IBM Security QRadar SIEM
Version 7.1.0 (MR2)

Getting Started Guide

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 35.

CONTENTS

ABOUT THIS GUIDE

1 OVERVIEW

2 ACCESS THE QRADAR SIEM USER INTERFACE

3 QRADAR SIEM DEPLOYMENT

4 USING QRADAR SIEM

A GLOSSARY

B NOTICES AND TRADEMARKS

INDEX

ABOUT THIS GUIDE

The *IBM Security QRadar SIEM Getting Started Guide* provides instructions for getting started using QRadar SIEM.

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.

Documentation Conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

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

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

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

Technical Documentation

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

Contacting Customer Support

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

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 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.

1 OVERVIEW

You can perform basic QRadar SIEM configuration, begin collecting event and flow data, and learn how to generate your own custom or default reports.

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.

Log activity tab

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

The **Log Activity** tab displays event information as records from a log source, such as a firewall or router device. Using the **Log Activity** tab, you can:

- Perform in-depth investigations on event data.
- Investigate event logs sent to QRadar SIEM in real time.
- Perform advanced events searches.
- View log activity using configurable time-series charts.
- Quickly identify false positives and tune QRadar SIEM.

For more information, see **Using QRadar SIEM**.

Network activity tab

You can investigate the communication sessions between two hosts.

The **Network Activity** tab display information about how network traffic is communicated, and what was communicated (if the content capture option is enabled). Using the **Network Activity** tab, you can:

- Investigate flows sent to QRadar SIEM in real time.
- Perform powerful searches.
- View network activity using configurable time-series charts.

For more information, see **Using QRadar SIEM**.

Assets tab

QRadar SIEM automatically creates asset profiles by discovering your network assets (servers and hosts) using passive flow data and vulnerability data.

Asset profiles provide information about each known asset in your network, including the services that are running. Asset profile information is used for correlation purposes, which helps reduce false positives. Using the **Assets** tab, you can:

- Search for assets.
- View all the learned assets.
- View identity information for learned assets.
- Tune false positive vulnerabilities.

For more information, see **Using QRadar SIEM**.

Offenses tab

You can investigate offenses to determine the root cause of a network issue.

The **Offenses** tab allows you to view all offenses occurring on your network. To locate offenses, you can use various navigation and search options. Using the **Offenses** tab, you can:

- Investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.
- Correlate events and flows sourced from multiple networks to the same destination IP address.
- Investigate each offense in your network. You can navigate the various pages of the **Offenses** tab to investigate event and flow details to determine the unique events that caused the offense.

For more information about **Offenses** tab, see **Investigate offenses**.

Reports tab

You can create custom reports in QRadar SIEM or use default reports.

You can customize and rebrand default reports and distribute these to other QRadar SIEM users. Administrative users can view all reports created by other QRadar SIEM users. Non-administrative users can only view reports that they created or reports which are shared by other users. Using the **Reports** tab, you can:

- Create, distribute, and manage reports for any data within QRadar SIEM.
- Create customized reports for operational and executive use.
- Combine information (such as, security or network) into a single report.
- Use pre-installed report templates.

- Brand your reports with customized logos enabling you to support various unique logos for each report. This is beneficial for distributing reports to different audiences.

For more information about reports, see **Manage reports**.

2 ACCESS THE QRADAR SIEM USER INTERFACE

You access the IBM Security QRadar SIEM console from a supported web browser and log in using a default user name and the password assigned to you by your administrator.

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

Communication between the web browser and QRadar SIEM is encrypted with Secure Socket Layer (SSL) and Transport Layer Security (TLS).

Supported web browsers

The QRadar SIEM user interface is accessed using a supported web browser.

If you are using Mozilla Firefox, you must add an exception to Mozilla Firefox to log in to QRadar SIEM. For more information, see your Mozilla documentation. If you are using Internet Explorer, a certificate error message is displayed. You must select the **Continue to this website** option to continue.

Supported browsers are described in the following table:

Table 3-1 QRadar SIEM supported web browsers

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

Logging in to QRadar SIEM

You can log in to QRadar SIEM using a default user name and password assigned to you by your administrator.

About this task

QRadar SIEM uses a self-assigned SSL certificate for encryption. These certificates are not recognized by most web browsers. An error message can be displayed regarding an invalid SSL certificate.

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

Procedure

Step 1 Open your web browser.

Step 2 Type the following address in the address bar:

https://**`<IP Address>`**

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

Step 3 Type the default user name and password.

The default values are:

User name: **admin**

Password: **<root password>**

Where `<root password>` is the password assigned to QRadar SIEM during the installation process. For more information, see the *IBM Security QRadar SIEM Installation Guide*.

Click **Login To QRadar**.

Enabling compatibility view for Internet Explorer

You can enable compatibility view for Internet Explorer 8.0 and 9.0.

Procedure

Step 1 Press F12 to open the Developer Tools window.

Step 2 Configure the following compatibility settings:

Table 3-2 Internet explorer compatibility settings

Browser Version	Option	Description
Internet Explorer 8.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 8.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**
Internet Explorer 9.0	Browser Mode	From the **Browser Mode** list box, select **Internet Explorer 9.0.**
	Document Mode	From the **Document Mode** list box, select **Internet Explorer 7.0 Standards.**

3 QRADAR SIEM DEPLOYMENT

Before you can evaluate QRadar SIEM key capabilities, you must first deploy QRadar SIEM.

Administrators can perform the following tasks:

- Install the QRadar SIEM appliance. For more information, see **Installing the QRadar SIEM appliance**.
- Configure your QRadar SIEM installation. For more information, see **QRadar SIEM configuration**.
- Collect event, flow, and Vulnerability Assessment (VA) data. For more information, see **Data collection**.
- Tune your QRadar SIEM installation. For more information, see **Tune QRadar SIEM**.

QRadar SIEM appliance

The QRadar SIEM evaluation appliance is a two-unit rack mount server. Rack rails or shelving are not provided with evaluation equipment.

The QRadar SIEM appliance includes four network interfaces. For this evaluation, use the interface that is labeled ETH0 as the management interface.

You can use the three remaining monitoring interfaces for flow collection. The QRadar QFlow Collector provides full network application analysis and can perform packet captures on the beginning of each conversation. Depending on the QRadar SIEM appliance, flow analysis automatically begins when a span port or tap is connected to any interface other than ETH0. Extra steps can be required to enable the QRadar QFlow Collector component within QRadar SIEM.

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

Note: The QRadar SIEM evaluation appliance has a 50 Mbps limit for flow analysis. Ensure that the aggregate traffic on the monitoring interfaces for flow collection does not exceed 50 Mbps.

Installing the QRadar SIEM appliance

Administrators must install the QRadar SIEM appliance to enable access to the user interface.

Before you begin

Before you install the QRadar SIEM evaluation appliance, ensure that you have:

- Space for a two-unit appliance.
- Rack rails and shelving (mounted).
- USB keyboard and standard VGA monitor for Console access (optional).

Procedure

Step 1 Connect the management network interface to the port labeled ETH0.

Step 2 Plug the dedicated power connections into the rear of the appliance.

Step 3 If you need Console access, connect the USB keyboard and standard VGA monitor.

Step 4 If there is a front panel on the appliance. Remove the panel by pushing in the tabs on either side and pulling the panel away from the appliance.

Step 5 Power on the appliance.

Note: The power button is on the front of the appliance.

QRadar SIEM configuration

By configuring QRadar SIEM you can review your network hierarchy and customize automatic updates.

Before you configure QRadar SIEM, confirm that the desktop you use to access the QRadar SIEM Console has the following installed:

- Java[TM] Runtime Environment (JRE) - You can download Java version 1.6.0_u20 at the following website: *http://java.com/*.
- Adobe Flash 10.x

To set up your configuration, you must:

- Review you network hierarchy. For more information, see **Network hierarchy** and **Reviewing your network hierarchy**.
- Configure automatic update settings. For more information, see **Configuring automatic update settings**.

Network hierarchy

You can view different areas of your network that is organized by business function and prioritize threat and policy information according to business value risk.

QRadar SIEM uses the network hierarchy to:

- Understand network traffic and view network activity.
- Monitor specific logical groups or services in your network, such as marketing, DMZ, or VoIP.
- Monitor traffic and profile the behavior of each group and host within the group.
- Determine and identify local and remote hosts.

For evaluation purposes, a default network hierarchy is included that contains predefined logical groups. Review the network hierarchy for accuracy and completeness. If your environment includes network ranges that are not displayed in the preconfigured network hierarchy, you must add them manually.

The objects that are defined in your network hierarchy do not have to be physically in your environment. All logical network ranges belonging to your infrastructure must be defined as a network object.

Note: If your system does not include a completed network hierarchy, use the **Admin** tab to create a hierarchy specific to your environment. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

Reviewing your network hierarchy

You can review your network hierarchy.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Network Hierarchy** icon.

Step 4 From the **Manage Group:Top** list, click **Regulatory_Compliance_Servers**.

If your network hierarchy does not include a regulatory compliance server component, you can use your Mail component for the remainder of this procedure.

Step 5 Click the **Edit this object** icon.

Step 6 To add compliance servers:

a In the **IP/CIDR(s)** field, type the IP address or CIDR range of your compliance servers.

b Click **Add**.

c Repeat for all compliance servers.

d Click **Save**.

e Repeat this process for any other networks that you want to edit.

Step 7 On the **Admin** tab menu, click **Deploy Changes**.

Step 8 Close the Network Hierarchy window.

Configuring automatic update settings

You can customize the frequency of QRadar SIEM updates, update types, server configuration, and backup settings.

About this task

Using the automatic update settings, QRadar SIEM update files can include the following updates:

- Configuration updates, which include configuration file changes, vulnerability, QID map, and security threat information updates.

- DSM updates, which include corrections to parsing issues, scanner changes, and protocol updates.
- Major updates, which include items such as updated Java^{TM} Archive (JAR) files.
- Minor updates, which include items such as extra Online Help Content or updated scripts.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Auto Update** icon.

Step 4 On the navigation menu, click **Change Settings**.

Step 5 In the **Auto Update Schedule** pane, accept the default parameters.

Step 6 In the **Update Types** pane, configure the following parameters:

a From the **Configuration Updates** list box, select **Auto Update**.

b For the following parameters accept the default values:

- DSM, Scanner, Protocol Updates.
- Major Updates.
- Minor Updates.

Step 7 Clear the **Auto Deploy** check box.

By default, the check box is selected. If the check box is not selected, a system notification is displayed on the **Dashboard** tab to indicate that you must deploy changes after updates are installed.

Step 8 Click the **Advanced** tab.

Step 9 In the Server Configuration pane, accept the default parameters.

Step 10 In the Other Settings pane, accept the default parameters.

Step 11 Click **Save** and close the Updates window.

Step 12 From the toolbar, click **Deploy Changes**.

What to do next

For detailed information about automatic update settings, parameters, and configurations options, see the *IBM Security QRadar SIEM Users Guide*.

Data collection

QRadar SIEM accepts information in various formats and from a wide range of devices, including security events, network traffic, and scan results.

Collected data is categorized into three major sections: events, flows, and VA information.

Events

Events are generated by log sources such as firewalls, routers, UNIX, Linux, or Windows servers, and Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS).

The majority of log sources send information to QRadar SIEM using the syslog protocol. QRadar SIEM also supports Simple Network Management Protocol (SNMP), Java Database Connectivity (JDBC), and Security Device Event Exchange (SDEE).

By default, QRadar SIEM automatically detects log sources after a specific number of identifiable logs are received within a certain time frame. After the log sources are successfully detected, QRadar SIEM adds the appropriate Device Support Module (DSM) to the Log Sources window in the **Admin** tab.

Although most DSMs include native log sending capability, several DSMs require extra configuration or an agent or both to send logs. Configuration varies between DSM types. You must ensure the DSMs are configured to send logs in a format that QRadar SIEM supports. For more information about configuring DSMs, see the *DSM Configuration Guide*.

Certain log source types, such as routers and switches, do not send enough logs for QRadar SIEM to quickly detect and add them to the Log Source list. You can manually add these log sources. For more information about manually adding log sources, see the *Log Sources User Guide*.

Flows

Flows provide information about network traffic and can be sent to QRadar SIEM in various formats, including flowlog files, NetFlow, J-Flow, sFlow, and Packeteer.

By accepting multiple flow formats simultaneously, QRadar SIEM can detect threats and activities that would otherwise be missed by relying strictly on events for information.

QRadar QFlow Collectors provides full application detection of network traffic regardless of the port on which the application is operating. For example, if the Internet Relay Chat (IRC) protocol is communicating on port 7500/TCP, a QRadar QFlow Collector identifies the traffic as IRC and provides a packet capture of the beginning of the conversation. NetFlow and J-Flow only notify you that there is traffic on port 7500/TCP without providing any context for what protocol is being used.

Common mirror port locations include core, DMZ, server, and application switches, with NetFlow providing supplemental information from border routers and switches.

QRadar QFlow Collectors are enabled by default and require a mirror, span, or tap to be connected to an available interface on the QRadar SIEM appliance. Flow analysis automatically begins when the mirror port is connected to one of the network interfaces on the QRadar SIEM appliance. By default, QRadar SIEM monitors on the management interface for NetFlow traffic on port 2055/UDP. You can assign extra NetFlow ports, if required.

Vulnerability Assessment information

QRadar SIEM can import VA information from various third-party scanners. VA information helps QRadar SIEM identify active hosts, open ports, and potential vulnerabilities. QRadar SIEM uses VA information to rank the magnitude of offenses on your network. Depending on the VA scanner type, QRadar SIEM can import scan results from the scanner server or remotely start a scan.

Collecting events

By collecting events, you can investigate the logs sent to QRadar SIEM in real time.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 Click the **Log Sources** icon.

Step 4 Review the list of log sources and make any necessary changes to the log source.

For information about configuring log sources, see the *Log Sources User Guide*.

Step 5 Close the Log Sources window.

Step 6 On the **Admin** tab menu, click **Deploy Changes**.

Collecting flows

By collecting flows, you can investigate the network communication sessions between hosts.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, select **Data Sources > Flows**.

Step 3 Click the **Flow Sources** icon.

Step 4 Review the list of flow sources and make any necessary changes to the flow sources.

For instructions on how to configure flow sources, see the *IBM Security QRadar SIEM Administration Guide*.

Step 5 Close the Flow Sources window.

Step 6 On the **Admin** tab menu, click **Deploy Changes**.

Note: For more information about how to enable flows on third-party network devices, such as switches and routers, see your vendor documentation.

Importing vulnerability assessment information

By importing VA information, you can identify active hosts, open ports, and potential vulnerabilities.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, select **Data Sources > Vulnerability**.

Step 3 Click the **VA Scanners** icon.

Step 4 Click **Add**.

Step 5 Enter the values for the parameters.

The parameters depend on the scanner type you want to add. For more information, see the *Vulnerability Assessment Configuration Guide*.

Note: The CIDR Range specifies which networks QRadar SIEM integrates into the scan results. For example, if you want to conduct a scan against the 192.168.0.0/16 network and specify 192.168.1.0/24 as the CIDR range, only results from the 192.168.1.0/24 range are integrated.

Step 6 Click **Save**.

Step 7 On the **Admin** tab menu, click **Deploy Changes**.

Step 8 Click the **Schedule VA Scanners** icon.

Step 9 Click **Add**.

Step 10 Specify the criteria for how often you want the scan to occur.

Depending on the scan type, this includes how frequently QRadar SIEM imports scan results or starts a new scan. You also must specify the ports to be included in the scan results.

Step 11 Click **Save**.

Tune QRadar SIEM

You can tune QRadar SIEM to meet the needs of your environment.

CAUTION: *Before you tune QRadar SIEM, wait one day to enable* QRadar SIEM *to detect servers on your network, store event and flows, and create offenses that are based on existing rules.*

Administrators can perform the following tuning tasks:

- Optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity** Quick Filter property**.** For more information, see **Payload indexing**.

- Provide a faster initial deployment and easier tuning by automatically or manually adding servers to building blocks. For more information, see **Servers and building blocks**.
- Configure responses to event, flow, and offense conditions by creating or modifying custom rules and anomaly detection rules. For more information, see **QRadar SIEM rules**.
- Ensure that each host in your network creates offenses that are based on the most current rules, discovered servers, and network hierarchy. For more information, see **Cleaning the SIM model**.

Payload indexing

Use Quick Filter, which is available on the **Log Activity** and **Network Activity** tabs, to search event and flow payloads.

To optimize this search feature, you can enable a payload index on the Quick Filter property. By default, the payload index retention period is one week. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

CAUTION: *Enabling payload indexing might decrease system performance. Monitor the index statistics after you enable payload indexing on the Quick Filter property. For more information about index management and statistics, see the IBM Security QRadar SIEM Administration Guide.*

Enabling payload indexing

You can optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity** Quick Filter property**.**

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Index Management** icon.

Step 4 In the **Quick Search** field, type **Quick Filter**.

Step 5 Click the **Quick Filter** property that you want to index.

Step 6 Click **Enable Index**.

Step 7 Click **Save**.

Step 8 Click **OK**.

What to do next

For detailed information about the parameters that are displayed in the Index Management window, see the *IBM Security QRadar SIEM Administration Guide*.

Disabling payload indexing

You can disable payload indexing on the **Log** and **Network Activity** tabs Quick Filter property.

Procedure

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **System Configuration**.

Step 3 Click the **Index Management** icon.

Step 4 In the **Quick Search** field, type **Quick Filter**.

Step 5 Click the **Quick Filter** property that you want to disable.

Step 6 Choose one of the following options:

- Click **Disable Index**.
- Right-click a property and select **Disable Index** from the menu.

Step 7 Click **Save**.

Step 8 Click **OK**.

Results

The selected properties are no longer indexed. In lists that include event or flow properties which are indexed, property names are no longer appended with the following text: `[Indexed]`.

What to do next

For detailed information about the parameters that are displayed in the Index Management window, see the *IBM Security QRadar SIEM Administration Guide*.

Servers and building blocks

QRadar SIEM automatically discovers and classifies servers in your network, providing a faster initial deployment and easier tuning when network changes occur.

The Server Discovery function uses the asset profile database to discover several types of servers on your network. The Server Discovery function lists automatically discovered servers, enabling you to select which servers you want to include in building blocks.

Note: For extra information about discovering servers, see the *IBM Security QRadar SIEM Administration Guide*.

Using Building blocks, you can reuse specific rule tests in other rules. QRadar SIEM uses building blocks to tune the system and enable extra correlation rules. This helps you to reduce the number of false positives that are detected by QRadar SIEM and focus on identifying business critical assets.

Adding servers to building blocks automatically

You can automatically add servers to building blocks.

Procedure

Step 1 Click the **Assets** tab.

Step 2 On the navigation menu, click **Server Discovery**.

Step 3 From the **Server Type** list box, select the server type that you want to discover.

Leave the remaining parameters as default.

Step 4 Click **Discover Servers**.

Step 5 In the **Matching Servers** table, select the check box of all servers you want to assign to the server role.

Step 6 Click **Approve Selected Servers**.

Note: You can right-click any IP address or hostname to display DNS resolution information.

Adding servers to building blocks manually

If a server is not automatically detected, you can manually add the server to its corresponding Host Definition Building Block.

About this task

To ensure that the appropriate rules are applied to the server type, you can add individual devices or entire address ranges of devices. You can manually enter server types, that do not conform to unique protocols, into their respective Host Definition Building Block. For example, adding the following server types to building blocks reduces the need for further false positive tuning:

- Add **Network management servers** to BB:HostDefinition: Network Management Servers building block.
- Add **Proxy servers** to BB:HostDefinition: Proxy Servers building block.
- Add **Virus and Windows Update Servers** to BB:HostDefinition: Virus Definition and Other Update Servers building block.
- Add **VA Scanners** to BB-HostDefinition: VA Scanner Source IP building block.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 From the **Display** list box, select **Building Blocks**.

Step 4 From the **Group** list box, select **Host Definitions**.

The name of the building block corresponds with the server type. For example, *BB:HostDefinition: Proxy Servers* applies to all proxy servers in your environment.

Building blocks include hosts that were automatically discovered when you performed the **Adding servers to building blocks automatically** task.

Step 5 To manually add a host or network, double-click the corresponding host definition Building Block appropriate to your environment.

Step 6 In the **Building Block** field, click the underlined value after the phrase ***when either the source or destination IP is one of the following***.

Step 7 In the **Enter an IP address or CIDR and click 'Add'** field, type the hostnames or IP address ranges that you want to assign to the building block.

Step 8 Click **Add**.

Step 9 Click **Submit**.

Step 10 Click **Finish**.

What to do next

Repeat these steps for each server type that you want to add.

QRadar SIEM rules

Rules perform tests on events, flows, or offenses, and if all the conditions of a test are met, the rule generates a response.

QRadar SIEM includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. For more information on rules, see the *IBM Security QRadar SIEM Administration Guide*.

The two rule categories are:

- Custom Rules - Custom rules perform tests on events, flows, and offenses to detect unusual activity in your network.
- Anomaly Detection Rules - Anomaly detection rules perform tests on the results of saved flow or event searches to detect when unusual traffic patterns occur in your network.

Note: A user with non-administrative access can create rules for areas of the network that they can access. You must have the appropriate role permissions to manage rules. For more information about user role permissions, see the *IBM Security QRadar SIEM Administration Guide*.

Configuring rules

You can modify the default QRadar SIEM rules to match your security needs.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 On the navigation menu, click **Rules**.

Step 3 Click the **Enabled** column header to sort the rules by their enabled or disabled status.

Step 4 From the **Group** list box, select **Compliance**.

Step 5 Select the **Compliance: Compliance Events Become Offenses** rule.

Step 6 From the menu, select **Actions > Enable/Disable**.

Step 7 If you want to modify the rule criteria, select **Action > Edit**.

Cleaning the SIM model

You can ensure that each host creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

About this task

When you clean the SIM model, all existing offenses are closed. Cleaning the SIM model does not affect existing events and flows.

Procedure

Step 1 Click the **Admin** tab.

Step 2 From the **Advanced** menu, select **Clean SIM Model**.

Step 3 Select the **Hard Clean** option.

Step 4 Select the **Are you sure you want to reset the data model?** check box.

Step 5 Click **Proceed**.

What to do next

After the SIM reset process is complete, refresh your browser.

4 USING QRADAR SIEM

You can use QRadar SIEM to perform event, flow, and asset searches, investigate offenses, and create reports.

QRadar SIEM provides a powerful and flexible engine for searching large volumes of information. You can search information by using default searches (Saved Searches) in the Log Activity and Network Activity tabs, or you can create and save your own custom searches.

Administrators can perform the following tasks:

- Search event data by using specific criteria and display events that match the search criteria in a results list. Select, organize, and group the columns of event data. For more information, see **Searching events**.
- Visually monitor and investigate flow data in real time, or perform advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated. For more information, see **Searching flows**.
- View all the learned assets or search for specific assets in your environment. For more information, see **Searching assets**.
- Investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network. For more information, see **Investigate offenses**.
- Edit, create, schedule, and distribute default or custom reports. For more information, see **Manage reports**.

Searching events

You can search for all authentication events that QRadar SIEM received in the last six hours.

Procedure

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

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

Step 3 In the Time Range pane, define the time range for the event search:

a Select the **Recent** option.

b From the list box under the **Recent** option, select **Last 6 Hours**.

Step 4 In the **Search Parameters** pane, define the search parameters:

a From the first list box, select **Category**.

b From the second list box, select **Equals**.

c From the **High Level Category** list box, select **Authentication**.

Leave the **Low Level Category** list box option as **Any**.

d Click **Add Filter**.

The filter is displayed in the **Current Filters** text box.

Step 5 From the **Display** list box in the Column Definition pane, select **Event Name**.

Step 6 Click **Search**.

What to do next

Save your event search criteria. For more information, see **Saving event search criteria**.

Saving event search criteria

You can save specified event search criteria for future use.

Procedure

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

Step 2 On the Log Activity toolbar, click **Save Criteria**.

Step 3 In the **Search Name** field, type the name `Example Search 1`.

Step 4 In the Timespan options pane, select the **Recent** option.

Step 5 From the list box, select **Last 6 Hours**.

Step 6 Select the **Include in my Quick Searches** and **Include in my Dashboard** check boxes.

Note: *If the **Include in my Dashboard** check box is not displayed, click **Search > Edit Search** to verify that you selected **Event Name** in* the Column Definition pane.

Step 7 Click **OK**.

What to do next

Configure a time series chart. For more information, see **Configuring a time series chart**.

Configuring a time series chart

You can display interactive time series charts that represent the records that are matched by a specific time interval search.

Before you begin

This procedure assumes that you have performed an event search and saved your search criteria. For more information, see **Searching events** and **Saving event search criteria**.

Procedure

Step 1 In the left chart title bar, click the **Configure** icon.

Step 2 From the **Value to Graph** list box, select **Destination IP (Unique Count)**.

Step 3 From the **Chart Type** list box, select **Time Series**.

Step 4 Select the **Capture Time Series Data** check box.

Step 5 Click **Save**.

Wait a few minutes for the time series data to accumulate and for the chart to display.

Step 6 Click **Update Details**.

Step 7 Filter your search results:

- **a** Right-click the event that you want to filter.
- **b** Select **Filter on Event Name is <Event Name>**.

  The event list refreshes to include only that particular event.

Step 8 To display the event list that is grouped by the username, select **Username** from the **Display** list box on the toolbar.

Step 9 Verify that your search is available from the Dashboard:

- **a** Click the **Dashboard** tab.
- **b** Click the **New Dashboard** icon.
- **c** In the **Name** field, type `Example Custom Dashboard`.
- **d** Click **OK**.

  The new dashboard is displayed on the Dashboard page and is listed in the **Show Dashboard** list box. By default, the dashboard is empty.
- **e** From the **Add Item** list box, select **Log Activity > Event Searches > Example Search 1**.

Results

The results from your saved event search display in the Dashboard.

Searching flows

You can search, visually monitor, and investigate flow data in real time.

Procedure

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

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

Step 3 In the **Time Range** pane, define the flow search time range:

- **a** Select the **Recent** option.
- **b** From the list box, select **Last 6 Hours**.

Step 4 In the Search Parameters pane, define your search criteria:

a From the first list box, select **Flow Direction**.

b From the second list box, select **Equals**.

c From the third list box, select **R2L**.

d Click **Add Filter**.

The filter is displayed in the **Current Filters** text box.

Step 5 From the **Display** list box in the Column Definition pane, select **Application**.

Step 6 Click **Search**.

Results

All flows with a flow direction of remote to local (R2L) in the last 6 hours are displayed and sorted by the **Application Name** field.

What to do next

Save your flow search criteria. For more information, see **Saving flow search criteria**.

Saving flow search criteria

You can save specified flow search criteria for future use.

Step 1 On the Network Activity toolbar, click **Save Criteria**.

Step 2 In the **Search Name** field, type the name `Example Search 2`.

Step 3 From the list box under the **Recent** option, select **Last 6 Hours**.

Step 4 Select the **Include in my Dashboard** and **Include in my Quick Searches** check boxes.

Step 5 Click **OK**.

What to do next

Create a dashboard item. For more information, see **Creating a dashboard item**.

Creating a dashboard item

You can create a dashboard item by using saved flow search criteria.

Procedure

Step 1 From the Network Activity toolbar, select **Quick Searches > Example Search 2**.

The search results page displays your flow search results.

Step 2 Verify that your search is included in the Dashboard:

a Click the **Dashboard** tab.

b From the **Show Dashboard** list box, select **Example Custom Dashboard**.

The Example Custom Dashboard is displayed in the new dashboard.

c From the **Add Item** list box, select **Flow Searches > Example Search 2**.

The results from your saved search are displayed on the Dashboard.

Step 3 Configure your dashboard chart:

a Click the **Settings** icon to access configuration options.

b Using the configuration options, change the value that is graphed, how many objects are displayed, the chart type, or the time range that is displayed in the chart.

The chart updates to represent your chart configuration changes.

Step 4 To investigate flows that are currently displayed in the chart, click **View in Network Activity**.

Results

The Network Activity page displays results that match the parameters of your time series chart. For more information on time series charts, see the *IBM Security QRadar SIEM Users Guide*.

Searching assets

Using the **Assets** tab, you can view all the learned assets or search for specific assets in your network environment.

About this task

QRadar SIEM automatically discovers assets on your network based on flows, vulnerability data, MAC addresses, and authentication information. QRadar SIEM uses this information to create an asset profile for each host. Asset profiles display what services are running on each asset. QRadar SIEM uses profile data to reduce false positives.

For example, if an exploit occurs on an asset, QRadar SIEM can determine if the asset is vulnerable to the exploit by correlating the exploit to the asset profile.

Procedure

Step 1 Click the **Assets** tab.

Step 2 Choose one of the following options:

a To search for specific asset profiles, configure values for the search criteria and click **Search**.

b To search for all asset profiles in your deployment, click **Show All**.

Step 3 Double-click an asset for more information about that particular host.

Step 4 To view event history:

a Double-click the asset that you want to investigate.

b On the toolbar, click **History**.

Step 5 Click **Search**.

Results

The search results display all events within the last 24 hours for the asset you are investigating.

Investigate offenses

Using the **Offenses** tab, you can investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.

About this task

QRadar SIEM can correlate events and flows with destination IP addresses located across multiple networks in the same offense, and ultimately the same network incident. This enables you to effectively investigate each offense in your network.

Viewing offenses

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Double-click the offense that you want to investigate.

Step 3 From the toolbar, select **Display > Destinations**.

You can investigate each destination to determine if the destination is compromised or exhibiting suspicious behavior.

Step 4 From the toolbar, click **Events**.

Results

The **List of Events** window displays all events that are associated with the offense. You can search, sort, and filter events. For more information, see **Searching events**.

Configuring rules

From the **Log Activity**, **Network Activity**, and **Offenses** tab, you can configure rules or building blocks.

For more information on QRadar SIEM rules, see **QRadar SIEM rules**.

Procedure

Step 1 Click the **Offenses** tab.

Step 2 Double-click the offense that you want to investigate.

Step 3 Click **Display > Rules**.

Step 4 Double-click a rule.

Note: You can further tune the rules. For more information about tuning rules, see the *IBM Security QRadar SIEM Administration Guide*.

Step 5 Close the Rules wizard.

Step 6 From the Rules page, click **Actions** and select one of the following options:

Table 5-3 Rules page parameters

Option	Description
Follow up	Select this option to flag the offense for follow-up.
Hide	Select this option to hide the offense.

Table 5-3 Rules page parameters (continued)

Option	Description
Protect Offense	Select this option to protect the offense from being removed from the database after the offense retention period is elapsed.
Close	Select this option to close the offense.
Email	Select this option to email a summary of the offense to an administrator.
Add note	Select this option to add a note to the offense.
Assign	Select this option to assign the offense to a user.

Note: For more information about the **Offenses** tab, see the *IBM Security QRadar SIEM Users Guide*.

Manage reports

QRadar SIEM provides default report templates that you can use to generate reports.

The report templates are grouped into report types, such as Compliance, Device, Executive, and Network reports. Using the Reports tab, you can:

- Edit a default report template to present customized data.
- Create custom report templates.
- Set a schedule for generating both custom and default reports.
- Publish the report in various formats.
- Distribute reports to other QRadar SIEM users.

Enabling reports

Using the **Reports** tab, you can enable, disable, and edit the report templates.

About this task

This task provides an example for enabling Payment Card Industry (PCI) report templates.

Procedure

Step 1 Click the **Reports** tab.

Step 2 Clear the **Hide Inactive Reports** check box.

Step 3 From the **Group** list box, select **Compliance > PCI**.

The list of PCI templates is displayed.

Step 4 Select all report templates on the list:

a Click the first report on the list.

b Select all report templates by holding down the Shift key, while you click the last report on the list.

Step 5 From the **Actions** list box, select **Toggle Scheduling**.

All PCI report templates are enabled. The next run time for report generation is displayed in the **Next runtime** column.

Step 6 To access generated reports:

a From the list box in the **Generated Reports** column, select the time-stamp of the report you want to view.

b From the **Format** column, click the icon for report format you want to view.

The report is displayed in the selected format.

What to do next

Create a custom report. For more information, see **Creating a custom report**.

Creating a custom report

You can create report by importing a search or creating custom criteria.

About this task

This task provides an example for creating a report that is based on the event and flow searches you created in **Searching events** and **Searching flows**.

Procedure

Step 1 Click the **Reports** tab.

Step 2 From the **Actions** list box, select **Create**.

The Report Wizard is displayed.

Note: You can select the check box to disable the Welcome page.

Step 3 Click **Next**.

Step 4 Configure the report schedule:

a Select the **Daily** option.

b Select the **Monday**, **Tuesday**, **Wednesday**, **Thursday**, and **Friday** options.

c Using the list boxes, select **8:00** and **AM**.

d Make sure the **Yes - Manually generate report** option is selected.

e Click **Next**.

Step 5 Configure the layout of your report:

a From the **Orientation** list box, select **Landscape**.

b Select the layout with two chart containers.

c Click **Next**.

Step 6 In the **Report Title** field, type **Sample Report**.

Step 7 Configure the top chart container:

a From the **Chart Type** list box, select **Events/Logs**.

The Container Details - Events/Logs page is displayed.

- **b** In the **Chart Title** field, type **Sample Event Search**.
- **c** From the **Limit Events/Logs To Top** list box, select **10**.
- **d** From the **Graph Type** list box, select **Stacked Bar**.
- **e** Select the **All data from the previous (24 hours)** option.
- **f** Using the **Base this event report on** list box, select **Example Search 1**.

  The remaining parameters automatically populate using the settings from the *Example Search 1* saved search.
- **g** Click **Save Container Details**.

Step 8 Configure the bottom chart container:

- **a** From the **Chart Type** list box, select **Flows**.
- **b** In the **Chart Title** field, type **Sample Flow Search**.
- **c** From the **Limit Flows To Top** list box, select **10**.
- **d** From the **Graph Type** list box, select **Stacked Bar**.
- **e** Select the **All data from the previous 24 hours** option.
- **f** From the **Available Saved Searches** list box, select **Example Search 2**.

  The remaining parameters are automatically populated by using the settings from the *Example Search 2* saved search.
- **g** Click **Save Container Details**.

  The Report Layout Preview page is displayed.

Step 9 Click **Next**.

A preview of the report is displayed.

Step 10 Click **Next**.

The Report Format page is displayed.

Step 11 Choose the report format:

- **a** Select the **PDF** and **HTML** check boxes.
- **b** Click **Next**.

Step 12 Choose the report distribution channels:

- **a** Ensure the **Report Console** check box is selected.
- **b** Select the **Email** check box.

  More parameters are displayed.
- **c** In the **Enter the report destination email address(es)** field, type your email address.
- **d** Select the **Include Report as attachment** check box.
- **e** Click **Next**.

Step 13 Complete the final Report Wizard details:

- **a** In the **Report Description** field, type a description of the template.

b Select the **Yes - Run this report when the wizard is complete** check box.

c Click **Finish**.

The Reports Wizard closes. Wait for the report to generate. Report generation can take several minutes.

Step 14 Using the list box in the **Generated Reports** column, select the time-stamp of your report.

d Click the **PDF** or **HTML** icon to view the report.

A GLOSSARY

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
Addressing scheme for the Internet, which allocates and species Internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.

Demilitarized Zone (DMZ)
A demilitarized zone, or perimeter network, is a network area located between an organization’s internal network and external network, usually the internet. It is separated by a firewall which only allows certain types of network traffic to enter or leave.

Device Support Module (DSM)
Device Support Modules (DSMs) allow you to integrate QRadar with log sources.

DNS
See Domain Name System.

DSM
See Device Support Module (DSM).

Domain Name System (DNS)
An online, distributed database used to map human-readable machine names into an IP address for resolving machine names to IP addresses.

encryption
Encryption provides greater security for all QRadar traffic between managed hosts. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host to provide protected access to the servers.

event
Record from a device that describes an action on a network or host.

false positive
When an event is tuned as false positive, the event no longer contributes to custom rules, therefore, offenses do not generate based on the false positive event. The event is still stored in the database and contributes to reports.

flow
Communication session between two hosts. A flow describes how traffic is communicated, what was communicated (if content capture option has been selected), and includes such details as when, who, how much, protocols, priorities, or options.

flow data Specific properties of a flow including: IP addresses, ports, protocol, bytes, packets, flags, direction, application ID, and payload data (optional).

flow logs Record of flows that enables the system to understand the context of a particular transmission over the network. Flows are stored in flow logs.

flow sources Source of flows that the QFlow Collector receives. Using the deployment editor, you can add internal and external flow sources from either the System or Event Views in the deployment editor.

IP See Internet Protocol.

Internet Protocol (IP) The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.

item A Dashboard option that creates a customized portal that displays any permissible view for monitoring purposes.

log source Log sources are external event log sources such as security equipment (for example, firewalls and IDSs) and network equipment (for example, switches and routers).

magnitude Specifies the relative importance of the offense and is a weighted value calculated from the Relevance, Severity, and Credibility measures. The magnitude bar on the **Offenses** tab and Dashboard provides a visual representation of all correlated variables of the offense, source, destination, or network. The magnitude of an offense is determined by several tests that performed on an offense every time it has been scheduled for re-evaluation, typically because events have been added or the minimum time for scheduling has occurred.

network hierarchy Contains each component of your network, and identifies which objects belong within other objects. The accuracy and completeness of this hierarchy is essential to traffic analysis functions. The network hierarchy provides for storage of flow logs, databases, and TopN files.

offense A message sent or event generated in response to a monitored condition. For example, an offense can inform you about a policy breach or network attack.

Packeteer Packeteer devices collect, aggregate, and store network performance data. When you configure an external flow source for Packeteer, you can send flow information from a Packeteer device to QRadar.

payload data The actual application data, excluding any header or administrative information, contained in an IP flow.

Payment Card Industry
An information security standard for organizations handling payment card information. It is used to increase controls and demonstrate compliance in the handling of sensitive data.

PCI
See Payment Card Industry.

protocol
A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It may still require an authorization exchange with a policy module or external policy server before admission.

R2L
See Remote To Local.

Remote to Local (R2L)
External traffic from a remote network to a local network.

reports
A function that creates executive or operational level charting representations of network activity based on time, sources, offenses, security, and events.

report interval
A configurable time interval at which the Event Processor must send all captured event and flow data to the Console.

rules
Collection of conditions and consequent actions. You can configure rules that allow QRadar to capture and respond to specific event sequences. The rules enables you to detect specific, specialized events and forward notifications to either the **Offenses** tab or log file, or e-mail a user.

severity
Indicates the amount of threat a source poses in relation to how prepared the destination is for the attack. This value is mapped to an event category in the QID map that is correlated to the offense.

Simple Network Management Protocol (SNMP)
A network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.

SNMP
See Simple Network Management Protocol.

System Time
The right corner of the user interface displays System time, which is the time on the QRadar Console. This is the time that determines the time of events and offenses.

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A reliable stream service that operates at the transport-layer Internet protocol, which ensures successful end-to-end delivery of data packets without error.

B NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM 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*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

INDEX