Extreme Networks SIEM Tuning Guide

Release 7.2.5

Published July 2015
9034874

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Contact

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

Table of Contents

1 Introduction to Extreme Security Analytics Tuning

This information is intended for use with *Extreme Security Analytics* and provides information on how to tune your Extreme Security deployment.

Intended audience

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

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. Extreme Networks systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME 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.

2 Overview

This document provides an overview of the steps to setup and tune Extreme SIEM software.

It assumes that your Extreme SIEM system is installed and functional. For more information on installing Extreme SIEM, see the *Extreme SIEM Installation Guide*.

Tuning your Extreme SIEM system is completed in two phases; deployment and tuning. Table 1-1 describes the tasks required to complete each phase.

Table 1: Tuning Checklist

Phase	Task	Complete
Deployment	Create your network hierarchy.	
	Optional. Configure VA Scanners.	
	Update your Device Support Modules (DSMs).	
	Detecting Log Sources.	
	Establish and configure flow sources.	
	Configure your Asset Profile.	
	For more information, see The Deployment Phase on page 3.	
Tuning	Discover and validate servers.	
	Understanding and using rules and offenses.	
	Populating building blocks.	
	Tuning false positives.	
	Optimize Custom Rules	
	Cleaning the SIM model.	
	For more information, see The Tuning Phase on page 11.	

For assistance with tuning your Extreme SIEM system, contact Customer Support.

3 The Deployment Phase

In the deployment phase you configure essential network, scanner, log source, and asset configurations that are required to effectively tune Extreme SIEM.

The network hierarchy is used to determine which hosts are local or remote and monitor specific logical groups or services in your network, such as marketing, Demilitarized Zones (DMZs), or Voice Over IP (VOIP).

You must ensure that all internal address spaces, both routable and non-routable, are defined within your network hierarchy. Failure to do so can result in Extreme SIEM generating an excessive number of false positives.

Administrators must define the following top-level objects:

- DMZ: Internet facing IP address.
- Virtual Private Network (VPN): IP addresses used for remote access.
- Data centers and server networks.
- Network management and network devices.
- You must configure a weight value 1 - 100 for each network component. A weight enables Extreme SIEM to determine the severity of the same event interacting with two different hosts.

NOTE

Assign higher weight values to servers that contain critical information.

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

VA scanners

Extreme SIEM user 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 Extreme SIEM with VA tools such as third-party scanners. Depending on the scanner type, Extreme SIEM imports scan results from the scanner server or remotely initiates a scan.

The results of a scan provide the system and version of each Classless Inter-Domain Routing (CIDR), server, and port. Scan information describes the ports that are open and the vulnerabilities on the system.

Ensure that you download and apply the latest scanner plug-ins from the following location: *http://www.ibm.com/support*

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

DSM updates

Extreme SIEM 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 Extreme SIEM can correctly interpret and parse security event information that is provided by external devices. DSMs can be updated both automatically and manually. For more information see, Updating DSMs automatically on page 4 and Updating DSMs manually on page 5.

NOTE

Although most 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 format that SIEM supports.

For a list of supported devices, see the *Configuring DSMs Guide*.

Updating DSMs automatically

You can automatically download and install DSM updates to Extreme SIEM.

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, select the DSM update frequency:
   a Frequency - Select the frequency that you want to receive updates.
   b Hour - Select the time of day that you want to receive updates.
   c Week Day - Select this option if you select Weekly as the update frequency.
   d Day of the Month- Select this option if you select Monthly as the update frequency.

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 *Extreme SIEM Administration Guide.*

Updating DSMs manually

You can manually install DSM updates at any time irrespective of the automatic update schedule.

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.

5 From the toolbar, select Install > DSM, Scanner, Protocol Updates.

6 Click OK.

Log source detection

Extreme SIEM automatically detects log sources that send syslog messages to an Event Collector.

Log sources are detected when Extreme SIEM receives a specific number of identifiable syslog messages. A Traffic Analysis function processes syslog messages. The Traffic Analysis function identifies the DSMs installed on the system and assigns the appropriate DSM to the log source. Automatically discovered log sources are displayed in the Log Sources window. For more information, see Displaying log sources on page 5.

Extreme SIEM might not automatically detect log sources with low activity levels These devices must be added manually. For more information, see Adding log sources manually on page 6.

NOTE

DSMs are used to interpret log source data. To receive log source data, you must ensure that the correct DSMs are installed in Extreme SIEM. For more information, see DSM updates on page 4.

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

Displaying log sources

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 Extreme SIEM 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. For more information about the Log Source parameters, see the *Extreme Security Analytics Log Sources User Guide*.

6 Click Save.

7 On the Admin tab, click Deploy Changes.

Establish and configure flow sources

Flow information is used to detect threats and activity that would otherwise be missed by relying only on event information.

Flows provide network traffic information and can be sent simultaneously to Extreme SIEM 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 Extreme SIEM. NetFlow, J-Flow, and sFlow are configured in a similar way, but each is deployed according to the protocol that each network device supports.

NOTE

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

QFlow Collectors

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

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

The QFlow Collector provides full application detection of network traffic regardless of the port on which the application is operating. For example, if the Internet Relay Chat (IRC) protocol is communicating on port 7500 TCP, the QFlow Collector identifies the traffic as IRC and provides a packet capture of the beginning of the conversation. This differs from

NetFlow and J-Flow, which indicate that there is traffic on port 7500 TCP without identifying the protocol.

NetFlow data collection

Netflow must be configured to send data to the nearest QFlow Collector or Flow Processor appliance.

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 do this). If you are configuring a router that only provides 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 Extreme SIEM NetFlow Data. For more information, see Verifying NetFlow data collection on page 8.

Verifying QFlow Collector data collection

You can verify that your QFlow Collector is receiving network flow data.

Procedure

1 Click the Network Activity tab.

2 From the Network Activity toolbar, select Search > New Search.

3 In the Search Parameters pane, add a flow source search filter:
   a From the first list down, select Flow Source.
   b From the third list box, 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 box, select Protocol.
   b From the third list box, select TCP.

6 Click Add Filter.

7 Click Filter.

What to do next

If the Source Bytes or Destination Bytes column displays a large volume of results with zero bytes, your network tap or span might not be correctly configured. You must verify your QFlow configuration. For more information, see Configuring QFlow Collector devices on page 8.

Configuring QFlow Collector devices

You can verify that your QFlow Collector is operational.

About this task

If you are running dynamic routing protocols, traffic might follow different paths to and from a host. If you have more than one traffic path or route at the locations where you are collecting flow data, check with your network administrator to ensure that you are collecting flows from all routers that the traffic can traverse.

Procedure

1 Ensure that span ports or taps are configured correctly to process both received and transmitted packets.

2 Ensure visibility into both sides of any asymmetric routes.

Verifying NetFlow data collection

To ensure your NetFlow configuration is functioning correctly, you must validate your Extreme SIEM NetFlow Data. Netflow should be configured to send data to the nearest QFlow Collector or Flow Processor appliance.

About this task

By default, Extreme SIEM listens on the management interface for NetFlow traffic on port 2055 UDP. You can assign additional NetFlow ports if necessary.

Procedure

1 Click the Network Activity tab.

2 From the Network Activity toolbar, select Search > New Search.

3 In the Search Parameters pane, add a flow source search filter.
   a From the first list box, select Flow Source.
   b From the third list box, select your NetFlow router's name or IP address.

NOTE

If your NetFlow router is not displayed in the third list box, Extreme SIEM might not detect traffic from the router. For further assistance, contact Customer Support.

4 Click Add Filter.

5 In the Search Parameters pane, add a protocol search filter.
   a From the first list box, select Protocol.
   b From the third list box, select TCP.

6 Click Add Filter.

7 Click Filter.

What to do next

Locate the Source Bytes and Destination Bytes columns. If either column displays a large volume of results with zero bytes, your NetFlow configuration might be incomplete. You must verify your NetFlow configuration.

Disabling NetFlow log messages

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

About this task

If your NetFlow router is configured to sample flows, the following message can be logged in your Extreme SIEM log file. This message indicates that the sequence number on the packet was missed. If the number of missed flows is consistent with your sampling rate then, you can ignore this message.

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

Procedure

1. Click the Admin tab.
2. On the Admin toolbar, click Deployment Editor.
3. Right-click the component that is specified in the error message and select Configure.
4. On the toolbar, click Advan.
5. From the General Settings expansion list, identify the Verify NetFlow Sequence Numbers field, and select No from the list box.
6. Click Save.
7. Click the Saves recent changes and closes editor icon to close the Deployment Editor.
8. Click Deploy Changes.

Asset profile configuration

Extreme SIEM automatically discovers the assets on your network, which are based on passive QFlow data and vulnerability data. Extreme SIEM then builds an asset profile that displays the services running on each asset.

Asset profile data is used for correlation purposes to help reduce false positives. For example, if an attack attempts to exploit a specific service running on a specific asset,

Extreme SIEM determines if the asset is vulnerable to this attack by correlating the attack against the asset profile.

NOTE

Flow data or VA scanners must be configured for asset profiles to be displayed in the user interface. If no flow data or scanners are present, no data will exist to compile an asset profile.

You can define specific IP addresses (servers) as assets by importing existing assets in Comma-Separated Value (CSV) format. For more information, see Import assets in CSV format on page 10. Adding an asset profile enables you to identify an IP address by name and provide a description and weight for the asset.

For more information about managing assets, see the *Extreme SIEM Administration Guide*.

Import assets in CSV format

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 and invalidate the import process. For example, WebServer01.
Weight	Specifies a number from 0 to 10, which indicates the importance of the asset on your network. A value of 0 denotes low importance, while 10 denotes a very high importance.
Description	Specifies a textual description for this asset up to 255 characters in length. This value is optional.

Examples of Acceptable CSV Entries

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 Extreme SIEM system.

For more information about configuring assets, see the *Extreme SIEM Administration Guide*.

4 The Tuning Phase

In the tuning phase, you discover servers, investigate offenses, modify building blocks, tune false positives, optimize custom rules, and improve search performance. Before you tune Extreme SIEM, you must wait 24 hours to enable Extreme SIEM to detect the servers on the network, store events and flows, and create offenses based on existing rules.

Server discovery

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

The Server Discovery function uses the asset profile database to discover many types of servers on your network. This function lists automatically discovered servers and enables you to select which servers you want to include in building blocks. For more information, see Extreme Security building blocks on page 14.

For more information on server discovery, see the *Extreme SIEM Administration Guide*.

NOTE

To discover servers, Extreme SIEM 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 on VA, see the *Vulnerability Assessment Configuration Guide*.

Extreme SIEM uses building blocks to tune the system and allow additional correlation rules to be enabled. This reduces the number of false positives detected by Extreme SIEM, and helps you to identify business critical assets. For more information on false positives, see Tuning false positives on page 20.

Administrators must determine which servers to discover.

Authorized servers

You can enable the Server Discovery function to add authorized infrastructure servers to a selected building block. The Server Discovery function selects the correct building block or rule for discovered servers and enables Extreme SIEM to monitor these servers while suppressing false positives that are specific to the server category.

Multiple building blocks

Servers might be present in multiple categories. You must enable Extreme SIEM to place these servers in multiple building blocks. For example, active directory domain controllers might be identified as both Windows and DNS servers.

Identify authorized servers

After reviewing the server discovery list, not all the servers displayed in the list might be familiar to you. These servers might be located 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. For more information, see Extreme Security building blocks on page 14.

Categorize servers

You can enable Extreme SIEM to categorize unauthorized servers or servers running unauthorized services into a related building block. For more information, see Table 3. If categorizing servers generates an excessive number of offenses, then use the Server Discovery function to place the servers in a building block.

Discovering servers

The server discovery function uses the Extreme SIEM Asset Profile database to discover different server types based on port definitions.

About this task

Server discovery enables you to select which servers to add to a server type building block. This feature makes the discovery and tuning process simpler and faster by providing a fast mechanism to insert servers into building blocks.

Procedure

1 Click the Assets tab.

2 On the navigation menu click Server Discovery.

3 From the Server Type drop-down list box, select the server type you want to discover. The default is Database Servers.

4 Select the option to determine the servers you want to discover:

- All - Search all servers in your deployment with the currently selected server type.
- Assigned - Search servers in your deployment that have been previously assigned to the currently selected server type.
- Unassigned - Search servers in your deployment that have not been previously assigned.

5 From the Network list box, select the network 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 on discovering servers, see the *Extreme SIEM Administration Guide*.

Extreme Security rules and offenses

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

CRE

The CRE displays the rules and building blocks that are used by Extreme SIEM. 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 the rule performs, and the responses each rule generates. For more information on viewing your CRE configuration, see Viewing the current CRE configuration on page 13.

For more information on Rules and Offenses, see the *Extreme SIEM Users Guide*.

Rules

A rule is a collection of tests that perform an action when certain 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 can include sending an email or generating a syslog message. A rule can reference multiple building blocks by using the tests found in the function sections of the test groups within the Rule Editor. For more information on building blocks, see Extreme Security building blocks on page 14.

Offenses

As event and flow data passes through the CRE, it is correlated against the rules that are configured and an offense is generated based on this correlation.

Offenses are displayed using the Offenses tab. For more information on offenses, see Investigating offenses on page 14.

Viewing the current CRE configuration

You can view the rules that are deployed in your Extreme SIEM.

About this task

Double-click any rule to display the Rule Wizard. This displays the tests associated with each rule and enables you to configure the response to each rule.

Procedure

1 Click the Offenses tab.

2 On the navigation menu click Rules.

For more information on your CRE configuration, see the *Extreme SIEM Users Guide*.

What to do next

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

Investigating offenses

Extreme SIEM generates offenses by testing event and flow conditions. To investigate Extreme SIEM 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 you are interested in.

4 From the All Offenses Summary toolbar, select Display > Rules.

5 From the List of Rules Contributing to Offense pane, double-click the Rule Name you are interested in.

NOTE

The All Offenses Rules pane can display multiple Rule Names, since the offense generated by Extreme SIEM might have been triggered by a series of different tests.

For more information on investigating offenses, see the *Extreme SIEM Users Guide*.

Extreme Security building blocks

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

Building blocks use the same tests as rules, but have no actions associated with them and are often configured to test groups of IP addresses, privileged usernames, 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 should be reviewed and edited based on the needs of your network.

You can configure the host definition building blocks (BB:HostDefinition) to enable Extreme SIEM to discover and classify additional 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 entire address ranges as opposed to individual devices.

Commonly edited building blocks

You can reduce the number of offenses generated by high volume traffic servers, such as proxy servers and virus servers. For more information, see Building block tuning on page 15.

To reduce the number of offenses, administrators must edit the following building blocks:

- 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: TrustedNetwork

Building block tuning

You can edit building blocks to reduce the number of false positives generated by Extreme SIEM. For more information on false positives, see Tuning false positives on page 20.

You can edit building blocks if you have certain server types present on the networks that you want to monitor. If you do not have these server types on the networks, then you can choose to skip this step. For more information, see Editing a Building Block on page 18.

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

For more information, see the *Extreme SIEM Administration Guide*. Also, see Identifying Network Assets on page 27.

Table 3 provides the list of building blocks that you can edit.

Table 3: List of recommended 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. Only edit this building block if you have detection in the non-NATd address space. Editing this building block means that offenses are not created for attacks 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. Extreme 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 following servers: Network Management Servers (NMS). Other hosts that normally perform network discovery or monitoring.

Table 3: List of recommended building blocks to edit (Continued)

Building Block	Description
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 targeted or sourced from the proxy server. This is useful when hundreds of hosts use a single proxy server and that single IP address of the proxy server may 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 which should be prevented from accessing your network. This enables the use of rules, such as anomaly: Remote Access from Foreign Country to create an offense when successful logins have been 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 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.
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 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 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.

Table 3: List of recommended building blocks to edit (Continued)

Building Block	Description
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 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 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 a Darknet. Any traffic or events directed towards a Darknet is considered suspicious as no hosts should be on the network.
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 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 ports that are allowed outbound on the network.
BB:NetworkDefinition: Watch List Addresses	Edit the and when the local network is to include the remote networks that are considered to be on a watch list. This enables you to identify when events occur with hosts of interest.
BB:FalsePositive: User Defined Server Type False Positive Category	Edit this building block to include any categories you want to consider false positives for hosts defined in the BB:HostDefinition: User Defined Server Type building block.
BB:FalsePositive: User Defined Server Type False Positive Events	Edit this building block to include any events you want to consider false positives for hosts 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 have added the servers you must add any events or categories that you want to consider 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.

NOTE

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.

Editing a Building Block

You can edit a building block

Procedure

1 Click the Offenses tab.

2 On the navigation menu, click Rules.

3 From the Display drop-down list box, select Building Blocks.

4 Double-click the building block you want to edit. See Table 3 for a list of building blocks that you can populate with your network information.

5 Update the building block as required.

6 Click Finish.

Tuning Methodology

How you tune Extreme SIEM depends on different scenarios and whether you have one target or many targets within your network.

To ensure reliable system performance, administrators must consider the following best practice guidelines:

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

For more information, see the *Extreme Security LM 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 this specific event.	Use the False Positive Wizard to tune 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 building blocks using the Custom Rules Editor to tune specific event.
Many attackers, many events in the same category	Use the False Positive Wizard to tune the category.	Edit building blocks 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 building blocks using the Custom Rules Editor to tune categories for the host IP.	Investigate the offense and determine the nature of the attacker. If the offense or offenses can be tuned out, edit building blocks using the Custom Rules Editor to tune categories for the host IP.
Many attackers, many unique events in different categories	Edit building blocks using the Custom Rules Editor to tune the categories.	Edit building blocks 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.

About this task

You must have appropriate permissions for creating customized rules to tune false positives. For more information on roles and permissions, see the *Extreme SIEM Administration Guide*.

Procedure

1 Click the Log Activity tab, or alternatively click the Network Activity tab.

2 Select the event or flow you want to tune.

3 Click False Positive.

NOTE

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 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.

NOTE

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

For more information on tuning false positives, see the *Extreme SIEM Users Guide*.

False positive rule chains

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

If the rule is successfully matched in Extreme SIEM, 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.

When creating false positive building blocks within Extreme SIEM, administrators must review the following information.

Naming conventions

Use a methodology similar to the default rule set, by creating new building blocks with 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 enables you to quickly find and identify customizations.

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.

NOTE

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.

CAUTION

If you add a rule or building block that includes a rule to the FalsePositive: False Positive Rules and Building Blocks rule, the rule you have added will execute before the event is dropped by the CRE and could create offenses by overriding the false positive test.

Optimize custom rules

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

The tests in a rule are executed in the order in which 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

NOTE

You can further optimize Extreme SIEM 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 on optimizing custom rules, see the *Extreme SIEM Users Guide*.

Creating an OR condition within the CRE

You can create a conditional OR test within the CRE.

About this task

As you add more tests to a rule, each test can only be 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 utilizes the And When An Event 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 box, 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. Click Next.

You are prompted to choose the source from which you want this rule to apply. The default is the rule type you selected on the Offenses tab.

5 If required, select the rule type you want to apply to the rule. Click Next.

6 Locate the when an event matches any/all of the following rules test and click the + icon beside the test.

7 On the and when an event matches any of the following rules test, 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 +.

9 Click Submit.

Improving search performance

When you are searching Event or Flow information, you can improve performance by adding filters to search indexed fields.

About this task

Table 5 provides information about the fields that are indexed:

Table 5: Log Viewer and Flow Viewer Indexed Fields

Extreme 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

NOTE

You can monitor the performance of your search by expanding the Current Statistics option on the Search page. This displays the volume of data loading 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. For more information, see Adding Indexed Filters on page 24.

Adding Indexed Filters

Indexed filters can be added to both log activity and network activity data.

Procedure

1 Click the Log Activity tab, or alternatively click the Network Activity tab.

2 On the toolbar, click Add Filter.

3 From the first list box, select an index filter. See Table 5.

4 From the second list box, 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 you selected in step 3.

6 Click Add Filter.

Enabling quick filtering

You can enable the Quick Filter property to optimize event and flow search times.

About this task

For Extreme SIEM 7.0 MR3 installations and above, you can enable Quick Filters. This option must be enabled in the System Settings page. You can use the Quick Filter option to search event and flow payloads by typing your exact free text search criteria.

Procedure

1 Log in to Extreme Security.

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 you want to index.

You can identify the event and flow Quick Filter properties 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.

Results

The selected Quick Filter properties are indexed. If a list includes event or flow properties, indexed property names are appended with the following text: `[Indexed]`.

Custom extracted properties

The Custom Extracted Properties function in Extreme SIEM is used to expand normalized fields by adding numerous custom fields for reports, searches, and the CRE. For example, to extract proxy URLs, virus names, or secondary usernames.

Administrators must review the following information:

- You must restrict your custom extracted properties to a particular log source type or individual log source.
- If your extracted property is only applicable to certain events, you can reduce the workload on Extreme SIEM by limiting the extracted property to that event type.
- By using the extracted properties function to optimize rules, reports and searches, the custom property can be used by the custom rules engine. This moves the processing of the extracted property 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. Enabling the optimize feature for an extracted property minimizes the search time against the property.
- The extracted property field is not indexed, but if an event matches the property, it stores an index to the offset and length of the property which reduces the amount of data that must be searched.

Cleaning the SIM model

When the tuning process is complete then clean the SIM model to ensure that Extreme SIEM only displays recent offenses.

About this task

Cleaning the SIM model ensures that offenses are based on the most current rules, discovered servers, and network hierarchy. When you clean the SIM model, all existing offenses are closed. This does not affect existing events and flows.

NOTE

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

Procedure

1 Click the Admin tab.

2 From the Admin toolbar, select Advanced > Clean SIM Model.

3 Select the Hard Clean option.

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

5 Click Proceed.

NOTE

This process may take several minutes, depending on the volume of data in your system.

6 When the SIM reset process is complete, refresh your browser.

NOTE

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

5 Identifying Network Assets

Use this reference to identify network assets that you might want to include in building blocks.

Table 6: Identifying Network Assets

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

6 Glossary

CIDR

See Classless Inter-Domain Routing (CIDR).

Classless Inter-Domain Routing (CIDR)

Addressing scheme for the internet, which allocates and specifies internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.

CRE

See Custom Rules Engine (CRE)

Custom Rules Engine

The collection of rules that Extreme SIEM uses to correlate event and flow information into offenses.

Demilitarized Zone (DMZ)

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

Device Support Module (DSM)

Device Support Modules (DSMs) allow you to integrate Extreme SIEM with log sources.

DNS

See Domain Name System (DNS).

Domain Name System

An online, distributed database used to map human-readable machine names into an IP address for resolving machine names to IP addresses.

DSM

See Device Support Module (DSM).

egress traffic

Network traffic that begins inside a network and proceeds to a destination somewhere outside of the network.

event

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

Event Collector

Collects security events and flows from various types of devices in your network. The Event Collector gathers events and flows from local, remote, and device sources. The Event Collector then normalizes the events and flows, and sends the information to the Event Processor.

Event Processor

Processes events collected from one or more Event Collector(s). The events are bundled once again to conserve network usage. Once received, the Event Processor correlates the information from Extreme SIEM and distributed to the appropriate area, depending on the type of event.

false positive

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

flow

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

flow data

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

flow logs

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

flow sources

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

GLBA

See Gramm-Leach-Bliley Act (GLBA).

Gramm-Leach-Bliley Act

Also known as the Financial Services Modernization Act of 1999, GLBA allows banking, securities and insurance companies to combine investment banking, commercial banking, and insurance activities.

Health Insurance Portability and Accountability Act (HIPPA)

A series of laws and regulations, organizations must comply with to demonstrate they are protecting the private health information of patients and customers.

HIPPA

See Health Insurance Portability and Accountability Act (HIPPA).

ICMP

See Internet Control Message Protocol (ICMP).

Internet Control Message Protocol (ICMP)

Part of the internet protocol suite, normally used by the operating systems of networked computers to send error messages.

Ingress Traffic

Network traffic originating from outside of the network and proceeding to a destination inside of the network.

Internet Protocol (IP)

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

Internet Relay Chat

A set of scripts or an independent program that connects to internet relay chat as a client, and so appears to other IRC users as another user.

IP

See Internet Protocol.

IRC

See Internet Relay Chat (IRC).

J-Flow

A proprietary accounting technology used by Juniper® Networks that allows you to collect IP traffic flow statistics.

log source

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

NetFlow

A proprietary accounting technology developed by Cisco Systems® Inc. that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a NetFlow collector. You can configure Extreme SIEM to accept NDE's and thus become a NetFlow collector.

offense

A message sent or event generated in response to a monitored condition. For example, an offense informs you if a policy has been breached or the network is under attack.

Packeteer

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

Payment Card Industry Data Security Standard (PCI DSS)

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

PCI DSS

See Payment Card Industry Data Security Standard (PCI DSS).

QFlow Collector

Collects data from devices and various live or recorded data feeds, such as, network taps, span/mirror ports, NetFlow, and Extreme SIEM flow logs.

Sarbanes-Oxley (SOX)

Legislation that protects shareholders and the general public from accounting errors and fraudulent practice by defining rules around the storage and handling of electronic records and data.

sFlow

A multi-vendor and end-user standard for sampling technology that provides continuous monitoring of application level traffic flows on all interfaces simultaneously.

SOX

See Sarbanes-Oxley Act (SOX).

UDP

See User Datagram Protocol (UDP).

User Datagram Protocol

A connectionless transport layer protocol which provides a simple message service for transaction-oriented services.

Virtual Private Network

A Virtual Private Network simulates a private network over the public internet by encrypting communications between the two private end-points.

Voice Over IP

VOIP uses the internet protocol to transmit voice as packets over an IP network.

VOIP

See Voice Over IP (VOIP).

VPN

See Virtual Private Network (VPN).

Index

F

G

I

L

M

N

O

Q

R

S

T

U

V