



Extreme Networks Security Risk Manager Getting Started Guide

Copyright © 2016 All rights reserved.

Legal Notice

Extreme 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 on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks

Support

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

For information, contact:

Extreme Networks, Inc.

145 Rio Robles

San Jose, California 95134

USA

Table of Contents

Preface	4
Text Conventions.....	4
Providing Feedback to Us.....	4
Getting Help.....	5
Related Publications.....	5
Chapter 1: Get started with Extreme Networks Security Risk Manager	7
Chapter 2: Deploy Extreme Networks Security Risk Manager	8
Before you install.....	8
Configure port access on firewalls.....	9
Identify network settings.....	9
Unsupported features in Extreme Networks Security Risk Manager.....	9
Supported web browsers	9
Access the Extreme Networks Security Risk Manager user interface.....	10
Setting up a Extreme Networks Security Risk Manager appliance.....	10
Adding Extreme Networks Security Risk Manager to Extreme Networks SIEM Console.....	11
Establishing communication.....	12
Adding the Risk Manager user role.....	12
Chapter 3: Manage audits	13
Use case: Device configuration audit.....	13
Use case: View network paths in the topology.....	15
Chapter 4: Use case: Monitor policies	17
Use case: Assess assets that have suspicious configurations.....	17
Use case: Assess assets with suspicious communication.....	18
Use case: Monitor policies for violations.....	19
Risk priority by vulnerability.....	19
Chapter 5: Use cases for simulations	21
Use case: Simulate attacks on network assets.....	21
Use case: Simulate the risk of network configuration changes.....	22



Preface

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons






Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc] . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- **Global Technical Assistance Center (GTAC) for Immediate Support**
 - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
 - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- **GTAC Knowledge** — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- **The Hub** — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- **Support Portal** — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers

Related Publications

The ExtremeSecurity product documentation listed below can be downloaded from <http://documentation.extremenetworks.com>.

ExtremeSecurity Analytics

- *Extreme Security Release Notes*
- *Extreme SIEM Administration Guide*
- *Extreme SIEM Getting Started Guide*
- *Extreme SIEM High Availability Guide*
- *Extreme SIEM User Guide*
- *Extreme SIEM Tuning Guide*

- *ExtremeSecurity API Reference Guide*
- *ExtremeSecurity Ariel Query Language Guide*
- *ExtremeSecurity Application Configuration Guide*
- *ExtremeSecurity DSM Configuration Guide*
- *ExtremeSecurity Hardware Guide*
- *ExtremeSecurity Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *ExtremeSecurity Log Manager Administration Guide*
- *ExtremeSecurity Log Manager Users Guide*
- *Migrating ExtremeSecurity Log Manager to Extreme SIEM*
- *ExtremeSecurity Managing Log Sources Guide*
- *ExtremeSecurity Offboard Storage Guide*
- *ExtremeSecurity Release Notse*
- *ExtremeSecurity Risk Manager Adapter Configuration Guide*
- *ExtremeSecurity Risk Manager Getting Started Guide*
- *ExtremeSecurity Risk Manager Installation Guide*
- *ExtremeSecurity Troubleshooting System Notifications Guide*
- *ExtremeSecurity Upgrade Guide*
- *ExtremeSecurity Vulnerability Manager User Guide*
- *ExtremeSecurity Vulnerability Assessment Configuration Guide*
- *ExtremeSecurity WinCollect User Guide*

1 Get started with Extreme Networks Security Risk Manager

Risk Manager is accessed from the **Risks** tab on the Extreme Networks SIEM Console.

Risk Manager enhances Extreme SIEM by providing administrators with tools to complete the following tasks:

- Centralize risk management.
- Use a topology to view your network.
- Configure and monitor network devices.
- View connections between network devices.
- Search firewall rules.
- View existing rules and the event count for triggered rules.
- Search for devices and paths for your network devices.
- Monitor and audit your network to ensure compliance.
- Define, schedule, and run exploit simulations on your network.
- Search for vulnerabilities.

Centralized risk management and compliance for increased intelligence of information might involve the cooperation of many internal teams. As a next generation SIEM with an additional Risk Management appliance, we reduce the number of steps that are required from first-generation SIEM products. We provide network topology and risk assessment for assets that are managed in Extreme SIEM.

During the evaluation process, you consolidate your system, security, risk analysis, and network information through aggregation and correlation, providing complete visibility into your network environment. You also define a portal to your environment, which provides visibility and efficiency that you cannot achieve by using manual processes and other point product technologies.

2 Deploy Extreme Networks Security Risk Manager

Before you install

Configure port access on firewalls

Identify network settings

Unsupported features in Extreme Networks Security Risk Manager

Supported web browsers

Access the Extreme Networks Security Risk Manager user interface

Setting up a Extreme Networks Security Risk Manager appliance

Adding Extreme Networks Security Risk Manager to Extreme Networks SIEM Console

Establishing communication

Adding the Risk Manager user role

You must install the Risk Manager evaluation appliance. The software requires activation and you must assign an IP address to the Risk Manager appliance.

The appliance is ready to accept information from your network devices.

For information about using Risk Manager, see the [ExtremeSecurity Risk Manager User Guide](#).

To deploy Risk Manager in your environment, you must:

- 1 Ensure that the latest version of Extreme SIEM is installed.
- 2 Ensure all pre-installation requirements are met.
- 3 Set-up and power on your Risk Manager appliance.
- 4 Install the Risk Manager plug-in on your Extreme Networks SIEM Console.
- 5 Establish communication between Extreme SIEM and the Risk Manager appliance.
- 6 Define user roles for your Risk Manager users.

Before you install

Before you install the Risk Manager evaluation appliance, ensure that you have:

- space for a two-unit appliance
- rack rails and shelving that are mounted

Optionally, you might want a USB keyboard and standard VGA monitor to access the Extreme Networks SIEM Console.

Configure port access on firewalls

Ensure that any firewall located between the Extreme Networks SIEM Console and Risk Manager allows traffic on the following ports:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time)

Identify network settings

Gather the following information for your network settings:

- Host name
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server (optional) address
- Public IP address for networks that use Network Address Translation (NAT) email server name
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

Unsupported features in Extreme Networks Security Risk Manager

The following features are not supported in Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP)
- IPv6
- Non-contiguous network masks
- Load-balanced routes

Supported web browsers

When you access the ExtremeSecurity system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 3: Supported web browsers for ExtremeSecurity products

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
64-bit Microsoft™ Internet Explorer with Microsoft™ Edge mode enabled.	11.0
Google Chrome	Version 46

Enabling document mode and browser mode in Internet Explorer

- 1 In your Internet Explorer web browser, press F12 to open the **Developer Tools** window.
- 2 Click **Browser Mode** and select the version of your web browser.
- 3 Click **Document Mode**, and select the **Internet Explorer standards** for your Internet Explorer release.

Access the Extreme Networks Security Risk Manager user interface

You access Risk Manager through the Extreme Networks SIEM Console. Use the information in the following table when you log in to your Extreme Security Console.

Table 4: Default login information for Risk Manager

Login information	Default
URL	<code>https://<IP address></code> , where <i><IP address></i> is the IP address of the Extreme Security Console.
User name	admin
Password	The password that is assigned to Risk Manager during the installation process.
License key	A default license key provides access to the system for 5 weeks.

Setting up a Extreme Networks Security Risk Manager appliance

Read, understand, and obtain the prerequisites.

The Risk Manager evaluation appliance is a two-unit rack mount server. Rack rails and shelving are not provided with evaluation equipment.

The Risk Manager appliance includes four network interfaces. For this evaluation, use the network interface that is labeled ETH0 as the management interface. The other interfaces are monitoring interfaces. All of the interfaces are on the back panel of the Risk Manager appliance.

The power button is on the front panel.

- 1 Connect the management network interface to the port labeled ETH0.
- 2 Ensure that the dedicated power connections are plugged into the rear of the appliance.
- 3 Optional. To access the Extreme Networks SIEM Console, connect the USB keyboard and a standard VGA monitor.
- 4 If there is a front pane on the appliance, remove the pane by pushing in the tabs on either side and pull the pane away from the appliance.
- 5 Press the power button on the front to turn on the appliance.

The appliance begins the boot process.

Adding Extreme Networks Security Risk Manager to Extreme Networks SIEM Console

If you want to enable compression, then the minimum version for each managed host must be Extreme Security Console V7.1 or Risk Manager V7.1.

To add a managed host that is not NATed to your deployment where the Console is NATed, you must change the Extreme Security Console to a NATed host. You must change the console before you add the managed host to your deployment. For more information, see the [Extreme SIEM Administration Guide](#).

- 1 Open your web browser.
- 2 Type the URL, `https://<IP Address>`, where `<IP Address>` is the IP address of the Extreme Security Console.
- 3 Type your user name and password.
- 4 Click the **Admin** tab.
- 5 In the **System Configuration** pane, click **System and License Management**.
- 6 In the **System and License Management** window, click **Deployment Actions**, and then select **Add Host**.
- 7 Click **Next**.
- 8 Enter values for the following parameters:

Option	Description
Host IP	The IP address of Risk Manager.
Host Password	The root password for the host.
Confirm Host Password	Confirmation for your password.
Encrypt Host Connections	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running Extreme Security Console V7.1 or Risk Manager V7.1.
Encryption Compression	Enables data compression between 2 managed hosts.
Network Address Translation	To enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the Extreme SIEM Administration Guide .

- 9 If you select the **Network Address Translation** check box, then you must enter values for the NAT parameters:

Option	Description
NAT Group	The network that you want this managed host to use. If the managed host is on the same subnet as the Extreme Security Console, select the console of the NATed network. If the managed host is not on the same subnet as the Extreme Security Console, select the managed host of the NATed network.
Public IP	The public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks that use NAT.

- 10 Click **Add**.
This process can take several minutes to complete. If your deployment includes changes, then you must deploy all changes.

- From the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Clear your web browser cache and then log in to Extreme Security Console. The **Risks** tab is now available.

Establishing communication

The process to establish communications might take several minutes to complete. If you change the IP address of your Risk Manager appliance or need to connect Risk Manager to another QRadar® SIEM console, you can use the **Risk Manager Settings** on the Extreme SIEM **Admin** tab.

- Open your web browser, and then clear the web browser cache.
- Log in to Extreme SIEM. For information about the IP address, user name or root password, see [Accessing the IBM® Security QRadar® Risk Manager user interface](#).
- Click the **Risks** tab.
- Type values for the following parameters:

Option	Description
IP/Host	The IP address or host name of the Risk Manager appliance
Root Password	The root password of the Risk Manager appliance.

- Click **Save**.

[Define user roles.](#)

Adding the Risk Manager user role

By default, Extreme SIEM provides a default administrative role, which provides access to everything in Risk Manager. A user that is assigned administrative privileges, including the default administrative role, cannot edit their own account. Another administrative user must make any required changes.

For information about creating and managing user roles, see the [Extreme SIEM Administration Guide](#).

- Click the **Admin** tab.
- On the navigation menu, click **System Configuration**.
- In the **User Management** pane, click **User Roles**.
- In the left pane, select the user role that you want to edit.
- Select the **Risk Manager** check box.
- Click **Save**
- Click **Close**.
- On the **Admin** tab, click **Deploy Changes**.

3 Manage audits

Use case: Device configuration audit

Use case: View network paths in the topology

Compliance auditing is a necessary and complex task for security administrators. Risk Manager helps you answer the following questions:

- How are my network devices configured?
- How are my network resources communicating?
- Where is my network vulnerable?

Use case: Device configuration audit

Configuration backups provide a centralized and automatic method of recording device changes for your audit compliance. Configuration backups archive configuration changes and provide a historical reference; you can capture a historical record or compare a configuration against another network device.

Configuration auditing in Risk Manager provides you with the following options:

- A historical record of your network device configurations.
- A normalized view, which displays device changes when you compare configurations.
- A tool to search for rules on your device.

The configuration information for your devices is collected from device backups in Configuration Source Management. Each time Risk Manager backs up your device list, it archives a copy of your device configuration to provide a historical reference. The more often you schedule Configuration Source Management, the more configuration records you have for comparison and for historical reference.

Viewing device configuration history

You can view history information for network devices that were backed up. This information is accessible from the **History** pane on the **Configuration Monitor** page. The history pane provides information about a network device configuration and the date that the device configuration was last backed up using Configuration Source Management.

The configuration displays the type of files that are stored for your network device in Extreme Networks Security Risk Manager. The common configuration types are:

- **Standard-Element-Document** (SED), which are XML data files that contain information about your network device. Individual SED files are viewed in their raw XML format. If an SED is compared to another SED file, then the view is normalized to display the rule differences.

- **Config**, which are configuration files that are provided by certain network devices. These files depend on the device manufacturer. A configuration file can be viewed by double-clicking the configuration file.



Note

Depending on your device, several other configuration files might be displayed. Double-clicking these files displays the contents in plain text. The plain text view supports the find (Ctrl+f), paste (Ctrl+v), and copy (Ctrl+C) functions from the web browser window.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Configuration Monitor**.
- 3 Double-click a configuration to view the detailed device information.
- 4 Click **History**.
- 5 On the **History** pane, select a configuration.
- 6 Click **View Selected**.

Comparing device configurations for a single device

If the files that you compare are Standard-Element-Documents (SEDs), then you can view the rule differences between the configuration files.

When you compare normalized configurations, the color of the text indicates the following rules:

- Green dotted outline indicates a rule or configuration that was added to the device.
- Red dashed outline indicates a rule or configuration that was deleted from the device.
- Yellow solid outline indicates a rule or configuration that was modified on the device.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Configuration Monitor**.
- 3 Double-click any device to view the detailed configuration information.
- 4 Click **History** to view the history for this device.
- 5 Select a primary configuration.
- 6 Press the Ctrl key and select a second configuration for comparison.
- 7 On the **History** pane, click **Compare Selected**.
- 8 Optional. To view the raw configuration differences, click **View Raw Comparison**.

If the comparison is for a configuration file or another backup type, then the raw comparison is displayed.

Comparing device configurations for different devices

When you compare normalized configurations, the color of the text indicates the following rules:

- Green dotted outline indicates a rule or configuration that was added to the device.
- Red dashed outline indicates a rule or configuration that was deleted from the device.
- Yellow solid outline indicates a rule or configuration that was modified on the device.

- 1 Click the **Risks** tab.

- 2 On the navigation menu, click **Configuration Monitor**.
- 3 Double-click any device to view the detailed configuration information.
- 4 Click **History** to view the history for this device.
- 5 Select a primary configuration.
- 6 Click **Mark for Comparison**.
- 7 From the navigation menu, select **All Devices** to return to the device list.
- 8 Double-click the device to compare and click **History**.
- 9 Select another configuration backup to compare with the marked configuration.
- 10 Click **Compare with Marked**.
- 11 Optional. To view the raw configuration differences, click **View Raw Comparison**.
If the comparison is for a configuration file or another backup type, then the raw comparison is displayed.

Use case: View network paths in the topology

A topology path search can determine how your network devices are communicating and the network path that they use to communicate. Path searching allows Risk Manager to visibly display the path between a source and destination, along with the ports, protocols, and rules.

You can view how devices communicate, which is important on secured or restricted access assets.

Key features include:

- Ability to view communications between devices on your network.
- Use filters to search the topology for network devices.
- Quick access to view device rules and configuration.
- Ability to view events that are generated from a path search.

Searching the topology

A path search is used to filter the topology model. A path search includes all network subnets that contain the source IP addresses or CIDR ranges and subnets that contain destination IP addresses or CIDR ranges that are also allowed to communicate by using the configured protocol and port. The search examines your existing topology model and includes the devices that are involved in the communication path between the source and destination and detailed connection information.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Topology**.
- 3 From the **Search** list box, select **New Search**.
- 4 In the **Search Criteria** pane, select **Path**.
- 5 In the **Source IP/CIDR** field, type the IP address or CIDR range on which you want to filter the topology model. Separate multiple entries by using a comma.
- 6 In the **Destination IP/CIDR** field, type the destination IP address or CIDR range on which you want to filter the topology model. Separate multiple entries by using a comma.
- 7 From the **Protocol** list, select the protocol that you want to use to filter the topology model.
- 8 In the **Destination Port** field, type the destination port on which you want to filter the topology model. Separate multiple ports by using a comma.

- 9 Optional: Select a protocol from the **Protocol** menu.
- 10 Optional: Type a destination port.
- 11 Optional: Click **Select Applications**.
 - a From the **Device Adapter** menu, select the device adapter type.
 - b Type a partial or full search term or leave the **Application Name** field empty, and then click **Search**.
 - c Select any of the displayed applications in the **Search Results** field, and click **Add** to add your selections to the **Selected Items** box.
 - d Click **OK**.
- 12 Optional: Click **Select Vulnerabilities**.
 - a From the **Search By** menu, select the vulnerability category.
 - b In the **Field** beside the **Search By** menu, enter the ID number of the vulnerability.
 - c Click **Search**.
 - d Select any of the displayed vulnerabilities in the **Search Results** field, and then click **Add** to add your selections to the **Selected Items** box.
 - e Click **Save**.

If your topology includes an Intrusion Prevention System (IPS), the vulnerabilities search option is displayed. For more information, see the [ExtremeSecurity Risk Manager User Guide](#).
- 13 Optional: Click **Select Users/Groups**.
 - a Type a partial or full search term or leave the **User/Group Name** field empty, and then click **Search**.
 - b Select the user or group name in the **Search Results** field, and then click **Add** to add your selections to the **Selected Items** box.
 - c Click **OK**, and then click **Search**.
- 14 Click **Search** to view the results.

4 Use case: Monitor policies

Use case: Assess assets that have suspicious configurations

Use case: Assess assets with suspicious communication

Use case: Monitor policies for violations

Risk priority by vulnerability

The criteria for policy monitoring can include monitoring of assets and communications for the following scenarios:

- Does my network contain assets with risky configurations for PCI Section 1 audits?
- Do my assets allow communications using risky protocols for PCI Section 10 audits?
- How do I know when a policy change puts my network in violation?
- How do I view vulnerabilities for hardened or high risk assets?

Use Policy Monitor to define tests that are based on the risk indicators, and then restrict the test results to filter the query for specific results, violations, protocols, or vulnerabilities.

Extreme Networks Security Risk Manager includes several Policy Monitor questions that are grouped by PCI category. For example, PCI 1, PCI 6, and PCI 10 questions. Questions can be created for assets or devices and rules to expose network security risk. After a question about an asset or a device/rule is submitted to Policy Monitor, the returned results specify the level of risk. You can approve results that are returned from assets or define how you want the system to respond to unapproved results.

Policy Monitor provides the following key features:

- Predefined Policy Monitor questions to assist with workflow.
- Determines if users used forbidden protocols to communicate.
- Assessing if users on specific networks can communicate to forbidden networks or assets.
- Assessing if firewall rules meet corporate policy.
- Continuous monitoring of policies that generate offenses or alerts to administrators.
- Prioritizing vulnerabilities by assessing which systems can be compromised as a result of device configuration.
- Help identifying compliance issues.

Use case: Assess assets that have suspicious configurations

PCI compliance dictates that you identify devices that contain cardholder data, then diagram, verify communications, and monitor firewall configurations to protect assets that contain sensitive data. Policy Monitor provides methods for quickly meeting these requirements and allows administrators to adhere to corporate policies. Common methods of reducing risk include identifying and monitoring assets that communicate with unsecured protocols. These are protocols such as routers, firewalls, or switches that

allow FTP or telnet connections. Use Policy Monitor to identify assets in your topology with risky configurations.

PCI section 1 questions might include the following criteria:

- Assets that allow banned protocols.
- Assets that allow risky protocols.
- Assets that allow out-of-policy applications across the network.
- Assets that allow out-of-policy applications to networks that contain protected assets.

Assessing devices that allow risky protocols

Extreme Networks Security Risk Manager evaluates a question and displays the results of any assets, in your topology, that match the test question. Security professionals, administrators, or auditors in your network can approve communications that are not risky to specific assets. They can also create offenses for the behavior.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 From the Group list box, select **PCI 1**.
- 4 Select the test question **Assess any devices (i.e. firewalls) that allow risky protocols (i.e. telnet and FTP traffic - port 21 & 23 respectively) from the internet to the DMZ**.
- 5 Click **Submit Question**.

Use case: Assess assets with suspicious communication

Extreme Networks Security Risk Manager can help to identify PCI section 10 compliance by identifying assets in the topology that allow questionable or risky communications. Risk Manager can examine these assets for actual communications or possible communications. Actual communications display assets that used your question criteria to communicate. Possible communications display assets that can use your question criteria to communicate.

PCI section 10 questions can include the following criteria:

- Assets that allow incoming questions to internal networks.
- Assets that communicate from untrusted locations to trusted locations.
- Assets that communicate from a VPN to trusted locations.
- Assets that allow unencrypted out-of-policy protocols within a trusted location.

Finding assets that allow communication

Extreme Networks Security Risk Manager evaluates the question and displays the results of any internal assets that allow inbound connections from the Internet. Security professionals, administrators, or auditors in your network can approve communications to assets that don't represent risk in your network. As more events are generated, you can create offenses in Extreme SIEM to monitor this type of risky communication.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.

- 3 From the Group list, select **PCI 10**.
- 4 Select the test question **Assess any inbound connections from the internet to anywhere on the internal network**.
- 5 Click **Submit Question**.

Use case: Monitor policies for violations

When you select a question to be monitored, Risk Manager analyzes the question against your topology every hour to determine if an asset or rule change generates an unapproved result. If Risk Manager detects an unapproved result, an offense can be generated to alert you about a deviation in your defined policy. In monitor mode, Risk Manager can simultaneously monitor the results of 10 questions.

Question monitoring provides the following key features:

- Monitor for rule or asset changes hourly for unapproved results.
- Use your high and low-level event categories to categorize unapproved results.
- Generating offenses, emails, syslog messages, or dashboard notifications on unapproved results.
- Use event viewing, correlation, event reporting, custom rules, and dashboards in Extreme SIEM.

Configuring a question

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 Select the question that you want to monitor.
- 4 Click **Monitor**.
- 5 Configure any of the options that you require to monitor your question.
- 6 Click **Save Monitor**.

Monitoring is enabled for the question and events or offenses are generated based on your monitoring criteria.

Risk priority by vulnerability

Extreme Networks Security Risk Manager uses asset information and vulnerability information in policy monitor. This information is used to determine whether your assets are susceptible to input type attacks, such as; SQL injection, hidden fields, and *clickjacking*.

Vulnerability asset questions can include the following criteria:

- Assets with new vulnerabilities reported after a specific date.
- Assets with specific vulnerabilities or CVSS score.
- Assets with a specific classification of vulnerability, such as input manipulation or denial of service.

Finding assets with specific vulnerabilities

Security professionals, administrators, or auditors can identify assets in your network that contain known SQL injection vulnerabilities. They can promptly patch any assets that are connected to a

protected network. As more events are generated, you can create events or offenses in Extreme SIEM to monitor assets that contain SQL injection vulnerabilities.

- 1 Click the **Risks** tab.
- 2 On the navigation menu, click **Policy Monitor**.
- 3 From the **Group** list, select **Vulnerability**.
- 4 Select the test question **Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network)**.
- 5 Click **Submit Question**.

5 Use cases for simulations

Use case: Simulate attacks on network assets

Use case: Simulate the risk of network configuration changes

Use case: Simulate attacks on network assets

You can use attack simulations to audit device configurations in your network.

Simulations provide the following key features:

- Simulations display the theoretical path permutations an attack can take against your network.
- Simulations display how attacks can propagate through your network devices to spread to other assets.
- Simulations allow monitoring to detect new exposure sites.

Creating a simulation

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 From the **Actions** list, select **New**.
- 4 Type a name for the simulation.
- 5 Select **Current Topology**.
- 6 Select the **Use Connection Data** check box.
- 7 From the **Where do you want the simulation to begin** list, select an origin for the simulation.
- 8 Add the simulation attack, **Attack targets one of the following open ports using protocols**.
- 9 For this simulation, click **open ports**, and then add port 22.
- 10 Click **protocols**, and then select **TCP**.
SSH uses TCP.
- 11 Click **OK**.
- 12 Click **Save Simulation**.
- 13 From the **Actions** list, select **Run Simulation**.

The results column contains a list with the date the simulation was run and a link to view the results.

- 14 Click **View Results**.

A list of assets containing SSH vulnerabilities is displayed in the results, allowing network administrators to approve SSH connections that are allowed or expected in your network. The communications that are not approved can be monitored for events or offenses.

The results that are displayed provide your network administrators or security professionals with a visual representation of the attack path and the connections that the attack could take in your network. For example, the first step provides a list of the directly connected assets affected by the simulation.

The second step lists assets in your network that can communicate to first level assets in your simulation.

The information provided in the attack allows you to strengthen and test your network against thousands of possible attack scenarios.

Use case: Simulate the risk of network configuration changes

You can use a topology model to determine the effect of configuration changes on your network using a simulation.

Topology models provide the following key functionality:

- Create virtual topologies for testing network changes.
- Simulate attacks against virtual networks.
- Lower risk and exposure to protected assets through testing.
- Virtual network segments allow you to confine and test sensitive portions of your network or assets.

To simulate a network configuration change:

- 1 Create a topology model.
- 2 Simulate an attack against the topology model.

Creating a topology model

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulations > Topology Models**.
- 3 From the **Actions** list, select **New**.
- 4 Type a name for the model.
- 5 Select any modifications you want to apply to the topology.
- 6 Configure the tests added to the **Configure model as follows** pane.
- 7 Click **Save Model**.

Create a simulation for your new topology model.

Simulating an attack

- 1 Click the **Risks** tab.
- 2 On the navigation menu, select **Simulation > Simulations**.
- 3 From the **Actions** list box, select **New**.
- 4 Type a name for the simulation.
- 5 Select a topology model that you created.
- 6 From the **Where do you want the simulation to begin** list, select an origin for the simulation.
- 7 Add the simulation attack, **Attack targets one of the following open ports using protocols**.
- 8 For this simulation, click **open ports**, and then add port 22.
- 9 Click **protocols**, and then select TCP.
SSH uses TCP.

10 Click **OK**.

11 Click **Save Simulation**.

12 From the **Actions** list, select **Run Simulation**.

The results column contains a list box with the date the simulation was run and a link to view the results.

13 Click **View Results**.