IBM Security QRadar
Version 7.2.6

Tuning Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 27.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to QRadar tuning

This information is intended for use with IBM® Security QRadar® and provides information on how to tune and optimize your QRadar system.

Intended audience

System administrators responsible for tuning must have administrative access to IBM Security QRadar and your network devices and firewalls. The system administrator must have knowledge of your corporate network and networking technologies.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

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

Statement of good security practices

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

Please Note:

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

Chapter 1. Deployment and application tuning overview

Tuning your IBM Security QRadar SIEM environment involves processes in which one or more parameters of an appliance, deployment, or running system are adjusted to run more efficiently.

After you install QRadar and it is running, you can tune your QRadar SIEM system in the following two phases:

Deployment phase
: During this phase, you configure essential network, scanner, log source, and asset configurations. This phase is done at the start of your lifecycle management for QRadar systems.

Application phase
: During this phase, you discover servers, investigate offenses, optimize custom rules, edit building blocks, tune false positives, and improve search performance in QRadar.

Chapter 2. Deployment tuning phase

In the deployment phase, you configure essential network, scanner, log source, and asset configurations that are required to tune IBM Security QRadar. The deployment phase is done close to start up, after you install, and configure QRadar and it is operational.

Network hierarchy

IBM Security QRadar uses the network hierarchy to determine which hosts are local or remote. QRadar also uses the hierarchy to monitor specific logical groups or services that are in your network, such as specific office locations, regions, departments, or network ranges such as DMZs, VPN pools, or VOIP networks.

You must ensure that all internal address spaces, both routable and non-routable, are defined within your network hierarchy. Otherwise, QRadar might generate an excessive number of false positives, because QRadar treats internal systems differently from external systems. QRadar ignores typical internal network activity from internal IP address ranges.

Administrators must define the following top-level objects:

- Internet facing IP address for a DMZ.
- IP addresses used for remote access in Virtual Private Network (VPN) systems.
- Data centers and server networks.
- Network devices and network management devices.

For more information about creating your network hierarchy, see the *IBM Security QRadar SIEM Administration Guide*.

VA scanners

IBM Security QRadar uses vulnerability assessment (VA) information to determine offense threat levels and remove false positives, by correlating event data, network activity, and behavioral changes.

To schedule scans and maintain your VA data, you can integrate QRadar with VA tools such as third-party scanners. Depending on the scanner type, QRadar imports scan results from the scanner server or initiates a scan remotely.

Scan results provide the system version and port number of each server in the Classless Inter-Domain Routing (CIDR) address range. The information shows the ports that are open and the vulnerabilities on the system.

Ensure that you download and apply the most recent scanner plug-ins.

For more information about configuring VA scanners, see the *Vulnerability Assessment Configuration Guide*.

DSM updates

IBM Security QRadar uses Device Support Modules (DSMs) to log and correlate the data that is collected from external log sources, such as firewalls, switches, or routers.

DSMs are regularly updated to ensure that QRadar can correctly interpret and parse security event information that is provided by external devices. DSMs can be updated both automatically and manually.

Although QRadar devices include native log sending capabilities, several devices require extra configuration, or an agent, or both, to send logs. Configuration varies between device types. You must ensure that the devices are configured to send logs in a supported format.

For a list of supported devices, see the *DSM Configuration Guide*.

Updating DSMs automatically

You can automatically download and install DSM updates, which include corrections to parsing issues, scanner changes, and protocol updates.

Before you begin

The Console must be connected to the Internet to receive the updates. If your Console is not connected to the Internet, you must configure an internal update server for your Console to download the files from.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Auto Update** icon.
4. On the navigation menu, click **Change Settings**.
5. From the **Auto Update Schedule** pane, configure the DSM update frequency. To reduce performance impacts on your system, schedule a large update to run during off-peak hours.
6. From the **Update Types** pane, select **Auto Install** from the **DSM, Scanner, Protocol Updates** list box.
7. Click **Save**.

   For more information about configuring DSM updates, see the *IBM Security QRadar SIEM Administration Guide*.

Updating DSMs manually

IBM provides DSM updates regularly. By default, updates are automatically downloaded and installed on your system. However, you can manually install DSM updates at any time.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **Auto Update** icon.
4. On the navigation menu, click **Check for Updates**.

The system retrieves the new updates from Fix Central (www.ibm.com/support/fixcentral/). This might take an extended period. When complete, new updates are listed on the Updates window.

5. On the toolbar, click **Install** > **DSM, Scanner, Protocol Updates**.
6. Click **OK**.

Log source detection

IBM Security QRadar automatically detects log sources that send syslog messages to an Event Collector.

Log sources are detected when QRadar receives a specific number of identifiable syslog messages. The *traffic analysis* component processes syslog messages, identifies the DSMs that are installed on the system, and then assigns the appropriate DSM to the log source. Automatically discovered log sources are displayed in the Log Sources window.

QRadar might not automatically detect log sources that have low activity levels. You must add these devices manually.

Note: DSMs are used to interpret log source data. To receive log source data, you must ensure that the correct DSMs are installed in QRadar.

For more information about automatically detecting log sources, see the *IBM Security QRadar Log Sources User Guide*.

Related concepts:

"DSM updates" on page 4
IBM Security QRadar uses Device Support Modules (DSMs) to log and correlate the data that is collected from external log sources, such as firewalls, switches, or routers.

Displaying log sources

A log source is any external device, system, or cloud service that is configured to either send events to your IBM Security QRadar system or to be collected by your QRadar system. You can display the log sources that are automatically discovered.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.

Adding log sources manually

You can manually add log sources that IBM Security QRadar does not detect automatically.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **Data Sources**.
3. Click the **Log Sources** icon.
4. On the toolbar, click **Add**.
5. Configure the parameters.
6. Click **Save**.

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

   The following table describes the common log source parameters for all log source types:

Table 1. Log source parameters

Parameter	Description
Log Source Identifier	The IPv4 address or host name that identifies the log source. If your network contains multiple devices that are attached to a single management console, specify the IP address of the individual device that created the event. A unique identifier for each, such as an IP address, prevents event searches from identifying the management console as the source for all of the events.
Enabled	When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
Credibility	Credibility is a representation of the integrity or validity of events that are created by a log source. The credibility value that is assigned to a log source can increase or decrease based on incoming events, or it is adjusted in response to user-created event rules. The credibility of events from log sources contributes to the calculation of the offense magnitude and can increase or decrease the magnitude value of an offense.
Target Event Collector	Specifies the QRadar Event Collector that polls the remote log source. Use this parameter in a distributed deployment to improve Console system performance by moving the polling task to an Event Collector.
Coalescing Events	Increases the event count when the same event occurs multiple times within a short time interval. Coalesced events provide a way to view and determine the frequency with which a single event type occurs on the **Log Activity** tab. When this check box is clear, events are viewed individually and events are not bundled. New and automatically discovered log sources inherit the value of this check box from the **System Settings** configuration on the **Admin** tab. You can use this check box to override the default behavior of the system settings for an individual log source.

Flow sources

Flow information is used to detect threats and other suspicious activity that might be missed if you rely only on event information.

Flows provide network traffic information that is sent simultaneously to IBM Security QRadar in various formats, including Flowlog files, NetFlow, J-Flow, sFlow, and Packeteer.

NetFlow, J-Flow, and sFlow are protocols that collect flow data from network devices, such as routers, and send this data to QRadar.

NetFlow, J-Flow, and sFlow are configured in a similar way, but each one is deployed according to the protocol that each network device supports.

If you are collecting NetFlow, J-Flow, or sFlow data, verify that QRadar is collecting complete flow sets. Incomplete or missing flows can make it difficult to analyze network activity.

QRadar QFlow Collectors and packet-based sources

IBM Security QRadar captures traffic from mirror ports or taps within your network by using an IBM Security QRadar QFlow Collector.

The QRadar QFlow Collector is enabled by default, while the mirror port or tap is connected to a monitoring interface on your QRadar appliance. Common mirror port locations include core, DMZ, server, and application switches.

QRadar QFlow Collector combined with QRadar and flow processors provides Layer 7 application visibility and flow analysis 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), QRadar QFlow Collector identifies the traffic as IRC and provides a packet capture of the beginning of the conversation. This process differs from NetFlow and J-Flow, which indicate that there is traffic on port 7500 (TCP) without identifying the protocol.

QRadar QFlow Collectors are not full packet capture engines, but you can adjust the amount of content that is captured per flow. The default capture size is 64 bytes, and you can collect helpful data by using this setting. However, you might want to adjust this setting to 256 bytes to capture more content per flow. Increasing the capture size increases network traffic between your QRadar QFlow Collector and Flow Processor, and more disk storage is required.

NetFlow flow collectors and external sources

You must configure NetFlow, which collects IP network traffic as it enters or exits an interface, to send data to the nearest QRadar QFlow Collector or QRadar Flow Processor appliance.

QRadar QFlow Collectors also support external flow sources, such as routers that send NetFlow, sFlow, J-Flow, and Packeteer data.

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

You must configure NetFlow to send data as quickly as possible by configuring the external network device's **ip-cache flow timeout** value to one. Ensure that ingress

and egress traffic is forwarded from the router. Not all routers can forward ingress and egress traffic. If you are configuring a router that provides only a sample of data, then configure the router to use the lowest possible sampling rate, without increasing the load on the switch.

To ensure your NetFlow configuration is functioning correctly, you must validate your QRadar NetFlow data.

For more information, see "Verifying NetFlow data collection."

Verifying QRadar QFlow Collector data collection

QRadar QFlow Collectors collect network traffic passively through network taps and span ports and can detect over 1000 networked applications. You can easily verify that your QRadar QFlow Collector is receiving network flow data.

Procedure

1. Click the **Network Activity** tab.
2. From the **Network Activity** toolbar, click **Search** > **New Search**.
3. In the Search Parameters pane, add a flow source search filter.
   a. From the first list, select **Flow Source**.
   b. From the third list, select your QFlow interface name.
4. Click **Add Filter**.
5. In the Search Parameters pane, add a protocol search filter.
   a. From the first list, select **Protocol**.
   b. Click **Filter**.
6. Click **Add Filter**.
7. Click **Filter**.

What to do next

If the **Source Bytes** or **Destination Bytes** column displays many results with zero bytes, your network tap or span might be incorrectly configured. You must verify your QFlow configuration.

Configuring QRadar QFlow Collector devices

You can verify that your QRadar QFlow Collector is operational and is capturing flows from routers or span ports.

Procedure

If you are running dynamic routing protocols, traffic might follow different paths to and from a host.

1. Check that you are collecting flows from all routers where the traffic might cross, especially where there are multiple routes or paths.
2. Ensure that span ports or taps are configured correctly to process both received and transmitted packets.
3. Ensure that there is visibility to both sides of any asymmetric routes.

Verifying NetFlow data collection

To ensure that your NetFlow configuration is working correctly, you must validate your QRadar NetFlow data.

About this task

Configure NetFlow to send data to the nearest QRadar QFlow Collector or QRadar Flow Processor appliance.

By default, QRadar listens on the management interface for NetFlow traffic on port 2055 (UDP). If you need more NetFlow ports, you can assign more ports.

Procedure

1. Click the **Network Activity** tab.
2. From the **Network Activity** toolbar, click **Search** > **New Search**.
3. In the **Search Parameters** pane, add a flow source search filter.
   a. From the first list, select **Flow Source**.
   b. From the third list, select your NetFlow router's name or IP address.

   If your NetFlow router is not displayed in the third list, QRadar might not detect traffic from that router.
4. Click **Add Filter**.
5. In the **Search Parameters** pane, add a protocol search filter.
   a. From the first list, select **Protocol**.
   b. From the third list, select **TCP**.
6. Click **Add Filter**.
7. Click **Filter**.
8. Locate the **Source Bytes** and **Destination Bytes** columns to verify data collection.

   If either column displays many results that have zero bytes, your configuration might be incomplete. You must verify your NetFlow configuration.

Disabling NetFlow log messages

You can disable NetFlow log messages to prevent them from using log file space.

About this task

If your NetFlow router is configured to sample flows, the following message might be logged in your QRadar log file.

```
Nov  3 16:01:03 qflowhost \[11519\] qflow115: \[WARNING\]
default_Netflow: Missed 30 flows from 10.10.1.1 (2061927611,2061927641)
```

This message indicates that the sequence number of the packet is missed. If the number of missed flows is consistent with your sampling rate, then you can ignore the message.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management**.
4. Click **Systems** from the **Display** menu.
5. Select the **Console**.
6. From the **Deployment Actions** menu, click **Edit Host**.
7. Click the **Component Management** icon.
8. From the **Verify NetFlow Sequence Numbers** field, select **No**.

9. Click **Save**.
10. Click **Save** on the Edit Managed Host pane.
11. Close the System and License Management window.
12. On the toolbar, click **Deploy Changes**.

Asset profile configuration

IBM Security QRadar automatically discovers the assets on your network, which are discovered by passive monitoring of QFlow flow data, and active monitoring of vulnerability scan data. QRadar then builds an asset profile, which displays the services that run on each asset.

The asset profile data is used for correlation purposes to help reduce false positives. For example, if an attack attempts to exploit a specific service that runs on a specific asset, QRadar determines whether the asset is vulnerable to this attack by correlating the attack against the asset profile.

Note: Flow data, vulnerability assessment (VA) scanners, or log sources that provide identity must be configured so that asset profiles are displayed in the user interface. If no flow data or scanners exist, no data is compiled for an asset profile.

You can define specific IP addresses (servers) as assets by importing existing assets in comma-separated value (CSV) format. Adding an asset profile helps you to identify an IP address by name and provide a description and weight for that asset.

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

Asset profile data in CSV format

An asset profile is a collection of information about a specific asset. The profile includes information about the services that are running on the asset and any identity information that is known. You can import asset profile data in CSV format.

When you import asset profile data in CSV format, the file must be in the following format:

```
ip,name,weight,description
```

The following table describes the parameters that you must configure.

Table 2. Asset profile import CSV format parameters

Parameter	Description
IP	Specifies any valid IP address in the dot decimal format, for example, 192.168.5.34.
Name	Specifies the name of the asset up to 255 characters in length. Commas are not valid in this field because they invalidate the import process, for example, WebServer01.
Weight	Specifies a number 0 - 10, which indicates the importance of the asset on your network. A value of 0 denotes low importance, while 10 denotes a high importance.

Table 2. Asset profile import CSV format parameters (continued)

Parameter	Description
Description	Specifies a textual description for this asset up to 255 characters in length. This value is optional.

The following entries can be included in a CSV file:

- `192.168.5.34,WebServer01,5,Main Production Web Server`
- `192.168.5.35,MailServ01,0,`

The CSV import process merges any asset profile information that is stored in your QRadar system.

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

Chapter 3. Application tuning phase

In the application tuning phase, you discover servers, investigate offenses, modify building blocks, tune false positives, optimize custom rules, and improve search performance.

Before you tune the application, you must wait 24 hours to enable IBM Security QRadar to detect the servers on the network, store events and flows, and create offenses based on existing rules.

Server discovery

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

Server discovery uses the asset profile database to discover several types of servers in your network. You can select the servers that you want to include in your building blocks.

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

Note: To discover servers, QRadar must receive vulnerability assessment (VA) scanner data or flow traffic. Server discovery uses this data to configure port mappings in the asset profile. For more information, see the *Vulnerability Assessment Configuration Guide*.

QRadar uses building blocks to tune the system and allow more correlation rules to be enabled. This reduces the number of false positives that are detected by QRadar, and helps you to identify business critical assets.

Administrators must determine what servers to discover.

Authorized servers
: You can add authorized infrastructure servers to a selected building block. QRadar monitors these servers while it suppresses false positives that are specific to the server category.

Multiple building blocks
: Servers might be in multiple categories. You must enable QRadar to place these servers in multiple building blocks. For example, Active Directory domain controllers might be identified as both Microsoft Windows and DNS servers.

Identify authorized servers
: After you review the server discovery list, you might not be familiar with all the servers in the list. These servers might be in another business unit or operate within a testing or staging environment. If you identify these servers as authorized, then add them to the building block.

Categorize servers
: You can enable QRadar to categorize unauthorized servers or servers that run unauthorized services into a related building block. If you find that

categorizing servers results in generating an excessive number of offenses, then use server discovery to place the servers in a building block.

Related tasks:

"Tuning building blocks" on page 16
You can edit building blocks to reduce the number of false positives that are generated by IBM Security QRadar.

"Tuning false positives" on page 20
You can tune false positive events and flows to prevent them from creating offenses.

Discovering servers

Server discovery uses the IBM Security QRadar asset profile database to discover different server types that are based on the port definitions. Use **Server Discovery** to select the servers to add to a server type building block.

Procedure

1. Click the **Assets** tab.
2. On the navigation menu, click **Server Discovery**.
3. From the **Server Type** list, select the server type that you want to discover. The default is **Database Servers**.
4. Select one of the following options to determine the servers that you want to discover:
   - **All** To search all servers in your deployment with the currently selected server type.
   - **Assigned** To search servers in your deployment that were assigned to the currently selected server type.
   - To search servers in your deployment that have no previous assignment, select **Unassigned**.
5. From the **Network** list, select the network that you want to search.
6. Click **Discover Servers**.
7. Click **Approve Selected Servers**.
8. In the **Matching Servers** table, select the check box or boxes of all the servers you want to assign to the server role.

What to do next

If you want to modify the search criteria, click either **Edit Ports** or **Edit Definition**.

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

QRadar rules and offenses

The configuration rule that is defined in the Custom Rules Engine (CRE) is used to generate offenses.

The following list describes rules and offenses:

CRE The Custom Rules Engine (CRE) displays the rules and building blocks that are used by IBM Security QRadar. Rules and building blocks are stored in two separate lists because they function differently. The CRE provides information about how the rules are grouped, the types of tests

that the rule performs, and the responses that each rule generates. For more information about rules and offenses, see the *IBM Security QRadar SIEM Users Guide*.

Rules A rule is a collection of tests that triggers an action when specific conditions are met. Each rule can be configured to capture and respond to a specific event, sequence of events, flow sequence, or offense. The actions that can be triggered include sending an email or generating a syslog message. A rule can reference multiple building blocks by using the tests that are found in the function sections of the test groups within the **Rule Editor**.

Offenses
As event and flow data passes through the CRE, it is correlated against the rules that are configured and an offense can be generated based on this correlation. You view offenses on the **Offenses** tab.

Related concepts:

"IBM Security QRadar building blocks" on page 16
Building blocks group commonly used tests, to build complex logic, so that they can be used in rules.

Viewing rules that are deployed

You can view the rules that are deployed in your IBM Security QRadar deployment. For example, you can determine which rules are most active in generating offenses.

Procedure

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

   To determine which rules are most active in generating offenses, from the rules page, click **Offense Count** to reorder the column in descending order.

   For more information about your CRE configuration, see the *IBM Security QRadar SIEM Users Guide*.
3. Double-click any rule to display the **Rule Wizard**. You can configure a response to each rule.

Investigating offenses

IBM Security QRadar generates offenses by testing event and flow conditions. To investigate QRadar offenses, you must view the rules that created the offense.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **All Offenses**.
3. Double-click the offense that you are interested in.
4. On the **All Offenses Summary** toolbar, click **Display** > **Rules**.
5. From the List of Rules Contributing to Offense pane, double-click the **Rule Name** that you are interested in.

   Note: The All Offenses Rules pane might display multiple rule names, if the offense generated by QRadar is triggered by a series of different tests.
   For more information about investigating offenses, see the *IBM Security QRadar SIEM Users Guide*.

IBM Security QRadar building blocks

Building blocks group commonly used tests, to build complex logic, so that they can be used in rules.

Building blocks use the same tests that rules use, but have no actions that are associated with them, and are often configured to test groups of IP addresses, privileged user names, or collections of event names. For example, you might create a building block that includes the IP addresses of all mail servers in your network, then use that building block in another rule, to exclude those hosts. The building block defaults are provided as guidelines, which can be reviewed and edited based on the needs of your network.

You can configure the host definition building blocks (**BB:HostDefinition**) to enable QRadar to discover and classify more servers on your network. If a particular server is not automatically detected, you can manually add the server to its corresponding host definition building block. This ensures that the appropriate rules are applied to the particular server type. You can also manually add IP address ranges instead of individual devices.

Edit the following building blocks to reduce the number of offenses that are generated by high volume traffic servers:

BB:HostDefinition
VA Scanner Source IP

BB:HostDefinition
Network Management Servers

BB:HostDefinition
Virus Definition and Other Update Servers

BB:HostDefinition
Proxy Servers

BB:NetworkDefinition
NAT Address Range

BB:NetworkDefinition
Trusted Network

Tuning building blocks

You can edit building blocks to reduce the number of false positives that are generated by IBM Security QRadar.

About this task

To edit building blocks, you must add the IP address or IP addresses of the server or servers into the appropriate building blocks.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Display** list, select **Building Blocks**.
4. Double-click the building block that you want to edit.
5. Update the building block.

6. Click **Finish**.

   The following table describes editable building blocks.

Table 3. List of building blocks to edit.

Building Block	Description
BB:NetworkDefinition: NAT Address Range	Edit the **and where either the source or destination IP is one of the following** test to include the IP addresses of the Network Address Translation (NAT) servers. Edit this building block only if you have a detection in the *non-NATd* address space. Editing this building block means that offenses are not created for attacks that are targeted or sourced from this IP address range.
BB:HostDefinition: Network Management Servers	Network management systems create traffic, such as ICMP (Internet Control Message Protocol) sweeps, to discover hosts. QRadar SIEM might consider this threatening traffic. To ignore this behavior and define network management systems, edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of the Network Management Servers (NMS), and other hosts that normally perform network discovery or monitoring.
BB:HostDefinition: Proxy Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of the proxy servers. Edit this building block if you have sufficient detection on the proxy server. Editing this building block prevents offense creation for attacks that are targeted or sourced from the proxy server. This adjustment is useful when hundreds of hosts use a single proxy server and that single IP address of the proxy server might be infected with spyware.
BB:HostDefinition: VA Scanner Source IP	Vulnerability assessment products launch attacks that can result in offense creation. To avoid this behavior and define vulnerability assessment products or any server that you want to ignore as a source, edit the **and when the source IP is one of the following** test to include the IP addresses of the following scanners: • VA Scanners • Authorized Scanners
BB:HostDefinition: Virus Definition and Other Update Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of virus protection and update function servers.
BB:Category Definition: Countries with no Remote Access	Edit the **and when the source is located in** test to include geographic locations that you want to prevent from accessing your network. This change enables the use of rules, such as **anomaly: Remote Access from Foreign Country** to create an offense when successful logins are detected from remote locations.
BB:ComplianceDefinition: GLBA Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers that are used for GLBA (Gramm-Leach-Bliley Act) compliance. By populating this building block, you can use rules such as **Compliance: Excessive Failed Logins to Compliance IS**, which create offenses for compliance and regulation-based situations.

Table 3. List of building blocks to edit. (continued)

Building Block	Description
BB:ComplianceDefinition: HIPAA Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers that are used for HIPAA (Health Insurance Portability and Accountability Act) compliance. By populating this building block, you can use rules, such as **Compliance: Excessive Failed Logins to Compliance IS**, which creates offenses for compliance and regulation-based situations.
BB:ComplianceDefinition: SOX Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers that are used for SOX (Sarbanes-Oxley Act) compliance. By populating this building block, you can use rules, such as **Compliance: Excessive Failed Logins to Compliance IS**, which creates offenses for compliance and regulation-based situations.
BB:ComplianceDefinition: PCI DSS Servers	Edit the **and when either the source or destination IP is one of the following** test to include the IP addresses of servers that are used for PCI DSS (Payment Card Industry Data Security Standards) compliance. By populating this building block, you can use rules such as **Compliance: Excessive Failed Logins to Compliance IS**, which creates offenses for compliance and regulation-based situations.
BB:NetworkDefinition: Broadcast Address Space	Edit the **and when either the source or destination IP is one of the following** test to include the broadcast addresses of your network. This change removes false positive events that might be caused by the use of broadcast messages.
BB:NetworkDefinition: Client Networks	Edit the **and when the local network is** test to include workstation networks that users are operating.
BB:NetworkDefinition: Server Networks	Edit the **when the local network is** test to include any server networks.
BB:NetworkDefinition: Darknet Addresses	Edit the **and when the local network is** test to include the IP addresses that are considered to be a *darknet*. Any traffic or events that are directed towards a *darknet* is considered suspicious.
BB:NetworkDefinition: DLP Addresses	Edit the **and when the any IP is a part of any of the following** test to include the remote services that might be used to obtain information from the network. This change can include services, such as *webmail* hosts or file sharing sites.
BB:NetworkDefinition: DMZ Addresses	Edit the **and when the local network** test to include networks that are considered to be part of the network's DMZ.
BB:PortDefinition: Authorized L2R Ports	Edit the **and when the destination port is one of the following** test to include common outbound ports that are allowed on the network.
BB:NetworkDefinition: Watch List Addresses	Edit the **and when the local network is** to include the remote networks that are on a watch list. This change helps to identify events from hosts that are on a watch list.
BB:FalsePositive: User Defined Server Type False Positive Category	Edit this building block to include any categories that you want to consider as false positives for hosts that are defined in the **BB:HostDefinition**: User Defined Server Type building block.

Table 3. List of building blocks to edit. (continued)

Building Block	Description
BB:FalsePositive: User Defined Server Type False Positive Events	Edit this building block to include any events that you want to consider as false positives for hosts that are defined in the **BB:HostDefinition**: User Defined Server Type building block.
BB:HostDefinition: User Defined Server Type	Edit this building block to include the IP address of your custom server type. After you add the servers, you must add any events or categories that you want to consider as false positives to this server, as defined in the **BB:FalsePositives**: User Defined Server Type False Positive Category or the **BB:False Positives**: User Defined Server Type False Positive Events building blocks.

You can include a CIDR range or subnet in any of the building blocks instead of listing the IP addresses. For example, 192.168.1/24 includes addresses 192.168.1.0 to 192.168.1.255. You can also include CIDR ranges in any of the **BB:HostDefinition building** blocks.

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

Related reference:

"Identifying network assets" on page 25
Identify network assets that you might want to include in your building blocks.

Guidelines for tuning system performance

How you tune IBM Security QRadar depends on different scenarios and whether you have one target or many targets within your network.

To ensure reliable system performance, you must consider the following guidelines:

- Disable rules that produce numerous unwanted offenses.
- To tune CRE rules, increase the rule threshold by doubling the numeric parameters and the time interval.
- Consider modifying rules to consider the local network context rather than the remote network context.
- When you edit a rule with the **attach events for the next 300 seconds** option enabled, wait 300 seconds before you close the related offenses.

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

The following table provides information on how to tune false positives according to these differing scenarios.

Table 4. Tuning methodology.

Scenario	One Target	Many Targets
One attacker, one event	Use the **False Positive Wizard** to tune the specific event.	Use the **False Positive Wizard** to tune the specific event.
One attacker, many unique events in the same category	Use the **False Positive Wizard** to tune the category.	Use the **False Positive Wizard** to tune the category.
Many attackers, one event	Use the **False Positive Wizard** to tune the specific event.	Edit the building blocks by using the **Custom Rules Editor** to tune the specific event.

Table 4. Tuning methodology. (continued)

Scenario	One Target	Many Targets
Many attackers, many events in the same category	Use the **False Positive Wizard** to tune the category.	Edit building blocks by using the **Custom Rules Editor** to tune the category.
One attacker, many unique events in different categories	Investigate the offense and determine the nature of the attacker. If the offense or offenses can be tuned out, edit the building blocks by using the **Custom Rules Editor** to tune categories for the host IP address.	Investigate the offense and determine the nature of the attacker. If the offense or offenses can be tuned out, edit the building blocks by using the **Custom Rules Editor** to tune the categories for the host IP address.
Many attackers, many unique events in different categories	Edit the building blocks by using the **Custom Rules Editor** to tune the categories.	Edit the building blocks by using the **Custom Rules Editor** to tune the categories.

Tuning false positives

You can tune false positive events and flows to prevent them from creating offenses.

Before you begin

To create a new rule, you must have the **Offenses** > **Maintain Custom Rules** permission for creating customized rules to tune false positives. For more information about roles and permissions, see the *IBM Security QRadar SIEM Users Guide*.

Procedure

1. Click the **Log Activity** tab, or the **Network Activity** tab.
2. Select the event or flow that you want to tune.
3. Click **False Positive**.

   If you are viewing events or flows in streaming mode, you must pause streaming before you click **False Positive**.
4. Select one of the following **Event** or **Flow Property** options:
   - Event/Flow(s) with a specific QID of <*Event*>
   - Any Event/Flow(s) with a low-level category of <*Event*>
   - Any Event/Flow(s) with a high-level category of <*Event*>
5. Select one of the following **Traffic Direction** options:
   - <*Source IP Address*> to <*Destination IP Address*>
   - <*Source IP Address*> to Any Destination
   - Any Source to <*Destination IP Address*>
   - Any Source to any Destination
6. Click **Tune**.

   QRadar prevents you from selecting **Any Events/Flow(s)** and **Any Source To Any Destination**. This change creates a custom rule and prevents QRadar from creating offenses.

   For more information about tuning false positives, see the *IBM Security QRadar SIEM Users Guide*.

False positives configuration

Manage the configuration of false positives to minimize their impact on legitimate threats and vulnerabilities. To prevent IBM Security QRadar from generating an excessive number of false positives, you can tune false positive events and flows to prevent them from creating offenses.

False positive rule chains

The first rule to execute in the custom rules engine (CRE) is **FalsePositive**:**False Positive Rules and Building Blocks**. When it loads, all of its dependencies are loaded and tested.

If the rule is successfully matched in QRadar, the rule drops the detected event or flow. This stops the event or flow from progressing through the CRE and prevents the flow or event from creating an offense.

Creating false positive building blocks

When you create false positive building blocks within QRadar, you must review the following information:

Naming conventions

Use a methodology similar to the default rule set, by creating new building blocks by using the following naming convention:

<*CustomerName*>**-BB:False Positive: All False Positive Building Blocks**, where: <*CustomerName*> is a name that you assign to the false positive building block.

False positive building blocks

Building blocks must contain the test: **and when a flow or an event matches any of the following rules**. This test is a collection point for false positive building blocks and helps you to quickly find and identify customizations. Note the following guidelines when you create your false positive building blocks:

- When the <*CustomerName*>**-BB:False Positive: All False Positive Building Block** is created, add it to the test in the rule **FalsePositive: False Positive Rules and Building Blocks**.
- When the new false positive building block is created, you can create new building blocks to match the traffic that you want to prevent from creating offenses. Add these building blocks to the <*CustomerName*>**-BB:False Positive: All False Positive Building block**.
- To prevent events from creating offenses, you must create a new building block that matches the traffic that you are interested in. Save this as a building block <*CustomerName*>**-BB:False Positive:** <*name_of_rule*>, then edit <*CustomerName*>**-BB:False Positive: All False Positive building blocks**, to include the rule that you created.

Note: If you add a rule or building block that includes a rule to the **FalsePositive: False Positive Rules and Building Blocks** rule, the rule that you add runs before the event is dropped by the CRE and might create offenses by overriding the false positive test.

Custom rule testing order

When you build custom rules, you must optimize the order of the testing to ensure that the rules do not impact custom rules engine (CRE) performance.

The tests in a rule are executed in the order that they are displayed in the user interface. The most memory intensive tests for the CRE are the payload and regular expression searches. To ensure that these tests run against a smaller subset of data and execute faster, you must first include one of the following tests:

- **when the event(s) were detected by one or more of these log source types**
- **when the event QID is one of the following QIDs**
- **when the source IP is one of the following IP addresses**
- **when the destination IP is one of the following IP addresses**
- **when the local IP is one of the following IP addresses**
- **when the remote IP is one of the following IP addresses**
- **when either the source or destination IP is one of the following IP addresses**
- **when the event(s) were detected by one of more of these log sources**

You can further optimize QRadar by exporting common tests to building blocks. Building blocks execute per event as opposed to multiple times if tests are individually included in a rule.

For more information about optimizing custom rules, see the *IBM Security QRadar SIEM Users Guide*.

Creating an OR condition within the CRE

You can create a conditional OR test within the Custom Rules Engine (CRE), which gives you more options for defining your rules by using building blocks.

About this task

For each extra test that you add, it can be only an AND or AND NOT conditional test. To create an OR condition within the CRE you must place each separate set of conditions into a building block, and then create a new rule or building block that uses the **when <*selected_rule*> matches any of the following rules** rule.

This ensures that both building blocks are loaded when the test is applied.

Procedure

1. Click the **Offenses** tab.
2. On the navigation menu, click **Rules**.
3. From the **Actions** list, select one of the following options:
   - **New Event Rule** Select this option to configure a rule for events.
   - **New Flow Rule** Select this option to configure a rule for flows.
   - **New Common Rule** Select this option to configure a rule for events and flows.
   - **New Offense Rule** Select this option to configure a rule for offenses.
4. Read the introductory text and then click **Next**.

   You are prompted to **Choose the source from which you want this rule to generate**.

   The default is the rule type that you selected on the **Offenses** tab.
5. If it is required, select the rule type that you want to apply to the rule, and then click **Next**.

6. From the **Type to filter** menu, select one of the following corresponding tests that is based on the option that you choose in step 3, and then click the (**+**) icon beside the test.
   - **when an event matches any | all of the following rules**
   - **when a flow matches any | all of the following rules**
   - **when a flow or an event matches any | all of the following rules**
   - **when the offense matches any of the following offense rules**

   For example, if you select **New Event Rule** in step 3, select **when an event matches any | all of the following rules**.
7. In the Rule pane, select one of the following corresponding tests that is based on the option that you choose in step 3, and then click **rules.**
   - **and when an event matches any of the following rules**
   - **and when a flow matches any of the following rules**
   - **and when a flow or an event matches any of the following rules**
   - **and when the offense matches any of the following offense rules**

   For example, if you select **New Event Rule** in step 3, select **and when an event matches any of the following rules**, and then click **rules.**
8. From the **Select the rule(s) to match and click 'Add'** field, select multiple building blocks by holding down the Ctrl key and click **Add +**.

   If you select the offense rule, select building blocks from the **Select an offense rule and click 'Add' field**.
9. Click **Submit**.

Adding filters to improve search performance

When you search for event or flow information, you can improve performance by adding filters to search fields that are indexed.

About this task

The following table provides information about the fields that are indexed:

Table 5. Log viewer and flow viewer indexed fields

QRadar SIEM Tab	Indexed Filter
Log Activity tab (Events)	Username
	Source or Destination IP
	Destination Port
	Has Identity
	Device Type
	Device ID
	Category
	Matches Custom Rule
Network Activity tab (Flows)	Application
	Source or Destination IP
	Destination Port

Procedure

1. Click the **Log Activity** tab, or the **Network Activity** tab.
2. On the toolbar, click **Add Filter**.
3. From the first list, select an index filter.
4. From the second list, select the modifier that you want to use.
5. Type or select the information for your filter. The controls that are displayed depend on the index filter that you added.
6. Click **Add Filter**.

What to do next

You can monitor the performance of your search by expanding the **Current Statistics** option on the **Search** page. This displays the volume of data that loads from data files and indexes. If your search does not display a count in the **index file count**, then add an indexed filter to the search.

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.

Procedure

1. Log in to QRadar as an administrator.
2. Click the **Admin** tab.
3. On the navigation menu, click **System Configuration**.
4. Click the **Index Management** icon.
5. In the **Quick Search** field, type **Quick Filter**.
6. Select the **Quick Filter** property that you want to index.

   You can identify the event and flow **Quick Filter** properties by using the value in the **Database** column.
7. On the toolbar, click **Enable Index**.

   A green dot indicates that the payload index is enabled.
8. Click **Save**.
9. Click **OK**.

   The selected **Quick Filter** properties are indexed.

   If a list includes event or flow properties that are indexed, these indexed property names are appended with the following text:

   `[Indexed]`

Custom properties

Use the **Custom Extracted Properties** function in IBM Security QRadar to expand normalized fields by adding custom fields for reports, searches, and the custom rules engine (CRE).

To extract proxy URLs, virus names, or secondary user names, review the following information:

- Restrict your **Custom Extracted Properties** to a particular log source type or individual log source.

- If your extracted property is applicable to only certain events, reduce the workload on QRadar by limiting the extracted property to that event type.
- By using custom extracted properties to optimize rules, reports and searches, custom rules engine can use the custom property. The processing of the extracted property moves to the time when the event is collected, as opposed to when it is searched. By default, custom extracted properties are processed when they are searched or displayed. Optimizing an extracted property minimizes the search time against the property.
- The **extracted property** field is not indexed. However, when an event matches the property, it stores an index to the offset and length of the property, which reduces the amount of data that is searched.

Cleaning the SIM model

Cleaning the SIM model ensures that offenses are based on the most current rules, discovered servers, and network hierarchy. When the tuning process is complete, clean the SIM model to ensure that IBM Security QRadar displays only recent offenses.

About this task

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

False positive offenses might occur before you complete the tuning tasks. Clean the SIM model to ensure that each host on the network creates new offenses based on the current configuration.

Procedure

1. Click the **Admin** tab.
2. From the **Admin** toolbar, click **Advanced** > **Clean SIM Model**.
3. Click **Hard Clean**.
4. Select the **Are you sure you want to reset the data model?** check box.
5. Click **Proceed**.

   Depending on the volume of data in your system, this process might take several minutes.
6. When the SIM reset process is complete, refresh your browser.

   If you attempt to go to other areas of the user interface during the SIM reset process, an error message is displayed.

Identifying network assets

Identify network assets that you might want to include in your building blocks.

Use the following table as a reference to help you create building blocks.

Table 6. Identifying Network Assets

Category	How to Identify and Examples	Building Block
NAT Address	IP addresses and/or CIDR blocks that are used for Network Address Translation (NAT). These are commonly configured on firewalls and routers.	**BB-NetworkDefinition**: NAT Address Range.

Table 6. Identifying Network Assets (continued)

Category	How to Identify and Examples	Building Block
Network and Desktop Management Servers	Altiris, BindView, CA Unicenter, CiscoWorks, Dell OpenManage, HP OpenView, IBM Director, Marimba, McAfee ePolicy Orchestrator, Norton Antivirus server, Tivoli®, Sitescope, Sophos server, SMS, What's Up Gold	**BB-HostDefinition**: Network Management Servers.
Proxy Servers	In-Line PaloAlto firewalls, Sidewinder, ISA, Bluecoat, Microsoft Proxy Server, Squid, Websense, Wingate	**BB-HostDefinition**: Proxy Servers.
Server Networks	CIDRs used by data centers or server populations.	**BB-HostDefinition:** Server Networks.
Vulnerability/ Security Scanners	Acunetix, CyberCop Scanner, Foundstone, HackerShield, ISS Internet Scanner, Nessus, Retina, nCircle, Nmap.	**BB-HostDefinition**: VA Scanner Source ID.

Notices

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

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP See Dynamic Host Configuration Protocol.

DNS See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

flow A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a

managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS See intrusion prevention system.

ISP See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L See Local To Local.

L2R See Local To Remote.

LAN See local area network.

LDAP See Lightweight Directory Access Protocol.

leaf In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L See Remote To Local.

R2R See Remote To Remote.

recon See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

Printed in USA