factor for all policy questions within the selected policy groups, select **Policy Risk Score**.
   - If you want to see how many policy checks changed within the selected policy groups, select **Policies Checks**.
   - If you want to see how many policies changed within the selected policy groups, select **Policies**.
9. Select the risk change period that you want to monitor from the **Delta Time** list:
   - If you want to compare risk changes from 12:00 a.m. today with yesterday's risk changes, select **Day**.
   - If you want to compare risk changes from Monday 12:00 a.m. this week with last week's risk changes, select **Week**.
   - If you want to compare risk changes from the 12:00 a.m. on the first day of the current month with last month's risk changes, select **Month**.
10. Click **Save**.

Vulnerability Management items

Vulnerability Management dashboard items are only displayed when IBM Security QRadar Vulnerability Manager is purchased and licensed.

For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*.

You can display a custom dashboard item that is based on saved search criteria from the **Vulnerabilities** tab. Search items are listed in the **Add Item** > **Vulnerability Management** > **Vulnerability Searches** menu. The name of the search item matches the name of the saved search criteria the item is based on.

QRadar includes default saved search criteria that is preconfigured to display search items on your **Dashboard tab** menu. You can add more search dashboard items to your **Dashboard tab** menu.

The supported chart types are table, pie, and bar. The default chart type is bar. These charts are configurable.

System notification

The Systems Notification dashboard item displays event notifications that are received by your system.

For notifications to show in the **System Notification** dashboard item, the Administrator must create a rule that is 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 Guide*.

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

- **Flag** - Displays a symbol to indicate severity level of the notification. Point to 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 elapsed since the notification was created.
- **Description** - Displays information about the notification.
- **Dismiss icon (x)** - Will allow you to close 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 that is associated with the incident that generated this notification. For example: Service Disruption.
- **Payload** - Displays the payload content that is associated with the incident that generated this notification.
- **Created** - Displays the amount of time 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 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.

In the System Notifications pop-up window, the number of notifications in the queue is highlighted. For example, if (1 - 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 more 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.

Creating a custom dashboard

You can create a custom dashboard 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.

Procedure

1. Click the **Dashboard** tab.
2. Click the **New Dashboard** icon.
3. In the **Name** field, type a unique name for the dashboard. The maximum length is 65 characters.
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.
5. Click **OK**.

Using the dashboard to investigate log or network activity

Search-based dashboard items provide a link to the **Log Activity** or **Network Activity** tabs, allowing you to further investigate log or network activity.

About this task

To investigate flows from a **Log Activity** dashboard item:

1. Click the **View in Log Activity** link. The **Log Activity** tab is displayed, displaying results and two charts that match the parameters of your dashboard item.

To investigate flows from a **Network Activity** dashboard item:

1. Click the **View in Network Activity** link. The Network Activity tab is displayed, displaying results and two charts that match the parameters of your dashboard item.

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

Chart type	Description
Bar, Pie, and Table	The **Log Activity** or **Network Activity** tab displays a bar chart, pie chart, and table of flow details.

Chart type	Description
Time Series	The **Log Activity** or **Network Activity** tab displays charts according to the following criteria: 1. 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. 2. 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.

About this task

Table 11. Configuring Charts. Parameter options.

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 that you want to view. Options include: 1. **Bar Chart** - Displays data in a bar chart. This option is only available for grouped events or flows. 2. **Pie Chart** - Displays data in a pie chart. This option is only available for grouped events or flows. 3. **Table** - Displays data in a table. This option is only available for grouped events or flows. 4. **Time Series** - Displays an interactive line chart that represents the records that are matched by a specified time interval.
Display Top	From the list box, select the number of objects you want to 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.

Table 11. Configuring Charts (continued). Parameter options.

Option	Description
Time Range	From the list box, select the time range that you want to view.

Your custom chart configurations are retained, so that they are displayed as configured each time that you access the **Dashboard** tab.

Data is accumulates so that when you perform a time series saved search, there is a cache of event or flows 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

1. Click the **Dashboard** tab.
2. From the **Show Dashboard** list box, select the dashboard that contains the item you want to customize.
3. On the header of the dashboard item you want to configure, click the **Settings** icon.
4. Configure the chart parameters.

Removing dashboard items

You can remove items from a dashboard and add the item again at any time.

About this task

When you remove an item from the dashboard, the item is not removed completely.

Procedure

1. Click the **Dashboard** tab.
2. From the **Show Dashboard** list box, select the dashboard from which you want to remove an item.
3. On the dashboard item header, click the red [x] icon to remove the item from the dashboard.

Detaching a dashboard item

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

About this task

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 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

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

1. Click the **Dashboard** tab.
2. From the **Show Dashboard** list box, select the dashboard that you want to edit.
3. On the toolbar, click the **Rename Dashboard** icon.
4. In the **Name** field, type a new name for the dashboard. The maximum length is 65 characters.
5. In the **Description** field, type a new description of the dashboard. The maximum length is 255 characters
6. Click **OK**.

Deleting a dashboard

You can delete a dashboard.

About this task

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

Procedure

1. Click the **Dashboard** tab.
2. From the **Show Dashboard** list box, select the dashboard that you want to delete.
3. On the toolbar, click **Delete Dashboard**.
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 close system notifications after you read them.

Before you begin

Ensure the **System Notification** dashboard item is added to your dashboard.

Procedure

1. On the System Notification dashboard item header, click the **Settings** icon.
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 that are logged in the past 24 hours, click **All**.

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

Adding search-based dashboard items to the Add Items list

You can add search-based dashboard items to your **Add Items** menu.

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

1. Choose:
   - To add a flow search dashboard item, click the **Network Activity** tab.
   - To add an event search dashboard item, click the **Log Activity** tab.
2. From the **Search** list box, choose one of the following options:
   - To create a search, select **New Search**.
   - To edit a saved search, select **Edit Search**.
3. Configure or edit your search parameters, as required.
   - 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.
4. Click **Filter**. The search results are displayed.
5. Click **Save Criteria**. See Saving search criteria on the Offense tab
6. Click **OK**.
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:
   a. To verify an event search item, select **Add Item** > **Log Activity** > **Event Searches** > **Add Item**.
   b. To verify a flow search item, select **Add Item** > **Network Activity** > **Flow Searches**. The dashboard item is displayed on the list with the same name as your saved search criteria.

Chapter 4. Offense Management

Events and flows with destination IP addresses located across multiple networks in the same offense can be correlated. You can effectively investigate each offense in your network.

Restriction: You cannot manage offenses in IBM Security QRadar Log Manager. For more information about the differences between IBM Security QRadar SIEM and IBM Security QRadar Log Manager, see "Capabilities in your security intelligence product" on page 5.

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 an offense, source and destination IP addresses, network behaviors, and anomalies on your network.

You can also search for offenses that are based on various criteria. For more information about searching offenses, see "Offense searches" on page 163.

Offense permission considerations

All users can view all offenses regardless of which log source or flow source is associated with the offense.

The **Offenses** tab does not use device level user permissions to determine which offenses each user is able to view; as determined by network permissions.

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 Offenses, Source IP addresses, and Destination IP addresses.

Item	Description
Offenses	An offense includes multiple events or flows that originate 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.

Item	Description
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 time period.

The default offense retention period is three days. You must have administrative permission to access the **Admin** tab and configure system settings. When you configure the thresholds, five days are added to any defined threshold.

When you close offenses, the closed offenses are removed from the database after the offense retention period elapses. If more 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 if 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 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 that are listed in the table below.

Table 12. Pages that can be accessed from the **Offenses** *tab*

Page	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 that are grouped by the high and low-level category.
By Source IP	Displays all offenses that are grouped by the source IP addresses that are involved in an offense.
By Destination IP	Displays all offenses that are grouped by the destination IP addresses that are involved in an offense.

Table 12. Pages that can be accessed from the **Offenses** *tab (continued)*

Page	Description
By Network	Displays all offenses that are 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.

Before you begin

The All Offenses page displays a list of all offenses that are 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 about 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 about the toolbar options, see Offense tab toolbar functions.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, select **All Offenses** or **My Offenses**.
3. You can refine the list of offenses with the following options:
   - From the **View Offenses** list box, select an option to filter the list of offenses for a specific time frame.
   - Click the **Clear Filter** link beside each filter that is displayed in the **Current Search Parameters** pane.
4. Double-click the offense that you want to view.
5. On the Offense Summary page, review the offense details. See Offense parameters.
6. Perform any necessary actions on the offense.

Monitoring offenses grouped by category

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

About this task

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

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **By Category**.
3. To view low-level category groups for a particular high-level category, click the arrow icon next to the high-level category name.
4. To view a list of offenses for a low-level category, double-click the low-level category.
5. Double-click the offense that you want to view.
6. On the Offense Summary page, review the offense details. See Offense parameters.
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 that are 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

1. Click the **Offenses** tab.
2. Click **By Source IP**.
3. You can refine the list of offenses that use the following options:
   - From the **View Offenses** list box, select an option to filter the list of offenses for a specific time frame.
   - Click the **Clear Filter** link beside each filter that is displayed in the **Current Search Parameters** pane.
4. Double-click the group that you want to view.
5. To view a list of local destination IP addresses for the source IP address, click **Destinations** on the Source page toolbar.
6. To view a list of offenses that are associated with this source IP address, click **Offenses** on the Source page toolbar.
7. Double-click the offense that you want to view.
8. On the Offense Summary page, review the offense details. See Offense parameters.
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 that are grouped by local destination IP addresses.

About this task

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

Procedure

1. Click the **Offenses** tab.
2. Click **By Destination IP**.
3. You can refine the list of offenses that use the following options:
   - From the **View Offenses** list box, select an option to filter the list of offenses for a specific time frame.
   - Click the **Clear Filter** link beside each filter that is displayed in the **Current Search Parameters** pane.
4. Double-click the destination IP address that you want to view.
5. To view a list of offenses that are associated with this destination IP address, click **Offenses** on the Destination page toolbar.
6. To view a list of source IP addresses associated with this destination IP address, click **Sources** on the Destination page toolbar.
7. Double-click the offense that you want to view.
8. On the Offense Summary page, review the offense details. See Offense parameters.
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 that are grouped by network.

About this task

All networks are listed with the highest magnitude first.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **By Network**.
3. Double-click the network that you want view.
4. To view a list of source IP addresses associated with this network, click **Sources** on the Network page toolbar.
5. To view a list of destination IP addresses associated with this network, click **Destinations** on the Network page toolbar.
6. To view a list of offenses that are associated with this network, click **Offenses** on the Network page toolbar.
7. Double-click the offense that you want to view.
8. On the Offense Summary page, review the offense details. See Offense parameters.
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 an offense.

Adding notes

You can add notes to any offense on the **Offenses** tab. Notes can include information that 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 2000 characters.

Procedure

1. Click the **Offenses** tab.
2. Navigate to the offense to which you want to add notes.
3. Double-click the offense.
4. From the **Actions** list box, select **Add Note**.
5. Type the note you want to include for this offense.
6. Click **Add Note**.

Results

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 in the **Flag** column of the **Offenses** list, 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

1. Click the **Offenses** tab.
2. Click **All Offenses**.
3. Select the offense that you want to hide.
4. From the **Actions** list box, select **Hide**.
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

1. Click the **Offenses** tab.
2. Click **All Offenses**.
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**.
4. Locate and select the hidden offense that you want to show.
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 elapses. The default offense retention period is three days. If more 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 if 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 that is entered for the previous offense closing. Notes® must not exceed 2,000 characters. This note displays 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

1. Click the **Offenses** tab.
2. Click **All Offenses**.
3. Choose one of the following options:
   - Select the offense that you want to close, and then select **Close** from the **Actions** list box.
   - From the **Actions** list box, select **Close Listed**.
4. From the **Reason for Closing** list box, select a reason. The default reason is **non-issue**.

5. Optional. In the **Notes** field, type a note to provide more information about closing the note.
6. Click **OK**.

Results

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 elapses.

About this task

Offenses are retained for a configurable retention period. The default retention period is three 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 elapses.

For more information about the Offense Retention Period, see the *IBM Security QRadar SIEM Administration Guide*.

CAUTION:
When the SIM data model is reset from 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.

Procedure

1. Click the **Offenses** tab.
2. Click **All Offenses**.
3. Choose one of the following options:
   - Select the offense that you want to protect, and then select **Protect** from the **Actions** list box.
   - From the **Actions** list box, select **Protect Listed**.
4. Click **OK**.

Results

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

Unprotecting offenses

You can unprotect offenses that were 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 that all other options are selected under the **Excludes option** list on the Search Parameters pane, only protected offenses are displayed.

Procedure

1. Click the **Offenses** tab.
2. Click **All Offenses**.
3. Optional. Perform a search that displays only protected offenses.
4. Choose one of the following options:
   - Select the offense that you want to protect, and then select **Unprotect** from the Actions list box.
   - From the **Actions** list box, select **Unprotect Listed**.
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 reuse or store your offense data, you can export offenses. For example, you can export offenses to create non QRadar product based reports. You can 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 that are specified in the Column Definition pane of your search parameters. The length of time that is required to export your data depends on the number of parameters specified.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **All Offenses**.
3. Select the offense that you want to export.
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
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.
6. Click **OK**.

Assigning offenses to users

Using the **Offenses** tab, you can assign offenses to 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.

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.

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

Procedure

1. Click the **Offenses** tab.
2. Click **All Offenses**.
3. Select the offense that you want to assign.
4. From the **Actions** list box, select **Assign**.
5. From the **Username** list box, select the user that you want to assign this offense to.
6. Click **Save**.

Results

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 that contains 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 user interface
- Contributing CRE rules

Procedure

1. Click the **Offenses** tab.
2. Navigate to the offense for which you want to send an email notification.
3. Double-click the offense.
4. From the **Actions** list box, select **Email**.
5. Configure the following parameters:

Option	Description
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 that you want to accompany the notification email.

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 will allow you to track a particular item for further investigation.

Procedure

1. Click the **Offenses** tab.
2. Navigate to the offense you want to mark for follow-up.
3. Double-click the offense.
4. From the **Actions** list box, select **Follow up**.

Results

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.

Table 13. 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

Table 13. Offense tab toolbar functions (continued)

Function	Description
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. • **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
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. • **Time** - Specifies the date and time when the annotation was created.
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.

Table 13. Offense tab toolbar functions (continued)

Function	Description
Categories	Click **Categories** to view category information for the offense. To further investigate the events that are 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.
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 User 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.
Destination	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 that is 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.
Flows	Click **Flows** to further investigate the flows that are associated with an offense. When you click **Flows**, the flow search results are displayed.
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

Table 13. Offense tab toolbar functions (continued)

Function	Description
Offenses	Click **Offenses** to view a list of offenses that are associated with a 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 start the Edit Rules page. If the rule was 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 IP's 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 that 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**.
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**.

Table 13. Offense tab toolbar functions (continued)

Function	Description
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 that are 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 User 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 User Guide*.

Offense parameters

This table provides descriptions of parameters that are provided on the Offenses tab.

Table 14. 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.
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.

Table 14. Offense parameters (continued)

Parameter	**Location**	**Description**
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 that is associated with the flow.
Application Name	Offense Source table, if the Offense Type is App ID	Specifies the application that is 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 that is 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 by 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 by using the Asset Profile function. For more information, see Asset management.
Assigned to	Offense table	Specifies the user that is 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.
Chained	• Offense Source table, if the Offense Type is Destination IP • Top 5 Destination IP's 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that are applied to the search results. To clear these search parameters, click **Clear Filter**. **Note:** This parameter is only displayed after you apply a filter.
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 IP's 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.
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 more details.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that is 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.
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.
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 event name, as identified in the QID map, which is 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Event/Flow Count	Destination page Network page	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 that are 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 that are 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 version 7.1.0 (MR1) of your QRadar product. Therefore, flows cannot be counted. You can, however, click the N/A link to investigate the associated flows in the flow search results.
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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Event/Flow Count	Destination page Network page	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 that are 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 that are 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 version 7.1.0 (MR1) of your QRadar product. Therefore, flows cannot be counted. You can, however, click the N/A link to investigate the associated flows in the flow search results.
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 14. 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 that are 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 14. 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 that is 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 added notes to the offense. Notes can include any information that you want to capture for the offense. For example, you can 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. Point your mouse over the icon to display more information.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Flag (continued)		- Inactive Offense - Indicates 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 product 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.
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 that is taken on the source IP address, destination IP address, or network. For example, if a flag is displayed, the offense is flagged for follow-up. Point your mouse over the icon to display more 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 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that is associated with the source or destination IP address. If no host name is identified, this field specifies Unknown.
Historical Correlation Profile Name	• Offense summary	Specifies the name of the historical correlation profile that created the offense.
Historical Correlation catalog	• Offense summary	Specifies the historical correlation catalog that contains the events that triggered the offense. To see all events in the catalog, click **View History** on the Historical Correlation window.
Historical Correlation Profile ID	• Offense summary	Specifies the unique identifier of the historical correlation profile that created the offense.
Host Name	Offense Source table, if the Offense Type is Hostname	Specifies the host name that is associated with the flow that created the offense.
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 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 that is associated with the event or flow that created the offense.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that is associated with the event or flow that created the offense.
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 that is 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 associated, the value for this field is Unknown. **Note:** This field does not display historical information.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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.
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 that is 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Local Destination(s)	Source Details page	Specifies the local destination IP addresses associated with the source IP address. To view more 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.
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, which is associated with the event that created the offense. **Note:** The information that is 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 *Managing Log Sources 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 that are associated with the offense. If more than 1 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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.
MAC Address	Offense Source table, if the Offense Type is Source MAC Address or Destination MAC Address	Specifies the MAC address that is 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that is associated with the IP address. Point your mouse over the magnitude bar to display the calculated magnitude.
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 1 destination network, this field displays the network leaf. Click the link to view the network information. If the offense has more than 1destination network, the term Multiple is displayed. Click the link to view more details.
Notes	• Offense Source table, if the Offense Type is Rule • Last 5 Notes table	Specifies the notes for the rule.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that is 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 14. Offense parameters (continued)

Parameter	Location	Description
Offense Type	• 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 that are 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 that are associated with the source or destination IP address. To view more 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 that are launched from the network. If multiple offenses are responsible, this field specifies Multiple and the number of offenses.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Offense(s) Targeted	Network page	Specifies the offenses that are targeted for the network. If multiple offenses are responsible, this field specifies Multiple and the number of offenses
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 that are 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 that are originated from the network.
Offenses Targeted	By Network Details page	Specifies the number of offenses that are targeted for the network.
Port	Offense Source table, if the Offense Type is Source Port or Destination Port	Specifies the port that is 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.
Rule Description	Offense Source table, if the Offense Type is Rule	Specifies the summary of the rule parameters.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Rule Name	Offense Source table, if the Offense Type is Rule	Specifies the name of the rule that is associated with the event or flow that created the offense. **Note:** The information that is displayed for rule offenses is derived from the **Rules** tab.
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 more details. For more information about source IP addresses, see Monitoring offenses grouped by source IP.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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.
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 that is associated with the destination IP address or network. To view more 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that is associated with the offense.
Status	Offense Source table, if the Offense Type is Log Source	Specifies the status of the log source.

Table 14. Offense parameters (continued)

Parameter	Location	Description
Status	Offense table	Displays icons to indicate the status of an offense. Status icons include: **Inactive Offense**. An offense becomes inactive after five days have elapsed since the offense received the last event. All offenses become inactive after upgrading your QRadar product 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 protect, flag for follow up, add notes, and assign to users to an inactive offense. A **Hidden Offense** flag on the on the All Offenses page indicates that the offense is hidden from view . If you search for hidden offenses, they are visible only on the All Offenses page where they are flagged as a hidden offense. For more information, see Hiding offenses. **User** indicates that the offense is assigned to a user. When an offense is assigned to a user, the offense is displayed on the My Offenses page that belongs to that user. For more information, see Assigning offenses to users. **Protect** prevents specified offenses from being removed from the database after the retention period elapses. For more information, see Protecting offenses. **Closed Offense** indicates that the offense is closed. For more information, see Closing offenses.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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.
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 that is 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 that is 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 that is associated with the most recent user name information from the Assets tab instead of the username that is associated with the event or flow that created the offense.
Username	Last 5 Notes table	Specifies the user who created the note.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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 that are 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 that are based on a time range. From the list box, select the time range that you want to filter by.
Vulnerabilities	Offense Source table, if the Offense Type is Source IP or Destination IP	Specifies the number of identified vulnerabilities that are 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.

Table 14. Offense parameters (continued)

Parameter	Location	Description
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.

Chapter 5. Log activity investigation

You can monitor and investigate events in real time or perform advanced searches.

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.

Log activity tab toolbar

You can access several options from the Log Activity toolbar

Using the toolbar, you can access the following options:

Table 15. Log Activity 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.
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.
Cancel	Click **Cancel** to cancel a search in progress. This option is disabled in streaming mode.

Table 15. Log Activity toolbar options (continued)

Option	Description
False Positive	Click **False Positive** to open the False Positive Tuning window, which will allow you to tune out events that are known to be false positives from creating offenses. 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. 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. **Note:** The anomaly detection rule options are only visible if you have the **Log Activity** > **Maintain Custom Rules** permission. • **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 that is collected QRadar. For example, if you create a threshold rule indicating that no more than 220 clients can log in to the server between 8 am and 5 pm, the rules generate an alert when the 221st client attempts to log in. When you select the **Add Threshold Rule** option, the Rules wizard is displayed, prepopulated with the appropriate options for creating a threshold rule.

Table 15. Log Activity toolbar options (continued)

Option	Description
Rules (continued)	- **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. - **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.

Table 15. Log Activity toolbar options (continued)

Option	Description
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 that are 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.
Search toolbar	**Advanced Search** Select **Advanced Search** from the list box to enter an Ariel Query Language (AQL) search string to specify the fields that you want returned. **Quick Filter** Select Quick Filter from the list box to search payloads by using simple words or phrases.

Table 15. Log Activity toolbar options (continued)

Option	Description
View	The default view on the **Log Activity** tab is a stream of real-time events. The **View** list contains options to also view events from specified time periods. After you choose a specified time period from the **View** list, you can then modify the displayed time period by changing the date and time values in the **Start Time** and **End Time** fields.

Right-click menu options

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

The right-click menu options are:

Table 16. 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 will allow 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.
Quick Filter	Filter items that match, or do not match the selection.

Status bar

When streaming events, the status bar displays the average number of results that are 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 more status information, move your mouse pointer over the status bar.

When events are not being streamed, the status bar displays the number of search results that are currently displayed on the tab and the amount of time that is 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 by 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 will enable you to view event data that enters 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 the streaming is paused, the last 1,000 events are displayed.

Procedure

1. Click the **Log Activity** tab.
2. From the **View** list box, select **Real Time (streaming)**. For information about the toolbar options, see Table 4-1. For more information about the parameters that are displayed in streaming mode, see Table 4-7.
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

Events are collected in raw format, and then normalized for display on the **Log Activity** tab.

About this task

Normalization involves parsing raw event data and preparing the data to display readable information about the tab. When events are normalized, the system normalizes the 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 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 17. Log Activity tab - Default (Normalized) parameters

Parameter	**Description**
Current Filters	The top of the table displays the details of the filters that are 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 that 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 that represent the records that are 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 Chart management. **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.

Table 17. Log Activity tab - Default (Normalized) parameters (continued)

Parameter	**Description**
Offenses icon	Click this icon to view details of the offense that is associated with this event. For more information, see Chart management. **Note:** Depending on your product, this icon is might not be available. You must have IBM Security QRadar SIEM.
Start Time	Specifies the time of the first event, as reported to QRadar by the log source.
Event Name	Specifies the normalized name of the event.
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events that are 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 time.
Time	Specifies the date and time when QRadar received the event.
Low Level Category	Specifies the low-level category that is 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 that is 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.

Procedure

1. Click the **Log Activity** tab.
2. From the **Display** list box, select **Default (Normalized)**.
3. From the **View** list box, select the time frame that you want to display.
4. Click the **Pause** icon to pause streaming.

5. Double-click the event that you want to view in greater detail. For more information, 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 18. Raw Event parameters

Parameter	**Description**
Current Filters	The top of the table displays the details of the filters that are 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 that 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.

Table 18. Raw Event parameters (continued)

Parameter	Description
Charts	Displays configurable charts that represent the records that are 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. **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 that is associated with this event.
Start Time	Specifies the time of the first event, as reported to QRadar by the log source.
Log Source	Specifies the log source that originated the event. If there are multiple log sources that are 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

1. Click the **Log Activity** tab.
2. From the **Display** list box, select **Raw Events**.
3. From the **View** list box, select the time frame that you want to display.
4. Double-click the event that you want to view in greater detail. See Event details.

Viewing grouped events

Using the **Log Activity** tab, you can view events that are 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 by using non-grouped search criteria, this option is displayed.

The Display list box provides the following options:

Table 19. Grouped events options

Group option	Description
Low Level Category	Displays a summarized list of events that are 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 that are grouped by the normalized name of the event.
Destination IP	Displays a summarized list of events that are grouped by the destination IP address of the event.
Destination Port	Displays a summarized list of events that are grouped by the destination port address of the event.
Source IP	Displays a summarized list of events that are grouped by the source IP address of the event.
Custom Rule	Displays a summarized list of events that are grouped by the associated custom rule.
Username	Displays a summarized list of events that are grouped by the user name that is associated with the events.
Log Source	Displays a summarized list of events that are grouped by the log sources that sent the event to QRadar.
High Level Category	Displays a summarized list of events that are grouped by the high-level category of the event.
Network	Displays a summarized list of events that are grouped by the network that is associated with the event.
Source Port	Displays a summarized list of events that are 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 20. 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 that is applied to the search results. To clear these filter values, click **Clear Filter**.

Table 20. Grouped event parameters (continued)

Parameter	Description
View	From the list box, select the time range that 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 20. Grouped event parameters (continued)

Parameter	Description
Charts	Displays configurable charts that represent the records that are 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. • 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. **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 that is associated with this event. If there are multiple IP addresses that are 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 that is associated with this event. If there are multiple IP addresses that are associated with this event, this field specifies the term Multiple and the number of IP addresses.
Destination Port (Unique Count)	Specifies the destination ports that are associated with this event. If there are multiple ports that are associated with this event, this field specifies the term Multiple and the number of ports.
Event Name	Specifies the normalized name of the event.

Table 20. Grouped event parameters (continued)

Parameter	Description
Log Source (Unique Count)	Specifies the log sources that sent the event to QRadar. If there are multiple log sources that are 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 that are 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 Log Manager Administration Guide*.
Low Level Category (Unique Count)	Specifies the low-level category of this event. If there are multiple categories that are associated with this event, this field specifies the term Multiple and the number of categories.
Protocol (Unique Count)	Specifies the protocol ID associated with this event. If there are multiple protocols that are associated with this event, this field specifies the term Multiple and the number of protocol IDs.
Username (Unique Count)	Specifies the user name that is associated with this event, if available. If there are multiple user names that are 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 that are 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 that are 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 time.
Count	Specifies the total number of normalized events in this event group.

Procedure

1. Click the **Log Activity** tab.
2. From the **View** list box, select the time frame that you want to display.
3. From the Display list box, choose which parameter you want to group events on. See Table 2.The events groups are listed. For more information about the event group details. See Table 1.
4. To view the List of Events page for a group, double-click the event group that you want to investigate. The List of Events page does not retain chart configurations that you might have defined on the **Log Activity** tab. For more information about the List of Events page parameters, see Table 1.

5. To view the details of an event, double-click the event that you want to investigate. For more information about event details, see Table 2.

Event details

You can view a list of events 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 21. Event details

Parameter	Description
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 that is 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 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. 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.

Table 21. Event details (continued)

Parameter	Description
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
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.
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.

Table 21. Event details (continued)

Parameter	Description
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 3 tabs to view the payload: • Universal Transformation Format (UTF) - Click UTF. • Hexadecimal - Click HEX. • Base64 - Click Base64.
Additional information	
Protocol	Specifies the protocol that is 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.
Log Source	Specifies the log source that sent the event to QRadar. If there are multiple log sources that are associated with this event, this field specifies the term Multiple and the number of log sources.
Event Count	Specifies the total number of events that are 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 time.
Custom Rules	Specifies custom rules that match this event. .
Custom Rules Partially Matched	Specifies custom rules that partially match this event.
Annotations	Specifies the annotation for this event. Annotations are text descriptions that rules can automatically add to events as part of the rule response.
Identity information - QRadar collects identity information, if available, from log source messages. Identity information provides extra details about assets on your network. Log sources only generate identity information if the log message sent to QRadar 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 that is associated with this event.
Identity IP	Specifies the IP address of the asset that is associated with this event.
Identity Net Bios Name	Specifies the Network Base Input/Output System (Net Bios) name of the asset that is associated with this event.

Table 21. Event details (continued)

Parameter	Description
Identity Extended field	Specifies more information about the asset that is 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 has collected identify information for the asset that is 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 that is associated with this event.
Identity MAC	Specifies the MAC address of the asset that is associated with this event.
Identity Group Name	Specifies the group name of the asset that is associated with this event.

Event details toolbar

The events details toolbar provides several functions for viewing events detail.

The **event details** toolbar provides the following functions:

Table 22. Event details toolbar

Return to Events List	Click **Return** to **Events List** to return to the list of events.
Offense	Click **Offense** to display the offenses that are 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 to prevent false positive events from generating into offenses.
Extract Property	Click **Extract Property** to create a custom event property from the selected event.
Previous	Click **Previous** to view the previous event in the event list.
Next	Click **Next** to view the next event in the event list.

Table 22. Event details toolbar (continued)

PCAP Data	**Note:** This option is only displayed if your QRadar Console is configured to integrate with the Juniper JunOS Platform DSM. For more information about managing PCAP data, see Managing PCAP data. • **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 that is 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*.

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

Procedure

1. Click the **Log Activity** tab.
2. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
3. Click the **Offense** icon beside the event you want to investigate.
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).

Before you begin

This manual action is used to map unknown log source events to known QRadar events so that they can be categorized and processed appropriately.

About this task

For normalization purposes, QRadar 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*.

If events are received from log sources that the system is unable to categorize, then the events are categorized as unknown. These events occur for several reasons, including:

- **User-defined Events** - Some log sources, such as Snort, allows 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 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

1. Click the **Log Activity** tab.
2. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event that you want to map.
4. Click **Map Event**.
5. If you know the QID that you want to map to this event, type the QID in the **Enter QID** field.
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**.
   c. Select the **QID** you want to associate this event with.
7. Click **OK**.

Tuning false positives

You can use the False Positive Tuning function to prevent false positive events from creating offenses.

Before you begin

You can tune false positive events from the event list or event details page.

About this task

You can tune false positive events from the event list or event details page.

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

1. Click the **Log Activity** tab.
2. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
3. Select the event that you want to tune.
4. Click **False Positive**.
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>
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
7. Click **Tune**.

PCAP data

If your QRadar Console is configured to integrate with the Juniper JunOS Platform DSM, then Packet Capture (PCAP) can be received, processed, data can be stored 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 *Managing Log Sources 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

1. Click the **Log Activity** tab.
2. From the **Search** list box, select **New Search**.
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**.
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.
5. Click **Filter**.
6. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
7. Double-click the event that 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 a readable version of the data in the PCAP file or download the PCAP file to your desktop system.

Before you begin

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

About this task

Before PCAP data can be displayed, the PCAP file must be retrieved for display on the user interface. If the download process takes an extended period, 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 that is displayed on the window, or download the information to your desktop system

Procedure

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 that you want to investigate, and then select **PCAP Data** > **View PCAP Information** from the event details toolbar.
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
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.
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

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.
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.
3. Click **OK**.

Exporting events

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

Before you begin

The length of time that is required to export your data depends on the number of parameters specified.

Procedure

1. Click the **Log Activity** tab.
2. Optional. If you are viewing events in streaming mode, click the **Pause** icon to pause streaming.
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.
4. If you want to resume your activities while the export is in progress, click **Notify When Done**.

Results

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.

Chapter 6. Network activity investigation

You can use the **Network Activity** tab to monitor and investigate network activity (flows) in real time or conduct advanced searches

Network tab overview

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

You must have permission to view the **Network Activity** tab.

For more information about permissions and assigning roles, see the *IBM Security QRadar SIEM Administration Guide*.

Select the **Network Activity** tab to visually monitor and investigate flow data in real time, or conduct 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

You can access several options from the **Network Activity** tab toolbar.

You can access the following options from the **Network Activity** tab toolbar::

Table 23. Network Activity tab toolbar options

Options	Description
Search	Click **Search** to complete advanced searches on flows. Search 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 23. Network Activity tab toolbar options (continued)

Options	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, 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 23. Network Activity tab toolbar options (continued)

Options	Description
Rules	The **Rules** option is visible only if you have permission to view custom rules. Select one of the following options: **Rules** to view or create a rule. If you have the permission to view rules, the summary page of the Rules wizard is displayed. If you have the permission to maintain custom rules, you can edit the rule. **Note:** The anomaly detection rule options are visible only if you have the **Network Activity** > **Maintain Custom Rules permission**. To enable the anomaly detection rule options, you must save aggregated search criteria. The saved search criteria specifies the required parameters. Select one of the following options **Add Threshold Rule** 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 that is collected. For example, if you create a threshold rule indicating that no more than 220 clients can log in to the server between 8 am and 5 pm, the rules generate an alert when the 221st client attempts to log in. **Add Behavioral Rule** 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. **Add Anomaly Rule** to create an anomaly rule. An anomaly rule tests flow traffic for abnormal activity, such as new or unknown traffic. 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. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

Table 23. Network Activity tab toolbar options (continued)

Options	Description
Actions	Click **Actions** to complete 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 that are 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 you are viewing partial search results.
Search toolbar	**Advanced search** Select **Advanced Search** from the list box and then enter an Ariel Query Language (AQL) search string to specify the fields that you want returned. **Quick filter** Select **Quick Filter** from the list box to search payloads by using simple words or phrases.
View	The default view on the **Network Activity** tab is a stream of real-time events. The **View** list contains options to also view events from specified time periods. After you choose a specified time period from the **View** list, you can then modify the displayed time period by changing the date and time values in the **Start Time** and **End Time** fields.

Right-click menu options

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

The right-click menu options are:

Table 24. 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.

Table 24. Right-click menu options (continued)

Option	Description
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.
Quick Filter	Filter items that match, or do not match the selection.

Status bar

When streaming flows, the status bar displays the average number of results that are 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 more status information, move your mouse pointer over the status bar.

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

OverFlow records

With administrative permissions, you can specify the maximum number of flows you want to send from the QRadar QFlow Collector to the Event processors.

If you have administrative permissions, you can specify the maximum number of flows you want to send from the QRadar QFlow Collector to the Event processors. All data that is 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

1. Click the **Network Activity** tab.
2. From the View list box, select **Real Time (streaming)**.

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

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

Data flow is collected, normalized and then displayed on the **Network Activity** tab.

About this task

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

Note: If you select 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 25. Parameters for the Network Activity tab

Parameter	Description
Current Filters	The top of the table displays the details of the filters that are applied to the search results. To clear these filter values, click **Clear Filter**. **Note:** This parameter is only displayed after you apply a filter.

Table 25. Parameters for the Network Activity tab (continued)

Parameter	Description
View	From the list box, you can select the time range that 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 that represent the records that are 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 that is associated with this flow.

Table 25. Parameters for the Network Activity tab (continued)

Parameter	Description
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 that performs 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 flow is received.
Storage time	Specifies the time that the flow is stored in the QRadar 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 that are sent from the source host.
Destination Packets	Specifies the total number of packets that are sent from the destination host.
Total Packets	Specifies the total number of packets that are associated with the flow.
Protocol	Specifies the protocol that is 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*.
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.

Table 25. Parameters for the Network Activity tab (continued)

Parameter	Description
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.
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

1. Click the **Network Activity** tab.
2. From the **Display** list box, select **Default (Normalized)**.
3. From the **View** list box, select the time frame that you want to display.
4. Click the **Pause** icon to pause streaming.
5. Double-click the flow that you want to view in greater detail. See Flow details.

Viewing grouped flows

Using the **Network Activity** tab, you can view flows that are 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 26. Grouped flow options

Group option	**Description**
Source or Destination IP	Displays a summarized list of flows that are grouped by the IP address that is associated with the flow.
Source IP	Displays a summarized list of flows that are grouped by the source IP address of the flow.
Destination IP	Displays a summarized list of flows that are grouped by the destination IP address of the flow.
Source Port	Displays a summarized list of flows that are grouped by the source port of the flow.
Destination Port	Displays a summarized list of flows that are grouped by the destination port of the flow.
Source Network	Displays a summarized list of flows that are grouped by the source network of the flow.
Destination Network	Displays a summarized list of flows that are grouped by the destination network of the flow.
Application	Displays a summarized list of flows that are grouped by the application that originated the flow.
Geographic	Displays a summarized list of flows that are grouped by geographic location.
Protocol	Displays a summarized list of flows that are grouped by the protocol that is associated with the flow.
Flow Bias	Displays a summarized list of flows that are grouped by the flow direction.
ICMP Type	Displays a summarized list of flows that are 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 a flow group. The **Network Activity** tab provides the following information for each flow group.

Table 27. Grouped flow parameters

Header	**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 that is applied to the search results. To clear these filter values, click **Clear Filter**.
View	From the list box, select the time range that you want to filter for.

Table 27. Grouped flow parameters (continued)

Header	Description
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 that are 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.
Destination Port (Unique Count)	Specifies the destination port of the flow. If there are multiple destination ports that are associated with this flow, this field specifies the term Multiple and the number of ports.

Table 27. Grouped flow parameters (continued)

Header	Description
Source Network (Unique Count)	Specifies the source network of the flow. If there are multiple source networks that are 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 that are 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 that are 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.
Source Packets (Sum)	Specifies the number of packets from the source.
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 that are associated with the flow.
Count	Specifies the number of flows that are sent or received.

Procedure

1. Click the **Network Activity** tab.
2. From the **View** list box, select the time frame that you want to display.
3. From the **Display** list box, choose which parameter you want to group flows on. See Table 2. The flow groups are listed. For more information about the flow group details. See Table 1.
4. To view the List of Flows page for a group, double-click the flow group that you want to investigate. The List of Flows page does not retain chart configurations that you might have defined on the **Network Activity** tab. For more information about the List of Flows parameters, see Table 2.
5. To view the details of a flow, double-click the flow that you want to investigate. For more information about the flow details page, see Table 1.

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 28. Flow details

Parameter	Description
Flow information	
Protocol	Specifies the protocol that is 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 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 by the flow source.
Storage Time	Specifies the time that the flow was stored in the QRadar 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.

Table 28. Flow details (continued)

Parameter	**Description**
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.
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 3 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, `MN_TTL=x`

Table 28. Flow details (continued)

Parameter	**Description**
Destination Payload	Specifies destination payload content from the flow. This field offers 3 formats to view the payload: • Universal Transformation Format (UTF) - Click **UTF**. • Hexidecimal - Click **HEX**. • Base64 - Click **Base64**.
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.
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.

Flow details toolbar

The flow details toolbar provides various functions.

The flow details toolbar provides the following functions

Table 29. Description of the flow details toolbar

Function	Description
Return to Results	Click **Return to Results** to return to the list of flows.
Extract Property	Click **Extract Property** to create a custom flow property from the selected flow. For more information, see Custom event and flow properties.
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 flow list.
Next	Click **Next** to view the next flow in the flow list.
Print	Click **Print** to print the flow details.
Offense	If **Offense** is available, click to view the Offense Summary page.

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

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

You must have appropriate permissions for creating customized rules to tune false positives. For more information about false positives, see the Glossary.

Procedure

1. Click the **Network Activity** tab.
2. Optional. If you are viewing flows in streaming mode, click the **Pause** icon to pause streaming.
3. Select the flow that you want to tune.
4. Click **False Positive**.
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>
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

7. Click **Tune**.

Exporting flows

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

Procedure

1. Click the **Network Activity** tab.
2. Optional. If you are viewing flows in streaming mode, click the **Pause** icon to pause streaming.
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.
4. If you want to resume your activities, click **Notify When Done**.

Results

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.

Chapter 7. Asset Management

Collecting and viewing asset data helps you to identify threats and vulnerabilities. An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network.

Restriction: QRadar Log Manager only tracks asset data if QRadar Vulnerability Manager is installed. For more information about the differences between IBM Security QRadar SIEM and IBM Security QRadar Log Manager, see “Capabilities in your security intelligence product” on page 5.

Asset data

An *asset* is any network endpoint that sends or receives data across your network infrastructure. For example, notebooks, servers, virtual machines, and handheld devices are all assets. Every asset in the asset database is assigned a unique identifier so that it can be distinguished from other asset records.

Detecting devices is also useful in building a data set of historical information about the asset. Tracking asset information as it changes helps you monitor asset usage across your network.

Asset profiles

An *asset profile* is a collection of all information that IBM Security QRadar SIEM collected over time about a specific asset. The profile includes information about the services that are running on the asset and any identity information that is known.

QRadar SIEM automatically creates asset profiles from identity events and bidirectional flow data or, if they are configured, vulnerability assessment scans. The data is correlated through a process that is called *asset reconciliation* and the profile is updated as new information comes into QRadar. The asset name is derived from the information in the asset update in the following order of precedence:

- Given name
- NETBios host name
- DNS host name
- IP address

Collecting asset data

Asset profiles are built dynamically from identity information that is passively absorbed from event or flow data, or from data that QRadar actively looks for during a vulnerability scan. You can also import asset data or edit the asset profile manually.

Sources of asset data

Asset data is received from several different sources in your IBM Security QRadar deployment.

Asset data is written to the asset database incrementally, usually two or three pieces of data at a time. With exception of updates from network vulnerability scanners, each asset update contains information about only one asset at a time.

Asset data usually comes from one of the following asset data sources:

Events

Event payloads, such as those created by DHCP or authentication servers, often contain user logins, IP addresses, host names, MAC addresses, and other asset information. This data is immediately provided to the asset database to help determine which asset the asset update applies to.

Events are the primary cause for asset growth deviations.

Flows

Flow payloads contain communication information such as IP address, port, and protocol that is collected over regular, configurable intervals. At the end of each interval, the data is provided to the asset database, one IP address at a time.

Because asset data from flows is paired with an asset based on a single identifier, the IP address, flow data is never the cause of asset growth deviations.

Vulnerability scanners

QRadar integrates with both IBM and third-party vulnerability scanners that can provide asset data such as operating system, installed software, and patch information. The type of data varies from scanner to scanner, and can vary from scan to scan. As new assets, port information, and vulnerabilities are discovered, data is brought into the asset profile based on the CIDR ranges that are defined in the scan.

It is possible for scanners to introduce asset growth deviations, but it is rare.

User interface

Users who have the Assets role can import or provide asset information directly to the asset database. Asset updates that are provided directly by a user are for a specific asset, and therefore the asset reconciliation stage is bypassed.

Asset updates that are provided by users do not introduce asset growth deviations.

Domain-aware asset data

When an asset data source is configured with domain information, all asset data that comes from that data source is automatically tagged with the same domain. Because the data in the asset model is domain-aware, the domain information is applied to all QRadar components, including identities, offenses, asset profiles, and server discovery.

When you view the asset profile, some fields might be blank. Blank fields exist when the system did not receive this information in an asset update, or the information exceeded the asset retention period. The default retention period is 120 days. An IP address that appears as 0.0.0.0 indicates that the asset does not contain IP address information.

Workflow for incoming asset data

This workflow describes how QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

1. QRadar receives the event. The asset profiler examines the event payload for identity information.
2. If the identity information includes a MAC address, NetBIOS host names, or DNS host name that are already associated with an asset in the asset database, that asset is updated with any new information.
3. If the only available identity information is an IP address, the system reconciles the update to the existing asset that has the same IP address.
4. If an asset update includes an IP address that matches an existing asset, but also includes more identity information that does not match the existing asset, the system uses other information to rule out a false-positive match before the existing asset is updated.
5. If the identity information does not match an existing asset in the database, a new asset is created based on the information in the event payload.

Updates to asset data

IBM Security QRadar uses identity information in an event payload to determine whether to create a new asset or update an existing asset.

Each asset update must contain trusted information about a single asset. When QRadar receives an asset update, the system determines which asset the update applies to.

Asset reconciliation is the process of determining the relationship between asset updates and the related asset in the asset database. Asset reconciliation occurs after QRadar receives the update but before the information is written to the asset database.

Identity information

Every asset must contain at least one piece of identity data. Subsequent updates that contain one or more pieces of that same identity data are reconciled with the asset that owns that data. Updates that are based on IP addresses are handled carefully to avoid false-positive asset matches. False-positive asset matches occur when one physical asset is assigned ownership of an IP address that was previously owned by another asset in the system.

When multiple pieces of identity data are provided, the asset profiler prioritizes the information in the following order:

- MAC address (most deterministic)
- NetBIOS host name
- DNS host name
- IP address (least deterministic)

MAC addresses, NetBIOS host names, and DNS host names must be unique and therefore are considered as definitive identity data. Incoming updates that match an existing asset only by the IP address are handled differently than updates that match more definitive identity data.

Related concepts:

"Asset reconciliation exclusion rules"
With each asset update that enters IBM Security QRadar, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

Asset reconciliation exclusion rules

With each asset update that enters IBM Security QRadar, the asset reconciliation exclusion rules apply tests to the MAC address, NetBIOS host name, DNS host name, and IP address in the asset update.

By default, each piece of asset data is tracked over a two-hour period. If any one piece of identity data in the asset update exhibits suspicious behavior two or more times within 2 hours, that piece of data is added to the asset blacklists. There is a separate blacklist for each type of identity asset data that is tested.

In domain-aware environments, the asset reconciliation exclusion rules track the behavior of asset data separately for each domain.

The asset reconciliation exclusion rules test the following scenarios:

Table 30. Rule tests and responses

Scenario	Rule response
When a MAC address is associated to three or more different IP addresses in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When a DNS host name is associated to three or more different IP addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a NetBIOS host name is associated to three or more different IP addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different MAC addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a DNS host name is associated to three or more different MAC addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When an IPv4 address is associated to three or more different DNS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different DNS host names in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a MAC address is associated to three or more different DNS host names in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When an IPv4 address is associated to three or more different NetBIOS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist

Table 30. Rule tests and responses (continued)

Scenario	Rule response
When a DNS host name is associated to three or more different NetBIOS host names in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a MAC address is associated to three or more different NetBIOS host names in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist

You can view these rules on the **Offenses** tab by clicking **Rules** and then selecting the **asset reconciliation exclusion** group in the drop-down list.

Related concepts:

"Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist"
You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

Example: Asset exclusion rules that are tuned to exclude IP addresses from the blacklist

You can exclude IP addresses from being blacklisted by tuning the asset exclusion rules.

As the Network security administrator, you manage a corporate network that includes a public wifi network segment where IP address leases are typically short and frequent. The assets on this segment of the network tend to be transient, primarily notebooks and hand-held devices that log in and out of the public wifi frequently. Commonly, a single IP address is used multiple times by different devices over a short time.

In the rest of your deployment, you have a carefully managed network that consists only of inventoried, well-named company devices. IP address leases are much longer in this part of the network, and IP addresses are accessed by authentication only. On this network segment, you want to know immediately when there are any asset growth deviations and you want to keep the default settings for the asset reconciliation exclusion rules.

Blacklisting IP addresses

In this environment, the default asset reconciliation exclusion rules inadvertently blacklist the entire network in a short time.

Your security team finds the asset-related notifications that are generated by the wifi segment are a nuisance. You want to prevent the wifi from triggering any more deviating asset growth notifications.

Tuning asset reconciliation rules to ignore some asset updates

You review the **Asset deviation by log source** report in the last system notification. You determine that the blacklisted data is coming from the DHCP server on your wifi.

The values in the **Event Count** column, **Flow Count** column and the **Offenses** column for the row corresponding to the **AssetExclusion: Exclude IP By MAC Address** rule indicate that your wifi DHCP server is triggering this rule.

You add a test to the existing asset reconciliation exclusion rules to stop rules from adding wifi data to the blacklist.

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

The updated rule tests only the events from the log sources that are not on your wifi DHCP server. To prevent wifi DHCP events from undergoing more expensive reference set and behavior analysis tests, you also moved this test to the top of the test stack

Asset merging

Asset merging is the process where the information for one asset is combined with the information for another asset under the premise that they are actually the same physical asset.

Asset merging occurs when an asset update contains identity data that matches two different asset profiles. For example, a single update that contains a NetBIOS host name that matches one asset profile and a MAC address that matches a different asset profile might trigger an asset merge.

Some systems can cause high volumes of asset merging because they have asset data sources that inadvertently combine identity information from two different physical assets into a single asset update. Some examples of these systems include the following environments:

- Central syslog servers that act as an event proxy
- Virtual machines
- Automated installation environments
- Non-unique host names, common with assets like iPads and iPhones.
- Virtual private networks that have shared MAC addresses
- Log source extensions where the identity field is `OverrideAndAlwaysSend=true`

Assets that have many IP addresses, MAC addresses, or host names show deviations in asset growth and can trigger system notifications.

Related concepts:

"Identification of asset growth deviations" on page 121
Sometimes, asset data sources produce updates that IBM Security QRadar cannot handle properly without manual remediation. Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.

Identification of asset growth deviations

Sometimes, asset data sources produce updates that IBM Security QRadar cannot handle properly without manual remediation. Depending on the cause of the abnormal asset growth, you can either fix the asset data source that is causing the problem or you can block asset updates that come from that data source.

Asset growth deviations occur when the number of asset updates for a single device grows beyond the limit that is set by the retention threshold for a specific type of the identity information. Proper handling of asset growth deviations is critical to maintaining an accurate asset model.

At the root of every asset growth deviation is an asset data source whose data is untrustworthy for updating the asset model. When a potential asset growth deviation is identified, you must look at the source of the information to determine whether there is a reasonable explanation for the asset to accumulate large amounts of identity data. The cause of an asset growth deviation is specific to an environment.

DHCP server example of unnatural asset growth in an asset profile

Consider a virtual private network (VPN) server in a Dynamic Host Configuration Protocol (DHCP) network. The VPN server is configured to assign IP addresses to incoming VPN clients by proxying DHCP requests on behalf of the client to the network's DHCP server.

From the perspective of the DHCP server, the same MAC address repeatedly requests many IP address assignments. In the context of network operations, the VPN server is delegating the IP addresses to the clients, but the DHCP server can't distinguish when a request is made by one asset on behalf of another.

The DHCP server log, which is configured as a QRadar log source, generates a DHCP acknowledgment (DHCP ACK) event that associates the MAC address of the VPN server with the IP address that it assigned to the VPN client. When asset reconciliation occurs, the system reconciles this event by MAC address, which results in a single existing asset that grows by one IP address for every DHCP ACK event that is parsed.

Eventually, one asset profile contains every IP address that was allocated to the VPN server. This asset growth deviation is caused by asset updates that contain information about more than one asset.

Threshold settings

When an asset in the database reaches a specific number of properties, such as multiple IP addresses or MAC addresses, QRadar blocks that asset from receiving more updates.

The Asset Profiler threshold settings specify the conditions under which an asset is blocked from updates. The asset is updated normally up to the threshold value. When the system collects enough data to exceed the threshold, the asset shows an asset growth deviation. Future updates to the asset are blocked until the growth deviation is rectified.

System notifications that indicate asset growth deviations

IBM Security QRadar generates system notifications to help you identify and manage the asset growth deviations in your environment.

The following system messages indicate that QRadar identified potential asset growth deviations:

- `The system detected asset profiles that exceed the normal size threshold`
- `The asset blacklist rules have added new asset data to the asset blacklists`

The system notification messages include links to reports to help you identify the assets that have growth deviations.

Asset data that changes frequently

Asset growth can be caused by large volumes of asset data that changes legitimately, such as in these situations:

- A mobile device that travels from office-to-office frequently and is assigned a new IP address whenever it logs in.
- A device that connects to a public wifi with short IP addresses leases, such as at a university campus, might collect large volumes of asset data over a semester.

Example: How configuration errors for log source extensions can cause asset growth deviations

Customized log source extensions that are improperly configured can cause asset growth deviations.

You configure a customized log source extension to provide asset updates to QRadar by parsing user names from the event payload that is on a central log server. You configure the log source extension to override the event host name property so that the asset updates that are generated by the custom log source always specify the DNS host name of the central log server.

Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.

Troubleshooting asset profiles that exceed the normal size threshold

IBM Security QRadar generates the following system notification when the accumulation of data under a single asset exceeds the configured threshold limits for identity data.

```
The system detected asset profiles that exceed the normal size threshold
```

Explanation

The payload of the notification shows a list of the top five most frequently deviating assets and why the system marked each asset as a growth deviation. As shown in the following example, the payload also shows the number of times that the asset attempted to grow beyond the asset size threshold.

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

When the asset data exceeds the configured threshold, QRadar blocks the asset from future updates. This intervention prevents the system from receiving more corrupted data and mitigates the performance impacts that might occur if the system attempts to reconcile incoming updates against an abnormally large asset profile.

Required user action

Use the information in the notification payload to identify the assets that are contributing to the asset growth deviation and determine what is causing the abnormal growth. The notification provides a link to a report of all assets that experienced deviating asset growth over the past 24 hours.

After you resolve the asset growth deviation in your environment, you can run the report again.

1. Click the **Log Activity** tab and click **Search** > **New Search**.
2. Select the **Deviating Asset Growth: Asset Report** saved search.
3. Use the report to identify and repair inaccurate asset data that was created during the deviation.

If the asset data is valid, QRadar administrators can increase the threshold limits for IP addresses, MAC addresses, NetBIOS host names, and DNS host names in the **Asset Profiler Configuration** on the QRadar **Admin** tab.

New asset data is added to the asset blacklists

IBM Security QRadar generates the following system notification when a piece of asset data exhibits behavior that is consistent with deviating asset growth.

```
The asset blacklist rules have added new asset data to the asset blacklists
```

Explanation

Asset exclusion rules monitor asset data for consistency and integrity. The rules track specific pieces of asset data over time to ensure that they are consistently being observed with the same subset of data within a reasonable time.

For example, if an asset update includes both a MAC address and a DNS host name, the MAC address is associated with that DNS host name for a sustained period. Subsequent asset updates that contain that MAC address also contain that same DNS host name when one is included in the asset update. If the MAC address suddenly is associated with a different DNS host name for a short period, the change is monitored. If the MAC address changes again within a short period, the MAC address is flagged as contributing to an instance of deviating or abnormal asset growth.

Required user action

Use the information in the notification payload to identify the rules that are used to monitor asset data. Click the **Asset deviations by log source** link in the notification to see the asset deviations that occurred in the last 24 hours.

If the asset data is valid, QRadar administrators can configure QRadar to resolve the problem.

- If your blacklists are populating too aggressively, you can tune the asset reconciliation exclusion rules that populate them.
- If you want to add the data to the asset database, you can remove the asset data from the blacklist and add it to the corresponding asset whitelist. Adding asset data to the whitelist prevents it from inadvertently reappearing on the blacklist.

Asset blacklists and whitelists

IBM Security QRadar uses a group of asset reconciliation rules to determine if asset data is trustworthy. When asset data is questionable, QRadar uses asset blacklists and whitelists to determine whether to update the asset profiles with the asset data.

An *asset blacklist* is a collection of data that IBM Security QRadar considers untrustworthy. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

Your QRadar administrator can modify the asset blacklist and whitelist data to prevent future asset growth deviations.

Asset blacklists

An *asset blacklist* is a collection of data that IBM Security QRadar considers untrustworthy based on the asset reconciliation exclusion rules. Data in the asset blacklist is likely to contribute to asset growth deviations and QRadar prevents the data from being added to the asset database.

Every asset update in QRadar is compared to the asset blacklists. Blacklisted asset data is applied globally for all domains. If the asset update contains identity information (MAC address, NetBIOS host name, DNS host name, or IP address) that is found on a blacklist, the incoming update is discarded and the asset database is not updated.

The following table shows the reference collection name and type for each type of identity asset data.

Table 31. Reference collection names for asset blacklist data

Type of identity data	Reference collection name	Reference collection type
IP addresses (v4)	Asset Reconciliation IPv4 Blacklist	Reference Set [Set Type: IP]
DNS host names	Asset Reconciliation DNS Blacklist	Reference Set [Set Type: ALNIC*]

Table 31. Reference collection names for asset blacklist data (continued)

Type of identity data	Reference collection name	Reference collection type
NetBIOS host names	Asset Reconciliation NetBIOS Blacklist	Reference Set [Set Type: ALNIC*]
MAC Addresses	Asset Reconciliation MAC Blacklist	Reference Set [Set Type: ALNIC*]
* ALNIC is an alphanumeric type that can accommodate both host name and MAC address values.		

Your QRadar administrator can modify the blacklist entries to ensure that new asset data is handled correctly.

Asset whitelists

You can use asset whitelists to keep IBM Security QRadar asset data from inadvertently reappearing in the asset blacklists.

An *asset whitelist* is a collection of asset data that overrides the asset reconciliation engine logic about which data is added to an asset blacklist. When the system identifies a blacklist match, it checks the whitelist to see whether the value exists. If the asset update matches data that is on the whitelist, the change is reconciled and the asset is updated. Whitelisted asset data is applied globally for all domains.

Your QRadar administrator can modify the whitelist entries to ensure that new asset data is handled correctly.

Example of a whitelist use case

The whitelist is helpful if you have asset data that continues to show up in the blacklists when it is a valid asset update. For example, you might have a round robin DNS load balancer that is configured to rotate across a set of five IP addresses. The Asset Reconciliation Exclusion rules might determine that the multiple IP addresses associated with the same DNS host name are indicative of an asset growth deviation, and the system might add the DNS load balancer to the blacklist. To resolve this problem, you can add the DNS host name to the Asset Reconciliation DNS Whitelist.

Mass entries to the asset whitelist

An accurate asset database makes it easier to connect offenses that are triggered in your system to physical or virtual assets in your network. Ignoring asset deviations by adding mass entries to the asset whitelist is not helpful in building an accurate asset database. Instead of adding mass whitelist entries, review the asset blacklist to determine what is contributing to the deviating asset growth and then determine how to fix it.

Types of asset whitelists

Each type of identity data is kept in a separate whitelist. The following table shows the reference collection name and type for each type of identity asset data.

Table 32. Reference collection name for asset whitelist data

Type of data	Reference collection name	Reference collection type
IP addresses	Asset Reconciliation IPv4 Whitelist	Reference Set [Set Type: IP]

Table 32. Reference collection name for asset whitelist data (continued)

Type of data	Reference collection name	Reference collection type
DNS host names	Asset Reconciliation DNS Whitelist	Reference Set [Set Type: ALNIC*]
NetBIOS host names	Asset Reconciliation NetBIOS Whitelist	Reference Set [Set Type: ALNIC*]
MAC addresses	Asset Reconciliation MAC Whitelist	Reference Set [Set Type: ALNIC*]
* ALNIC is an alphanumeric type that can accommodate host name and MAC address values.		

Assets profile page parameters

You can find Asset profile page parameter descriptions for the Asset Summary pane, Network Interface pane, Vulnerability pane, Services pane, Packages pane, Windows Patches pane, Properties pane, Risk Policies pane, and Products pane.

This reference includes tables that describe the parameters that are displayed in each pane of the **Asset Profile** tab.

Asset profiles

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, then QRadar determines if the asset is vulnerable to this attack by correlating the attack to the asset profile.

Asset profiles are automatically discovered if you have flow data or vulnerability assessment (VA) scans configured. For flow data to populate asset profiles, bidirectional flows are required. Asset profiles can also be automatically created from identity events. 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*.

Vulnerabilities

You can use QRadar Vulnerability Manager and third-party scanners to identify vulnerabilities.

Third-party scanners identify and report discovered vulnerabilities using external references, such as the Open Source Vulnerability Database (OSVDB), National Vulnerability Database (NVDB), and Critical Watch. Examples of third-party scanners include QualysGuard and nCircle ip360. The OSVDB assigns a unique reference identifier (OSVDB ID) to each vulnerability. External references assign a unique reference identifier to each vulnerability. 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 Vulnerability Manager User Guide*.

QRadar Vulnerability Manager is a component that you can purchase separately and enable using a license key. QRadar Vulnerability Manager is a network scanning platform that provides awareness of the vulnerabilities that exist within the applications, systems, or devices on your network. After scans identify vulnerabilities, you can search and review vulnerability data, remediate vulnerabilities, and rerun scans to evaluate the new level of risk.

When QRadar Vulnerability Manager is enabled, you can perform vulnerability assessment tasks on the **Vulnerabilities** tab. From the **Assets** tab, you can run scans on selected assets.

For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*

Assets tab overview

The **Assets** tab provides you with a workspace from which you can manage your network assets and investigate an asset's vulnerabilities, ports, applications, history, and other associations.

Using the **Assets** tab, you can:

- View all the discovered assets.
- Manually add asset profiles.
- Search for specific assets.
- View information about discovered assets.
- Edit asset profiles for manually added or discovered assets.
- Tune false positive vulnerabilities.
- Import assets.
- Print or export asset profiles.
- Discover assets.
- Configure and manage third-party vulnerability scanning.
- Start QRadar Vulnerability Manager scans.

For information about the Server Discovery option in the navigation pane, see the *IBM Security QRadar SIEM Administration Guide*

For more information about the VA Scan option in the navigation pane, see the *IBM Security QRadar Risk Manager User Guide*.

Asset tab list

The Asset Profiles page provides information about ID, IP address, Asset name, Aggregate CVSS score, Vulnerabilities, and Services.

The Asset Profiles page provides the following information about each asset:

Table 33. Asset Profile page parameters

Parameter	Description
ID	Displays the Asset ID number of the asset. The Asset ID number is automatically generated when you add an asset profile manually or when assets are discovered through events, flows, or vulnerability scans.
IP Address	Displays the last known IP address of the asset.

Table 33. Asset Profile page parameters (continued)

Parameter	Description
Asset Name	Displays the given name, NetBios name, DSN name, or MAC address of the asset. If unknown, this field displays the last known IP address. **Note:** These values are displayed in priority order. For example, if the asset does not have a given name, the aggregate NetBios name is displayed. If the asset is automatically discovered, this field is automatically populated, however, you can edit the asset name if required.
Risk Score	Displays the one of the following Common Vulnerability Scoring System (CVSS) scores: • Coalesced aggregate environmental CVSS score • Aggregate temporal CVSS score • Aggregate CVSS base score • These scores are displayed in priority order. For example, if the coalesced aggregate environmental CVSS score is not available, the aggregate temporal CVSS score is displayed. 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. The CVSS score is calculated from the following user-defined parameters: • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement For more information about how to configure these parameters, see “Adding or editing an asset profile” on page 131. For more information about CVSS, see http://www.first.org/cvss/ .
Vulnerabilities	Displays the number of unique vulnerabilities that are discovered on this asset. This value also includes the number of active and passive vulnerabilities.
Services	Displays the number of unique Layer 7 applications that run on this asset.
Last User	Displays the last user associated with the asset.
User Last Seen	Displays the time when the last user associated with the asset was last seen.

Right-click menu options

Right-clicking an asset on the Asset tab displays menus for more event filter information.

On the **Assets** tab, you can right-click an asset to access more event filter information.

Table 34. Right-click menu options

Option	Description
Navigate	The **Navigate** menu provides the following options: • **View by Network** - Displays the List of Networks window, which displays all networks that are associated with the selected IP address. • **View Source Summary** - Displays the List of Offenses window, which displays all offenses that are associated with the selected source IP address. • **View Destination Summary** - Displays the List of Offenses window, which displays all offenses that are associated to the selected destination IP address.
Information	The **Information** menu provides the following options: • **DNS Lookup** - Searches for DNS entries that are based on the IP address. • **WHOIS Lookup** - Searches for the registered owner of a remote IP address. The default WHOIS server is whois.arin.net. • **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. • **Asset Profile** - Displays asset profile information. This menu option is only available when an profile data is acquired actively by a scan or passively by flow sources. • **Search Events** - Select the **Search Events** option to search events that are associated with this IP address. • **Search Flows** - Select the Search Flows option to search for flows that are associated with this IP address.
Run Vulnerability Scan	Select this option to run a Vulnerability Manager scan on the selected asset. This option is displayed only after you install QRadar Vulnerability Manager.

Viewing an asset profile

From the asset list on the **Assets** tab, you can select and view an asset profile. An asset profile provides information about each profile.

About this task

Asset profile information is automatically discovered through Server Discovery or manually configured. You can edit automatically generated asset profile information.

The Asset Profile page provides the information about the asset that is organized into several panes. To view a pane, you can click the arrow **(>)** on the pane to view more detail or select the pane from the **Display** list box on the toolbar.

The Asset Profile page toolbar provides the following functions:

Table 35. Asset Profile page toolbar functions

Options	Description
Return to Asset List	Click this option to return to the asset list.
Display	From the list box, you can select the pane that you want to view on the Asset Profile pane. The Asset Summary and Network Interface Summary panes are always displayed. For more information about the parameters that are displayed in each pane, see Assets profile page parameters.
Edit Asset	Click this option to edit the Asset Profile. See "Adding or editing an asset profile" on page 131.
View by Network	If this asset is associated with an offense, this option will allow you to view the list of networks that are associated with this asset. When you click **View By Network**, the List of Networks window is displayed. See "Monitoring offenses grouped by network" on page 37.
View Source Summary	If this asset is the source of an offense, this option will allow 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" on page 36.
View Destination Summary	If this asset is the destination of an offense, this option will allow 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" on page 36.

Table 35. Asset Profile page 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 event search criteria: You can customize the search parameters, if required. Click **Search** to view the event history information.
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 event search criteria. You can customize the search parameters, if required. Click **Search** to view the application information.
Search Connections	Click **Search Connections** to search for connections. The Connection Search window is displayed. This option is only displayed when IBM Security QRadar Risk Manager is been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager User Guide*.
View Topology	Click **View Topology** to further investigate the asset. The Current Topology window is displayed. This option is only displayed when IBM Security QRadar Risk Manager is been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager User Guide*.
Actions	From the **Actions** list, select **Vulnerability History.** This option is only displayed when IBM Security QRadar Risk Manager is been purchased and licensed. For more information, see the *IBM Security QRadar Risk Manager User Guide*.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**
3. Double-click the asset that you want to view.
4. Use the options on the toolbar to display the various panes of asset profile information. See Editing an asset profile.
5. To research the associated vulnerabilities, click each vulnerability in the Vulnerabilities pane. See Table 10-10
6. If required, edit the asset profile. See Editing an asset profile.
7. Click **Return to Assets List** to select and view another asset, if required.

Adding or editing an asset profile

Asset profiles are automatically discovered and added; however, you might be required to manually add a profile

About this task

When assets are discovered using the Server Discovery option, some asset profile details are automatically populated. You can manually add information to the asset profile and you can edit certain parameters.

You can only edit the parameters that were manually entered. Parameters that were system generated are displayed in italics and are not editable. You can delete system generated parameters, if required.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Choose one of the following options:
   - To add an asset, click **Add Asset** and type the IP address or CIDR range of the asset in the **New IP Address** field.
   - To edit an asset, double-click the asset that you want to view and click **Edit Asset** .
4. Configure the parameters in the MAC & IP Address pane. Configure one or more of the following options:
   - Click the **New MAC Address** icon and type a MAC Address in the dialog box.
   - Click the **New IP Address** icon and type an IP address in the dialog box.
   - If **Unknown NIC** is listed, you can select this item, click the **Edit** icon, and type a new MAC address in the dialog box.
   - Select a MAC or IP address from the list, click the **Edit** icon, and type a new MAC address in the dialog box.
   - Select a MAC or IP address from the list and click the **Remove** icon.
5. Configure the parameters in the Names & Description pane. Configure one or more of the following options:

Parameter	**Description**
DNS	Choose one of the following options: • Type a DNS name and click **Add**. • Select a DNS name from the list and click **Edit**. • Select a DNS name from the list and click **Remove**.
NetBIOS	Choose one of the following options: • Type a NetBIOS name and click **Add**. • Select a NetBIOS name from the list and click **Edit**. • Select a NetBIOS name from the list and click **Remove**.
Given Name	Type a name for this asset profile.
Location	Type a location for this asset profile.
Description	Type a description for the asset profile.
Wireless AP	Type the wireless Access Point (AP) for this asset profile.

Parameter	Description
Wireless SSID	Type the wireless Service Set Identifier (SSID) for this asset profile.
Switch ID	Type the switch ID for this asset profile.
Switch Port ID	Type the switch port ID for this asset profile.

6. Configure the parameters in the Operating System pane:
   a. From the **Vendor** list box, select an operating system vendor.
   b. From the **Product** list box, select the operating system for the asset profile.
   c. From the **Version** list box, select the version for the selected operating system.
   d. Click the **Add** icon.
   e. From the **Override** list box, select one of the following options:
      - **Until 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.
      - **Forever** - Select this option to specify that you want to manually enter operating system information and disable the scanner from updating the information.
   f. Select an operating system from the list.
   g. Select an operating system and click the **Toggle Override** icon.
7. Configure the parameters in the CVSS & Weight pane. Configure one or more of the following options:

Parameter	Description
Collateral Damage Potential	Configure this parameter to indicate the potential for loss of life or physical assets through damage or theft of this asset. You can also use this parameter to indicate potential for economic loss of productivity or revenue. Increased collateral damage potential increases the calculated value in the CVSS Score parameter. From the **Collateral Damage Potential** list box, select one of the following options: • None • Low • Low-medium • Medium-high • High • Not defined When you configure the **Collateral Damage Potential** parameter, the **Weight** parameter is automatically updated.

Parameter	Description
Confidentiality Requirement	Configure this parameter to indicate the impact on confidentiality of a successfully exploited vulnerability on this asset. Increased confidentiality impact increases the calculated value in the CVSS Score parameter. From the **Confidentiality Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Availability Requirement	Configure this parameter to indicate the impact to the asset's availability when a vulnerability is successfully exploited. Attacks that consume network bandwidth, processor cycles, or disk space impact the availability of an asset. Increased availability impact increases the calculated value in the CVSS Score parameter. From the **Availability Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Integrity Requirement	Configure this parameter to indicate the impact to the asset's integrity when a vulnerability is successfully exploited. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the calculated value in the CVSS Score parameter. From the **Integrity Requirement** list box, select one of the following options: • Low • Medium • High • Not defined
Weight	From the **Weight** list box, select a weight for this asset profile. The range is 0 - 10. When you configure the **Weight** parameter, the **Collateral Damage Potential** parameter is automatically updated.

8. Configure the parameters in the Owner pane. Choose one or more of the following options:

Parameter	Description
Business Owner	Type the name of the business owner of the asset. An example of a business owner is a department manager. The maximum length is 255 characters.
Business Owner Contact	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	Type the contact information for the technical owner. The maximum length is 255 characters.
Technical User	From the list box, select the username that you want to associate with this asset profile. You can also use this parameter to enable automatic vulnerability remediation for IBM Security QRadar Vulnerability Manager. For more information about automatic remediation, see the *IBM Security QRadar Vulnerability Manager User Guide*.

9. Click **Save**.

Searching asset profiles

You can configure search parameters to display only the asset profiles you want to investigate from the Asset page on the **Assets** tab.

About this task

When you access the **Assets** tab, the Asset page is displayed populated with all discovered assets in your network. To refine this list, you can configure search parameters to display only the asset profiles you want to investigate.

From the Asset Search page, you can manage Asset Search Groups. For more information about Asset Search Groups. See Asset search groups.

The search feature will allow you to search host profiles, assets, and identity information. Identity information provides more detail 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 whether known vulnerabilities exist in your deployment.

For example:

You receive a notification that CVE ID: CVE-2010-000 is being actively used in the field. To verify whether any hosts in your deployment are vulnerable to this exploit, you can select **Vulnerability External Reference** from the list of search parameters, select **CVE**, and then type the

```
2010-000
```

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/* .

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. On the toolbar, click **Search** > **New Search**.
4. Choose one of the following options:
   - To load a previously saved search, go to Step 5.
   - To create a new search, go to Step 6.
5. Select a previously saved search:
   a. Choose one of the following options:
      - Optional. From the **Group** list box, select the asset search group that you want to display in the **Available Saved Searches** list.
      - From the **Available Saved Searches** list, select the saved search that 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** .
6. In the Search Parameters pane, define your search criteria:
   a. From the first list box, select the asset parameter that you want to search for. For example, **Hostname**, **Vulnerability Risk Classification**, or **Technical Owner**.

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

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

   d. Click **Add Filter**.

   e. Repeat these steps for each filter that you want to add to the search criteria.
7. Click **Search**.

Results

You can save your asset search criteria. See Saving asset search criteria.

Saving asset search criteria

On the **Asset** tab, you can save configured search criteria so that you can reuse the criteria. Saved search criteria does not expire.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Perform a search.
4. Click **Save Criteria** .
5. Enter values for the parameters:

Parameter	Description
Enter the name of this search	Type the unique name that you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. This option is only displayed if you have administrative permissions.
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.
Include in my Quick Searches	Select this check box to include this search in your **Quick Search** list box, which is on the **Assets** tab toolbar.
Set as Default	Select this check box to set this search as your default search when you access the **Assets** tab.
Share with Everyone	Select this check box to share these search requirements with all users.

Asset search groups

Using the Asset Search Groups window, you can create and manage asset search groups.

These groups allow you to easily locate saved search criteria on the **Assets** tab.

Viewing search groups

Use the Asset Search Groups window to view a list group and subgroups.

About this task

From the Asset Search Groups window, you can view details about each group, including a description and the date the group was last modified.

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

The Asset Search Groups window displays the following parameters for each group:

Table 36. Asset Search Groups 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 group.

Table 36. Asset Search Groups window toolbar functions (continued)

Function	Description
Remove	To remove a search group or a saved search from a search group, select the item that you want to remove, and then click **Remove**. See Removing a group or a saved search from a group.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search**.
4. Click on **Manage Groups**.
5. View the search groups.

Creating a new search group

On the Asset Search Groups window, you can create a new search group.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search**.
4. Click **Manage Groups**.
5. Select the folder for the group under which you want to create the new group.
6. Click **New Group**.
7. In the **Name** field, type a unique name for the new group.
8. Optional. In the **Description** field, type a description.
9. Click **OK**.

Editing a search group

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

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search**.
4. Click **Manage Groups**.
5. Select the group that you want to edit.
6. Click **Edit**.
7. Type a new name in the **Name** field.
8. Type a new description in the **Description** field.
9. Click **OK**.

Copying a saved search to another group

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

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search**.
4. Click **Manage Groups**.
5. Select the saved search that you want to copy.
6. Click **Copy**.
7. On the Item Groups window, select the check box for the group you want to copy the saved search to.
8. 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:

- Asset Search Groups
- Other

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select **Search** > **New Search** .
4. Click **Manage Groups**.
5. Select the saved search that you want to remove from the group:
   - Select the saved search that you want to remove from the group.
   - Select the group that you want to remove.

Asset profile management tasks

You can delete, import, and export asset profiles using the Assets tab.

About this task

Using the **Assets** tab, you can delete, import, and export asset profiles.

Deleting assets

You can delete specific assets or all listed asset profiles.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. Select the asset that you want to delete, and then select **Delete Asset** from the **Actions** list box.
4. Click **OK**.

Importing asset profiles

You can import asset profile information.

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 invalidate 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

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. From the **Actions** list box, select **Import Assets**.
4. Click **Browse** to locate and select the CSV file that you want to import.
5. Click **Import Assets** to begin the import process.

Exporting assets

You can export listed asset profiles to an Extended Markup Language (XML) or Comma-Separated Value (CSV) file.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles**.
3. From the **Actions** list box, select one of the following options:
   - Export to XML
   - Export to CSV
4. View the status window for the status of the export process.
5. Optional: If you want to use other tabs and pages while the export is in progress, click the **Notify When Done** link.

   When the export is complete, the File Download window is displayed.

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.
7. Click **OK**.

Research asset vulnerabilities

The Vulnerabilities pane on the Asset Profile page displays a list of discovered vulnerabilities for the asset.

About this task

You can double-click the vulnerability to display more vulnerability details.

The Research Vulnerability Details window provides the following details:

Parameter	Description
Vulnerability 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.
Assets	Specifies the number of assets in your network that have this vulnerability. Click the link to view the list of assets.
Assets, including exceptions	Specifies the number of assets in your network that have vulnerability exceptions. Click the link to view the list of assets.
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.
xforce	Specifies the X-Force identifier for the vulnerability. Click the link to obtain more information. When you click the link, the IBM Internet Security Systems 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.

Parameter	Description
Plugin Details	Specifies the QRadar Vulnerability Manager ID. Click the link to view Oval Definitions, Windows Knowledge Base entries, or UNIX advisories for the vulnerability. This feature provides information on how QRadar Vulnerability Manager checks for vulnerability details during a patch scan. You can use it to identify why a vulnerability was raised on an asset or why it was not.
CVSS Score Base	Displays the aggregate Common Vulnerability Scoring System (CVSS) score of the vulnerabilities on this asset. 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. The CVSS score is calculated using the following user-defined parameters: • Collateral Damage Potential • Confidentiality Requirement • Availability Requirement • Integrity Requirement For more information about how to configure these parameters, see “Adding or editing an asset profile” on page 131. For more information about CVSS, see *http://www.first.org/cvss/* .
Impact	Displays the type of harm or damage that can be expected if this vulnerability is exploited.
CVSS Base Metrics	Displays the metrics that are used to calculate the CVSS base score, including: • Access Vector • Access complexity • Authentication • Confidentiality impact • Integrity impact • Availability impact
Description	Specifies a description of the detected vulnerability. This value is only available when your system integrates VA tools.
Concern	Specifies the effects that the vulnerability can have on your network.
Solution	Follow the instructions that are provided to resolve the vulnerability.

Parameter	Description
Virtual Patching	Displays virtual patch information that is associated with this vulnerability, if available. A virtual patch is a short-term mitigation solution for a recently discovered vulnerability. This information is derived from Intrusion Protection System (IPS) events. If you want to install the virtual patch, see your IPS vendor information.
Reference	Displays a list of external references, including: • **Reference Type** - Specifies the type of reference that is listed, such as 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.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Asset Profiles** .
3. Select an asset profile.
4. In the Vulnerabilities pane, click the **ID** or **Vulnerability** parameter value for the vulnerability you want to investigate.

Chapter 8. Chart management

You can view your data using various chart configuration options.

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

Chart management

You can use various chart configuration options to view your data.

If you select a time frame or a grouping option to view your data, then the 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 that represents the records that are matched by a specified time interval. For information about 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 by 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 activity over time.

Peaks and valleys that are 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.

To display time series charts, you must create and save a search that includes time series and grouping options. You can save up to 100 time series searches.

Default time series saved searches are accessible 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 timeline on a time series chart to investigate activity. The following table provides functions that you can use to view time series charts.

Table 37. 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.

Table 37. Time series charts functions (continued)

Function	Description
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 upper 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 to the left or right to scan the timeline.

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.
- 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 that are represented on the chart. For time series charts, you can also select a time range and enable time series data capture.

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 search criteria.
- On the toolbar, select a saved search from the **Quick Search** list.
- Perform a grouped search, and then click **Save Criteria** on the toolbar.

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

About this task

Data can be accumulated 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.

Procedure

1. Click the **Log Activity** or **Network Activity** tab.
2. In the Charts pane, click the **Configure** icon.
3. Configure values the following parameters:

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

4. If you selected the **Time Series** chart option and enabled the **Capture Time Series Data** option, click **Save Criteria** on the toolbar.
5. To view the list of events or flows if your time range is greater than 1 hour, click **Update Details**.

Chapter 9. Data searches

On the **Log Activity**, **Network Activity**, and **Offenses tabs**, you can search events, flows, and offenses by 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 for items that match your criteria

You can search for data that matches your search criteria.

About this task

Since the entire database is searched, searches might take an extended time, depending on the size of your database.

You can use the **Quick Filter** search parameter to search for items that match your text string in the event payload.

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

Table 38. Search options

Options	**Description**
Group	Select an event search group or flow search group to view in the **Available Saved Searches** list.
Type Saved Search or Select from List	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 use **Group or Type Saved Search** or **Select from List** options to apply a filter to the list. You can select a saved search on this list to display or edit.
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	Select this check box to include this search in your **Quick Search** menu.

Table 38. Search options (continued)

Options	**Description**
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.
Share with Everyone	Select this check box to share this search with all other users.
Real Time (streaming)	Displays results in streaming mode. For more information about 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)	Displays the search results in auto-refresh mode. In auto-refresh mode, the **Log Activity** and **Network Activity** tabs refresh at one-minute interval to display the most recent information.
Recent	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	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 38. Search options (continued)

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 might 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 that are applied to this search. The options to add a filter are located above **Current Filters** list.
Save results when the search is complete	Select this check box to save and name the search results.
Display	Select this list to specify a predefined column that is 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. Type the name of the column that you want to locate or type a keyword to display a list of column names. 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.

Table 38. Search options (continued)

Options	**Description**
Add and remove column icons (top set)	Use the top set of icons 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.
Add and remove column icons (bottom set)	Use the bottom set of icon 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. Use the following options to customize the Group By list further: • 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 that are 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** - Moves the selected column up the priority list. • **Move Down** - Moves the selected own the priority list. If the column type is numeric or time-based and there is an entry in the **Group By** list, then the column includes a list box. Use the list box to choose how you want to group the column. If the column type is group, the column includes a list box to choose how many levels you want to include for the group.

Table 38. Search options (continued)

Options	**Description**
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 that you want to display for the search results. Options include **Descending** and **Ascending**.
Results Limit	You can specify the number of rows a search returns on the Edit Search window. The **Results Limit** field also appears on the Results window. • For a saved search, the limit is stored in the saved search and re-applied when loading the search. • When sorting on a column in the search result that has row limit, sorting is done within the limited rows shown in the data grid. • For a grouped by search with time series chart turned on, the row limit only applies to the data grid. The **Top N** dropdown in the time series chart still controls how many time series are drawn in the chart.

Procedure

1. Choose one of the following options:
   - To search events, click the **Log Activity** tab.
   - To search flows, click the **Network Activity** tab.
2. From the **Search** list box, select **New Search**.
3. To 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 that you want for this search. See Table 1.
4. To create a search, in the Time Range pane, select the options for the time range you want to capture for this search.
5. 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 about enabling unique counts, see Table 1.
6. In the Search Parameters pane, define your search criteria:
   a. From the first list box, select a parameter that you want to search for. For example, Device, Source Port, or Event Name.
   b. From the second list box, select the modifier that you want to use for the search.

   c. In the entry field, type specific information that is 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.
7. 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.
8. 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 that is 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 1.
   d. Optional. In the **Results Limit** field, type the number of rows that you want the search to return .
9. Click **Filter**.

Results

The **In Progress (<percent>%Complete)** status is displayed in the upper 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 upper right corner.

Saving search criteria

You can save configured search criteria so that you can reuse the criteria and use the saved search criteria in other components, such as reports. Saved search criteria does not expire.

About this task

If you specify a time range for your search, then your search name is appended 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

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.

2. Perform a search.
3. Click **Save Criteria**.
4. Enter values for the parameters:

Option	**Description**
Parameter	Description
Search Name	Type the unique name that 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.
Timespan options:	Choose one of the following options: • **Real Time (streaming**) - Select this option to filter your search results while in streaming mode. • **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 that 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 on the toolbar.
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.
Share with Everyone	Select this check box to share these search requirements with all users.

5. Click **OK**.

Scheduled search

Use the Scheduled search option to schedule a search and view the results.

You can schedule a search that runs at a specific time of day or night.

Example:
If you schedule a search to run in the night, you can investigate in the morning.

Unlike reports, you have the option of grouping the search results and investigating further. You can search on number of failed logins in your network group. If the result is typically 10 and the result of the search is 100, you can group the search results for easier investigating. To see which user has the most failed logins, you can group by user name. You can continue to investigate further.

You can schedule a search on events or flows from the **Reports** tab. You must select a previously saved set of search criteria for scheduling.

1. Create a report

   Specify the following information in the **Report Wizard** window:

   - The chart type is Events/Logs or Flows.
   - The report is based on a saved search.
   - Generate an offense.

     You can choose the **create an individual offense** option or the **add result to an existing offense** option.

     You can also generate a manual search.
2. View search results

You can view the results of your scheduled search from the **Offenses** tab.

- Scheduled search offenses are identified by the **Offense Type** column.

  If you create an individual offense, an offense is generated each time that the report is run. If you add the saved search result to an existing offense, an offense is created the first time that the report runs. Subsequent report runs append to this offense. If no results are returned, the system does not append or create an offense.
- To view the most recent search result in the Offense Summary window, double-click a scheduled search offense in the offense list. To view the list of all scheduled search runs, click **Search Results** in the **Last 5 Search Results** pane.

You can assign a Scheduled search offense to a user.

Related tasks:

"Searching for items that match your criteria" on page 149
You can search for data that matches your search criteria.

"Assigning offenses to users" on page 41
Using the **Offenses** tab, you can assign offenses to users for investigation.

Advanced search options

Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

The **Advanced Search** field has auto completion and syntax highlighting.

Use auto completion and syntax highlighting to help create queries. For information about supported web browsers, see "Supported web browsers" on page 6

Accessing Advanced Search

Access the **Advanced Search** option from the **Search** toolbar that is on the **Network Activity** and **Log Activity** tabs to type an AQL query.

Select **Advanced Search** from the list box on the **Search** toolbar.

Expand the **Advanced Search** field by following these steps:

1. Drag the expand icon that is at the right of the field.
2. Press Shift + Enter to go to the next line.
3. Press Enter.

You can right-click any value in the search result and filter on that value.

Double-click any row in the search result to see more detail.

All searches, including AQL searches, are included in the audit log.

AQL search string examples

The following table provides examples of AQL search strings.

Table 39. Examples of AQL search strings

Description	Example

Select default columns from events.
Select default columns from flows.
	`SELECT * FROM events`
	`SELECT * FROM flows`

Select specific columns.	`SELECT sourceip, destinationip FROM events`
Select specific columns and order the results.	`SELECT sourceip, destinationip FROM events ORDER BY destinationip`
Run an aggregated search query.	`SELECT sourceip, SUM(magnitude) AS magsum FROM events GROUP BY sourceip`
Run a function call in a SELECT clause.	`SELECT CATEGORYNAME(category) AS namedCategory FROM events`
Filter the search results by using a WHERE clause.	`SELECT CATEGORYNAME(category) AS namedCategory, magnitude FROM events WHERE magnitude > 1`
Search for events that triggered a specific rule, which is based on the rule name or partial text in the rule name.	`SELECT LOGSOURCENAME(logsourceid), * from events where RULENAME(creeventlist) ILIKE '%suspicious%'`
Reference field names that contain special characters, such as arithmetic characters or spaces, by enclosing the field name in double quotation marks.	`SELECT sourceip, destinationip, "+field/name+" FROM events WHERE "+field/name+" LIKE '%test%'`

The following table provides examples of AQL search strings for X-Force.

Table 40. Examples of AQL search strings for X-Force

Description	Example
Check an IP address against an X-Force category with a confidence value.	`select * from events where XFORCE_IP_CONFIDENCE('Spam',sourceip)>3`
Search for X-Force URL categories associated with a URL.	`select url, XFORCE_URL_CATEGORY(url) as myCategories from events where XFORCE_URL_CATEGORY(url) IS NOT NULL`
Retrieve X-Force IP categories that are associated with an IP.	`select sourceip, XFORCE_IP_CATEGORY(sourceip) as IPcategories from events where XFORCE_IP_CATEGORY(sourceip) IS NOT NULL`

For more information about functions, search fields and operators, see the *Ariel Query Language guide*.

AQL search string examples

Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Note: When you build an AQL query, if you copy text that contains single quotation marks from any document and paste the text into IBM Security QRadar, your query will not parse. As a workaround, you can paste the text into QRadar and retype the single quotation marks, or you can copy and paste the text from the IBM Knowledge Center.

Reporting account usage

Different user communities can have different threat and usage indicators.

Use reference data to report on several user properties, for example, department, location, or manager.

You can use external reference data.

The following query returns metadata information about the user from their login events.

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

Insight across multiple account identifiers

In this example, individual users have multiple accounts across the network. The organization requires a single view of a users activity.

Use reference data to map local user IDs to a global ID.

The following query returns the user accounts that are used by a global ID on events that are flagged as suspicious.

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

The following query shows the activities that are completed by a global ID.

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

Identify suspicious long-term beaconing

Many threats use command and control to communicate periodically over days, weeks, and months.

Advanced searches can identify connection patterns over time. For example, you can query consistent, short, low volume, number of connections per day/week/month between IP addresses, or an IP address and geographical location.

Use the IBM Security QRadar REST API to generate an offense or to populate a reference set or reference table.

The following query detects potential instances of hourly beaconing.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'hh')) as 'different hours',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection = 'L2R'
GROUP BY sourceip, destinationip
HAVING 'different hours' > 20
AND 'total flows' < 25
LAST 24 hours
```

Tip: You can modify this query to work on proxy logs and other event types.

The following query detects potential instances of daily beaconing.

```
SELECT sourceip, destinationip,
UNIQUECOUNT(DATEFORMAT(starttime,'dd'))as 'different days',
COUNT(*) as 'total flows'
FROM flows
WHERE flowdirection='L2R'
GROUP BY sourceip, destinationip
HAVING 'different days' > 4
AND 'total flows' < 14
LAST 7 days
```

The following query detects daily beaconing between a source IP and a destination IP. The beaconing times are not at the same time each day. The time lapse between beacons is short.

```
SELECT
sourceip,
DATEFORMAT(starttime,'hh') as hourofday,
(AVG( hourofday*hourofday) - (AVG(hourofday)^2))as variance,
COUNT(*) as 'total flows'
FROM flows
GROUP BY sourceip, destinationip
HAVING variance < 01 and 'total flows' < 10
LAST 7 days
```

The following query detects daily beaconing to a domain by using proxy log events. The beaconing times are not at the same time each day. The time lapse between beacons is short.

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

The **url_domain** property is a custom property from proxy logs.

External threat intelligence

Usage and security data that is correlated with external threat intelligence data can provide important threat indicators.

Advanced searches can cross-reference external threat intelligence indicators with other security events and usage data.

This query shows how you can profile external threat data over many days, weeks, or months to identify and prioritize the risk level of assets and accounts.

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

Asset intelligence and configuration

Threat and usage indicators vary by asset type, operating system, vulnerability posture, server type, classification, and other parameters.

In this query, advanced searches and the asset model provide operational insight into a location.

The **Assetproperty** function retrieves property values from assets, which enables you to include asset data in the results.

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

The following query shows how you can use advanced searches and user identity tracking in the asset model.

The **AssetUser** function retrieves the user name from the asset database.

```
SELECT
APPLICATIONNAME(applicationid) as App,
ASSETUSER(sourceip, now()) as srcAssetUser,
COUNT(*) as 'Total Flows'
FROM flows
```

```
WHERE srcAssetUser IS NOT NULL
GROUP BY App, srcAssetUser
ORDER BY 'Total Flows' DESC
LAST 3 HOURS
```

Network LOOKUP function

You can use the **Network LOOKUP** function to retrieve the network name that is associated with an IP address.

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

Rule LOOKUP function

You can use the **Rule LOOKUP** function to retrieve the name of a rule by its ID.

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

The following query returns events that triggered a specific rule name.

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

Full TEXT SEARCH

You can use the TEXT SEARCH operator to do full text searches by using the **Advanced search** option.

In this example, there are a number of events that contain the word "firewall" in the payload. You can search for these events by using the **Quick filter** option and the **Advanced search** option on the **Log Activity** tab.

- To use the **Quick filter** option, type the following text in the **Quick filter** box: `'firewall'`
- To use the **Advanced search** option, type the following query in the **Advanced search** box:

  ```
  SELECT QIDNAME(qid) AS EventName, * from events where TEXT SEARCH 'firewall'
  ```

Custom property

You can access custom properties for events and flows when you use the **Advanced search** option.

The following query uses the custom property "MyWebsiteUrl" to sort events by a particular web URL:

```
SELECT "MyWebsiteUrl", * FROM events ORDER BY "MyWebsiteUrl"
```

Related concepts:

"Quick filter search options" on page 162
Search event and flow payloads by typing a text search string that uses simple words or phrases.

Related tasks:

"Creating a regex-based custom property" on page 182
You can create a regex-based custom property to match event or flow payloads to a regular expression.

Quick filter search options

Search event and flow payloads by typing a text search string that uses simple words or phrases.

You can filter your searches from these locations:

Log Activity toolbar and Network Activity toolbars
Select **Quick Filter** from the list box on the **Search** toolbar to type a text search string. Click the **Quick Filter** icon to apply your **Quick Filter** to the list of events or flows.

Add Filter Dialog box
Click the **Add Filter** icon on the **Log Activity** or **Network Activity** tab.

Select **Quick Filter** as your filter parameter and type a text search string.

Flow search pages
Add a quick filter to your list of filters.

When you view **flows** in real-time (streaming) or last interval mode, you can type only simple words or phrases in the **Quick Filter** field. When you view **events** or **flows** in a time-range, follow these syntax guidelines:

Table 41. Quick filter syntax guidelines

Description	Example
Include any plain text that you expect to find in the payload.	`Firewall`
Search for exact phrases by including multiple terms in double quotation marks.	`"Firewall deny"`
Include single and multiple character wildcards. The search term cannot start with a wildcard.	`F?rewall` or `F??ew*`
Group terms with logical expressions, such as AND, OR, and NOT. To be recognized as logical expressions and not as search terms, the syntax and operators must be uppercase.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") AND 10.100.100.*)`
When you create search criteria that includes the NOT logical expression, you must include at least one other logical expression type, otherwise, no results are returned.	`(%PIX* AND ("Accessed URL" OR "Deny udp src") NOT 10.100.100.*)`
Precede the following characters by a backslash to indicate that the character is part of your search term: `+ - && || ! () {} [] ^ " ~ * ? : \`.	`"%PIX\-5\-304001"`

Search terms are matched in sequence from the first character in the payload word or phrase. The search term `user` matches `user_1` and `user_2`, but does not match the following phrases: `ruser`, `myuser`, or `anyuser`.

Quick filter searches use the English locale. *Locale* is a setting that identifies language or geography and determines formatting conventions such as collation, case conversion, character classification, the language of messages, date and time representation, and numeric representation.

The locale is set by your operating system. You can configure QRadar to override the operating system locale setting. For example, you can set the locale to **English** and the QRadar Console can be set to **Italiano (Italian)**.

If you use Unicode characters in your Quick filter search query, unexpected search results might be returned.

If you choose a locale that is not English, you can use the Advanced search option in QRadar for searching event and payload data.

Related concepts:

Chapter 9, "Data searches," on page 149
On the **Log Activity**, **Network Activity**, and **Offenses tabs**, you can search events, flows, and offenses by using specific criteria.

"Advanced search options" on page 156
Use the **Advanced Search** field to enter an Ariel Query Language (AQL) that specifies the fields that you want and how you want to group them to run a query.

"AQL search string examples" on page 158
Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Related tasks:

"Updating user preferences" on page 16
You can set your user preference, such as locale, in the main IBM Security QRadar SIEM user interface.

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 that you can use to search offense data on the **My Offenses** and **All Offenses** pages.

For information about categories, see the *IBM Security QRadar SIEM Administration Guide*.

Table 42. 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.
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.

Table 42. My Offenses and All Offenses page search options (continued)

Options	Description
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 that you want to search for.
Assigned to user	From this list box, you can select the user name that you want to search for.
Direction	From this list box, you can select the offense direction that 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 42. My Offenses and All Offenses page search options (continued)

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 - 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 - 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 - 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 - 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™ 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 that you want to search for.
Destination Network	From this list box, you can select the destination network that you want to search for.
High Level Category	From this list box, you can select the high-level category that you want to search for. .
Low Level Category	From this list box, you can select the low-level category that you want to search for.
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

Table 42. My Offenses and All Offenses page search options (continued)

Options	Description
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 that you want to search closed offenses for or select `Any` to display 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 that you want to search closed offenses for or select **Any** to display all closed offenses.
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 that are assigned to the selected log source group.
Log Source	From this list box, you can select the log source that you want to search for.
Rule Group	From this list box, you can select a rule group that contains the contributing rule that you want to search for. The **Rule** list box displays all rules that are assigned to the selected rule group.
Rule	From this list box, you can select the contributing rule that you want to search for.
Offense Type	From this list box, you can select an offense type that you want to search for. For more information about the options in the **Offense Type** list box, see Table 2.

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

Table 43. 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 that 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 that you want to search for.
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 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 user name, you can select this option, and then type the user name that 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 that 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 that 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 that are assigned to the selected log source group. From the **Log Source** list box, select the log source that you want to search for.

Table 43. Offense type options (continued)

Offense types	Description
Host Name	To search for offenses with a specific host name, you can select this option, and then type the host name that 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 that 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 that 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 that 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 that 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.
Rule	To search for offenses that are 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 that are assigned to the selected rule group. From the **Rule** list box, you select the rule that you want to search for.
App ID	To search for offenses with an application ID, you can select the application ID from the **App ID** list box.

Procedure

1. Click the **Offenses** tab.
2. From the **Search** list box, select **New Search**.
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.
4. Select a previously saved search using one of the following options:
   - From the **Available Saved Searches** list, select the saved search that you want to load.
   - In the **Type Saved Search** or **Select from List** field, type the name of the search you want to load.

5. Click **Load**.
6. Optional. Select the **Set as Default** check box in the Edit Search pane 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.
7. On the Time Range pane, select an option for the time range you want to capture for this search. See Table 1.
8. On the Search Parameters pane, define your specific search criteria. See Table 1.
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 that you want to search for.
   b. Type your search parameters. See Table 2.
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 that you want to display for the search results. Options include Descending and Ascending.
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 that you can use to search offense data on the By Source IP page:

Table 44. 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 that you want to search for.

Table 44. By Source IP page search options (continued)

Options	Description
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 - 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 - 10.
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

1. Click the **Offenses** tab.
2. Click **By Source IP**.

3. From the **Search** list box, select **New Search**.
4. On the Time Range pane, select an option for the time range you want to capture for this search. See Table 1.
5. On the Search Parameters pane, define your specific search criteria. See Table 1.
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 that you want to display for the search results. Options include **Descending** and **Ascending**.
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 that are grouped by the destination IP address.

About this task

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

Table 45. 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 that 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: • To specify a particular interval to search for, you can select the **Specific Interval** option, and then select one of the following options: • **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.

Table 45. By Destination IP page search options (continued)

Options	Description
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 - 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

1. Click the **Offenses** tab.
2. On the navigation menu, click **By Destination IP**.
3. From the **Search** list box, select **New Search**.
4. On the Time Range pane, select an option for the time range you want to capture for this search. See Table 1.
5. On the Search Parameters pane, define your specific search criteria. See Table 1.
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**.
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 that are grouped by the associated networks.

About this task

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

Table 46. Search options for search offense data on the By Networks page

Option	Description
Network	From this list box, you can select the network that you want to search for.

Table 46. Search options for search offense data on the By Networks page (continued)

Option	Description
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

1. Click the **Offenses** tab.
2. Click **By Networks**.
3. From the **Search** list box, select **New Search**.
4. On the Search Parameters pane, define your specific search criteria. See Table 1.
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**.
6. Click **Search**.

What to do next

Saving search criteria on the Offense tab

Saving search criteria on the Offenses tab

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

Procedure

1. Procedure
2. Perform a search. See Offense searches.
3. Click **Save Criteria**.
4. Enter values for the following parameters:

Option	Description
Parameter	Description
Search Name	Type a name you want to assign to this search criteria.
Manage Groups	Click **Manage Groups** to manage search groups. See Managing search groups.

Option	Description
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 that 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.Last Event 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.

5. Click **OK**.

Deleting search criteria

You can delete search criteria.

About this task

When you delete a saved search, then objects that are associated with the saved search might not function. Reports and anomaly detection rules are QRadar objects that use saved search criteria. After you delete a saved search, edit the associated objects to ensure that they continue to function.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** list box, select **New Search** or **Edit Search**.
3. In the Saved Searches pane, select a saved search from the **Available Saved Searches** list box.
4. Click **Delete**.
   - If the saved search criteria is not associated with other QRadar objects, a confirmation window is displayed.

- If the saved search criteria is associated with other objects, the Delete Saved Search window is displayed. The window lists objects that are associated with the saved search that you want to delete. Note the associated objects.

5. Click **OK**.
6. Choose one of the following options:
   - Click **OK** to proceed.
   - Click **Cancel** to close the Delete Saved Search window.

What to do next

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

Using a subsearch to refine search results

You can use a subsearch to search within a set of completed search results. The subsearch is used to refine search results, without searching the database again.

Before you begin

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

About this task

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

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Perform a search.
3. When your search is complete, add another filter:
   a. Click **Add Filter**.
   b. From the first list box, select a parameter that you want to search for.
   c. From the second list box, select the modifier that you want to use for the search. The list of modifiers that are available depends on the attribute that is selected in the first list.
   d. In the entry field, type specific information that is related to your search.
   e. Click **Add Filter**.

Results

The Original Filter pane specifies the original filters that are applied to the base search. The Current Filter pane specifies the filters that are applied to the subsearch. You can clear subsearch 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 subsearch criteria, you still have access to saved subsearch criteria. If you add a filter, the subsearch searches the entire database since the search function no longer bases the search on a previously searched data set.

What to do next

Save search criteria

Managing search results

You can initiate multiple 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.

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

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** menu, select **Manage Search Results**.
3. Select the queued or in progress search result you want to cancel.
4. Click **Cancel**.
5. Click **Yes**.

Deleting a search

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

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** menu, select **Manage Search Results**.
3. Select the search result that you want to delete.
4. Click **Delete**.
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

A default set of groups and subgroups are available.

About this task

You can view search groups on the Event Search Group, Flow Search Group, or Offense Search Group windows.

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

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

Table 47. 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 48. 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 group.
Remove	To remove a search group or a saved search from a search group, select the item that you want to remove, and then click **Remove**. See Removing a group or a saved search from a group.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.

- Click the **Network Activity** tab.

2. **Select Search** >**Edit Search**.
3. Click **Manage Groups**.
4. View the search groups.

Creating a new search group

You can create a new search group.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. **Select Search Edit Search**.
3. Click **Manage Groups**.
4. Select the folder for the group under which you want to create the new group.
5. Click **New Group**.
6. In the **Name** field, type a unique name for the new group.
7. Optional. In the **Description** field, type a description.
8. Click **OK**.

Editing a search group

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

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Select the group that you want edit.
5. Click **Edit**.
6. Edit the parameters:
   - Type a new name in the **Name** field.
   - Type a new description in the **Description** field.
7. Click **OK**.

Copying a saved search to another group

You can copy a saved search to one or more groups.

Procedure

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Select the saved search that you want to copy.
5. Click **Copy**.

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

1. Choose one of the following options:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Select **Search** > **Edit Search**.
3. Click **Manage Groups**.
4. Choose one of the following options:
   - Select the saved search that you want to remove from the group.
   - Select the group that you want to remove.
5. Click **Remove**.
6. Click **OK**.

Chapter 10. Custom event and flow properties

Use Custom event and flow properties to search, view, and report on information in logs that QRadar does not typically normalize and display.

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

- From the **Log Activity** tab, double-click an event and click **Extract Property**.
- From the **Network Activity** tab, double-click a flow and click **Extract Property**.
- You can create or edit a custom event or flow property from the Search page. When you create a custom property from the Search page, the property is not derived from any particular event or flow; therefore, the Custom Event Properties window does not prepopulate. You can copy and paste payload information from another source.

Required permissions

To create custom properties if you have the correct permission.

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 that you have the correct permissions.

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

Custom property types

You can create a custom property type.

When you create a custom property, you can choose to create a Regex or a calculated property type.

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

For example, a report is created to report all users who make user permission changes on an Oracle server. A list of users and the number of times they made a change to the permission of another account is reported. However, typically the actual user account or permission that was changed cannot display. 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 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.

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.

Creating a regex-based custom property

You can create a regex-based custom 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 parameters. The following table provides reference information for some parameters.

Table 49. Custom Event Properties window parameters (regex)

Parameter	Description
Test field	
New 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	Parses and stores the property the first time that the event or flow is received. When you select the check box, the property does not require more 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 applied.
Log Source	If multiple log sources are associated with this event, this field specifies the term Multiple and the number of log sources.

Table 49. Custom Event Properties window parameters (regex) (continued)

Parameter	Description
RegEx	The regular expression that you want to use for extracting the data from the payload. Regular expressions are case-sensitive. The following examples show 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)` Capture groups must be enclosed in parentheses.
Capture Group	Capture groups treat multiple characters as a single unit. In a capture group, characters are grouped inside a set of parentheses.
Enabled	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.

Procedure

1. Click the **Log Activity** tab.
2. If you are viewing event or flows in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event or flow that you want to base the custom property on.
4. Double-click the event that you want to base the custom property on
5. Click **Extract Property**.
6. In the **Property Type Selection** pane, select the **Regex Based** option.
7. Configure the custom property parameters.
8. Click **Test** to test the regular expression against the payload.
9. Click **Save**.

Results

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

Related concepts:

"AQL search string examples" on page 158
Use the Ariel Query Language (AQL) to retrieve specific fields from the events, flows, and simarc tables in the Ariel database.

Creating a calculation-based custom property

You can create a calculation-based customer property to match 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 50. 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 that 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 that 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 that 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 50. 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.

Procedure

1. Choose one of the following: Click the **Log Activity** tab.
2. Optional. If you are viewing events or flows in streaming mode, click the **Pause** icon to pause streaming.
3. Double-click the event or flow that you want to base the custom property on.
4. Click **Extract Property**.
5. In the Property Type Selection pane, select the **Calculation Based** option.
6. Configure the custom property parameters.
7. Click **Test** to test the regular expression against the payload.
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.

Modifying a custom property

You can modify a custom property.

About this task

You can use the Custom Event Properties or Custom Flow Properties window to modify a custom property.

The custom properties are described in the following table.

Table 51. Custom properties window columns

Column	Description
Property Name	Specifies a unique name for this custom property.
Type	Specifies the type for this custom property.
Property Description	Specifies a description for this custom property.

Table 51. Custom properties window columns (continued)

Column	Description
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 that are 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 that you want to use for extracting the data from the payload. For a calculation-based custom property, this parameter specifies the calculation that 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 52. Custom property toolbar options

Option	Description
Add	Click **Add** to add a new custom property.
Edit	Click **Edit** to edit the selected custom property.
Copy	Click **Copy** to copy selected custom properties.
Delete	Click **Delete** to delete selected custom properties.

Table 52. Custom property toolbar options (continued)

Option	Description
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

1. Choose one of the following:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** list box, select **Edit Search**.
3. Click **Manage Custom Properties**.
4. Select the custom property that you want to edit and click **Edit**.
5. Edit the necessary parameters.
6. Optional. If you edited the regular expression, click **Test** to test the regular expression against the payload.
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

1. Choose one of the following:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. From the **Search** list box, select **Edit Search**.
3. Click **Manage Custom Properties**.
4. Select the custom property that you want to copy and click **Copy**.
5. Edit the necessary parameters.
6. Optional. If you edited the regular expression, click **Test** to test the regular expression against the payload.
7. Click **Save**.

Deleting a custom property

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

Procedure

1. Choose one of the following:
   - Click the **Log Activity** tab.
   - Click the **Network Activity** tab.
2. Click the **Log Activity** tab.
3. From the **Search** list box, select **Edit Search**.
4. Click **Manage Custom Properties**.

5. Select the custom property that you want to delete and click **Delete**.
6. Click **Yes**.

Chapter 11. 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 you have the View Custom Rules and Maintain Custom Rules user role permissions.

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.

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.

For a complete list of default rules, see the *IBM Security QRadar SIEM Administration Guide*.

Rule categories

There are two categories for rules; custom rules and anomaly rules.

Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network.

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.

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, threshold, and behavioral.

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.

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 that is collected. For example, you can create a threshold rule specifying that no more than 220 clients can log in to the server between 8 am and 5 pm. The threshold rule generates an alert when the 221st client attempts to log in.

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 types

There are four different types of rules; event, flow, common, and offense.

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.

Rule conditions

Each rule might contain functions, building blocks, or tests.

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 when an event matches any|all of the following rules function.

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 will allow you to reuse 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.

Note: Building blocks are not loaded by default. Define a rule to build building blocks.

For a complete list of building blocks, see the *IBM Security QRadar SIEM Administration Guide*.

You can run tests on the property of an event, flow, or offense, such as source IP address, severity of event, or rate analysis.

Rule responses

When rule conditions are met, a rule can generate one or more responses.

Rules can generate one or more of the following responses:

- Create an offense.
- Send an email.
- Generate system notifications on the Dashboard feature.
- Add data to reference sets.
- Add data to reference data collections.
- Generate a response to an external system.
- Add data to reference data collections that can be used in rule tests.
- Run a custom action script in response to an event.

Reference data collection types

Before you can configure a rule response to send data to a reference data collection, you must create the reference data collection by using the command line interface (CLI). QRadar supports the following data collection types:

Reference set
A set of elements, such as a list of IP addresses or user names, that are derived from events and flows occurring on your network.

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
Data is stored in records that map a key to multiple values. For example, to test for authorized access to a patent, use a custom event property for

Patent ID as the key and the **Username** parameter as the value. Use a map of sets to populate a list of authorized users.

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. Use the **Source IP** parameter as the first key, the **Application** parameter as the second key, and the **Total Bytes** parameter as the value.

Reference table
In a reference table, data is stored in a table that maps one key to another key, which is then mapped to single value. The second key has an assigned type. This mapping is similar to a database table where each column in the table is associated with a type. For example, you can create a reference table that stores the **Username** parameter as the first key, and has multiple secondary keys that have a user-defined assigned type such as **IP Type** with the **Source IP** or **Source Port** parameter as a value. You can configure a rule response to add one or more keys defined in the table. You can also add custom values to the rule response. The custom value must be valid for the secondary key's type.

Note: For information about reference sets and reference data collections, see the *Administration Guide* for your product.

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 about 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. 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.

Procedure

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.
2. From the **Display** list box, select **Rules**.
3. Double-click the rule that you want to view.
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.

Creating a rule

Rules evaluate incoming data against rule test conditions to generate a response from the system. When the conditions of a rule are met, several actions can be taken. For example, you can configure the system response to the rule, which ranges from generating offenses, sending emails, starting scans, adding reference data, or raising or lowering values like severity.

Before you begin

To create a new rule, you must have the **Offenses** > **Maintain Custom Rules** permission.

About this task

When you define rule tests, treat rules the same way you treat searches and test against the smallest data possible. Testing this way helps rule test performance and ensures that you don't create expensive rules. To optimize performance, start with broad categories that narrows the data that a rule test evaluates. For example, start with a rule test for a specific log source type, network location, flow source, or context (R2L, L2R, L2L). Any mid-level tests that you do might include IP addresses, port traffic, or any other associated test. Keep payload and regex tests as the last rule test.

Most rule tests evaluate a single condition, like the existence of an element in a reference data collection or testing a value against a property of an event. For complex comparisons, you can test event rules by building an Ariel Query Language (AQL) query with WHERE clause conditions. You can use all the WHERE clause functions to write complex criteria that can eliminate the need to run numerous individual tests. For example, use an AQL WHERE clause to check whether inbound SSL or web traffic is being tracked on a reference set.

Procedure

1. From the **Offenses**, **Log Activity**, or **Network Activity** tabs, click **Rules**.
2. From the **Actions** list, select a rule type.

   Each rule type tests against incoming data from different sources in real time. For example, event rules test incoming log source data and offense rules test the parameters of an offense to trigger more responses.
3. On the Rule Test Stack Editor page, in the Rule pane, type a unique name that you want to assign to this rule in the **Apply** text box.
4. From the list box, select **Local** or **Global**.

   Local rules send events and flows to the local event processor to trigger the rule. This is the default action.

   Global rules send events and flows to the central event processor, which might decrease performance on the Console. The custom rules engine (CRE) on the Console tracks the event matches as provided by each managed host in the deployment. As partial matches are made or counters need to be updated, each managed host sends an update to the CRE on the Console. When the overall rule becomes true, the Console triggers the rule response.

For more information about local and global rule tests, see the *IBM Security QRadar SIEM Administration Guide*

5. From the **Test Group** list, select one or more tests that you want to add to this rule. The CRE evaluates rule tests line-by-line in order. The first test is evaluated and when true, the next line is evaluated until the final test is reached.

   If you select the **when the event matches this AQL filter query** test for a new event rule, enter an AQL WHERE clause query in the **Enter an AQL filter query** text box.

   Learn more about using rules for events that are not detected:

   The following rule tests can be triggered individually, but subsequent rule tests in the same rule test stack are not acted upon.

   - **when the event(s) have not been detected by one or more of these log source types for this many seconds**
   - **when the event(s) have not been detected by one or more of these log sources for this many seconds**
   - **when the event(s) have not been detected by one or more of these log source groups for this many seconds**

   These rule tests are not activated by an incoming event, but instead are activated when a specific event is not seen for a specific time interval that you configured. QRadar uses a *watcher task* that periodically queries the last time that an event was seen (last seen time), and stores this time for the event, for each log source. The rule is triggered when the difference between this last seen time and the current time exceeds the number of seconds that is configured in the rule.

6. To export the configured rule as a building block to use with other rules, click **Export as Building Block**.

   A building block is a subset of rule tests that don't have any responses. Think of building blocks as a reusable set of rule tests that you can use within other rules. A common example is to populate the BB:Host Definition building blocks with the addresses of servers. Administrators can then either exclude or include rule tests by specific server types, such as VPN servers, mail servers, or LDAP servers.

7. On the Rule Responses page, configure the responses that you want this rule to generate.

   Rule responses are the action that the QRadar appliance takes when all of the rule tests are true. The rule responses, such as emails, syslog messages, and forwarding events occurs for local rules on the processor, and for global rules on the Console, where the rule becomes true.

Related concepts:

“Rule Response page parameters” on page 203
Configure the parameters for the Rule Response page to specify how you want IBM Security QRadar to respond when a rule is triggered.

Creating an anomaly detection rule

Use the Anomaly Detection Rule wizard to create rules that apply time range criteria by 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 display 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 **Network 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 or 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 that are 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

1. Click the **Log Activity** or **Network Activity** tab.
2. Perform a search.
3. From the **Rules** menu, select the rule type that you want to create. Options include:
   - Add Anomaly Rule
   - Add Threshold Rule
   - Add Behavioral Rule
4. Read the introductory text on the Rule wizard. Click **Next**. The rule that you previously choose is selected.

5. Click **Next** to view the Rule Test Stack Editor page.
6. In the **enter rule name here** field, type a unique name that you want to assign to this rule.
7. To add a test to a rule:
   a. Optional. To filter the options in the Test Group list box, type the text that 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**.
8. Optional. To test the total selected accumulated properties for each event or flow group, clear the **Test the [Selected Accumulated Property] value of each [group] separately** check box.
9. In the groups pane, select the check boxes of the groups you want to assign this rule to. For more information, see Rule group management.
10. In the **Notes** field, type any notes that you want to include for this rule. Click **Next**.
11. On the Rule Responses page, configure the responses that you want this rule to generate. "Rule Response page parameters" on page 203
12. Click **Next**.
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.

You can create anomaly detection rules only on the **Log Activity** and **Network Activity** tabs.

To manage default and previously created anomaly detection rules, you must use the Rules page on the **Offenses** tab.

Enabling and disabling rules

When you tune 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

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.

3. From the **Display** list box on the **Rules** page, select **Rules**.
4. Select the rule that you want to enable or disable.
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 enable or disable a rule.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Display** list box on the **Rules** page, select **Rules**.
4. Double-click the rule that you want to edit.
5. From the **Actions** list box, select **Open**.
6. Optional. If you want to change the rule type, click **Back** and select a new rule type.
7. On the Rule Test Stack Editor page, edit the parameters.
8. Click **Next**.
9. On the Rule Response page, edit the parameters.
10. Click **Next**.
11. Review the edited rule. Click **Finish**.

Copying a 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 enable or disable a rule.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Display** list box, select **Rules**.
4. Select the rule that you want to duplicate.
5. From the **Actions** list box, select **Duplicate**.
6. In the Enter name for the copied rule field, type a name for the new rule. Click **OK**.

Deleting a rule

You can delete a rule from your system.

About this task

You must have the **Offenses** > **Maintain Custom Rules** role permission to be able to enable or disable a rule.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Display** list box, select **Rules**.
4. Select the rule that you want to delete.
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 that are related to compliance.

As you create new rules, you can assign the rule to an existing group. For information about 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 that belong to a specific group.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Display** list box, select whether you want to view rules or building blocks.
4. From the **Filter** list box, select the group category that you want to view.

Creating a group

The Rules page provides default rule groups, however, you can create a new group.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Click **Group**s.
4. From the navigation tree, select the group under which you want to create a new group.
5. Click **New Group**.
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 that you want to assign to this group. The description can be up to 255 characters in length.

7. Click **OK**.
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.

Assigning an item to a group

You can assign a selected rule or building block to a group.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Select the rule or building block you want to assign to a group.
4. From the **Actions** list box, select **Assign Groups**.
5. Select the group that you want to assign the rule or building block to.
6. Click **Assign Groups**.
7. Close the **Choose Groups** window.

Editing a group

You can edit a group to change the name or description.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Click **Groups**.
4. From the navigation tree, select the group that you want to edit.
5. Click **Edit**.
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 that you want to assign to this group. The description can be up to 255 characters in length.
7. Click **OK**.
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.

Copying an item to another group

You can copy a rule or building block from one group to other groups.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Click **Groups**.
4. From the navigation tree, select the rule or building block you want to copy to another group.
5. Click **Copy**.
6. Select the check box for the group you want to copy the rule or building block to.
7. Click **Copy**.

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

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Click **Groups**.
4. Using the navigation tree, navigate to and select the item you want to delete.
5. Click **Remove**.
6. Click **OK**.

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

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. Click **Groups**.
4. Using the navigation tree, navigate to and select the group that you want to delete.
5. Click **Remove**.
6. Click **OK**.

Editing building blocks

You can edit any of the default building blocks to match the needs of your deployment.

About this task

A building block is a reusable 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.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Display** list box, select **Building Blocks**.
4. Double-click the building block that you want to edit.
5. Update the building block, as necessary.
6. Click **Next**.
7. Continue through the wizard. For more information, see Creating a custom rule.
8. Click **Finish**.

Rule page parameters

A description of the parameters on the Rules page.

The list of deployed rules provides the following information for each rule:

Table 53. 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 and Anomaly Detection Rule.
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 and 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 that are associated with this rule when the rule contributes to an offense.
Offense Count	Displays the number of offenses that are generated by this rule.
Origin	Displays whether this rule is a default rule (System) or a custom rule (User).

Table 53. Rules page parameters (continued)

Parameter	Description
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

You use the Rules page toolbar to display rules, building blocks or groups. You can manage rule groups and work with rules.

The Rules page toolbar provides the following functions:

Table 54. 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.
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.
Actions	Click **Actions** and select one of the following options: • **New Event Rule** - Select this option to create a new event rule. • **New Flow Rule** - Select this option to create a new flow rule. • **New Common Rule** - Select this option to create a new common rule. • **New Offense Rule** - Select this option to create a new offense rule. • **Enable/Disable** - Select this option to enable or disable selected rules. • **Duplicate** - Select this option to copy a selected rule. • **Edit** - Select this option to edit a selected rule. • **Delete** - Select this option to delete a selected rule. • **Assign Groups** - Select this option to assign selected rules to rule groups.
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. To revert the rule and maintain a modified version, duplicate the rule and use the **Revert Rule** option on the modified rule.

Table 54. 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

Configure the parameters for the Rule Response page to specify how you want IBM Security QRadar to respond when a rule is triggered.

Note: When you build an AQL query, if you copy text that contains single quotation marks from any document and paste the text into IBM Security QRadar, your query will not parse. As a workaround, you can paste the text into QRadar and retype the single quotation marks, or you can copy and paste the text from the IBM Knowledge Center.

The following table provides the Rule Response page parameters.

Table 55. Event , Flow and Common Rule Response page parameters

Parameter	Description
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. The dropped event is written to storage and bypasses rules tests. This event does not display on the **Offenses** tab.
Dispatch New Event	Select this check box to dispatch a new event in addition to the original event or flow, which is processed like all other events in the system. Select this check box to dispatch a new event in addition to the original event, which is 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.

Table 55. Event , Flow and Common Rule Response page parameters (continued)

Parameter	Description
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.
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.
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.
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 Annotation pane of the event details.
High-Level Category	From the list box, select the high-level event category that you want this rule to use when processing events.
Low-Level Category	From the list box, select the low-level event category that you want this rule to use when processing events.
Annotate this offense	Select this check box to add an annotation to this offense and type the annotation.
Email	Select this check box to display the email options. **Note:** To change the **Email Locale** setting, select **System Settings** on the **Admin** tab.
Enter email addresses to notify	Type the email address to send notification if this rule generates. Use a comma to separate multiple email addresses.
Select event/flow email template	Select the email template for emails associated with this rule. For more information about configuring custom email notifications, see the *IBM Security QRadar SIEM Administration Guide*.
SNMP Trap	This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. 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 MIB.
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. **Note:** Only normalized events can be logged locally on an appliance. If you want to send raw event data, you must use the Send to Forwarding Destinations option to send the data to a remote syslog host.

Table 55. Event , Flow and Common Rule Response page parameters (continued)

Parameter	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.
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. If you enable notifications, configure the **Response Limiter** parameter.
Add to Reference Set	Select this check box if you want events that are 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 that you want to add. Options include all normalized or custom data. 2. Using the second list box, select the reference that is 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.

Table 55. Event , Flow and Common Rule Response page parameters (continued)

Parameter	Description
Add to Reference Data	Before you can use this rule response, you must create the reference data collection by using the command line interface (CLI). For more information about how to create and use reference data collections, see the *Administration Guide* for your product. Select this check box if you want events that are 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 that 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. **Add to a Reference Table** Select this option to send data to a collection of multiple key/single value pairs, where a type was assigned to the secondary keys. Select the reference table that you want to add data to, and then select a primary key. Select your inner keys (secondary keys) and their values for the data records.
Execute Custom Action	You can write scripts that do specific actions in response to network events. For example, you might write a script to create a firewall rule that blocks a particular source IP address from your network in response to repeated login failures. Select this check box and select a custom action from the **Custom action to execute** list. You add and configure custom actions by using the **Define Actions** icon on the **Admin** tab.
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 about the IF-MAP server.
Response Limiter	Select this check box and use the list boxes to configure the frequency in which you want this rule to respond.

Table 55. Event , Flow and Common Rule Response page parameters (continued)

Parameter	Description
Enable Rule	Select this check box to enable this rule.

The following table provides the Rule Response page parameters if the rule type is Offense.

Table 56. Offense Rule Response page parameters

Parameter	Description
Name/Annotate the detected offense	Select this check box to display Name options.
New Offense Name	Type the name that you want to assign to the offense.
Offense Annotation	Type the offense annotation that 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.
Email	Select this check box to display the email options. **Note:** To change the **Email Locale** setting, select **System Settings** on the **Admin** tab.
Enter email address to notify	Type the email address to send the notification if the event generates. Use a comma to separate multiple email addresses.
SNMP Trap	This parameter is only displayed when the SNMP Settings parameters are configured in the system settings. 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 MIB.
Send to Local SysLog	Select this check box if you want to log the event or flow locally.
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.
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 about the IF-MAP server.
Response Limiter	Select this check box and use the list boxes to configure the frequency with which you want this rule to respond.

Table 56. Offense Rule Response page parameters (continued)

Parameter	Description
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 57. Anomaly Detection Rule Response page parameters

Parameter	Description
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. **Note:** After you replace the name of the offense, the name won't change until the offense is closed. For example, if an offense is associated with more than one rule, and the last event doesn't trigger the rule that is configured to override the name of the offense, the offense's name won't be updated by the last event. Instead, the offense name remains the name that is set by the override rule. **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.
Severity	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.
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.
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.

Table 57. Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
High Level Category	From the list box, select the high-level event category that you want this rule to use when processing events.
Low Level Category	From the list box, select the low-level event category that you want this rule to use when processing events.
Annotate this offense	Select this check box to add an annotation to this offense and type the annotation.
Ensure that 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 is added. If no offense was created on the Offenses tab, a new offense is created. 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. **Note:** To change the **Email Locale** setting, select **System Settings** on the **Admin** tab.
Enter email address to notify	Type the email address to send notification if this rule generates. Use a comma to separate multiple email addresses.
Select event email template	Select the email template for emails associated with this rule. For more information about configuring custom email notifications, see the *IBM Security QRadar 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 in the **Dashboard** tab. If you enable notifications, configure the **Response Limiter** parameter.
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. **Note:** Only normalized events can be logged locally on a QRadar appliance. If you want to send raw event data, you must use the Send to Forwarding Destinations option to send the data to a remote syslog host.

Table 57. Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
Add to Reference Set	Select this check box if you want events that are 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 that 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.

Table 57. Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
Add to Reference Data	Before you can use this rule response, you must create the reference data collection by using the command line interface (CLI). For more information about how to create and use reference data collections, see the *Administration Guide* for your product. Select this check box if you want events that are 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 that 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. **Add to a Reference Table** Select this option to send data to a collection of multiple key/single value pairs, where a type was assigned to the secondary keys. Select the reference table that you want to add data to, and then select a primary key. Select your inner keys (secondary keys) and their values for the data records.
Execute Custom Action	You can write scripts that do specific actions in response to network events. For example, you might write a script to create a firewall rule that blocks a particular source IP address from your network in response to repeated login failures. Select this check box and select a custom action from the **Custom action to execute** list. You add and configure custom actions by using the **Define Actions** icon on the **Admin** tab.
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 about the IF-MAP server.
Response Limiter	Select this check box and use the list boxes to configure the frequency with which you want this rule to respond

Table 57. Anomaly Detection Rule Response page parameters (continued)

Parameter	Description
Enable Rule	Select this check box to enable this rule. By default, the check box is selected.

An SNMP notification might resemble:

```
"Wed Sep 28 12:20:57 GMT 2005, Custom Rule Engine Notification -
 Rule 'SNMPTRAPTst' 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"
```

A 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
```

Related tasks:

"Creating a rule" on page 193
Rules evaluate incoming data against rule test conditions to generate a response from the system. When the conditions of a rule are met, several actions can be taken. For example, you can configure the system response to the rule, which ranges from generating offenses, sending emails, starting scans, adding reference data, or raising or lowering values like severity.

Chapter 12. Historical correlation

Use historical correlation to run past events and flows through the custom rules engine (CRE) to identify threats or security incidents that already occurred.

Restriction: You cannot use historical correlation in IBM Security QRadar Log Manager. For more information about the differences between IBM Security QRadar SIEM and IBM Security QRadar Log Manager, see “Capabilities in your security intelligence product” on page 5.

By default, an IBM Security QRadar SIEM deployment analyzes information that is collected from log sources and flow sources in near real-time. With historical correlation, you can correlate by either the start time or the device time. *Start time* is the time that the event was received by QRadar. *Device time* is the time that the event occurred on the device.

Historical correlation can be useful in the following situations:

Analyzing bulk data
If you bulk load data into your QRadar deployment, you can use historical correlation to correlate the data against data that was collected in real-time. For example, to avoid performance degradation during normal business hours, you load events from multiple log sources every night at midnight. You can use historical correlation to correlate the data by device time to see the sequence of network events as they occurred in the last 24 hours.

Testing new rules
You can run historical correlation to test new rules. For example, one of your servers was recently attacked by new malware for which you do not have rules in place. You can create a rule to test for that malware. Then, you can use historical correlation to check the rule against historical data to see whether the rule would trigger a response if it were in place at the time of the attack. Similarly, you can use historical correlation to determine when the attack first occurred or the frequency of the attack. You can continue to tune the rule and then move it into a production environment.

Re-creating offenses that were lost or purged

If your system lost offenses because of an outage or other reason, you can re-create the offenses by running historical correlation on the events and flows that came in during that time.

Identifying previously hidden threats
As information becomes known about the latest security threats, you can use historical correlation to identify network events that already occurred but did not trigger an event. You can quickly test for threats that have already compromised your organization's system or data.

Historical correlation overview

You configure a historical correlation profile to specify the historical data that you want to analyze and the rule set that you want to test against. When a rule is triggered, an offense is created. You can assign the offense for investigation and remediation.

Data selection

The profile uses a saved search to collect the historical event and flow data to use in the run. Ensure that your security profile grants permission to view the events and flows that you want to include in the historical correlation run.

Rule selection and handling

The QRadar console processes data against only the rules that are specified in the historical correlation profile.

Common rules test data in both events and flows. You must have permission to view both events and flows before you can add common rules to the profile. When a profile is edited by a user who doesn't have permission to view both events and flows, the common rules are automatically removed from the profile.

You can include disabled rules in a historical correlation profile. When the profile runs, the disabled rule is evaluated against the incoming events and flows. If the rule is triggered, and the rule action is to generate an offense, the offense is created even when the rule is disabled. To avoid generating unnecessary distractions, rule responses, such as report generation and mail notifications, are ignored during historical correlation.

Because historical correlation processing occurs in a single location, the rules that are included in the profile are treated as global rules. The processing does not change the rule from local to global, but handles the rule as if it were global during the historical correlation run. Some rules, such as stateful rules, might not trigger the same response as they would in a normal correlation that is run on a local event processor. For example, a local stateful rule that tracks five failed logins in 5 minutes from the same user name behaves differently under normal and historical correlation runs. Under normal correlation, this local rule maintains a counter for the number of failed logins that are received by each local event processor. In historical correlation, this rule maintains a single counter for the entire QRadar system. In this situation, offenses might be created differently compared to a normal correlation run.

Offense creation

Historical correlation runs create offenses only when a rule is triggered and the rule action specifies that an offense must be created. A historical correlation run does not contribute to a real-time offense, nor does it contribute to an offense that was created from an earlier historical correlation run, even when the same profile is used.

The maximum number of offenses that can be created by a historical correlation run is 100. The historical correlation run stops when the limit is reached.

You can view historical offenses on the Threat and Security Monitoring dashboard and on the **Offenses** tab at the same time that you review real-time offenses.

Creating a historical correlation profile

You create a historical correlation profile to rerun past events and flows through the custom rules engine (CRE). The profile includes information about the data set and the rules to use during the run.

Restriction: You can create historical profiles only in IBM Security QRadar SIEM. You cannot create historical profiles in IBM Security QRadar Log Manager.

Before you begin

Common rules test data in both events and flows. You must have permission to view both events and flows before you can add common rules to the profile. When a profile is edited by a user who doesn't have permission to view both events and flows, the common rules are automatically removed from the profile.

About this task

You can configure a profile to correlate by either start time or device time. *Start time* is the time when the events arrive at the event collector. *Device time* is the time that the event occurred on the device. Events can be correlated by start time or device time. Flows can be correlated by start time only.

You can include disabled rules in the profile. Rules that are disabled are indicated in the rules list with **(Disabled)** after the rule name.

A historical correlation run does not contribute to a real-time offense, nor does it contribute to an offense that was created from an earlier historical correlation run, even when the same profile is used.

Procedure

1. Open the Historical Correlation dialog box.
   - On the **Log Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Network Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Offenses** tab, click **Rules** > **Actions** > **Historical Correlation**.
2. Click **Add** and select **Event Profile** or **Flow Profile**.
3. Type a name for the profile and select a saved search. You can use only non-aggregated saved searches.
4. On the **Rules** tab, select the rules to be run against the historical data, and choose the correlation time.

   If you select the **Use all enabled rules** check box, you cannot include disabled rules in the profile. If you want to include both enabled and disabled rules in the profile, you must select them individually from the rules list and click **Add Selected**.
5. On the **Schedule** tab, enter the time range for the saved search and set the profile schedule settings.
6. On the **Summary** tab, review the configuration and choose whether to run the profile immediately.
7. Click **Save**.

   The profile is put into a queue to be processed. Queued profiles that are based on a schedule take priority over manual runs.

Viewing information about historical correlation runs

View the history of a historical correlation profile to see information about past runs for the profile. You can see the list of offenses that were created during the run and the catalog of events or flows that match the triggered the rules in the profile. You can view the history for historical correlation runs that are queued, running, complete, complete with errors, and canceled.

About this task

A historical correlation catalog is created for each rule that is triggered for each unique source IP address during the run, even if an offense was not created. The catalog contains all the events or flows that either fully or partially match the triggered rule.

You cannot build reports on historical correlation data directly from QRadar. If you want to use third-party programs to build reports, you can export the data from QRadar.

Procedure

1. Open the Historical Correlation dialog box.
   - On the **Log Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Network Activity** tab, click **Actions** > **Historical Correlation**.
   - On the **Offenses** tab, click **Rules** > **Actions** > **Historical Correlation**.
2. Select a profile and click **View History**.
   a. If the historical correlation run status is **Completed** and the **Offense Count** is 0, the profile rules did not trigger any offenses.
   b. If the historical correlation run created offenses, in the **Offense Count** column, click the link to see a list of the offenses that were created. If only one offense was created, the offense summary is shown.
3. In the **Catalogs** column, click the links to see the list of events that either fully or partially match the profile rules.

   The **StartTime** column in the event list represents the time that QRadar received the event.
4. Click **Close**.

Chapter 13. X-Force Threat Intelligence feed integration

The IBM Security X-Force Threat Intelligence feed provides an up-to-the-minute list of potentially malicious IP addresses and URLs. This information can be incorporated into rules, offenses, and events, and used to identify any undesirable activity in your network environment before it threatens the stability of your network.

You must have a QRadar license extension to use X-Force Threat Intelligence feed with QRadar.

The content in the X-Force Threat Intelligence feed is given a threat score, which you use to help you prioritize incidents and offenses that are generated through this content. The data from these intelligence sources is automatically incorporated into the QRadar correlation and analysis functions and enriches its threat detection capabilities with Internet threat data. Any security event or network activity data that involves these addresses is automatically flagged, and therefore adds valuable context to security incident analysis and investigations

To prioritize the threat and identify security incidents that require more examination, you can choose which X-Force feeds to incorporate into QRadar rules, offenses, and events. For example, you can use the feeds to identify these types of incidents:

- A series of attempted logins for a dynamic range of IP addresses
- An anonymous proxy connection to a Business Partner portal
- A connection between an internal endpoint and a known botnet command and control
- Communication between an endpoint and a known malware distribution site

The X-Force Threat Intelligence feed categorizes IP addresses and then assigns a confidence rating value to this categorization. A confidence factor value from 0 - 100 is assigned to categorization of the IP reputation data. This confidence value represents how confident X-Force is that the data from this IP address is categorized accurately. An IP reputation categorization of spam with a confidence factor value of 0 indicates that the source IP traffic is definitely not spam, whereas a value of 100 indicates a definite spam source. When you tune your rules, you can use the confidence factor value to adjust the sensitivity of your rule triggers. By adjusting this confidence factor value, you adjust the number of offenses that are generated.

The IP addresses are grouped into the following categories:

- Malware hosts
- SPAM sources
- Dynamic IP addresses
- Anonymous proxies
- Botnet Command and Control
- Scanning IP addresses

The X-Force Threat Intelligence feed also categorizes URL addresses. For example, URL addresses might be categorized as dating, gambling, or pornography sites. To see the complete list of categories for URL classification, see the IBM X-Force Exchange website (https://exchange.xforce.ibmcloud.com/faq).

Before you can use URL-based rules, you must create a custom event property to extract the URL from the payload. The URL custom property is already defined for events from a number of sources such as Blue Coat SG and Juniper Networks Secure Access.

For more information about creating custom event properties, see Custom event and flow properties.

X-Force Threat Intelligence updates and servers

After you add the IBM Security X-Force Threat Intelligence feed to QRadar, you can receive advanced threat data immediately.

Overall, the data set from X-Force is updated every 3 minutes, and the QRadar Console is responsible for all external communications.

The following servers are contacted for both X-Force data updates, licensing, dashboard widget feeds, and QRadar automatic updates:

Table 58. X-Force servers

Server contacted	Server description
www.iss.net	X-Force Threat Intelligence dashboard widget for QRadar (AlertCon / RSS feed)
update.xforce-security.com	X-Force Threat Intelligence Feed update server for IP reputation and URL data
license.xforce-security.com	X-Force Threat Intelligence licensing server
qmmunity.q1labs.com	QRadar automatic updates. For more information about auto-update servers, see www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881).

Enabling X-Force rules in IBM Security QRadar

By adding the X-Force IP Reputation Intelligence Feed license to your QRadar system, enhanced X-Force rules are added.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, click **Rules** > **Rules**.
3. From the **Group** menu, click **XForce Premium**.

   The **Group** column might show both legacy and enhanced rules. By default, X-Force legacy rules are disabled. However, you might see legacy rules that are enabled. Use the newer enhanced rules and not the legacy rules that use the remote nets. The remote nets option is removed.
4. Disable any Legacy Rules, X-Force Premium rules, by selecting the rule row and click **Actions** > **Enable/Disable**.

Enhanced X-Force Threat Intelligence rules

After you add the X-Force Threat Intelligence feed to QRadar, you can start using rules from the Enhanced X-Force rules group.

The following rules are part of the **Enhanced X-Force Rules** group. They can be used as is or you can customize them.

The following rules are IP-based:

X-Force Premium: Internal Connection to Possible Malware Host
This communication indicates a strong possibility that an attempt to infect the client system was made or that malware was downloaded.

X-Force Premium: Internal Hosts Communicating With Anonymous Proxies
Anonymous proxies are addresses that are known for masking identity. They are often used by malware or during advanced persistent threats to hide the origin of communications with external sources. These addresses might be related to activities such as malware communication or data exfiltration.

X-Force Premium: Internal Mail Server Sending Mail to Possible SPAM Host
Typically, mail servers that are communicating with SPAM hosts are being misused.

X-Force Premium: Non-Mail Servers Communicating with Known SPAM Sending Hosts
This behavior is a strong indicator that the server was compromised and is being used as a spam relay.

X-Force Premium: Non-Servers Communicating with an External Dynamic IP
Dynamically assigned IP addresses are not typically associated with legitimate servers on the Internet. Internal workstations that are communicating with dynamic addresses might indicate suspicious internal activity, or malware or botnet activity.

X-Force Premium: Server Initiated Connection to Dynamic Hosts
Generally, servers communicate with hosts that have a fixed identity and not dynamic IP addresses.

Because the URL is a more specific indicator of the data that is transferred, URL-based rules can be more accurate than IP-based rules.

The following rules are URL-based:

X-Force Premium: Internal Host Communicating with Botnet Command and Control URL
Legitimate servers can sometimes be used to provide botnet connectivity at specific URL addresses.

X-Force Premium: Internal Host Communication with Malware URL
Legitimate servers can sometimes be used to deliver malware to specific URL addresses.

Creating a rule using URL categorization to monitor access to certain types of websites

You can create a rule that sends an email notification if users of the internal network access URL addresses that are categorized as gambling websites.

Before you begin

To use URL categorization rules, you must have a subscription to the X-Force Threat Intelligence feed.

To create a new rule, you must have the **Offenses** > **Maintain Custom Rules** permission.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Actions** list, select **New Event Rule**.
4. Read the introductory text on the Rule wizard and click **Next**.
5. Click **Events** and click **Next**.
6. From the **Test Group** list box, select **X-Force Tests**.
7. Click the plus (+) sign beside the **when this URL property is categorized by X-Force as one of the following categories** test.
8. In the **enter rule name here** field in the Rule pane, type a unique name that you want to assign to this rule.
9. From the list box, select **Local** or **Global**.
10. Click the underlined configurable parameters to customize the variables of the test.
    a. Click **URL (custom)**.
    b. Select the URL property that contains the URL that was extracted from the payload and click **Submit**.
    c. Click **one of the following categories**.
    d. Select **Gambling / Lottery** from the X-Force URL categories, click **Add +** and click **Submit**.
11. 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**.
12. On the Groups pane, select the check boxes of the groups to which you want to assign this rule.
13. In the **Notes** field, type a note that you want to include for this rule, and click **Next**.
14. On the Rule Responses page, click **Email** and type the email addresses that receive the notification. For information about other response parameters for an event rule, see Event, Flow and Common Rule Response page parameters.
15. Click **Next**.
16. If the rule is accurate, click **Finish**.

Looking up IP address and URL information in X-Force Exchange

Use right-click menu options in IBM Security QRadar to look up information about IP addresses and URLs that is found on IBM Security X-Force Exchange. You can use the information from your QRadar searches, offenses, and rules to research further or to add information about IP addresses or URLs to an X-Force Exchange collection.

About this task

You can contribute either public or private information to track data in collections when you research security issues.

A *collection* is a repository where you store the information that is found during an investigation. You can use a collection to save X-Force Exchange reports, comments, or any other content. An X-Force Exchange report contains both a version of the report from the time when it was saved, and a link to the current version of the report. The collection also contains a section (timeline) that has a wiki-style notepad where you can add comments that are relevant to the collection.

For more information about X-Force Exchange, see X-Force Exchange (https://exchange.xforce.ibmcloud.com/).

Procedure

1. To look up an IP address in X-Force Exchange from QRadar, follow these steps:
   a. Select the **Log Activity** or the **Network Activity** tab.
   b. Right-click the IP address that you want to view in X-Force Exchange and select **More Options** > **Plugin Options** > **X-Force Exchange Lookup** to open the X-Force Exchange interface.
2. To look up a URL in X-Force Exchange from QRadar, follow these steps:
   a. Select either the **Offenses** tab, or the event details windows available on the **Offenses**.
   b. Right-click the URL you want to look up in X-Force Exchange and select **Plugin Options > X-Force Exchange Lookup** to open the X-Force Exchange interface.

Management of false positives

You use X-Force Threat Intelligence to manage the sensitivity of your rule triggers so that you can reduce the number of false positives in your network. Use false positive tuning to prevent events and flows from correlating into offenses.

Confidence factor

X-Force categorizes IP reputation data, and assigns a confidence factor value from 0 - 100 to that categorization, where 0 represents no confidence, and 100 represents certainty. For example, X-Force might categorize a source IP address as a scanning IP with a confidence factor of 75, which is a moderately high level of confidence.

How do I enter a confidence value?

Enter a confidence value in the following X-Force rule test in QRadar: **when this host property is categorized by X-Force as this category with confidence value equal to this amount**

Guidelines for setting the confidence value

The confidence factor is one of the main tools that you can use to help limit the number of offenses that are created by triggered rules. Depending on the level of protection that you want, you can adjust the confidence values to a level that best matches your network environment.

In a DMZ, you might want to choose a higher confidence value, for example, 95% or higher, because you don't need to investigate many offenses in this area. With this level of confidence, the IP addresses are highly likely to match the category that is listed. If it is 95% certain that a host is serving malware, then you need to know about it.

You lower the confidence value for more secure areas of the network such as a server pool. By lowering the confidence level, more threats are potentially identified, and you spend less effort investigating because the threat pertains to a specific network segment.

For optimum false positive tuning, manage your rule triggers by segment. Look at your network infrastructure and decide what assets need a high level of protection, and what assets don't. You can apply different confidence values for the different network segments. Use building blocks for grouping commonly used tests, so that they can be used in rules.

URL-based rules

You might see false positives from shared virtual hosting sites because one site might serve legitimate content while another site from the same IP address serves malware. In a shared virtual hosting setup, URL information is helpful because the URL is a more specific indicator of the data that is transferred. URL-based rules can be more accurate than IP-based rules.

For URL-based rules, you must create a custom event property to extract the URL from the payload.

For more information about tuning false positives, see the *Tuning Guide*.

Chapter 14. Report management

You can use the **Reports** tab to create, edit, distribute, and manage reports.

Detailed, flexible reporting options satisfy your various regulatory standards, such as PCI compliance.

You can create your own custom reports or use a default reports. You can customize and rebrand default reports and distribute these to other users.

The **Reports** tab might require an extended period of time to refresh if your system includes many 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 session must be synchronized with your timezone.

During the installation and setup of QRadar products, the time zone is configured. Check with your administrator to ensure your QRadar session is synchronized with your timezone.

Report tab permissions

Administrative users can view all reports that are created by other users.

Non-administrative users can view reports that they created only or reports that are shared by other users.

Report 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.

If a report does not specify an interval schedule, you must manually generate the report.

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 layout

A report can consist of several data elements and can represent network and security data in various 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 many 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.

You can use any of the following types of charts:

- **None** - Use this option to display an empty container 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** - Use this 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. This chart is available after you install IBM Security QRadar Vulnerability Manager.
- **Connections** - This chart option is only displayed if you purchased and licensed IBM Security QRadar Risk Manager. For more information, see the *IBM Security QRadar Risk Manager User Guide*.
- **Device Rules** - This chart option is only displayed if you purchased and licensed IBM Security QRadar Risk Manager. For more information, see the *IBM Security QRadar Risk Manager User Guide*.
- **Device Unused Objects** - This chart option is only displayed if you purchased and licensed IBM Security QRadar Risk Manager. For more information, see the *IBM Security QRadar Risk Manager User Guide*.
- **Events/Logs** - Use this chart to view event information. You can base your charts on data from saved searches from the **Log Activity** tab. You can 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.
- **Log Sources** - Use this chart to export or report on log sources. Select the log sources and log source groups that you want to appear in the report. Sort log sources by report columns. Include log sources not reported for a defined time period. Include log sources that were created in a specified time.
- **Flows** - Use this 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** - Use this chart to display the top destination IPs in the network locations you select.
- **Top Offenses** - Use this chart to display the Top offenses that occur at present time for the network locations you select.

- **Top Source IPs** - Use this chart to display and sort the top offense sources (IP addresses) that attack your network or business assets.
- **Vulnerabilities** - The Vulnerabilities option is only displayed when the IBM Security QRadar Vulnerability Manager has been purchased and licensed. For more information, see the *IBM Security QRadar Vulnerability Manager User Guide*.

Report 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 59. Report toolbar options

Option	Description
Group	
Manage Groups	Click **Manage Groups** to manage report groups. Using the Manage Groups feature, you can organize your reports into functional groups. You can share report groups with other users.

Table 59. Report toolbar options (continued)

Option	Description
Actions	Click **Actions** to perform the following actions: • **Create** - Select this option to create a new 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. • **Assign Groups** - Select this option to assign the selected report to a report group. • **Share** - Select this option to share the selected report with other users. You must have administrative privileges to share reports. • **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. 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.
Hide Interactive 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.

Table 59. Report toolbar options (continued)

Option	Description
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 Group • Report Groups • Report Author User Name

Graph types

Each chart type supports various graph types that you can use to display data.

The network configuration files determine the colors that the charts use to depict network traffic. Each IP address is depicted by using a unique color. The following table provides examples of how network and security data is used in charts. The table describes the chart types that are available for each type of graph.

Table 60. Graph types

Graph type	Available chart types
Line	• Events/Logs • Flows • Connections • Vulnerabilities
Stacked Line	• Events/Logs • Flows • Connections • Vulnerabilities
Bar	• Events/Logs • Flows • Asset Vulnerabilities Connections • Connections • Vulnerabilities
Horizontal Bar	• Top Source IPs • Top Offenses • Top Destination IPs
Stacked Bar	• Events/Logs • Flows • Connections

Table 60. Graph types (continued)

Graph type	Available chart types
Pie	• Events/Logs • Flows • Asset Vulnerabilities • Connections • Vulnerabilities
Table	• Events/Logs • Flows • Top Source IPs • Top Offenses • Top Destination IPs • Connections • Vulnerabilities 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.

The following graph types are available for QRadar Log Manager reports:

- Line Graph
- Stacked Line Graph
- Bar Graph
- Stacked Bar Graph
- Pie Graph
- Table Graph

Note: When you create bar and stacked bar graph reports, the legend is presented in a fixed format, where the bars or bar sections are represented by color coded labels in most cases. If you select time as the value for the x axis, you can create time intervals on the x axis.

Creating custom reports

Use the Report wizard to create and customize a new report.

Before you begin

You must have appropriate network permissions to share a generated report with other users.

For more information about permissions, see the *IBM Security QRadar SIEM Administration Guide*.

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 you create a report that generates weekly or monthly, the scheduled time must elapse 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 seven days to build the data. This search will return results after 7 days.

When you specify the output format for the report, consider that the file size of generated reports can be one to 2 megabytes, depending on the selected output format. PDF format is smaller in size and does not use a large quantity of disk storage space.

Procedure

1. Click the **Reports** tab.
2. From the **Actions** list box, select **Create**.
3. On the Welcome to the Report wizard! window, click **Next**.
4. Select one of the following options:

Option	Description
Manually	By default, the report generates 1 time. You can generate the report as often as you want.
Hourly	Schedules the report to generate at the end of each hour. The data from the previous hour is used. 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.
Weekly	Schedules the report to generate weekly using the data from the previous week. Select the day that 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. From the list box, select the date that you want to generate the report. The default is the first day of the month. Select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

5. In the **Allow this report to generate manually** pane, **Yes** or **No**.

6. Configure the layout of your report:
   a. From the **Orientation** list box, select **Portrait** or **Landscape** for the page orientation.
   b. Select one of the six layout options that are displayed on the Report wizard.
   c. Click **Next** .
7. Specify values for the following parameters:

Parameter	Values
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.
Pagination Options	From the list box, select a location for page numbers to display on the report. You can choose not to have page numbers display.
Report Classification	Type a classification for this report. You can type up to 75 characters in length. You can use leading spaces, special characters, and double byte characters. The report classification displays in the header and footer of the report. You might want to classify your report as `confidential`, `highly confidential`, `sensitive`, or `internal`.

8. Configure each container in the report:
   a. From the **Chart Type** list box, select a chart type.
   b. On the Container Details window, configure the chart parameters.

      Note: You can also create asset saved searches. From the **Search to use** list box, select your saved search.
   c. Click **Save Container Details**.
   d. If you selected more than one container, repeat steps a to c.
   e. Click **Next** .
9. Preview the Layout Preview page, and then click **Next**.
10. Select the check boxes for the report formats you want to generate, and then click **Next**.

    Important: Extensible Markup Language is only available for tables.
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. **Report Console** is the default distribution channel.
Select the users that should be able to view the generated report.	This option displays after you select the **Report Console** check box. From the list of users, select the users that you want to grant permission to view the generated reports.

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 users to view the generated reports. You must have appropriate network permissions to share the generated report with other users.
Email	Select this check box if you want to distribute the generated report by 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 are 255. 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 to the Report Console in the email.

12. On the Finishing Up page, enter values for the following parameters.

Option	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.
Please select any groups you would like this report to be a member of	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.

13. Click **Next** to view the report summary.
14. On the Report Summary page, select the tabs available on the summary report to preview your report configuration.

Results

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 reconfigure 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.

Editing a report

Using the Report wizard, you can edit any default or custom report to change.

About this task

You can use or customize a significant number of default reports. The default **Reports** tab displays the list of reports. Each report captures and displays the existing data.

Note: When you customize a scheduled report to generate manually, select the time span **End Date** before you select the **Start Date**.

Procedure

1. Click the **Reports** tab.
2. Double-click the report that you want to customize.
3. On the Report wizard, change the parameters to customize the report to generate the content you require.

Results

If you reconfigure 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, which is 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 PDF, HTML, RTF, XML, and XLS formats.

Note: 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 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 starts a new browser window. This new window launch is the result of the Mozilla Firefox web browser configuration and does not affect QRadar. You can close the window and continue with your QRadar session.

Procedure

1. Click the **Reports** tab.

2. From the list box in the **Generated Reports** column, select the time-stamp of report you want to view.
3. Click the icon for the format you want to view.

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

1. Click the **Report**s tab.
2. Select the reports for which you want to delete the generated content.
3. From the **Actions** list box, click **Delete Generated Content**.

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 that 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

1. Click the **Reports** tab.
2. Select the report that you want to generate.
3. Click **Run Report**.

What to do next

After the report generates, you can view the generated report from the Generated Reports column.

Duplicating a report

To create a report that closely resembles an existing report, you can duplicate the report that you want to model, and then customize it.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to duplicate.
3. From the **Actions** list box, click **Duplicate**.
4. Type a new name, without spaces, for the report.

What to do next

You can customize the duplicated 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.

You can only share the report with users that have the appropriate access.

Procedure

1. Click the **Reports** tab.
2. Select the reports that you want to share.
3. From the **Actions** list box, click **Share**.
4. From the list of users, select the users with whom you want to share this report.

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 that 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, 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

1. Click the **Reports** tab.
2. On the navigation menu, click **Branding**.
3. Click **Browse** to browse the files that are located on your system.
4. Select the file that contains the logo you want to upload. Click **Open**.
5. Click **Upload Image**.
6. Select the logo that you want to use as the default and click **Set Default Image**.

Report groups

You can sort reports into functional groups. If you categorize reports into groups, you can efficiently organize and find reports.

For example, you can view all reports that are 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 report group

You can create new groups.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. Using the navigation tree, select the group under which you want to create a new group.
4. Click **New Group**.
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** - Optional. Type a description for this group. The description can be up to 255 characters in length.
6. Click **OK**.
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.

8. Close the Report Groups window.

Editing a group

You can edit a report group to change the name or description.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, select the group that you want to edit.
4. Click **Edit**.
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** - Optional. Type a description for this group. The description can be up to 255 characters in length. This field is optional.
6. Click **OK**.
7. Close the Report Groups window.

Sharing report groups

You can share report groups with other users.

Before you begin

You must have administrative permissions to share a report group with other users.

For more information about permissions, see the *IBM Security QRadar SIEM Administration Guide*.

You cannot use the Content Management Tool (CMT) to share report groups.

For more information about the CMT, see the *IBM Security QRadar SIEM Administration Guide*

About this task

On the Report Groups window, shared users can see the report group in the report list.

Any updates that the user makes to a shared report group does not affect the original version of the report. Only the owner can delete or modify.

A copy of the report is created when a user duplicates or runs the shared report. The user can edit or schedule reports within the copied report group.

The group sharing option overrides previous report sharing options that were configured for reports in the group.

Procedure

1. Click the **Reports** tab.
2. On the **Reports** window, click **Manage Groups**.

3. On the **Report Groups** window, select the report group that you want to share and click **Share**.
4. On the **Sharing Options** window, select one of the following options.

Option	Description
Default (inherit from parent)	The report group is not shared. Any copied report group or generated report remains in the users report list. Each report in the group is assigned any parent report sharing option that was configured.
Share with Everyone	The report group is shared with all users.
Share with users matching the following criteria...	The report group is shared with specific users. **User Roles** Select from the list of user roles and press the add icon (+). **Security Profiles** Select from the list of security profiles and press the add icon (+).

5. Click **Save**.

Results

On the Report Groups window, shared users see the report group in the report list. Generated reports display content based on security profile setting.

Assign a report to a group

You can use the **Assign Groups** option to assign a report to another group.

Procedure

1. Click the **Reports** tab.
2. Select the report that you want to assign to a group.
3. From the **Actions** list box, select **Assign Groups**.
4. From the **Item Groups** list, select the check box of the group you want to assign to this report.
5. Click **Assign Groups**.

Copying a report to another group

Use the **Copy** icon to copy a report to one or more report groups.

Procedure

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, select the report that you want to copy.
4. Click **Copy**.
5. Select the group or groups to which you want to copy the report.
6. Click **Assign Groups**.

7. Close the Report Groups window.

Removing a report

Use the **Remove** icon to 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

1. Click the **Reports** tab.
2. Click **Manage Groups**.
3. From the navigation tree, navigate to the folder that contains the report you want to remove.
4. From the list of groups, select the report that you want to remove.
5. Click **Remove**.
6. Click **OK**.
7. Close the Report Groups window.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may 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 may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may 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 may 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 may 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 may 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 may 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 wish 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 may 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 may vary significantly. Some measurements may 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 may have been estimated through extrapolation. Actual results may 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 may 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 may 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 www.ibm.com/legal/copytrade.shtml.

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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Java™
COMPATIBLE

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

“A” “B” “C” “D” on page 244 “E” on page 244 “F” on page 244 “G” on page 245 “H” on page 245 “I” on page 245 “K” on page 246 “L” on page 246 “M” on page 246 “N” on page 246 “O” on page 247 “P” on page 247 “Q” on page 247 “R” on page 247 “S” on page 248 “T” on page 248 “V” on page 249 “W” on page 249

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP See Dynamic Host Configuration Protocol.

DNS See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

flow A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a

managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS See intrusion prevention system.

ISP See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L See Local To Local.

L2R See Local To Remote.

LAN See local area network.

LDAP See Lightweight Directory Access Protocol.

leaf In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L See Remote To Local.

R2R See Remote To Remote.

recon See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report
In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule
A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

Index

Printed in USA