IBM QRadar SIEM
Version 7.3.3

Getting Started Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 31.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.3 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to getting started with QRadar SIEM

The IBM QRadar Getting Started Guide introduces you to key concepts, an overview of the installation process, and basic tasks that you perform in the user interface.

Intended audience

This information is intended for use by security administrators who are responsible for investigating and managing network security. To use this guide you must have a knowledge of your corporate network infrastructure 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?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 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 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 QRadar.

Chapter 1. QRadar SIEM overview

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

Get started by exploring the IBM QRadar Experience Center app

A great way to get started is to try out the IBM QRadar Experience Center app, which is supported on QRadar V7.3.1 or later. The app comes with several predefined security use cases that you can run to demonstrate how QRadar can help you detect security threats. Watch QRadar in action as the simulation data is sent to QRadar from the app. After you watch the video tutorial that explains the use case, explore the corresponding QRadar content, and see how you might investigate such a threat in your own environment.

Use the app to upload and play your own logs in QRadar. Access the IBM Security Learning Academy and other resources to explore how you can use the powerful threat detection capabilities of QRadar to protect your network.

Note: This app is not suitable for production systems because it sends events that cannot be removed from the system. Instead, use it in a test environment.

Download the IBM QRadar Experience Center app from the IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub/extension/4b8a49187611ae8f746c27c8da4727e3).

Related information

Using IBM QRadar SIEM

Log activity

In IBM QRadar SIEM, 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. Use the **Log Activity** tab to do the following tasks:

- Investigate event data.
- Investigate event logs that are sent to QRadar SIEM in real time.
- Search event.
- Monitor log activity by using configurable time-series charts.
- Identify false positives to tune QRadar SIEM.

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

Network activity

In IBM QRadar SIEM you can investigate the communication sessions between two hosts.

If the content capture option is enabled, the **Network Activity** tab displays information about how network traffic is communicated and what was communicated. Using the **Network Activity** tab, you can do the following tasks:

- Investigate the flows that are sent to QRadar SIEM in real time.
- Search network flows.
- Monitor network activity by using configurable time-series charts.

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

Assets

QRadar SIEM automatically creates asset profiles by using passive flow data and vulnerability data to discover your network servers and hosts.

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 to reduce false positives.

Use the **Assets** tab to do the following tasks:

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

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

Offenses

In IBM QRadar SIEM you can investigate offenses to determine the root cause of a network issue.

Use the **Offenses** tab to view all the offenses that occur on your network and complete the following tasks:

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

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

Reports

In IBM QRadar SIEM you can create custom reports or use default reports.

QRadar SIEM provides default report templates that you can customize, rebrand, and distribute to QRadar SIEM users.

Report templates are grouped into report types, such as compliance, device, executive, and network reports. Use the **Reports** tab to complete the following tasks:

- Create, distribute, and manage reports for QRadar SIEM data.
- Create customized reports for operational and executive use.
- Combine security and network information into a single report.
- Use or edit preinstalled report templates.
- Brand your reports with customized logos. Branding is beneficial for distributing reports to different audiences.
- Set a schedule for generating both custom and default reports.
- Publish reports in various formats.

For more information, see the *IBM QRadar User 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 vulnerability assessment (VA) information.

Event data collection

Events are generated by log sources such as firewalls, routers, servers, and intrusion detection systems (IDS) or intrusion prevention systems (IPS).

Most log sources send information to QRadar SIEM by using the syslog protocol. QRadar SIEM also supports the following protocols:

- Simple Network Management Protocol (SNMP)
- Java™ database Connectivity (JDBC)
- 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 *DSM Configuration Guide*.

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

Flow data collection

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 provide 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 notify you only that port 7500 (TCP) has traffic 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.

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

Vulnerability assessment (VA) information

QRadar SIEM can import VA information from various third-party scanners.

VA information helps QRadar Risk Manager identify active hosts, open ports, and potential vulnerabilities.

QRadar Risk Manager uses VA information to rank the magnitude of offenses on your network.

Depending on the VA scanner type, QRadar Risk Manager can import scan results from the scanner server or can remotely start a scan.

QRadar SIEM rules

Rules perform tests on events, flows, or offenses. 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 about rules, see the *IBM QRadar Administration Guide*.

The following list describes the two rule categories:

- 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 to detect when unusual traffic patterns occur in your network.

Important: 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 QRadar Administration Guide*.

Supported web browsers

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

The following table lists the supported versions of web browsers.

Table 1. Supported web browsers for QRadar products

Web browser	Supported versions
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
Microsoft Internet Explorer	11.0
64-bit Google Chrome	Latest

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.

Apps overview

IBM QRadar apps are created by developers. After a developer creates an app, IBM certifies and publishes it in the IBM Security App Exchange. QRadar administrators can then browse and download the apps and then install the apps into QRadar to address specific security requirements.

The IBM Security App Exchange is a community-based sharing hub, that you use to share apps across IBM Security products. By participating in App Exchange, you can use the rapidly assembled, innovative workflows, visualizations, analytics, and use cases that are packaged into apps to address specific security requirements. Easy-to-use solutions are developed by partners, consultants, developers to address key security challenges. To detect and remediate threats, use these shared security components, from real-time correlation and behavioral modeling to custom responses and reference data.

Note: The combined memory requirements of all the apps that are installed on a QRadar Console cannot exceed 10 per cent of the total available memory, or the apps won't work. If you exceed the 10 per cent memory allocation and want to run more apps, use a dedicated appliance for your apps (AppNode appliance for QRadar V7.3.1 or the new AppHost appliance for QRadar V7.3.2).

The IBM QRadar Assistant app helps you to manage and update your app and content extension inventory, view app and content extension recommendations, follow the QRadar Twitter feed, and get links to useful information. The app is automatically installed with QRadar V7.3.2.

The following diagram shows the workflow for an app and the role who is typically responsible for the work.

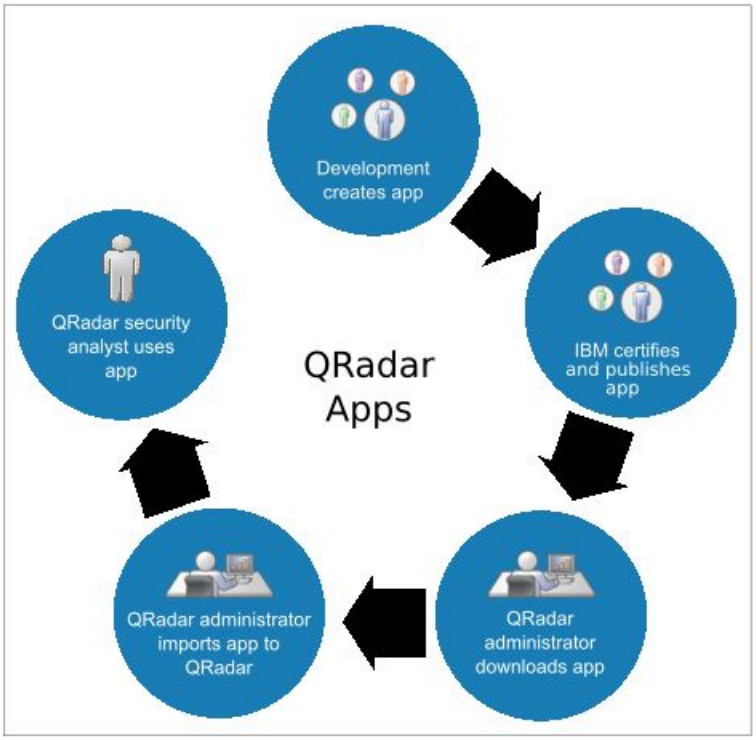

Figure 1. App workflow

FAQ

What is an app?

Apps create or add new functions in QRadar by providing new tabs, API methods, dashboard items, menus, toolbar buttons, configuration pages, and more within the QRadar user interface. You download apps from the IBM Security App Exchange. Apps that are created by using the GUI

Application Framework Software Development Kit integrate with the QRadar user interface to deliver new security intelligence capabilities or extend the current functions.

Every downloaded file from the IBM Security App Exchange is known as an extension. An extension can consist of an app or security product enhancement (content extension) that is packaged as an archive (.zip) file, which you can deploy on QRadar by using the **Extensions Management** tool on the **Admin** tab.

Who can create an app?

You can use the GUI Application Framework Software Development Kit to create apps. For more information about the GUI Application Framework Software Development Kit, see the *IBM Security QRadar App Framework Guide*.

You download (https://developer.ibm.com/qradar/) the SDK from IBM developerWorks®.

How do I share my app?

Only certified content is shared in the IBM Security App Exchange, a new platform for collaborating where you can respond quickly and address your security and platform enhancement requirements. In the IBM Security App Exchange, you can find available apps, discover their purpose, and what they look like, and learn what other users say about the apps.

How do I get an app that I downloaded into QRadar?

A QRadar administrator downloads an extension and imports it into QRadar by using the **Extensions Management** tool, which is used to upload the downloaded extension from a local source.

Where do I get help for an app?

You can see information about an app in the overview section when you download the app from the IBM Security App Exchange. For apps developed solely by IBM, you can find information in the IBM Knowledge Center.

How much memory does an app need?

The combined memory requirements of all the apps that are installed on a QRadar Console cannot exceed 10 per cent of the total available memory. If you install an app that causes the 10 per cent memory limit to be exceeded, the app does not work.

If your app requires a minimum memory allocation, you must specify this allocation as part of your app manifest. The default allocation is 200 MB.

What is the difference between an app, a content extension, and a content pack?

Extension

From within QRadar, an *extension* is a term that is used for everything that you download from the IBM Security App Exchange. Sometimes that extension contains individual content items, such as custom AQL functions or custom actions, and sometimes the extension contains an app that is developed by using the GUI App Framework Software Development Kit. You use the **Extensions Management** tool to install extensions.

App

An *app* is content that is created when you use the GUI App Framework Software Development Kit. The app extends or creates new functions in QRadar.

Content extension

A *content extension* is typically used to update QRadar security template information or add new content such as rules, reports, searches, logos, reference sets, custom properties. Content extensions are not created by using the GUI Application Framework Software Development Kit.

You download content packs from IBM Fix Central in RPM format.

Typically, content extensions differ from content packs because you download content packs (RPM files) from IBM Fix Central (www.ibm.com/support/fixcentral).

Chapter 2. Getting started with QRadar SIEM deployment

Before you can evaluate IBM QRadar SIEM key capabilities, an administrator must deploy QRadar.

To deploy QRadar, administrators must do the following tasks:

- Install the QRadar SIEM appliance.
- Configure your QRadar SIEM installation.
- Collect event, flow, and vulnerability assessment (VA) data.
- Tune your QRadar SIEM installation.

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 appliance, ensure that the following requirements are met:

- The required hardware is installed. For more information, see the *IBM QRadar Installation Guide*.
- A notebook is connected to the serial port on the back of the appliance, or a keyboard and monitor are connected.
- You are logged in as the root user.

About this task

Important: If QRadar is already installed on your appliance, use the following rules when you create the root password: Passwords must be at least 5 characters long, contain no spaces, and can contain the following special characters: @, #, ^, and *.

Procedure

1. Access the software and documentation.
   a) Review the release notes for the QRadar component that you want to install.
   b) Follow the instructions in the Download Document (https://www.ibm.com/support/docview.wss?uid=ibm10734615) to download QRadar from IBM Passport Advantage®.
2. Review the information about the front and back panel features for appliances to confirm proper connectivity and functionality. For more information on front and back panel features for appliances, see the *IBM QRadar Hardware Guide*.

   Note: On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed by using the Integrated Management Module. For more information on the Integrated Management Module, see the *Integrated Management Module User's Guide*.
3. Install the QRadar appliance.
   a) Create the `/media/cdrom` directory by typing the following command: `mkdir /media/cdrom`
   b) Mount the QRadar ISO image by typing the following command: `mount -o loop <path_to_the_QRadar_ISO> /media/cdrom`
   c) To begin the installation, type the following command: `/media/cdrom/setup`.
   d) Select **Appliance Install** for the appliance type.
   e) Select the appliance type from the list.

f) For the type of setup, select **normal**.

g) Set up the date and time.

h) Select the IP address type.

i) In the wizard, enter a fully qualified domain name in the **Hostname** field.

j) In the **IP address** field, enter a static IP address, or use the DHCP-assigned IP address.

Note: For information about setting IPv6 primary or secondary host, see the *IBM QRadar High Availability Guide*.

k) If you do not have an email server, enter `localhost` in the **Email server name** field.

l) Create root and admin passwords. The admin password must meet the minimum length and complexity requirements that are enforced.

m) Follow the instructions in the installation wizard to complete the installation. The installation process might take several minutes.

4. Apply your license key.
   a) Log in to QRadar as the admin user: `https://<QRadar_IP_Address>`
   b) Click the **Admin** tab.
   c) Click the **System and License Management** icon.
   d) Click **Upload License**, and upload your license key.
   e) Select the license and click **Allocate System to License**.
   f) From the list of licenses, select a license, and click **Allocate License to System**.

QRadar SIEM configuration

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

Procedure

1. Ensure that Java Runtime Environment (JRE) version 1.7 or IBM 64-bit Runtime Environment for Java V7.0 is installed on all desktop systems that you use to access the QRadar product user interface.
2. Ensure that you are using a supported web browser. See “Supported web browsers ” on page 4.
3. If you use Internet Explorer, enable document mode and browser mode.
   a) In your Internet Explorer web browser, press F12 to open the **Developer Tools** window.
   b) Click **Browser Mode** and select the version of your web browser.
   c) Click **Document Mode** and select **Internet Explorer 7.0 Standards**.
4. Log in to the QRadar SIEM user interface by typing the following URL with the IP address of the QRadar Console:

   `https://IP Address`

Related concepts

Supported web browsers

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

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 do the following tasks:

- 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.

When you develop your network hierarchy, consider the most effective method for viewing network activity. The network hierarchy does not need to resemble the physical deployment of your network. QRadar supports any network hierarchy that can be defined by a range of IP addresses. You can base your network on many different variables, including geographical or business units.

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, then use the **Admin** tab to create a hierarchy specific to your environment.

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

Defining your network hierarchy

A default network hierarchy that contains pre-defined network groups is included in IBM QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

About this task

Network objects are containers for Classless Inter-Domain Routing (CIDR) addresses. Any IP address that is defined in a CIDR range in the network hierarchy is considered to be a local address. Any IP address that is not defined in a CIDR range in the network hierarchy is considered to be a remote address. A CIDR can belong only to one network object, but subsets of a CIDR range can belong to another network object. Network traffic matches the most exact CIDR. A network object can have multiple CIDR ranges assigned to it.

Some of the default building blocks and rules in QRadar use the default network hierarchy objects. Before you change a default network hierarchy object, search the rules and building blocks to understand how the object is used and which rules and building blocks might need adjustments after you modify the object. It is important to keep the network hierarchy, rules, and building blocks up-to-date to prevent false offenses.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Network Hierarchy**.
3. From the menu tree on the **Network Views** window, select the area of the network in which you want to work.
4. To add network objects, click **Add** and complete the following fields:

Option	Description
Name	The unique name of the network object. **Tip:** You can use periods in network object names to define network object hierarchies. For example, if you enter the object name `D.E.F`, you create a three-tier hierarchy with E as a subnode of D, and F as a subnode of E.
Group	The network group in which to add the network object. Select from the **Group** list, or click **Add a New Group**. **Tip:** When you add a network group, you can use periods in network group names to define network group hierarchies. For example, if you enter the group name `A.B.C`, you create a three-tier hierarchy with B as a subnode of A, and C as a subnode of B.
IP/CIDR(s)	Type an IP address or CIDR range for the network object, and click **Add**. You can add multiple IP addresses and CIDR ranges.
Description	A description of the network object. This field is optional.

Option	Description
Country/Region	The country or region in which the network object is located. This field is optional.
Longitude and Latitude	The geographic location (longitude and latitude) of the network object. These fields are co-dependent and optional.

5. Click **Create**.
6. Repeat the steps to add more network objects, or click **Edit** or **Delete** to work with existing network objects.

Automatic updates

Using QRadar SIEM, you can either replace your existing configuration files or integrate the updated files with your existing files.

The QRadar SIEM console must be connected to the internet to receive updates. If your console is not connected to the internet, you must configure an internal update server. For information about setting up an automatic update server, see the *IBM QRadar User Guide*.

Download software updates from IBM Fix Central (www.ibm.com/support/fixcentral/).

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 JAR files.
- Minor updates, which include items such as extra online help content or updated scripts.

Configuring automatic update settings

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

About this task

You can select the **Auto Deploy** to automatically deploy updates. If **Auto Deploy** is not selected, then you must manually deploy changes, from the **Dashboard** tab, after updates are installed.

Restriction: In high-availability (HA) environment, automatic updates aren't installed when a secondary host is active. The updates are installed only after the primary host become the active node.

You can select **Auto Restart Service** to allow automatic updates that require the user interface to restart. A user interface disruption occurs when the service restarts. Alternatively, you can manually install the updated from the **Check for Updates** window.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **Auto Update**.
3. Click **Change Settings**.
4. On the **Basic** tab, select the schedule for updates.
   a) In the **Configuration Updates** section, select the method that you want to use for updating your configuration files.
      - To merge your existing configuration files with the server updates without affecting your custom signatures, custom entries, and remote network configurations, select **Auto Integrate**.
      - To override your customizations with server settings, select **Auto Update**.
   b) In the **DSM, Scanner, Protocol Updates** section, select an option to install updates.
   c) In the **Major Updates** section, select an option for receiving major updates for new releases.

d) In the **Minor Updates** section, select an option for receiving patches for minor system issues.

e) If you want to deploy update changes automatically after updates are installed, select the **Auto Deploy** check box.

f) If you want to restart the user interface service automatically after updates are installed, select the **Auto Restart Service** check box.

5. Click the **Advanced** tab to configure the update server and backup settings.

a) In **Web Server** field, type the web server from which you want to obtain the updates.

The default web server is `https://qmmunity.q1labs.com/`.

b) In the **Directory field**, type the directory location on which the web server stores the updates.

The default directory is `autoupdates/`.

c) Optional: Configure the settings for proxy server.

If the application server uses a proxy server to connect to the Internet, you must configure the proxy server. If you are using an authenticated proxy, you must provide the username and password for the proxy server.

d) In the **Backup Retention Period** list, type or select the number of days that you want to store files that are replaced during the update process.

The files are stored in the location that is specified in the **Backup Location**. The minimum is one day and the maximum is 65535 years.

e) In the **Backup Location** field, type the location where you want to store backup files.

f) In the **Download Path** field, type the directory path location to which you want to store DSM, minor, and major updates.

The default directory path is `/store/configservices/staging/updates`.

6. Click **Save**.

Collecting events

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

Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **Data Sources** > **Events**.
3. Click the **Log Sources** icon.
4. Review the list of log sources and make any necessary changes to the log source.
   For information about configuring log sources, see the *IBM QRadar Log Sources User Guide*.
5. Close the **Log Sources** window.
6. On the **Admin** tab menu, click **Deploy Changes**.

Collecting flows

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

Procedure

1. Click the **Admin** tab.
2. In the navigation menu, click **Data Sources** > **Flows**.
3. Click the **Flow Sources** icon.
4. Review the list of flow sources and make any necessary changes to the flow sources.
   For more information about configuring flow sources, see the *IBM QRadar Administration Guide*.
5. Close the **Flow Sources** window.
6. On the **Admin** tab menu, click **Deploy Changes**.

Importing vulnerability assessment information

By importing vulnerability assessment information, you identify active hosts, open ports, and potential vulnerabilities.

Procedure

1. Click the **Admin** tab.
2. In the navigation menu, click **Data Sources** > **Vulnerability**.
3. Click the **VA Scanners** icon.
4. On the toolbar, click **Add**.
5. Enter values for the parameters.

   The parameters depend on the scanner type that you want to add.

   Important: 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.
6. Click **Save**.
7. On the **Admin** tab menu, click **Deploy Changes**.
8. Click the **Schedule VA Scanners** icon.
9. Click **Add**.
10. Specify the criteria for how often you want the scan to occur.

    Depending on the scan type, the criteria 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.
11. Click **Save**.

Related concepts

"Vulnerability assessment (VA) information" on page 4
QRadar SIEM can import VA information from various third-party scanners.

QRadar SIEM tuning

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

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

Administrators can do the following tuning tasks:

- Optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity**.
- Provide a faster initial deployment and easier tuning by automatically or manually adding servers to building blocks.
- Configure responses to event, flow, and offense conditions by creating or modifying custom rules and anomaly detection rules.
- Ensure that each host in your network creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

Payload indexing

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

To optimize the **Quick Filter**, you can enable a payload index **Quick Filter** property.

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 QRadar 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

1. Click the **Admin** tab.
2. In the **System Configuration** section, click **Index Management**.
3. In the **Search** field, type `quick filter`.
4. Right-click the **Quick Filter** property that you want to index.
5. Click **Enable Index**.
6. Click **Save**, and then click **OK**.
7. To disable a payload index, choose one of the following options:
   - Click **Disable Index**.
   - Right-click a property and select **Disable Index** from the menu.

What to do next

For more information about the parameters that are displayed in the **Index Management** window, see the *IBM QRadar 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.

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 the **BB:HostDefinition: Network Management Servers** building block.
- Add proxy servers to the **BB:HostDefinition: Proxy Servers** building block.
- Add virus and Windows update servers to the **BB:HostDefinition: Virus Definition and Other Update Servers** building block.
- Add vulnerability assessment (VA) scanners to the **BB-HostDefinition: VA Scanner Source IP** building block.

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 and you can select which servers you want to include in building blocks.

For more information about discovering servers, see the *IBM QRadar Administration Guide*.

Using Building blocks, you can reuse specific rule tests in other rules. You can reduce the number of false positives by using building blocks to tune QRadar SIEM and enable extra correlation rules.

Adding servers to building blocks automatically

You can automatically add servers to building blocks.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Server Discovery**.
3. In the **Server Type** list, select the server type that you want to discover.

Keep the remaining parameters as default.

4. Click **Discover Servers**.
5. In the **Matching Servers** pane, select the check box of all servers you want to assign to the server role.
6. Click **Approve Selected Servers**.

   Remember: You can right-click any IP address or host name 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.

Procedure

1. Click the **Offenses** tab.
2. In the navigation pane, click **Rules**.
3. In the **Display** list, select **Building Blocks**.
4. In the **Group** list, 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.
5. To manually add a host or network, double-click the corresponding Host Definition Building Block appropriate to your environment.
6. In the **Building Block** field, click the underlined value after the phrase **and when either the source or destination IP is one of the following**.
7. In the **Enter an IP address or CIDR** field, type the host names or IP address ranges that you want to assign to the building block.
8. Click **Add**.
9. Click **Submit**.
10. Click **Finish**.
11. Repeat these steps for each server type that you want to add.

Configuring rules

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

Procedure

1. Click the **Offenses** tab.
2. Double-click the offense that you want to investigate.
3. Click **Display** > **Rules**.
4. Double-click a rule.

   You can further tune the rules. For more information about tuning rules, see the *IBM QRadar Administration Guide*
5. Close the Rules wizard.

   The **Creation Date** property changes to the date and time when you last updated a rule.
6. In the **Rules** page, click **Actions**.
7. If you want to prevent the offense from being removed from the database after the offense retention period is elapsed, select **Protect Offense**.
8. If you want to assign the offense to a QRadar SIEM user, select **Assign**.

Cleaning the SIM data model

Clean the SIM data model to ensure that each host creates offenses that are based on the most current rules, discovered servers, and network hierarchy.

Procedure

1. Click the **Admin** tab.
2. On the toolbar, select **Advanced** > **Clean SIM Model**.
3. Select an option:
   - `Soft Clean` to set the offenses to inactive.
   - `Soft Clean` with the optional `Deactivate all offenses` check box to close all offenses.
   - `Hard Clean` to erase all entries.
4. Check the **Are you sure you want to reset the data model?** box.
5. Click **Proceed**.
6. After the SIM reset process is complete, refresh your browser.

Results

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

Chapter 3. Getting started in QRadar SIEM

To get started in IBM QRadar SIEM, learn about investigating offenses, creating reports, and searching events, flows, and assets.

For example, you can search information by using default saved searches in the **Log Activity** and **Network Activity** tabs. You can also 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.
- 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.
- View all the learned assets or search for specific assets in your environment.
- Investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.
- Edit, create, schedule, and distribute default or custom reports.

Getting started for administrators

If you're an administrator, the following topics are a good place to get started to learn how to use IBM QRadar in your everyday workflow.

Administration

Do you know how the Network Hierarchy impacts the QRadar deployment?

- 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.
- Defining your network hierarchy

  A default network hierarchy that contains pre-defined network groups is included in QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Do you know how to create integrations with IBM solutions such as Guardium®, AppScan®, BigFix®?

- IBM Guardium integration

  IBM® Guardium® is a database activity and audit tracking tool for system administrators to retrieve detailed auditing events across database platforms.
- AppScan Enterprise integration

  QRadar retrieves HCL AppScan Enterprise reports with the Representational State Transfer (REST) web service to import vulnerability data and generate offenses for your security team.
- IBM BigFix integration

  IBM QRadar Vulnerability Manager integrates with IBM BigFix® to help you filter and prioritize the vulnerabilities that can be fixed.

Do you know how to configure multiple log source groups for filtering, rules, and reporting?

- Adding multiple log sources at the same time

  Use the QRadar Log Source Management app to add multiple log sources to QRadar at the same time. You can add as many log sources as you want.
- Editing multiple log sources at the same time

In the QRadar Log Source Management app, view and edit a number of log sources at the same time. You can edit the settings of up to 1000 log sources at one time. Edit multiple log sources at the same time when the log sources have similar settings that you want to change, instead of editing each log source individually.

Do you know how to quantify and prioritize data sources in your environment to ensure adequate data collection?

- Data collection

  QRadar 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 vulnerability assessment (VA) information.

- Adding a managed host

  Add managed hosts, such as event and flow collectors, event and flow processors, and data nodes, to distribute data collection and processing activities across your QRadar deployment.

APIs

Do you know how to create an authorization token for services to be used for remote access?

- Managing authorized services

  You can configure authorized services to authenticate an API call for your QRadar deployment. The QRadar RESTful API uses authorized services to authenticate API calls to the QRadar Console. You can add or revoke an authorized service at any time.

- Creating an authentication token for WinCollect agents

  Third-party or external applications that interact with QRadar require an authentication token. Before you install managed WinCollect agents in your network, you must create an authentication token.

Backup and restore

Do you know how the backup and recovery functions are configured?

- Backup and recovery

  You can use the backup and recovery feature to back up your event and flow data; however, you must restore event and flow data manually.

- Backup configurations and data

  By default, QRadar creates a backup archive of your configuration information daily at midnight. The backup archive includes your configuration information, data, or both from the previous day. You can customize this nightly backup and create an on-demand configuration backup, as required.

High Availability/Disaster Recovery

Do you know how to create an HA cluster, and how to implement HA nodes in QRadar, including moving online/offline?

- HA overview

  If your hardware or network fails, QRadar can continue to collect, store, and process event and flow data by using high-availability (HA) appliances.

- Creating an HA cluster

  Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address creates an HA cluster.

- Setting an HA host online

  You can set the primary or secondary HA host to Online.

- Setting an HA host offline

You can set the primary or secondary high-availability (HA) host to **Offline** from the **Active** or **Standby** state.

License management

Do you know how to measure license allocation vs. usage and ensure adequate coverage?

- License management

  License keys entitle you to specific QRadar products, and control the event and flow capacity for your QRadar deployment. You can add licenses to your deployment to activate other QRadar products, such as QRadar Vulnerability Manager.
- Burst handling

  QRadar uses burst handling to ensure that no data is lost when the system exceeds the allocated events per second (EPS) or flows per minute (FPM) license limits.
- Distributing event and flow capacity

  Use the License Pool Management window to ensure that the events per second (EPS) and flows per minute (FPM) that you are entitled to is fully used. Also, ensure that QRadar is configured to handle periodic bursts of data without dropping events or flows, or having excessive unused EPS and FPM.

Log sources

Do you know how to create a new log source?

- Adding log sources manually

  You can manually add log sources that QRadar does not detect automatically.
- Adding a log source

  Use the QRadar Log Source Management app to add new log sources to receive events from your network devices or appliances.

Do you know how to add Log Sources by using non-Syslog protocols, such as OpSec LEA and AWS S3?

- Configuring an OPSEC/LEA log source

  To integrate Check Point OPSEC/LEA with QRadar, you must create two Secure Internal Communication (SIC) files and enter the information in to QRadar as a Check Point log source.
- Configuring an Amazon AWS CloudTrail log source by using the Amazon AWS S3 REST API protocol

  If you want to collect AWS CloudTrail logs from Amazon S3 buckets, configure a log source on the QRadar Console so that Amazon AWS CloudTrail can communicate with QRadar by using the Amazon AWS S3 REST API protocol.

Do you know how to get logs from various cloud providers such as Amazon AWS or Microsoft Azure?

- Amazon AWS CloudTrail

  The QRadar DSM for Amazon AWS CloudTrail supports audit events that are collected from Amazon S3 buckets, and from a Log group in the AWS CloudWatch Logs.
- Microsoft Azure Platform

  The QRadar DSM for Microsoft Azure Platform collects events from Microsoft Azure Event Hubs.

Reference data and building blocks

Do you know how to adjust building block and reference set content to effectively tune QRadar rules?

- Review building blocks

  Building blocks are a reusable set of rule tests that can be used within rules when required. Host definition building blocks (BB:HostDefinition) categorize assets and server types into CIDR/IP ranges. By populating host definition building blocks, QRadar can identify the type of appliance that belongs to

an address or address range. These building blocks can then be used in rules to exclude or include entire asset categories in rule tests.

Rules

Do you know how to run correlation rules in "test mode" to avoid excessive offense generation?

- Configuring an event or flow as false positive

  You might have legitimate network traffic that triggers false positive flows and events that make it difficult to identify true security incidents. You can prevent events and flows from correlating into offenses by configuring them as false positives.
- Creating a custom rule

  QRadar includes rules that detect a wide range of activities, including excessive firewall denies, multiple failed login attempts, and potential botnet activity. You can also create your own rules to detect unusual activity.

Threat intelligence

Do you know how to use native X-Force threat feed data to enhance corporate security and visibility?

- IBM Security Threat Content Extension

  The Extension Threat Theme adds rule content and building blocks to QRadar that focus on threat events and detection. This extension enhances the base rule set of QRadar for administrators who have new QRadar installations.
- Enabling X-Force® Threat Intelligence in QRadar

  By enabling X-Force Threat Intelligence in QRadar, you can receive feeds of the X-Force Threat Intelligence information to your console.

Troubleshooting

Do you know how to collect logs from the QRadar deployment to help support troubleshoot issues?

- Collecting log files

  QRadar log files contain detailed information about your deployment, such as hostnames, IP addresses, and email addresses. If you need help with troubleshooting, you can collect the log files and send them to IBM Support.

Getting started for architects

If you're an architect, the following topics are a good place to get started to learn how to use IBM QRadar in your everyday workflow.

Architecture

Do you understand the distributed architecture and the roles of various components of QRadar?

- QRadar architecture overview

  IBM QRadar SIEM (Security Information and Event Management) is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. You can scale QRadar to meet your log and flow collection, and analysis needs. You can add integrated modules to your QRadar platform, such as QRadar Risk Manager, QRadar Vulnerability Manager, and QRadar Incident Forensics.
- QRadar components

  Use QRadar components to scale a deployment, and to manage data collection and processing in distributed networks.

- QRadar events and flows

  The core functions of QRadar are managing network security by monitoring flows and events. A significant difference between event and flow data is that an event, which typically is a log of a specific action such as a user login, or a VPN connection, occurs at a specific time and the event is logged then. A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session.

Do you know how to scope an environment for architectural requirements, data rates, and retention policies to optimally build a QRadar deployment?

- Data retention

  Retention buckets define how long event and flow data is retained in QRadar. As QRadar receives events and flows, each one is compared against the retention bucket filter criteria. When an event or flow matches a retention bucket filter, it is stored in that retention bucket until the deletion policy time period is reached. The default retention period is 30 days; then, the data is immediately deleted.
- Distributing event and flow capacity

  Use the License Pool Management window to ensure that the events per second (EPS) and flows per minute (FPM) that you are entitled to is fully used. Also, ensure that QRadar is configured to handle periodic bursts of data without dropping events or flows, or having excessive unused EPS and FPM.

Flow sources

Do you know how to instrument network segments to enhance visibility and security?

- Forensics and full packet collection

  Use IBM QRadar Incident Forensics in your deployment to retrace the step-by-step actions of a potential attacker, and conduct an in-depth forensics investigation of suspected malicious network security incidents.
- Forwarding packets to QRadar Packet Capture

  You can monitor network traffic by sending raw data packets to an IBM QRadar QFlow Collector 1310 appliance. The QRadar QFlow Collector uses a dedicated Napatech monitoring card to copy incoming packets from one port on the card to a second port that connects to an IBM QRadar Packet Capture appliance.

Do you know how to determine which network segments are reporting to QRadar?

- Guidelines for defining your network hierarchy

  Building a network hierarchy in QRadar is an essential first step in configuring your deployment. Without a configured network hierarchy, QRadar cannot determine flow directions, build a reliable asset database, or benefit from useful building blocks in rules.
- Defining your network hierarchy

  A default network hierarchy that contains pre-defined network groups is included in QRadar. You can edit the pre-defined network hierarchy objects, or you can create new network groups or objects.

Getting started for security analysts

If you're a security analyst, the following topics are a good place to get started to learn how to use IBM QRadar in your everyday workflow.

Offense Workflow

Do you understand offense elements such as magnitude, hosts, users, involved?

- Offense prioritization

The magnitude rating of an offense is a measure of the importance of the offense in your environment.QRadar uses the magnitude rating to prioritize offenses and help you to determine which offenses to investigate first.

- Managed hosts

  For greater flexibility over data collection and event and flow processing, build a distributed QRadar deployment by adding non-console managed hosts, such as collectors, processors, and data nodes.

- Assigning offenses to users

  By default, all new offenses are unassigned. You can assign an offense to a QRadar user for investigation.

Do you know how to investigate an offense, including viewing related events and flows?

- Offense investigations

  QRadar uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected.

- Network activity monitoring

  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.

- Log activity monitoring

  QRadar displays events in streaming mode so that you to view events in real time.

Searching and filtering

Do you know how to use columns (such as **Event Name**, **Username**) to show events grouped by one of those properties?

- Creating a customized search

  You can search for data that matches your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

Do you know how to use the Quick Filter to search the events for keywords?

- Quick filter search options

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

- Enabling quick filtering

  You can enable the **Quick Filter** property to optimize event and flow search times. You can use the **Quick Filter** option to search event and flow payloads by typing free text search criteria.

Do you know how to save search criteria for future use, scheduling, or dashboarding?

- 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.

Do you know how to specify content requirements for searches?

- Creating a customized search

  You can search for data that matches your criteria by using more specific search options. For example, you can specify columns for your search, which you can group and reorder to more efficiently browse your search results.

Do you know how to create time series charts?

- Creating a time series chart in QRadar Pulse dashboard app

Time series charts in the QRadar Pulse dashboard app illustrate data points at successive intervals of time. You use a time series chart to show trending or comparisons.

- Configuring a time series chart in QRadar

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

Reporting and dashboards

Do you know how to generate a QRadar published report with preexisting content?

- Manually generating a report

  A report can be configured to generate automatically; however, you can manually generate a report at any time.

- Creating custom reports

  Use the Report wizard to create and customize a new report. The Report wizard provides a step-by-step guide on how to design, schedule, and generate reports.

Do you know how to modify a dashboard's properties to what you want to visualize?

- Creating Pulse dashboard items from an AQL data source

  You can use Ariel Query Language (AQL) statements to create dashboard items. AQL is a structured query language that you use to extract, filter, and manipulate event and flow data that you extract from the Ariel database in QRadar.

Do you know how to use saved search criteria to create custom dashboard items?

- Creating a custom dashboard

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

Rules

Do you know how to determine which rules are associated with a specific log or flow record?

- Investigating threats in QRadar

  QRadar uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected. But knowing that an offense occurred is only the first step; identifying how it happened, where it happened, and who did it, requires some investigation.

- Investigating rules with the QRadar Use Case Manager app

  Tune your rules by filtering different properties to ensure that the rules are defined and working as intended, including log source coverage. Determine which rules you might need to edit in QRadar or investigate further in QRadar Use Case Manager.

DSMs and uDSMs

Do you know how to view raw log data versus normalized metadata in logs and flow records?

- Viewing raw events

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

- Viewing normalized events

  Events are collected in raw format, and then normalized for display. 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.

Searching events

You can search for all authentication events that QRadar SIEM received in the last 6 hours.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, select **Search** > **New Search**.
3. In the **Time Range** pane, define the time range for the event search:
   a) Click **Recent**.
   b) In the **Recent** list, select **Last 6 Hours**.
4. In the **Search Parameters** pane, define the search parameters:
   a) In the first list, select **Category**.
   b) In the second list, select **Equals**.
   c) In the **High Level Category** list, select **Authentication**.
   d) In the **Low Level Category** list, accept the default value of **Any**.
   e) Click **Add Filter**.
5. In the **Column Definition** pane, select **Event Name** in the **Display** list.
6. Click **Search**.

Related tasks

Example: Creating a custom report based on a saved search
You can create reports by importing a search or creating custom criteria.

Saving event search criteria

You can save specified event search criteria for future use.

Procedure

1. Click the **Log Activity** tab.
2. On the toolbar, click **Save Criteria**.
3. In the **Search Name** field, type **Example Search 1**.
4. In the **Timespan options** pane, click **Recent**.
5. In the **Recent** list, select **Last 6 Hours**.
6. Click **Include in my Quick Searches**.
7. Click **Include in my Dashboard**.

   If **Include in my Dashboard** is not displayed, click **Search** > **Edit Search** to verify that you selected **Event Name** in the **Column Definition** pane.
8. Click **OK**.

What to do next

Configure a time series chart. For more information, see “Configuring a time series chart” on page 25.

Related tasks

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.

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.

Procedure

1. In the chart title bar, click the **Configure** icon.
2. In the **Value to Graph** list, select **Destination IP (Unique Count)**.
3. In the **Chart Type** list, select **Time Series**.
4. Click **Capture Time Series Data**.
5. Click **Save**.
6. Click **Update Details**.
7. Filter your search results:
   a) Right-click the event that you want to filter.
   b) Click **Filter on Event Name is <Event Name>**.
8. To display the event list that is grouped by the user name, select **Username** from the **Display** list.
9. Verify that your search is visible on the **Dashboard** tab:
   a) Click the **Dashboard** tab.
   b) Click the **New Dashboard** icon.
   c) In the **Name** field, type **Example Custom Dashboard**.
   d) Click **OK**.
   e) In the **Add Item** list, select **Log Activity** > **Event Searches** > **Example Search 1**.

Results

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

Related tasks

Saving event search criteria
You can save specified event search criteria for future use.

Searching flows

You can search, monitor, and investigate flow data in real time. You can also run advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated.

Procedure

1. Click the **Network Activity** tab.
2. On the toolbar, click **Search** > **New Search**.
3. In the **Time Range** pane, define the flow search time range:
   a) Click **Recent**.
   b) In the **Recent** list, select **Last 30 Minutes**.
4. In the **Search Parameters** pane, define your search criteria.
   a) In the first list, select **Flow Direction**.

b) In the second list, select **Equals**.

c) In the third list, select **R2L**.

d) Click **Add Filter**.

5. In the **Display** list in the **Column Definition** pane, select **Application**.
6. Click **Search**.

Results

All flows with a flow direction of remote to local (R2L) in the last 30 minutes are displayed, grouped, and sorted by the **Application** field.

Saving flow search criteria

You can save specified flow search criteria for future use.

Procedure

1. On the **Network Activity** tab toolbar, click **Save Criteria**.
2. In the **Search Name** field, type the name **Example Search 2**.
3. In the **Recent** list, select **Last 6 Hours**.
4. Click **Include in my Dashboard** and **Include in my Quick Searches**.
5. Click **OK**.

What to do next

Create a dashboard item. For more information, see "Creating a dashboard item" on page 26.

Related tasks

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

Creating a dashboard item

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

Procedure

1. On the **Network Activity** toolbar, select **Quick Searches** > **Example Search 2**.
2. Verify that your search is included in the Dashboard:

   a) Click the **Dashboard** tab.

   b) In the **Show Dashboard** list, select **Example Custom Dashboard**.

   c) In the **Add Item** list, select **Flow Searches** > **Example Search 2**.
3. Configure your dashboard chart:

   a) Click the **Settings** icon.

   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.
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 *IBM QRadar User Guide*.

Related tasks

Saving flow search criteria
You can save specified flow search criteria for future use.

Searching assets

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.

About this task

Use the search feature to search host profiles, assets, and identity information. Identity information provides more details, such as DNS information, user logins, and MAC addresses on your network.

Procedure

1. Click the **Assets** tab.
2. In the navigation pane, click **Asset Profiles**.
3. On the toolbar, click **Search** > **New Search**.
4. If you want to load a saved search, do the following steps:
   a) In the **Group** list, select the asset search group that you want to display in the **Available Saved Searches** list.
   b) Choose one of the following options:
      - In the **Type Saved Search or Select from List** field, type the name of the search you want to load.
      - In the **Available Saved Searches** list, select the saved search that you want to load.
   c) Click **Load**.
5. In the **Search Parameters** pane, define your search criteria:
   a) In the first list, select the asset parameter that you want to search for.
   For example, **Hostname**, **Vulnerability Risk Classification**, or **Technical Owner**.
   b) In the second list, 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.
6. Click **Search**.

Example

You receive a notification that CVE ID: CVE-2010-000 is being actively exploited. To determine whether any hosts in your deployment are vulnerable to this exploit, do the following steps:

1. From the list of search parameters, select **Vulnerability External Reference**.
2. Select **CVE**.
3. To view a list of all hosts that are vulnerable to that specific CVE ID, type the following command:

   ```
   2010-000
   ```

For more information, see the Open Source Vulnerability Database (http://osvdb.org/) and the (National Vulnerability Database (http://nvd.nist.gov/).

Offense Investigations

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

QRadar SIEM can correlate events and flows with destination IP addresses located across multiple networks in the same offense and the same network incident. You can effectively investigate each offense in your network.

Viewing offenses

You can investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.

Procedure

1. Click the **Offenses** tab.
2. Double-click the offense that you want to investigate.
3. On the toolbar, select **Display** > **Destinations**.

   You can investigate each destination to determine whether the destination is compromised or exhibiting suspicious behavior.
4. On 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.

Example: Enabling the PCI report templates

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

About this task

Enable Payment Card Industry (PCI) report templates.

Procedure

1. Click the **Reports** tab.
2. Clear the **Hide Inactive Reports** check box.
3. In the **Group** list, select **Compliance** > **PCI**.
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.
5. In the **Actions** list, select **Toggle Scheduling**.
6. Access generated reports:
   a) From the list in the **Generated Reports** column, select the time stamp of the report that you want to view.
   b) In the **Format** column, click the icon for report format that you want to view.

Example: Creating a custom report based on a saved search

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

About this task

Create a report that is based on the event and flow searches you created in "Searching events" on page 24.

Procedure

1. Click the **Reports** tab.
2. In the **Actions** list, select **Create**.
3. Click **Next**.
4. Configure the report schedule.
   a) Select the **Daily** option.
   b) Select the **Monday, Tuesday, Wednesday, Thursday, and Friday** options.
   c) Using the lists, select **8:00** and **AM**.
   d) Make sure that the **Yes - Manually generate report** option is selected.
   e) Click **Next**.
5. Configure the report layout:
   a) In the **Orientation** list, select **Landscape**.
   b) Select the layout with two chart containers.
   c) Click **Next**.
6. In the **Report Title** field, type **Sample Report**.
7. Configure the top chart container:
   a) In the **Chart Type** list, select **Events/Logs**.
   b) In the **Chart Title** field, type **Sample Event Search**.
   c) In the **Limit Events/Logs To Top** list, select **10**.
   d) In the **Graph Type** list, select **Stacked Bar**.
   e) Click **All data from the previous (24 hours)**.
   f) In the **Base this event report on** list, select **Example Search 1**.

      The remaining parameters automatically populate by using the settings from the **Example Search 1** saved search.
   g) Click **Save Container Details**.
8. Configure the bottom chart container:
   a) In the **Chart Type** list, select **Flows**.
   b) In the **Chart Title** field, type **Sample Flow Search**.
   c) In the **Limit Flows To Top** list, select **10**.
   d) In the **Graph Type** list, select **Stacked Bar**.
   e) Click **All data from the previous 24 hours**.
   f) In the **Available Saved Searches** list, 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**.
9. Click **Next**.
10. Click **Next**.

11. Choose the report format:
    a) Click the **PDF and HTML** check boxes.
    b) Click **Next**.
12. Choose the report distribution channels:
    a) Click **Report Console**.
    b) Click **Email**.
    c) In the **Enter the report destination email address(es)** field, type your email address.
    d) Click **Include Report as attachment**.
    e) Click **Next**.
13. Complete the final Report wizard details:
    a) In the **Report Description** field, type a description of the template.
    b) Click **Yes - Run this report when the wizard is complete**.
    c) Click **Finish**.
14. Using the list box in the **Generated Reports** column, select the time stamp of your report.

Related tasks

Searching events

You can search for all authentication events that QRadar SIEM received in the last 6 hours.

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

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide 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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

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.

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 actual people or business enterprises is entirely coincidental.

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.

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

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

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

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.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr

Glossary

This glossary provides terms and definitions for the IBM QRadar SIEM 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

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
An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

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

G