IBM Security QRadar SIEM
Version 7.3.1

# *Getting Started Guide*

**Note**
Before you use this information and the product that it supports, read the information in "Notices" on page 21.

**Product information**

This document applies to IBM QRadar Security Intelligence Platform V7.3.1 and subsequent releases unless superseded by an updated version of this document.

# Contents

# Introduction to getting started with QRadar SIEM

The IBM® Security 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 Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

# 1 QRadar SIEM overview

IBM Security 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.

To get started, configure a basic QRadar SIEM installation, collect event and flow data, and generate reports.

## Log activity

In IBM Security 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.

## Network activity

In IBM Security 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.

## 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.

## Offenses

In IBM Security 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.

## Reports

In IBM Security 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.

## 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 *IBM Security QRadar Log Sources User 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.

## 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 Security 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 Security QRadar Administration Guide*.

## Supported web browsers

For the features in IBM Security 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 | 45.8 Extended Support Release and later |
| 64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled. | 11.0, Edge 38.14393 and later |
| 64-bit Google Chrome | Latest |

# 2 Getting started with QRadar SIEM deployment

Before you can evaluate IBM Security 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.

To use an interactive Getting Started launchpad, go to https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_gs_deployment.html (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_gs_deployment.html).

## Installing the QRadar SIEM appliance

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

### Before you begin

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

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

### Procedure

1. Connect the management network interface to the port labeled Ethernet 1.
2. Plug the dedicated power connections into the rear of the appliance.
3. If you need console access, connect the USB keyboard and standard VGA monitor.
4. If the appliance has a front panel, remove the panel by pushing in the tabs on either side and pulling the panel away from the appliance.
5. Power on the appliance.

## The QRadar SIEM appliance

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

The QRadar SIEM appliance includes four network interfaces. For this evaluation, use the interface that is labeled Ethernet 1 as the management interface.

You can use the three remaining monitoring interfaces for flow collection. The QRadar QFlow Collector provides full network application analysis and can perform packet captures on the beginning of each conversation. Depending on the QRadar SIEM appliance, flow analysis automatically begins when a span port or tap is connected to any interface other than Ethernet 1. Extra steps might be required to enable the QRadar QFlow Collector component within QRadar SIEM.

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

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

## 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" on page 4
For the features in IBM Security 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.

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

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

**Note:** If your system does not include a completed network hierarchy, then use the **Admin** tab to create a hierarchy specific to your environment.

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

## Reviewing your network hierarchy

You can review your network hierarchy.

### Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.

3. Click the **Network Hierarchy** icon.
4. In the **Name** column, expand **Regulatory_Compliance_Servers**.

   If your network hierarchy does not include a regulatory compliance server component, you can use your Mail component for the remainder of this procedure.
5. Click the nested **Regulatory_Compliance_Servers**.
6. Click the **Edit** icon.
7. To add compliance servers, follow these steps:
   a. In the **IP/CIDR(s)** field, type the IP address or CIDR range of your compliance servers.
   b. Click the **(+)** icon.
   c. Repeat for all compliance servers.
   d. Click **Save**.
   e. Repeat this process for any other networks that you want to edit.
8. On the **Admin** tab menu, click **Deploy Changes**.

   You can automatically or manually update your configuration files with the latest network security information. QRadar SIEM uses system configuration files to provide useful characterizations of network data flows.

## 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 Security 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.

### Procedure

1. Click the **Admin** tab.
2. In the navigation pane, click **System Configuration**.
3. Click the **Auto Update** icon.
4. In the navigation pane, click **Change Settings**.
5. Select the **Basic** tab.
6. In the **Auto Update Schedule** pane, accept the default parameters.
7. In the **Update Types** pane, configure the following parameters:
   a. In the **Configuration Updates** list box, select **Auto Update**.
   b. Accept the default values for the following parameters:

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

8. Clear the **Auto Deploy** check box.

   By default, the check box is selected. If the check box is not selected, a system notification is displayed on the **Dashboard** tab to indicate that you must deploy changes after updates are installed.
9. Click the **Advanced** tab.
10. In the **Server Configuration** pane, accept the default parameters.
11. In the **Other Settings** pane, accept the default parameters.
12. Click **Save** and close the Updates window.
13. On the toolbar, click **Deploy Changes**.

## 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 Security 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.

### Before you begin

This procedure is not available for IBM QRadar on Cloud. For more information about how to enable flows on third-party network devices, such as switches and routers, see your vendor documentation.

### 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 Security 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 3
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 perform the following tuning tasks:

- Optimize event and flow payload searches by enabling a payload index on the **Log Activity** and **Network Activity Quick Filter** property.
- 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 Security 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 navigation pane, click **System Configuration**.
3. Click the **Index Management** icon.
4. In the **Quick Search** field, type the following:
   ```
   quick filter
   ```
5. Right-click the **Quick Filter** property that you want to index.
6. Click **Enable Index**.
7. Click **Save**.
8. Click **OK**.
9. Optional: 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 detailed information about the parameters that are displayed in the Index Management window, see the *IBM Security 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 Security 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 Security QRadar Administration Guide*
5. Close the Rules wizard.
6. In the Rules page, click **Actions**.
7. Optional: If you want to prevent the offense from being removed from the database after the offense retention period is elapsed, select **Protect Offense**.
8. Optional: 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.

# 3 Getting started in QRadar SIEM

To get started in IBM Security 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.

## 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" on page 18
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."

**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" on page 13
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."

**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 Security QRadar User Guide*.

**Related tasks**:

"Saving flow search criteria" on page 15
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. Optional: 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 13.

### 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" on page 13
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 Security 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

Printed in USA