

IBM Security



IBM Security SiteProtector System User Guide for Security Analysts

Version 2.9

Note

Before using this information and the product it supports, read the information in “Notices” on page 83.

This edition applies to version 2.9 of the IBM Security SiteProtector System and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 1994, 2011.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

About this publication

This guide provides background information, procedures, and recommendations for using the IBM Security SiteProtector System to assess vulnerabilities and monitor and analyze suspicious activity on your network. This guide provides guidelines for analyzing event data from a variety of IBM® Security agents, including Network Intrusion Prevention System (IPS) appliances, Network Multi-Function Security appliances, IBM Security Server Protection, and IBM Internet Scanner. This guide does not provide guidelines for analyzing data from Proventia Network Enterprise Scanner or from third-party products.

Intended audience

The intended audience for the *IBM Security SiteProtector System User Guide for Security Analysts* is security analysts, network administrators, and risk assessment analysts who are responsible for monitoring and assessing threats and vulnerabilities in enterprise environments. This guide assumes you have intermediate knowledge of network security and networking technologies, and basic knowledge of SiteProtector system operations.

Information covered in this guide

- SecurityFusion™ Module
This guide provides procedures and guidelines for analyzing SecurityFusion Module events. Where appropriate, this guide provides guidelines for using the SecurityFusion Module to identify suspicious activity.
- Incidents, exceptions and tickets
The guide provides procedures and guidelines for creating incidents, exceptions, and tickets. Incidents and exceptions let you track and prioritize important events. Ticketing is a more powerful tracking system that lets you track and prioritize events and assign responsibility to the appropriate parties.
- Reporting module
This guide assumes that you have configured the SiteProtector system Reporting module. The Reporting module provides reports that are designed for a wide range of activities, including management, analyst, and audit activities.
- Agent policy settings
This guide assumes that you have effectively tuned agents to monitor or assess your network and to respond threats.

Related documentation

Use the following SiteProtector documents to install, configure, and start using SiteProtector.

Document	Contents
<i>IBM Security SiteProtector System Installation Guide</i>	Contains information that you need to install the SiteProtector system, including procedures for securing communication between components.
<i>IBM Security SiteProtector System Configuration Guide</i>	Contains information that you need to configure, update, and maintain the SiteProtector system.
<i>IBM Security SiteProtector System Policies and Responses Configuration Guide</i>	Contains information for a Security Manager to configure, update, and maintain policies and responses for a SiteProtector System

Document	Contents
<i>IBM Security SiteProtector System Configuring Firewalls for SiteProtector Traffic</i>	Contains information for a Security Manager to configure firewalls so that network devices and SiteProtector System components can communicate with each other.
<i>IBM Security SiteProtector Information Center (Help)</i>	Contains many of the procedures that you need to use the SiteProtector system.

The SiteProtector system guides are available as portable document format (PDF) files in one or more of the following places:

- The IBM Security product Information Center
- The Deployment Manager

Note: Documents must be manually downloaded to the Deployment Manager.

The installation and user guides for related products are available in one or more of the following places:

- the SiteProtector system box
- the IBM Security product DVD
- The IBM Security product Information Center

Contents

About this publication iii

Chapter 1. Introduction to the SiteProtector system 1

What is the SiteProtector system?	1
SiteProtector system architecture.	2
SiteProtector system components and features	3
SiteProtector system Web Console	4
Logging on to the Web Console	5
Troubleshooting Filters Applied	5
Add-on components	6

Chapter 2. Monitoring Your Network . . . 7

Section A: SiteProtector System Analysis Components	7
Section B: Analyzing Events	7
Selecting an Analysis view.	7
Selecting an Analysis perspective	8
Configuring columns	8
Filtering events	9
Using event detail filters	10
Sorting events	10
Grouping events.	11
Clearing events	11
Restoring cleared events	11
Viewing security information	11
Creating a custom Analysis view	12
Selecting guided questions	12
Managing views.	12
Exporting a view	13
Working with event details	13
Navigating analysis history	14
Managing view permissions	14
Section C: Monitoring system health	14
Health Summary	14
Health summary icons.	15
Notifications	15
Section D: Viewing Anomaly Detection Content	16
Accessing ADS content	16
Viewing ADS entity information	17
Section E: SecurityFusion Module Impact Analysis	18
Section F: Locating Assets and Agents	18
Finding groups for an agent or asset	18
Finding assets in a group.	19

Chapter 3. Reporting. 21

Creating reports	21
Selecting a template	21
Creating a new report	21
Scheduling a report.	22
Creating templates	24
Exporting a template	24
Importing a template	24
Deleting reports, templates, and schedules	24
Deleting a report	25
Deleting a schedule.	25

Deleting a template.	25
Finding reports	25
Sending reports in email	26
Setting a report sample image	26
Managing template permissions	27
Communicating data from the Analysis view	27
Exporting data	27
Scheduling exports of data	28
Creating reports in the Analysis view.	28
Scheduling reports in the Analysis view	29

Chapter 4. Identifying and resolving network vulnerabilities 31

Developing vulnerability assessment plans	31
Vulnerability data generated by the SiteProtector system	31
Gathering information about vulnerability events.	32
Deciding whether to resolve vulnerabilities.	33
Repairing and mitigating vulnerabilities.	33
Creating a plan of action	34
Implementing upgrades and patches	35

Chapter 5. Managing Scans. 37

Identifying hosts on your network.	37
Ensuring that vulnerability data is complete and accurate	38
Scheduling vulnerability scans	38
Running background scans	39
Reducing the time required to run scans.	40

Chapter 6. Detecting Suspicious Activity 41

Section A: Suspicious Activity	41
Section B: Monitoring Event Analysis Views	42
Choosing the traffic to monitor and correlate	42
Summary view	43
Event Name view	45
Target view	46
Attacker view	47
Scenarios for using guided questions and Event Analysis views	48
Section C: Filtering Activity from Analysis Views.	49
Creating baselines	49
Creating incidents and exceptions	51

Chapter 7. Is Suspicious Activity Significant? 55

Identifying the location of an attack	56
Analyzing the Event Analysis - Agent view.	56
Identifying activity caused by vulnerability scans.	56
Filtering authorized scans using attack patterns	57
Creating exceptions to filter scan activity	58
Creating exceptions for filtering scans from the Console.	58

Identifying activity caused by misconfigured systems.	58
Identifying normal activity commonly identified as suspicious.	59

Chapter 8. Is an Attack a Threat? 61

Section A: Using the SecurityFusion Module to Assess an Attack	61
Viewing attack statuses	61
Section B: Assessing an Attack Manually	65
Determining the X-Force risk level of an attack	66
Was the attack target vulnerable?	66
Was the target service or operating system susceptible?	68

Chapter 9. Tracking and Prioritizing Confirmed Attacks. 73

Guidelines for establishing ticket priority	73
Creating tickets	74

Creating tickets	75
Viewing tickets	75
Viewing and editing tickets	76

Chapter 10. Determining the Scope of Attack 79

Attack scope	79
Goals of typical attackers.	79
Viewing the number of assets targeted by an attacker.	80
Viewing the number of platforms targeted by an attacker.	81

Notices 83

Trademarks	84
----------------------	----

Index 85

Chapter 1. Introduction to the SiteProtector system

This chapter introduces SiteProtector system components and the agents that work with the SiteProtector system.

Terms to know

The following table describes the terms used for security products in this document:

Term	Description
agent	The generic term for all sensors, scanners, and Desktop Endpoint Security agents.
appliance	An inline security device on a network or gateway. Depending on the type of appliance, it can provide any combination of intrusion detection and prevention, antivirus, antispam, virtual private networking (VPN), Web filtering, and firewall functions.
scanner	An agent that scans assets for vulnerabilities and other security risks.
sensor	An agent that monitors network traffic on the network and on servers to identify and, in some cases, stop attacks.

What is the SiteProtector system?

A SiteProtector system is a centralized management system that unifies management and analysis for network, server, and Desktop Endpoint Security agents and appliances. You can easily scale the SiteProtector system to provide security for large, enterprise-wide deployments.

Reference: Refer to the "Supported agents and appliances" appendix in the *IBM Security SiteProtector System Installation Guide* for information about the agents and appliances that can be configured to communicate with and be managed by the SiteProtector system.

Components and agents

The components and agents in a SiteProtector system fall into these categories:

- The SiteProtector system consists of required and optional components that provide the base functionality necessary to accept, monitor, and analyze network events. Depending on your Site requirements, you may need to install more than one of some components.
- You can purchase add-on components for the SiteProtector system that provide additional functions.
- You can purchase agents that complete your security system, including vulnerability scanners, intrusion detection and prevention appliances and sensors, and integrated security appliances.

SiteProtector system components by type

The following table provides lists of the required and optional SiteProtector system components, add-on components, and the agents that the SiteProtector system manages:

SiteProtector System Components	Add-on Components	Agents That The SiteProtector System Manages
Agent Manager Console Site Database Deployment Manager Event Archiver Event Collector Event Viewer SP Core (includes the application server and sensor controller) SiteProtector Reporting SiteProtector system SecurityFusion Module X-Press Update Server Web Console	SiteProtector system SecureSync Integrated Failover System	sensors scanners appliances Desktop Endpoint Security agents

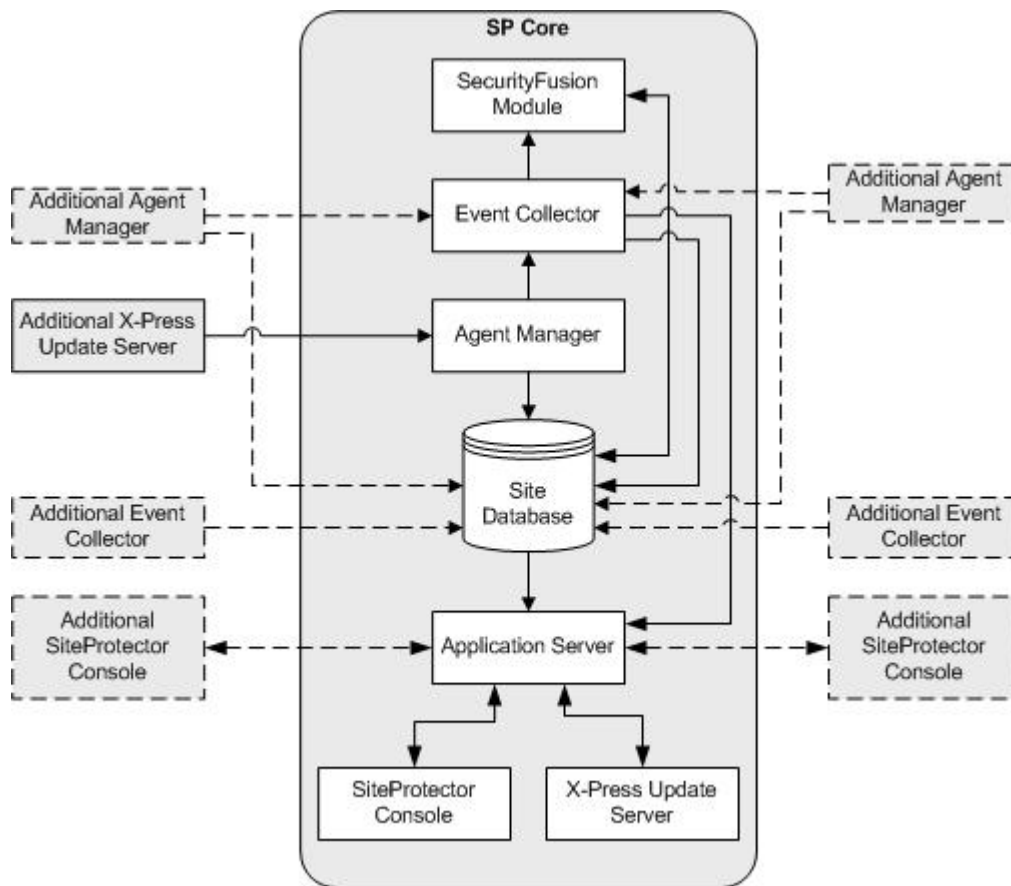
SiteProtector system architecture

The SiteProtector system has established communication channels that are set up when you install the product.

Depending on your Site requirements, you may need to install more than one of some components. The most typical SiteProtector system installations use one, two, or three computers. When you use more than one computer, the Recommended option (from the Deployment Manager) installs the components on the correct computers automatically.

Illustration of components

The following figure illustrates the components in a standard instance of the SiteProtector system that uses three computers:



SiteProtector system components and features

The IBM Security SiteProtector System consists of required and optional components that provide the base functionality necessary to accept, monitor, and analyze network events.

Component descriptions

The following table describes the purpose of the SiteProtector System core components:

SiteProtector System Component	Description
Agent Manager	The Agent Manager manages the command and control activities of the Desktop Protection agents, IBM Security Server Protection, and Proventia Network MFS, X-Press Update Server, and Event Archiver; and it also facilitates data transfer from agents to the Event Collector.
Console	The SiteProtector Console is the main interface to SiteProtector where you can perform most SiteProtector functions, such as monitoring events, scheduling scans, generating reports, and configuring agents.
Deployment Manager	The Deployment Manager is a Web server that lets you install any of the SiteProtector components and agents on computers on your network.
Event Archiver	The Event Archiver provides the capability to archive security events to a remote location, thereby reducing the number of events that the database must store.

SiteProtector System Component	Description
Event Collector	The Event Collector manages real-time events from sensors and agents as well as vulnerability data from scanners.
Event Viewer	The SiteProtector Event Viewer receives unprocessed events from the Event Collector to provide near real-time access to security data for troubleshooting.
Reporting module	The Reporting module generates graphical summary and compliance reports that provides the information that you need to assess the state of your security. Reports cover vulnerability assessment, attack activities, auditing, content filtering, Desktop Protection security, SecurityFusion and virus activity.
SecurityFusion module	<p>The SiteProtector SecurityFusion module greatly increases your ability to quickly identify and respond to critical threats at your Site. Using advanced correlation and analysis techniques, the module identifies both high impact events and patterns of events that may indicate attacks.</p> <p>Impact analysis — The module correlates intrusion detection events with vulnerability assessment and operating system data and immediately estimates the impact of events.</p>
Site database	The SiteProtector database stores raw agent data, occurrence metrics (statistics for security events triggered by agents), group information, command and control data, and the status of X-Press Updates (XPU's).
SP Core	<p>The SP core includes the following components:</p> <ul style="list-style-type: none"> • The application server enables communication between the SiteProtector System Console and the SiteProtector database. • The Sensor Controller manages the command and control activities of agents, such as the command to start or stop collecting events.
X-Press Update Server	A Web server that downloads requested X-Press Updates (XPU's) from the IBM Security Download center and makes them available to the agents and components on the network. The Update Server eliminates the need to download updates for similar products more than once and allows users to manage the update process more efficiently.
Web Console	The SiteProtector System Web Console is an interface that provides easy access to some of the features in the SiteProtector System for monitoring SiteProtector System assets and security events.

SiteProtector system Web Console

The SiteProtector system Web Console is a Web-based version of the Console. You can perform the following tasks through the Web Console:

- analyze event data
- apply filters to event data

- copy data to another application, such as a spreadsheet

You log on to the SiteProtector system Web Console using the same account information as you would using the Console. When you log on, the Site appears in the left pane in your browser, and the Site's Summary page appears in the right pane.

Web Console requirements

You must open the Web Console on a computer that has the Sun Java Runtime Environment (JRE).

If you open the Web Console on a computer that does not have the JRE installed, it directs the browser to install the JRE. You do not have to close the Web Console for the installation to complete successfully.

Reference: Refer to the "Hardware and software requirements" chapter in the *IBM Security SiteProtector System Installation Guide* for specific information about Web Console requirements.

Logging on to the Web Console

Log on to the SiteProtector Web Console for a high-level overview of your Site and the event activity on your Site.

Before you begin

- Obtain access rights to all groups you plan to monitor.
- Obtain the IP address or DNS name and port number for the application server.

Note: The default port number for the Deployment Manager and Application server is 3994. If the port number has been changed, contact your Site administrator to get the correct port number.

- In the SiteProtector System Console, move assets out of the Ungrouped Assets folder. Ungrouped assets are not displayed in the Web Console.
- Install Sun Java plugin version 1.6.0 or higher if any of the following conditions are true:
 - you use a computer that does not have access to the Internet
 - you use a computer behind a network proxy server

Note: The IBM Security SiteProtector System Web Console is designed to support Internet Explorer 8.0 and later.

Procedure

1. Type the address of the SiteProtector Deployment Manager or Application Server in the Address box of your Web browser using one of the following formats:
 - https://computer name:3994/siteprotector/
 - https://IP address:3994/siteprotector/
 - https://computer name: port number/siteprotector
 - https://IP address: port number/siteprotector
2. Type your Username and Password, and then click Submit.

Tip: You can bookmark the URL of the Web Console and use it the next time you want to log on.

Troubleshooting Filters Applied

When you click **Filters Applied**, if the Advanced Filters window does not load, you may need to manually install the Sun Microsystems Java SE Runtime Environment (JRE). You must manually install the Java plugin when your operating system is Microsoft Windows 2003 and your computer is behind a proxy server.

About this task

When you do not have the Java plug-in installed, the Web Console attempts to install the plug-in automatically. If your computer is behind a proxy server and running Microsoft Windows 2003, automatic installation of the plugin fails. When automatic installation fails, you must either install the plug-in as an off-line package or download the plug-in to another computer, copy it to the computer running the Web Console, and then install it.

Procedure

1. Go to <http://java.sun.com/j2se/index.jsp>
2. Download and install JRE 6 or higher.

Important: During installation, select Windows Offline Installation. Windows Online Installation fails on computers that are running Microsoft Windows 2003 behind a proxy server.

Add-on components

The add-on components for the SiteProtector system provide additional protection and functionality that go beyond the base protection of the SiteProtector system.

SecureSync Module

The Secure Sync Module provides a failover system that lets you transfer Site data between primary and back-up Sites and transfer agent management from one Site to another.

Chapter 2. Monitoring Your Network

The SiteProtector system provides several monitoring, correlation, and search tools that can assist you with event detection and threat investigation. Use the information in this chapter to become familiar with these tools as they are referenced frequently in this guide.

Section A: SiteProtector System Analysis Components

The SiteProtector system provides several components for monitoring events. These components let you filter and sort data at all stages of event detection and investigation.

SiteProtector system analysis components

The following table describes the SiteProtector system event analysis components. Some of these components are discussed in more detail later in this chapter:

Component	Description
Summary View	Provides several predefined panes that display different types of summary information in a portal-like user interface. Each type of information appears as a nested pane of the summary tab, and users can choose which types of information to display. The information displayed on the summary tab is dependent upon the currently selected group in the group tree.
Analysis Perspectives	Provide a different focus of the events that appear in the Analysis views, such as changing whether a selected asset is the target or the source of activity.
Analysis views	Provide event information that is organized in a tabular format. Provide predetermined filters that correspond to guided questions.
Guided questions	Provide a series of questions on the pop-up menu for one or more events that you select from the Analysis view. The questions focus on information you typically need when you investigate an event. By clicking on a question, you automatically change the filters and the analysis view that is displayed.
SiteProtector system toolbar	Provides options that enable you to perform common tasks with the analysis tool, such as refreshing the event data, moving backward or forward through the history, or opening the Filters window.
Analysis filter panel	Displays filters above the analysis view so they are easily accessible. The same filters are available in the Filters editor.
Filters window	Provides a list of filters available on the Site Protector Console. By selecting a filter, you can see the set of attributes with values that you can customize and a description of the filter.

Section B: Analyzing Events

This section provides procedures and background information about using analysis views, analysis modes, and guided questions and customizing these tools for specific tasks.

Selecting an Analysis view

Use analysis views as a starting point for event detection and for creating customized reports. Analysis views have predefined settings for filters and columns.

About this task

Application Monitoring, Appscan, Event Analysis , File Integrity, Virtual Infrastructure, and Vuln Analysis.

Analysis views are divided into the following categories:

- Application monitoring (only enabled with Proventia Desktop Endpoint Security)
- Appscan
- Event Analysis
- File Integrity (for Security Server Protection for Windows only)
- Virtual Infrastructure
- Vuln Analysis

Note: The name of the Analysis view appears above the event data. The name is followed by the Analysis Perspective surrounded by parentheses. The Analysis Perspective might vary because the SiteProtector system chooses the Analysis Perspective based on the Analysis view.

Procedure

1. In the Analysis view, click **View > Load**.
2. In the Load View window, select a view.

Selecting an Analysis perspective

Use Analysis perspectives to change the focus of data that is associated with a selected asset. An Analysis perspective can match the source, target, or agent IP address, or any combination of the three.

Procedure

1. In the Analysis view, select an asset or group of assets from the My Sites pane.
2. Click **Action > Analysis Perspective**, and then select one of the following perspectives:

Select this Analysis Perspective...	To view every instance of an event when the selected asset...
Target	was a target of events.
Agent	has an agent installed that detected events.
Source	was a source of events.
Source and Agent	was both the source of the events and has an agent installed that detected the events.
Target and Agent	was both the target of the events and has an agent installed that detected the events.
Target and Source	was both a target and a source of the events.
Target, Agent, and Source	was a target or source of events, an agent that detected the displayed events, or all three.

Example

You want to see if any agent in a group is the target of an attack. You select the group, and then choose Target as the Analysis Perspective. Each event with a target IP address that matches the IP address of the agent is displayed.

Configuring columns

Configure columns to specify the type of events you see in the Analysis view.

Procedure

1. In the Analysis view, click **View > Add or Remove Columns**.
2. In the Add or Remove Columns window, select or clear the check boxes for the columns you want to add or remove.
3. Select a column or columns and click **Move Up** or **Move Down** to change the order of the columns.

Tip: You can also click and drag columns in the Analysis view to a new position.

4. Click **OK**.

Filtering events

Apply filters to events in the Analysis view to view only the events you are interested in. Filtering events helps you to manage vulnerabilities, to investigate attacks, and to monitor applications.

Procedure

1. Select the group you want to examine in the My Sites pane.
2. Configure the **Time Filter** to specify the time period for which you want to view events.
3. Configure the most common filter types, **Tag Name**, **Source IP**, and **Target IP**, by typing a valid string or IP address. You can use IPv4 or IPv6 addresses.
 - Use a hyphen (-) or CIDR notation to specify an IP range.
 - Use the operator **Not** to exclude events with a specified value.
 - Use wildcard characters to find events with the value inside the tag name.

Note: Wildcard characters are * and %.

- For multiple entries insert a space between each entry.
- For multiple-word tag name entries use quotation marks.

Note: IPv6 address ranges must be specified by CIDR notation.

4. Click **Apply**.

Note: To configure the Console to refresh data automatically, click **Tools > Options** and then select Auto Refresh in the Options window.

Example

Use the following examples as guides for configuring the most common filter types: Tag Name, Source IP, or Target IP.

- *IRC*
- NOT 127.0.0.1
- 127.0.0.*
- 192.0.2.0 - 192.0.2.24
- 192.0.2.0/8
- 2001:DB8:0:0:0:0:0:0
- 2001:DB8:0:0:0:0:0:0/32
- 2001:DB8::/32

What to do next

Click **Filters** to configure additional filter types in the Edit Filters window.

Using event detail filters

Use event detail filters to filter on event detail columns that are generated for the Analysis view. The event detail columns are based on the contents of events that are logged in the Site database.

Before you begin

Before you can filter events according to event details, you must add the event details to your analysis view. Event details are always shown on the Event Analysis - Details and the Virtual Infrastructure - Details views, but you can add event details to any view by selecting Show Event Details in the Event Category Filter.

About this task

Important: Using event detail filters on a large set of data could result in a long query. For best results, filter the data as much as possible before you apply event detail filters.

Tip: You can right-click an event detail column to filter by a value in that column.

Procedure

1. In the Analysis view, click **Filters**.
2. In the Edit Filters window, click **Add** to add a detail filter.
3. In the Add an Event Detail Filter window, type the name of the event detail column that you would like to filter on, and then click **OK**. The Edit Filter window reappears, with the new event detail filter you added to the Column Filters pane.
4. In the new event detail filter pane, type the value you want to use, and then click **OK**.
 - Use the wildcard characters * to find events with the value inside the tag name.
 - Insert a space between multiple entries.
 - Do not use the operator Not to exclude events.

Example

Use the following examples as guides for filter event details:

- 8000001 6000125
- 8* 6*

Sorting events

Sort events in the Analysis view in ascending or descending order.

About this task

Arrows indicate that a column has been sorted. If the arrow is pointed up, the column is sorted in ascending order. If the arrow is pointed down, the column is sorted in descending order.

Procedure

Perform one of the following actions to sort a column:

- Click a column header to sort.
- Right-click a column header and select either **Sort Ascending** or **Sort Descending**.
- In the Analysis view, click **View > Sort**, and then in the Sort window, configure sorting for up to four columns.

Grouping events

Group events in the Analysis view by column.

About this task

You can group events by multiple columns. Plus signs, followed by the column name, indicate that data has been grouped by that column.

Procedure

Perform one of the following tasks to sort a column:

- Click **View > Group By**, and then select the columns to group by in the Group By Columns window.
- Right-click a column header and select **Group By** to group by that column.

Tip: To remove groupings click **View > Clear Groupings** or right-click a column header and select **Clear Groupings**.

Clearing events

Use the **Clear** option to clear unimportant events from an Analysis tab.

About this task

If you clear unimportant events, it is easier to identify events that are potential threats.

Important: If you clear all events in the view such that the view is empty, you cannot restore the cleared events.

Procedure

1. In an **Analysis** tab, select the events you want to clear.
2. Click **Action > Clear Events**.

Restoring cleared events

Use the Restore Events option to restore previously cleared events.

Procedure

1. On an **Analysis** tab, select the view for which you want to restore events.
2. Click **View > Add or Remove Columns**.
3. In the Add or Remove Columns window, select **Cleared Count** and then click **OK**.
4. Sort the Cleared Count column by descending order to see cleared events first.
5. Select the events you want to restore, and then click **Action > Restore Events**.
6. In the Restore Event(s) window, click **Yes**.

Viewing security information

If you are not interested in the details of an event, use the **View Security Information** option to view only the description of the event from the X-Force.

Procedure

1. Select an event on an **Analysis** tab.
2. Click **Action > View Security Information**. The security information appears in the Vulnerability Info window.

Creating a custom Analysis view

Create a custom Analysis View if none of the predefined views contain the information you want to see.

Procedure

1. On an **Analysis** tab, create the view you want by changing the sort criteria, the grouping, the filter options, and the columns to be displayed.
2. Click **View > Save**.
3. Type a name for the new view in the **View Name** field.

Note: You cannot use the **Description** or **File name** of a predefined view.

4. Click **Save**. The view you created appears at the end of the **Analysis View** list by the name you gave it in the **View Name** field.

Selecting guided questions

Guided questions provide a quick way for you to gather information about an event or group of events. Use guided questions to gather event information for monitoring and detecting events or for performing more focused inquiries.

What are guided questions?

Guided questions are a series of questions that appear on the pop-up menu for one or more selected events. These questions are based on the analysis views, and they try to anticipate information you may need. By clicking on a question, you automatically change the filters and the analysis view that is displayed.

Using guided questions

Use guided questions to select an Analysis View based on questions you have about an event.

About this task

When you choose a guided a question, the SiteProtector System automatically selects the **Analysis View** that corresponds to the question.

Procedure

1. In the left pane, select the group or asset whose information you want to view.
2. Select **Analysis** from the **Go to** list.
3. Right-click an event, and then select a question from the guided questions. The Analysis View list changes to the view the guided question selected.

Managing views



Use the Manage views window to rename, copy, delete, and import views. You can also manage permissions for Analysis views in the Manage Views window.

Procedure

1. In the Analysis view, click **View > Manage**.
2. Select one of the following options:

Option	Description
Rename	Rename a view.
Copy	Copy a view to create a new view with the same settings.
Delete	Permanently delete a view from your Console.

Option	Description
Permissions	Manage permissions for the selected view.
Import	Import a new view.

Note: You must have control permission to rename or delete a view created by a user (). The default views () that come with SiteProtector cannot be renamed or deleted.

Exporting a view

Export a view to work with large amounts of data, to work with data outside of SiteProtector, and to work with data that is not formatted.

Before you begin

You must select at least one event to use Export View.

About this task

Exporting a view is the same as exporting data.

Procedure

1. Click **View > Export View**.
2. In the Export window, type a **File** path, select a **File Type**, and specify what data to export in the **Exported Content** section.

Note: You can only exclude columns that are already in the Analysis view. To include a column in the exported data, go back to the Analysis view and add the column before you export the data.

3. Optional: Select **Include Security Information** to include remediation information for each event.

Working with event details

Use the Event Details window to view, copy, and export the details of specific events. The Event Details window displays basic event details, attribute value pair information, security information, and, if available, raw packet data.

About this task

- By default, multiple occurrences of the same type of event are combined in one row, and the **Event Count** column indicates the number of occurrences.
- The title bar of the Event Details window shows the number of events associated with the selected event and the sequence of the event you are viewing; for example, the first of five events is displayed as 1/5.

Procedure

1. On an Analysis tab, select the row with the event you want to investigate, and then click **Object > Open**.
2. If the row you selected contains multiple events, you can locate a specific event as follows:

If you want to view...	Then...
events in order	click >> to view the details of the next event in the sequence, or click << to view the details of the previous event in the sequence.
a specific event	type the event number in the Event Number field, and then click Go .

3. Optional: Click **Copy** to copy the event details to the clipboard.
4. Optional: Click **Export**, type or browse to the file you want to save the details, and then click **Save**.

Note: The .txt and .xls file extensions are supported.

5. Click **OK** to close the window.

Navigating analysis history



In the Analysis tab, use the **Back** and **Forward** icons to retrace your actions, such as, applying a different **Analysis View** or **Analysis Perspective**, or changing filter settings.

About this task

Data is cached when you navigate through the Analysis view.

Procedure

In an **Analysis** tab, do the following:

- Click the **Back**  icon to trace your actions prior to the current view.
- Click the **Forward**  icon to trace your actions applied after the current view.

Managing view permissions

Use permissions for an Analysis view to define which users or groups can view or control the Analysis view.

Procedure

1. In the Analysis view, click **View > Manage**.
2. In the Manage Views window, select a view, and then click **Permissions**
3. In the Manage Permissions window, select a user or group, and then select permissions for the user or group.

Note: If a user or group is not displayed in the Users and/or Groups box, click **Add** to add the user or group.

4. Optional: Click **Advanced** to change the current owner of the template.

Section C: Monitoring system health

System health options vary for each agent. Some options might not be available for all agents managed by SiteProtector.

Health Summary

Use the Health Summary pane to view agent messages, metrics, and the result of health checks performed on agents managed by SiteProtector.

Health checks are used to monitor the health of agents. Some checks are informational only and do not affect the agent's health status. Some health checks can be configured to enter a warning or failed state.

For health checks configured to enter a warning or failed state, information appears in the following places:

- a notification for that health check appears in the Notifications tab
- the agent's health status appears as warning or unhealthy in the Notifications tab and in the Agent view

Notifications are not created in the Console for Informational health checks.

Agent Messages include :

- *Info Events*: Agent info events that appear as Info, Warning, or Error.

Note: Previously, Info Events appeared in the Analysis view. Info Event do not affect agent health.

- *Application Artifacts*: Application Artifacts affect agent health.






The following options might be available for a health check:

Option	Action
Configure	Click Configure to set warning and fail notifications for a health check.
Ignore Health Status	Click Ignore Health Status to stop the Console from creating a notification in the Notifications tab. Information for the health check is still gathered by the Console and displayed in the Health Summary pane.
Remedy	Click the Remedy link for steps to correct a health check that is in a warning or failed state.

Note: You can configure email alerts and Console notifications in Console Options.

Health summary icons

Health summary icons appear next to the name of each health check and can appear in the health summary pane beside a group name.

Icon	Description
	Health check has failed. Icon also indicates that the agent has failed at least one health check in the group.
	Health check passed. Icon also indicates that the agent has passed all health checks in the group.
	Health check provides information, but does not produce a notification in the Console. Icon also indicates that health checks in the group do not produce notifications in the Console.
	Health check is in a warning state and about to fail.
	Health check is in an unknown state. Try updating SiteProtector agents before using the IBM Support Portal.

Notifications

Use the Notifications view to see notifications for health checks performed on agents managed by SiteProtector.

The Notifications view contains notifications from all Sites connected to your Console. To view details about a notification, click **Action > Open Notification**.

Notifications for a new or recurring event appears bold in the Notifications tab. Notifications are deleted from the Console after two weeks.

Note: Only notifications with severities you have configured to appear in the Console will appear in the Notifications view. Click **Tools > Options > Notifications** to specify the severity of notifications to display in the Console.

When you disconnect from a Site, notifications for that site are removed from your Console.

Current Agent Health refers to the following:

- *Healthy*: Agent has passed all health checks.
- *Unhealthy*: Agent has failed at least one health check.
- *Warning*: Agent is about to fail at least one health check or the agent has important information that requires attention.

Note: Severity is defined by each agent. See each agent's reference for severity levels and definitions.

Note: You can configure E-mail alerts and Console notifications in Console Options.

Viewing notifications

Use the Notifications view to see notifications for health checks that have failed or are about to fail.

Procedure

1. Click the **Notifications**  icon to open the Notifications tab.

Tip: The Notifications icon is animated when you have new notifications.

2. Optional: To view the agent's health summary, select a notification, and then click **Action > Open Notification**.

Note: You can only open one health summary at a time.

3. Optional: To delete the notification, select a notification, and then click **Action > Delete**.

Section D: Viewing Anomaly Detection Content

Anomaly detection content is crucial to detecting patterns of suspicious activity on your network. The SiteProtector system lets you view anomaly detection content in the Traffic Analysis view.

Important: To view ADS content, you must have an ADS appliance configured to communicate with the SiteProtector system.

Multiple ADS analyzer appliances

You can include multiple ADS analyzer appliances on your Site. If you have multiple ADS analyzers, you can set a preferred appliance to search for network behavior for host objects and view traffic analysis in the SiteProtector system. If you do not select one of the appliances as preferred, the first appliance registered will be chosen as the default.

ADS viewing options

You can set options for how to display ADS events in **Tools > Options > Browser**.

Accessing ADS content

You can navigate and access ADS content from the SiteProtector system in several different ways. This topic provides a procedure for accessing ADS content.

Starting the ADS Web Console Procedure

1. In the left pane of the SiteProtector system Console, select a group that contains the ADS appliance, and then select the ADS appliance.
2. Do one of the following:
 - Right-click the agent, and then select **Launch > Proventia Manager**.

- Select **Action**, and then select **Launch > Proventia Manager**.

A browser opens, displaying the ADS appliance Web Console.

Accessing ADS content Procedure

Use the options in the following table to access ADS content:

Option	Description
Action Menu	To navigate to the ADS event details, select one or more rows in the Agent, Analysis, or Asset view, and then select the Network Behavior option on the Action menu. You can also right-click on the agent(s) or asset(s) to view details.
Agent > Launch > Proventia Manager	From the Agent view, you can open a separate browser from the Launch option to view the ADS Web Console.
Event Analysis - Details	From the Analysis view, select Event Analysis–Details to display selected IP addresses for Analysis view, Agent view, and Asset view. Select Action > What are the ADS Event Details for information.
Event Analysis - Event Name	From the Analysis view, select the event, right-click, and then select Open Event Details to display the ADS event details. You can also link to the ADS event details by clicking on the icon next to ADSEvent.url attribute in the Event Attribute Value Pairs table.
Traffic Analysis tab	Select the Traffic Analysis tab to view ADS content for the selected group.

Viewing ADS entity information

Use the Network Behavior command to view ADS entity information in the Console.

Procedure

1. In the left pane of the Console, select a group or asset for which you want to view content.
2. Select the Agents, Event Analysis - Details, or Assets view.
3. Select the agents, assets, or event(s) you want to investigate.
4. Click **Action > Network Behavior**, and then select the ADS information you want to review.

Tip: You must select a single row to view event information. You can select multiple rows to view entity information, but only the first 15 unique items are displayed in the menu.

Using the What are the ADS event details? option

Use the What are the ADS event details? link to view event details from selected IP addresses in the Analysis view.

Procedure

1. Select **Analysis** from the **Go to** list, and then select a group or asset for which you want to view events.
2. Select **Event Analysis-Details**, and then select the event.
3. Click **Action > What are the ADS event details?**.

Viewing traffic analysis

Use the Traffic Analysis tab to view ADS content for a selected group.

About this task

The Traffic Analysis tab displays the ADS traffic content for the selected group. The information displayed for the selected assets is based over the last 24-hour time frame.

Procedure

Select the group for which you want to view Traffic Analysis, and then select **Traffic Analysis** from the **Go to** list.

Section E: SecurityFusion Module Impact Analysis

The SecurityFusion Module greatly increases your ability to identify and respond to critical threats quickly. Using correlation and analysis techniques, the Module escalates high impact attacks and critical attack patterns to help you focus on the most important attack activity.

Note: The SecurityFusion Module is a separately purchased, add-on component.

Impact analysis

Impact analysis is the process of determining whether an attack succeeded. As an intrusion detection sensor detects an attack, the Module correlates the attack with information about the host—such as operating system, vulnerabilities, and responses taken by host agents—to verify the success or failure of the attack. This information is displayed in the Status column of the Analysis view.

Section F: Locating Assets and Agents

If you are monitoring traffic in an enterprise environment, you may need to locate a group, asset, or agent. The SiteProtector system provides a quick way to search for agents and assets using the Find option.

Find option

Depending on where you select the asset or agent, the Find option lets you navigate to a group or perform a keyword search. The Find option is located on the Edit menu.

Topics

“Finding groups for an agent or asset”

“Finding assets in a group” on page 19

Finding groups for an agent or asset

Use the Find Groups window to find the groups and subgroups that a specific agent or asset belongs to.

About this task

In the Agent or Asset view, you can easily find the groups and subgroups that a specific agent or asset belongs to. You can then navigate to one of the groups from the Find Group window. You can also search for assets within a group and find out any other groups the asset belongs to.

Procedure

1. Select the agent or asset.

Tip: You can select multiple agents or assets and find groups for all of them.

2. Click **Edit > Find**.
3. Use the **Expand** and **Collapse** buttons to expand or collapse the group tree.
4. Select a group to navigate to, and then click **OK**.

Finding assets in a group

Use the Find Assets window to search for assets within a group and to find any other groups they belong to.

Procedure

1. Select the group, and then click **Edit > Find**.
2. Type the name of the asset in the Pattern box, and then click **Find**.
3. Use the **Expand** or **Collapse** buttons to expand or collapse the group tree.
4. To navigate to a group, select the group from the results list, and then click **OK**.

Chapter 3. Reporting

This chapter provides guidelines and procedures for creating reports in the SiteProtector system.

Creating reports

Create reports from templates in the Report view to examine trends, to establish consistent reports, or to format data.

Before you begin

You must purchase a separate license to use the SiteProtector Reporting feature.

About this task

Use a template in the Report view to create a report if:

- Data is not available in the Analysis view, such as permissions data
- Formatting is important
- You need to see trends
- You plan to produce the report multiple times
- You want to allow other SiteProtector users to access the report
- You want to establish consistency in reporting
- You want to reuse report settings

Results

Information about a report appears in the following places in SiteProtector:

- Saved templates are listed in the Templates pane.
- Reports that have been run and saved are listed in the My Reports pane.
- Scheduled reports are listed in the Schedules pane.

What to do next

In the report view, perform one of the following tasks:

Selecting a template

Templates have predefined filter and column settings.

Procedure

1. In the Report view, click **Templates**.
2. In the Templates pane, select a report template.

Tip: Select a template to see the template description in the Template Detail pane.

Creating a new report

When you create a new report, the report is generated immediately and displayed in the Report viewer inside the Console.

Procedure

1. In the Report view, select a template, and then click **Action > New Report**.
2. In the New Report window, click the **General** icon, and then type a meaningful **Report Name** and **Description**.
3. Optional: Click the **Parameters** icon, and configure any of the available tabs:

Tab	Configure
Groups	Groups you want to report data for
Content Settings	Filters, columns of data to include, sort settings, and Analysis perspective
Display Options	Maximum number of rows you want to display in your report Note: You can only define the maximum number of rows to display for reports generated from Analysis category templates.

CAUTION:

A scheduled report is performed outside of the Analysis view. Therefore, it is possible to select a set of parameters that requests an excessive amount of data, resulting in a report run-time failure. This is highly dependent on the specific SiteProtector hardware environment as well the event rate from managed agents.

4. Optional: Click the **Chart** icon and select the appropriate formatting choices.

Note: Charts are only available for reports generated from Analysis category templates.

Tab	Tips
Select Chart Type	When you select a dimension for your chart, consider using 2D with depth or 3D for charts in reports you plan to share, such as executive reports, because they are more visually engaging. Consider using 2D for charts when you analyze the data because there is less ambiguity about data values.
Select Series	Select Enable Grouping when you have multiple Y-Axis series: the Y-Axis series is summed according to the X-Axis series. Example: If you are charting event counts and severity, you can enable grouping to see one bar, point, or slice for High Severity, with a total event count for all High Severities. If you do not enable grouping, the chart includes multiple bars, points, or slices for each event with a High Severity and an event count specific to that single high severity event.
Format Options	<ul style="list-style-type: none">• When you have multiple Y-Axis series:<ol style="list-style-type: none">1. Select Color by Y-axis Series to make each bar, point, or slice a different color in the chart.2. Select Show Legend to show what each color represents.• Specify a Maximum number of X-Axis data points to prevent your chart from containing too much data to reasonably view in a chart. A good maximum number of X-Axis data points to display is 20. Important: When you exceed the maximum number of X-axis data points, only part of the data in the report is displayed in the chart. To ensure that all of your data is included in your chart, verify that your chart has fewer than the maximum number of X-axis data points.

5. Click **OK**.

Scheduling a report

Schedule a report to run in the background, to run at a later time, or to run on a recurring schedule.

Procedure

1. In the Report view, select a template, and then click **Action > Schedule Report**
2. In the Schedule Report window, click the **General** icon, and then type a meaningful **Report Name** and **Description** for the report.
3. Optional: Click the **Parameters** icon, and configure any of the available tabs:

Tab	Configure
Groups	Groups you want to report data for
Content Settings	Filters, columns of data to include, sort settings, and Analysis perspective
Display Options	Maximum number of rows you want to display in your report Note: You can only define the maximum number of rows to display for reports generated from Analysis category templates.

CAUTION:

A scheduled report is performed outside of the Analysis view. Therefore, it is possible to select a set of parameters that requests an excessive amount of data, resulting in a report run-time failure. This is highly dependent on the specific SiteProtector hardware environment as well the event rate from managed agents.

4. Optional: Click the **Chart** icon and select the appropriate formatting choices.

Tab	Tips
Select Chart Type	When you select a dimension for your chart, consider using 2D with depth or 3D for charts in reports you plan to share, such as executive reports. Consider using 2D for charts when you analyze the data.
Select Series	Select Enable Grouping when you have multiple Y-Axis series: the Y-Axis series is summed according to the X-Axis series. Example: If you are charting event counts and severity, you can enable grouping to see one bar, point, or slice for High Severity, with a total event count for all High Severities. If you do not enable grouping, the chart includes multiple bars, points, or slices for each event with a High Severity and an event count specific to that single high severity event.
Format Options	<ul style="list-style-type: none">• When you have multiple Y-Axis series:<ol style="list-style-type: none">1. Select Color by Y-axis Series to make each bar, point, or slice a different color in the chart.2. Select Show Legend to show what each color represents.• Specify a Maximum number of X-Axis data points to prevent your chart from containing too much data to reasonably view in a chart. A good maximum number of X-Axis data points to display is 20. Important: When you exceed the maximum number of X-axis data points, only part of the data in the report is displayed in the chart. To ensure that all of your data is included in your chart, verify that your chart has fewer than the maximum number of X-axis data points.

5. Click the **Schedule** icon and select the appropriate options.

If you want the report to run...	Then...
one time	<ol style="list-style-type: none">1. Select Run Once.2. If you want the report to run later, select the Start time.
on a recurring schedule	<ol style="list-style-type: none">1. Select Daily, Weekly, or Monthly.2. Select the time to Start running the report.3. If you want to limit the number of occurrences, select the End by date.

6. Optional: Click the **Notification** icon. Select or type the email address of the users you want to send the report to.
7. Click **OK**.

Creating templates

Create templates with custom data filters and formatting options that meet your specific needs for a report.

Before you begin

Install the Business Intelligence and Reporting Tools (BIRT) reporting system, version 2.5.2 from <http://www.eclipse.org/birt/phoenix/>.

About this task

You can create a template by running a report from a custom Analysis view, or by using BIRT, an open source Eclipse-based reporting system.

What to do next

You can create a custom view in the Analysis view and run a report from that custom view, or you can export an existing template from the Console, modify the settings of the template in BIRT, and then import the modified template back into the Console.

Exporting a template

Export an existing template into a directory to modify it.

Procedure

1. In the Report view, click the Templates icon and click **Action > Export**

Note: You cannot export templates that have been derived from an Analysis view.

2. Select a directory to **Save in** and type a meaningful **File name** for the report.
3. Click **Save**.

Importing a template

Import a new or modified template into the Console.

Procedure

1. In the Report view, click the **Template** icon.
2. Click **Action > Import**
3. In the Import Report Template window, type a meaningful **Template Name** and **Template Description**, select a category to display the new template in, and then browse to the report design file you want to import.

Tip: The file extension for a design file is **.rptdesign**

4. Click **Open**.

Deleting reports, templates, and schedules

Delete reports, templates, and schedules that are no longer useful.

About this task

There is a difference between deleting a template, deleting a report, and deleting a schedule.

Important: Deleting a template also deletes saved reports and schedules that are related to the template.

What to do next

In the Report view, perform one of the following tasks:

Deleting a report

Delete a saved report when data in the report is no longer useful.

About this task

Deleting a report does not delete the template or the schedule related to the report.

Procedure

1. In the Report view, click the **My Reports** icon.
2. Select the report you want to delete, and then click **Edit > Delete**
3. In the Delete Report confirmation window, click **OK**.

Deleting a schedule

Delete a schedule to stop SiteProtector from producing a report that has been scheduled.

About this task

Deleting a schedule does not delete the template or the saved reports that are related to the schedule.

Procedure

1. In the Report view, click the **Schedules** icon.
2. Select the schedule you want to delete, and then click **Edit > Delete**.

Deleting a template

Delete a template created by a SiteProtector user when the template is no longer useful.

About this task

Deleting a template also deletes the saved reports and schedules that are related to the template.

Procedure

1. In the Report view, click the **Templates** icon.
2. Select the report template you want to delete.
3. Click **Edit > Delete**.

Note: Only templates created by SiteProtector users can be deleted.

Finding reports

Find a report to open, rerun, schedule, save, delete, or set the report as a sample image.

About this task

If you have saved a report or scheduled a report to run, you can find the report in the My Report pane of the Report view. Otherwise, you must rerun the report.

Procedure

1. In the Report view, click the **My Reports** icon.

Tip: Click the column headers to sort reports.

2. Optional: Select the report, click **Action**, and then select one of the following options:
 - **Open**
 - **Rerun report**
 - **Schedule Report**
 - **Set as sample image**
 - **Save**
 - **Delete**

Sending reports in email

You can configure scheduled reports to be sent through email when the report runs or you can send a report in email directly from the Report Viewer.

Before you begin

You must schedule a report or generate a report to send the report in an email.

Procedure

Send a report in email from one of the following locations in the Console:

Option	Description
In the Report Viewer	When you create a new report, or open a saved report, click Action > Email report , and then select or type user email addresses for users you want to send the report to in an email.
Scheduled report in Report view	Schedule a report from the Analysis view or the Report view. In the Schedule Report window, click the Notification icon, and then select or type the email address of the users you want to send the report to.

Setting a report sample image

Set a report as the sample image for a template so that it is displayed as the sample image in the Template Detail pane.

Procedure

1. In the Report view, click the **My Reports** icon.

Tip: Click the column headers to sort reports.

2. Optional: Select the report, click **Action > Set as Sample Image**.

Managing template permissions

Use permissions for a report template to define which users or groups can view or control the report template.

Procedure

1. In the Report view, click the **Templates** icon, select a template, and then click **Action > Permissions**.
2. In the Manage Permissions window, select a user or group, and then select permissions for the user or group.

Note: If a user or group is not displayed in the Users and/or Groups box, click **Add** to add the user or group.

3. Optional: Click **Advanced** to change the current owner of the template.

Communicating data from the Analysis view

Create ad hoc reports from the Analysis view, export data to work outside of SiteProtector, or generate custom reports from the Analysis view that you can share.

About this task

Consider exporting data when you

- Want to use a reporting tool outside of SiteProtector
- Need to share data with an audience that does not have access to SiteProtector, but needs to manipulate the data
- Think formatting is not important
- Want to include remediation information for each event

Consider creating a new report or scheduling a report when you

- Plan to produce the report multiple times
- Want to allow other SiteProtector users access to the report
- Think formatting is important

Tip: To report small amounts of data, you can copy and paste data into external applications. For example, if you have a single workstation that has a vulnerability and you want to quickly notify the system administrator, you can copy and paste the data into an e-mail.

Example

- You have many assets that are owned by several system administrators. You export data into a spreadsheet and send the spreadsheet to all the system administrators.
- You have been asked to share your Site's security posture with management. You create a new report because the formatted data is easier to consume and has a more professional look.

What to do next

In the Analysis view, perform one of the following tasks:

Exporting data

Export data in the Analysis view to work with large amounts of data, to work with data outside of SiteProtector, and to work with data that is not formatted.

About this task

Exporting data is the same as exporting a view.

Tip: To schedule data exports click **Action > Schedule Export**.

Procedure

1. In the Analysis view, click **Action > Export**.
2. In the Export window, type a **File path**, select a **File Type**, and specify what data to export in the **Exported Content** section.

Note: You can only exclude columns that are already in the Analysis view. To include a column in the exported data, go back to the Analysis view and add the column before you export the data.

3. Optional: Select **Include Security Information** to include remediation information for each event.

Scheduling exports of data

In an Analysis tab, you can schedule a job to export data.

Procedure

1. Click **Action > Schedule Export**.
2. Click the **Parameters** tab.
3. In the **Output Parameters** area, type a **File Name**, select a **File Type**, and then select the time for which you want data to appear in the file.
4. Select a **Time Filter** to specify the time frame for the data you want to export.
5. In the **Analysis Data Export Parameters** area, select an **Analysis View** and filters.
6. Click the **Schedule** tab.
7. Select a **Recurrence pattern**, **Start time**, and **Range of recurrence**.
8. Click **OK**.

Creating reports in the Analysis view

Create ad hoc reports and custom reports in the Analysis view. When you create a new report, that report is generated immediately and is displayed in the Console.

Procedure

1. Click **Action > New Report**.
2. In the New Report window, click the **General** icon, and then type a meaningful **Report Name** and **Description** for the report.
3. Optional: Click the **Chart** icon and select the appropriate formatting choices.

Tab	Tips
Select Chart Type	When selecting a dimension for your chart, consider using 2D with depth or 3D for charts in reports that you plan to share, such as executive reports, because they are more visually engaging. Consider using 2D for charts when you analyze the data because there is less ambiguity about data values.
Select Series	Select Enable Grouping when you have multiple Y-Axis series. The Y-Axis series is summed according to the X-Axis series. Example: If you are charting event counts and severity, you can enable grouping to see one bar, point, or slice for High Severity, with a total event count for all High Severities. If you do not enable grouping, the chart includes multiple bars, points, or slices for each event with a High Severity and an event count specific to that single high severity event.

Tab	Tips
Format Options	<ul style="list-style-type: none"> When you have multiple Y-Axis series: <ol style="list-style-type: none"> Select Color by Y-axis Series to make each bar, point, or slice a different color in the chart. Select Show Legend to show what each color represents. Specify a Maximum number of X-Axis data points to prevent your chart from containing too much data to reasonably view in a chart. To ensure that all of your data is included in your chart, verify that your chart has fewer than the maximum number of X-axis data points. Important: When you exceed the maximum number of X-axis data points, only part of the data in the report is displayed in the chart.

4. Click **OK**.

Scheduling reports in the Analysis view

Schedule reports to run in the background, to run at a later time, or to run on a recurring schedule.

Procedure

- In the Analysis view, click **Action > Schedule Report**.
- Click the **General** icon, and then type a meaningful **Report Name** and **Description**.
- Optional: Click the **Chart** icon and select the appropriate formatting choices.

Tab	Tips
Select Chart Type	When selecting a dimension for your chart, consider using 2D with depth or 3D for charts in reports that you plan to share, such as executive reports because they are more visually engaging. Consider using 2D for charts when you analyze the data because there is less ambiguity about data values.
Select Series	<p>Select Enable Grouping when you have multiple Y-Axis series. The Y-Axis series is summed according to the X-Axis series.</p> <p>Example: If you are charting event counts and severity, you can enable grouping to see one bar, point, or slice for High Severity, with a total event count for all High Severities. If you do not enable grouping, the chart includes multiple bars, points, or slices for each event with a High Severity and an event count specific to that single high severity event.</p>
Format Options	<ul style="list-style-type: none"> When you have multiple Y-Axis series: <ol style="list-style-type: none"> Select Color by Y-axis Series to make each bar, point, or slice a different color in the chart. Select Show Legend to show what each color represents. Specify a Maximum number of X-Axis data points to prevent your chart from containing too much data to reasonably view in a chart. To ensure that all of your data is included in your chart, verify that your chart has fewer than the maximum number of X-axis data points. Important: When you exceed the maximum number of X-axis data points, only part of the data in the report is displayed in the chart.

4. Click the **Schedule** icon and select the appropriate options.

If you want the report to run...	Then...
one time	<ol style="list-style-type: none"> Select Run Once. If you want the report to run later, select the Start time.

If you want the report to run...	Then...
on a recurring schedule	<ol style="list-style-type: none"> 1. Select Daily, Weekly, or Monthly. 2. Select the time to Start running the report. 3. If you want to limit the number of occurrences, select the End by date.

5. Optional: Click the **Notification** icon. Select or type the email address of the users you want to send the report to.
6. Click **OK**.

Chapter 4. Identifying and resolving network vulnerabilities

This chapter discusses how to identify and respond to threats.

This chapter is not a comprehensive guide for developing a vulnerability assessment plan. For more information on developing a vulnerability assessment plan, contact Professional Services at IBM Security.

Developing vulnerability assessment plans

This topic explains what to consider as you develop a vulnerability assessment plan, and provides an overview of the vulnerability identification and resolution process.

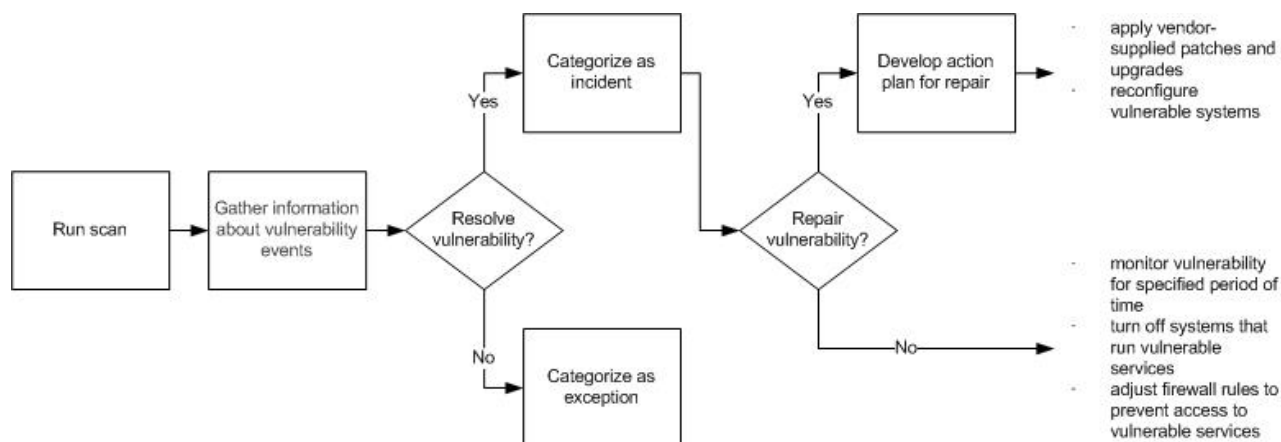
Importance of a vulnerability assessment plan

To effectively identify and resolve vulnerabilities, IBM Security recommends that you establish a vulnerability assessment plan. Consider the following as you develop your plan:

- which hosts to include in scans
- frequency of scans
- who is responsible for affected systems
- process by which vulnerabilities are reported, tracked, and resolved
- vulnerability assessment team's area of responsibility, including
 - organizational structure of team
 - relationship to upper management
 - services provided

Diagram of vulnerability identification and resolution process

The following figure illustrates the vulnerability identification and resolution process:



Vulnerability data generated by the SiteProtector system

This topic explains the types of vulnerability data generated by the SiteProtector system, categories of vulnerabilities, and vulnerabilities associated with specific attacks.

Definition: vulnerability

A vulnerability is a known flaw on your network that can be exploited.

Vulnerability data types

The types of vulnerability data generated by the SiteProtector system are as follows:

Network-based — Attackers usually exploit these vulnerabilities by accessing a service that is exposed to other machines on the network. Network-based vulnerabilities can occur on both hosts and networks.

Host-based — Attackers exploit host-based vulnerabilities by logging onto the host, as a local or a remote user.

Categories of vulnerabilities

Vulnerability categories are as follows:

Vendor-specific — Commercial software or hardware that is not secured properly such as software bugs, missing operating system patches, and services.

Improper configuration — Improperly configured software and hardware, such as poorly defined policies for password creation or unauthorized changes to system configurations, including uninstalling patches and hot fixes.

Improper user activity — Unauthorized use or neglect on the part of users sharing directories to unauthorized parties, failing to use or update antivirus software, and using dial-up modems to circumvent firewalls.

Vulnerabilities associated with specific attacks

The following table provides descriptions of vulnerabilities associated with specific attacks:

Vulnerability	Description
Backdoor	A hole in the security of a system or application due to one of the following: <ul style="list-style-type: none">• a security flaw• a hidden means of access
Buffer or field overflow	A system flaw that lets an attacker submit code into a variable that exceeds the field length of the variable. The code then runs, providing access for the attacker.
Default accounts and inappropriate access privileges	A user account enabled by default, predefined accounts, or accounts with access to more resources and commands than is appropriate for the level of access.
Weak access control	A system misconfiguration that weakens access control, such as permitting the use of blank or null passwords, or easily guessed passwords.
Information vulnerability	A system flaw that provides reconnaissance information about a host, such as the version of an operating system.

Gathering information about vulnerability events

After you scan your network, you must gather information about vulnerability events generated by the scan or scans. Use analysis views to navigate to important details about vulnerability events.

Reference: For more information about the event analysis, refer to “Section B: Analyzing Events” on page 7.

Deciding whether to resolve vulnerabilities

This topic includes questions to help you in determining which vulnerabilities to resolve.

Deciding whether to resolve vulnerabilities

Use the following questions when determining whether a vulnerability should be resolved:

Does the vulnerability affect critical assets? The most important factor in determining whether to resolve a vulnerability is whether the host or segment affected by the vulnerability is critical.

What’s the worst-case scenario if this vulnerability were exploited? The impact of an attack can vary. Some vulnerabilities allow attackers to potentially disable all the critical hosts in an organization while other vulnerabilities provide attackers with information that has little or no value.

How widely used is the platform that is affected by the vulnerability? The number of hosts running the platform affected by the vulnerability may determine whether this vulnerability will be exploited. Generally, the more hosts that are running a vulnerable platform, the more likely it is that the platform will be attacked.

Does the vulnerability require advanced skill to exploit? Most attackers lack advanced hacking techniques; therefore, they are not likely to exploit a vulnerability if it requires advanced skills.

Can the vulnerability be exploited by an outsider? Vulnerabilities that can be exploited by users remotely, without using local account privileges, open the door to a large number of potential attackers.

Repairing and mitigating vulnerabilities

You can often repair or mitigate vulnerabilities.

When you decide to resolve a vulnerability, do one of the following:

- repair the vulnerability
- mitigate the risk of the vulnerability

Repairing

The most effective way to resolve a vulnerability is to repair it. When you repair a vulnerability, you repair or reconfigure the system so that the system affected is no longer vulnerable.

Mitigating

When you mitigate a vulnerability, you attempt to lessen the impact of the vulnerability, but you do not eliminate it. Consider mitigating vulnerabilities as a temporary measure.

Exceptions and incidents

The SiteProtector system provides a simple way to categorize vulnerabilities, as follows:

- If you choose to resolve a vulnerability, categorize it as an incident.
- If you choose to ignore a vulnerability, categorize it as an exception.

Baseline feature

Consider using the baseline feature to track vulnerabilities that have been repaired or mitigated.

If a vulnerability cannot be resolved immediately

In special situations, consider categorizing a vulnerability as an exception especially if you know that a significant period of time will elapse before you can resolve it.

Resolving vulnerabilities

Use the following table as a guide when resolving vulnerabilities:

Methods	Task	Incident or Exception
Repair vulnerability	Apply vendor-supplied patches or upgrades	Categorize as an incident until patch or upgrade has been implemented and tested.
	Reconfigure vulnerable systems	<ol style="list-style-type: none">1. Categorize as an incident until vulnerable systems have been successfully re-configured.2. Categorize as an exception and schedule it to expire when the system can be successfully patched or upgraded.
Mitigate vulnerability	Monitor vulnerability for a specified period of time	Categorize as an incident.
	Turn off systems that run vulnerable services	<ol style="list-style-type: none">1. Categorize as an incident until vulnerable services are turned off.2. Categorize as an exception and schedule it to expire when the system can be successfully patched or upgraded.
	Adjust firewall rules to prevent access to vulnerable systems Note: This approach is not foolproof. Attackers can circumvent firewall rules to access vulnerable hosts.	<ol style="list-style-type: none">1. Categorize as an incident until vulnerable services are blocked.2. Categorize as exception and schedule it to expire after the system can be successfully patched or upgraded.

Reference: For more information on repairing vulnerabilities, refer to “Implementing upgrades and patches” on page 35.

Creating a plan of action

After you decide how to repair or mitigate a vulnerability, you should create a plan that includes detailed information about the vulnerability, how you plan to resolve it, and how you plan to test it after it is resolved.

How to create an action plan

The following is a list of information to include in an action plan:

- detailed description of the vulnerability
- list of systems affected by the vulnerability

- description of how you will repair or mitigate the vulnerability, including detailed implementation procedures, such as designating responsible parties and contacting system owners
- description of how you will assess the impact of the solution, including testing and rollback procedures

Implementing upgrades and patches

After you create an action plan for repair, you should implement upgrades and patches.

Definition: upgrade

An upgrade is a new version of, or an addition to, a hardware or software product that is already installed. Upgrades usually include new features and redesigned components.

Definition: patch

A patch is a temporary fix for software or hardware, which usually addresses a specific bug or flaw. Patches usually do not include new features or redesigned components.

How to ensure successful implementation

To implement upgrades and patches successfully, you must do the following:

- test the new software or reconfiguration
- obtain cooperation from system owners and business managers who are responsible for devices being patched or upgraded

Questions to consider when implementing upgrades and patches

Use the following questions as a guide when implementing upgrades and patches:

- Will the system be more vulnerable while it is being repaired?
- Will patched and unpatched systems co-residing on your network present incompatibilities?
- Could the fix you are implementing to repair one vulnerability create another?
- Will the fix require extensive testing? If so, have you allowed enough time?

Next step

Re-scan your network to determine if vulnerabilities have been repaired successfully.

Chapter 5. Managing Scans

This chapter discusses how to implement and manage network scans in your environment using the IBM Internet Scanner® or IBM Proventia Network Enterprise Scanner applications.

Identifying hosts on your network

This topic explains how to identify hosts on your network.

To identify hosts on your network, consider performing discovery scans as follows:

- after you install the SiteProtector system to generate host information and map out your network
- periodically to identify new hosts on the network

Definition: discovery scan

Discovery scans use the IBM Internet Scanner or IBM Proventia Network Enterprise Scanner discovery policies. These policies identify the host operating system, services currently running on the system, and perform basic vulnerability checks.

Purpose of launching discovery scans

Discovery scans provide useful information about hosts on your network without running the time-consuming checks that are enabled in other IBM Internet Scanner or IBM Proventia Network Enterprise Scanner policies. A discovery scan can help you to do the following:

- identify new hosts on a network
- determine the following:
 - how to segment scans across network and which policies to use
 - whether host operating systems are up-to-date or in compliance with company standards
 - whether the users accessing the network are authorized to do so
 - whether you have sufficient IT staff to support all the platforms on your network

Host information provided by discovery scans

Discovery scans add the following information to the host table:

- IP Address
- NetBIOS Name
- DNS Name
- OS Name
- NetBIOS Domain Name

Note: If a host does not respond to IBM Internet Scanner or IBM Proventia Network Enterprise Scanner connection requests, it will not be added to the host table.

Ensuring that vulnerability data is complete and accurate

This topic provides guidelines for ensuring that your vulnerability data is complete and accurate.

To ensure that vulnerability data is complete and accurate, do the following:

- maintain scan consistency
- ensure that all hosts are accessible
- use the highest level of user access possible

Maintaining consistency between scans

To maintain consistency, consider doing the following:

- use the same policy and XPU level as the previous scan when verifying that vulnerabilities have been repaired
- use the same account privileges and scanner configuration as the previous scan
- apply XPUs and scanner policies between scan cycles
- vary scan times to scan hosts that may not be available during your normal scanning schedule
- coordinate your scanning with intrusion detection efforts so that you identify vulnerabilities that might be exploited

Ensuring hosts are accessible

To ensure that hosts are accessible, do the following:

Ensure that hosts are available — A host may be unavailable due to the following conditions:

- turned off
- not connected to the IP network
- running nonstandard services
- communicating through nonstandard ports

Ensure that firewalls are allowing communication — Certain firewall configurations block the traffic IBM Internet Scanner or Proventia Network Enterprise Scanner uses to establish connections with hosts, such as the following:

- ICMP requests
- communication from the host used by the IBM Internet Scanner or IBM Proventia Network Enterprise Scanner instance

Note: You can achieve best performance if the IBM Internet Scanner or IBM Proventia Network Enterprise Scanner instance is located in the same segment as the assets you are scanning.

Use highest level of user access

To access all system resources, IBM Security recommends that you escalate access rights when you scan. Use domain administrator privileges when scanning critical domains or hosts. Scans using domain administrator rights can require significant time to finish.

Scheduling vulnerability scans

Schedule scans when they will least impact your network, and when they can generate useful data.

Considerations

When preparing a vulnerability scan schedule, consider doing the following:

Coordinate with system owners — Always coordinate scan times with system owners.

Allow for multiple time zones — If you have a network that services more than one time zone, consider staggering scan sessions so that you accommodate users in all the time zones.

Adhere to company policy — Schedule your scans so that you avoid scanning when devices are not available. Company policy may require that certain devices, such as desktops, be shut down at the following times:

- at the close of business
- during periodic maintenance

Avoid critical servers during peak times — To avoid impacting system performance, do not scan critical application servers during peak times when large numbers of users may be attempting to access those servers.

When to scan certain hosts

The following table provides some suggestions for scheduling scans:

Time of day	Type of scan
Early morning	Desktops
Midday	Non-critical NT and UNIX servers
Evening/late night	<ul style="list-style-type: none">• Critical application servers• Printer servers

Running background scans

This topic describes background scans.

Background scans are automatic, recurring scans that run on separately defined cycles for discovery and for assessment scanning.

Recommendations

Use a small range of IP addresses to keep the scan time short. Include assets that are known to have vulnerabilities, if possible.

Task overview

The following table describes the five-task process for setting up background scanning:

Task	Affected Policy	Policy Changes
1	Discovery	Enable background discovery scanning and define the range of IP addresses to scan.
2	Assessment	Enable background assessment scanning and define which checks to run.

Task	Affected Policy	Policy Changes
3	Scan Window	Optionally, define the days and hours that scanning is allowed.
4	Scan Control	Optionally, define when the first scanning cycle begins, and the length of each scanning cycle.
5	All	Save policies and monitor scans.

Reference: For detailed information on background scanning, refer to the *IBM Proventia Network Enterprise Scanner User Guide*.

Reducing the time required to run scans

This topic provides some scanning efficiency suggestions.

Network scans can generate large amounts of data. They can also be time consuming and can impact the performance of the IBM Internet Scanner or Proventia Network Enterprise Scanner instance and the network. To reduce the time required to run scans, consider doing the following:

- improve network bandwidth and accessibility
- limit the number of hosts included in scans
- reduce default policy levels or limit the number of vulnerability checks in policy

Improving network bandwidth and accessibility

To improve network bandwidth and accessibility, consider doing the following:

Improve network bandwidth — How quickly devices on your network respond to packets sent to them affects scan times. Ping responses or Internet Control Message Protocol (ICMP) echo requests that are longer than 50 milliseconds can increase scan times significantly. If you experience slow ping response, determine whether your network bandwidth is sufficient.

Improve accessibility — Perimeter scans that are configured to scan without ping responses take longer. If you must reduce scan times, consider moving the scanning device to a location inside the firewall.

Limit hosts included in scans

To limit the hosts included in scans, consider doing the following:

Limit the overall number of hosts — IBM Security recommends that you scan no more than 2500 hosts per scan session. If you exceed this number, the scans may not be completed successfully. The maximum number of hosts you are able to scan in one session will vary according to the performance of your network and the device on which the scanner engine is installed.

Limit domain controller hosts — Domain controller hosts with a large registry of user accounts can take longer to scan because of the user account enumeration and password checking. Consider disabling these checks when scanning domain controllers or removing these hosts from scans.

Reducing default policy levels

Medium to high level scan policies take longer to run than low level policies. As a last resort, consider reducing default policy levels or limiting the number of vulnerability checks in the policy.

Chapter 6. Detecting Suspicious Activity

This chapter describes several SiteProtector system views to use as starting points for detecting suspicious activity on your network. This chapter provides guidelines for using SiteProtector system analysis views and filtering tools.

Goals of detecting suspicious activity

The goals of detecting suspicious activity are as follows:

- monitor high level patterns to determine whether you need to monitor certain activity more closely
- look for early indicators of attack severity and scope while you continuously filter, sort, and correlate events
- determine whether you have sufficient justification to take additional actions, such as officially tracking an incident or starting a formal investigation

Section A: Suspicious Activity

Suspicious activity can come from a variety of sources. Use the descriptions in this section to help you identify and categorize suspicious activity when you monitor your network.

Iterative process

Detecting suspicious activity is an iterative process. Perform the following tasks in an iterative fashion when you are determining whether an activity is suspicious:

- alternate between Event Analysis views and guided questions
- create baselines and exceptions to exclude activity that is not part of your analysis

Authorized activity

Authorized activity is normal activity that may appear to be suspicious but is actually harmless. Consider creating an exception for authorized activity or including this activity in the Console baseline. See “Section C: Filtering Activity from Analysis Views” on page 49.

Example: A DNS zone transfer between authorized DNS servers may trigger an event, but in most cases it is authorized activity. A DNS transfer that is initiated by an external IP address, however, is unauthorized activity.

Unauthorized activity

Unauthorized activity is abnormal behavior that can harm your enterprise. Unauthorized activity is sometimes erroneously categorized as a false positive. However, unauthorized activity is usually cause for concern and it may require further investigation and remediation. The following table describes unauthorized activities:

Unauthorized Activity	Description
misuse	The perpetrator does not intend to cause harm to the organization but may have unknowingly created vulnerabilities. Typically, this activity is caused by lack of due diligence, but not gross negligence. An example is an administrator who attempts to configure a firewall but because of oversight or ignorance leaves an organization's assets open to attack.

Unauthorized Activity	Description
abuse	The perpetrator does not intend to cause harm to the organization, but often knows that the activity is wrong. Typically, this activity is caused by blatantly negligent behavior or by behavior that clearly violates laws or an organization's code of conduct. Examples of abuse are a user who browses the Web for pornography on the company's intranet or an administrator who neglects to configure a firewall and leaves assets vulnerable to attacks.
malicious activity	The perpetrator intends to do harm to the organization and knows that his or her activity is wrong. Examples are an attacker who starts a denial of service attack against a company's intranet or an internal user who intends to profit from privileged financial information that he or she obtained illegally from the company's accounting servers. Threat assessment and investigation deals primarily with detecting and investigating malicious activity.

Section B: Monitoring Event Analysis Views

Analysis views provide good starting points for detecting suspicious activity because they provide multiple perspectives with an appropriate level of detail. This section provides descriptions of selected analysis views and guidelines for using them.

Related information

See "Section B: Analyzing Events" on page 7 for procedures on using guided questions and managing analysis views.

Guidelines in this section

The guidelines in this section may apply to many tasks that are performed during threat analysis and remediation, in addition to event detection.

Choosing the traffic to monitor and correlate

The traffic you choose to monitor and correlate with event analysis views can depend on a number of factors. This topic provides guidelines for choosing the traffic to monitor and for manually correlating events by source.

Important: The process of organizing and prioritizing your assets is an integral part of planning and assessing your network security. You should have performed many of these tasks when you installed and configured the SiteProtector system.

Advantages of a grouping structure

A grouping structure can help you protect your assets more efficiently by grouping hosts and sensors according to tasks you perform frequently. Typically, a Site uses more than one structure, such as geography and topology, to group assets and sensors.

Grouping assets for monitoring

The following table lists some criteria for grouping assets for monitoring:

Grouping Structure	Description
Topology	Use the topology criteria to monitor traffic based on where it originated. This is an effective and commonly used criteria for monitoring internal assets (intranet) or external assets. These areas may be further divided according to topology, such as DMZs, VPNs, partner extranets, and internal gateways.

Grouping Structure	Description
Asset criticality	You may choose to monitor mission critical assets more closely than less critical assets. In most cases, asset criticality also influences how you investigate these assets and respond to attacks against them. The SiteProtector system lets you assign a criticality rating to an asset in Asset Properties.
Geography	Use the geography structure to group assets according to the physical locations in your organization. This structure may apply to the city, state, or continent your assets are located in, and lets you compare events from different locations in your organization.
Business function	Use the business function structure to monitor hosts located in specific departments, such as sales and accounting, that may contain critical information or process sensitive traffic.

Correlating events by source

One of the goals of event detection is to determine the source of suspicious activity. Event analysis views provide several source indicators. Source indicators can help narrow your search for the source of suspicious activity but may not always lead you directly to the source. Examples of source indicators are as follows:

- an attacker's IP address that is registered to an Internet Service Provider (ISP)
- the location of an agent that indicates where in the data stream suspicious activity was detected (but not the origin)
- firewall events that indicate a series of unsuccessful logins

Summary view

The Summary view displays a high-level summary of a selected Site or group. Use data in this view to perform high-level monitoring of Site or group events.

What is the Summary view?

The Summary view is divided into several portlets that each provide a snapshot of an aspect of your security, such Vulnerability History by Day or Today's Event Summary by Event Name. Many of these views are based on a specific time frame.

You can modify the data displayed in most of the portlets to change the timeframes and include exceptions. You can also navigate from most of the portlets directly to the source of the data in the SiteProtector system.

Portlets in the Summary view

By default, the Summary view contains six portlets. However, you can add and remove up to 16 portlets.

Adding or removing portlets

You can add or remove portlets in the Summary view.

Before you begin

Tip: You can configure the Summary view to display up to 16 portlets and specify how content is updated from the **Tools > Options** menu.

Procedure

1. In the Summary view, click **Action**.
2. Select or clear a portlet option from the menu.

Tip: You can also right-click the title bar in a portlet, and then select or clear a portlet option from the pop-up menu.

What to do next

Note: On the **Action** menu, check marks appear next to portlets that are enabled in the Summary view.

Modifying portlet information

You can specify the time periods and select whether to include exceptions for the data displayed in some of the portlets in the Summary view.

Procedure

1. To adjust the time period for the data displayed in a portlet, select a number from the **Number of Days**, **Number of Weeks**, **Number of Months**, or **Agents Active in Days** list in the portlet. The data in the portlet immediately refreshes based on the new time frame you selected.
2. To include events that are exceptions in the data displayed in a portlet, select the **Include Exceptions** check box in the portlet. The data in the portlet immediately refreshes to include the event exceptions.

Note: An exception is an event or an attack pattern that you do not consider a risk to your network or hosts. Examples of exceptions include the following:

- false positives
- a vulnerability you expect to eliminate soon

What to do next



Note: You cannot modify the data displayed in the **System Health**, **Site Summary**, **Group Summary**, **Scan Progress**, **Ticket Status**, and **Offline / Stopped Agents** portlets.

Navigating from the portlets

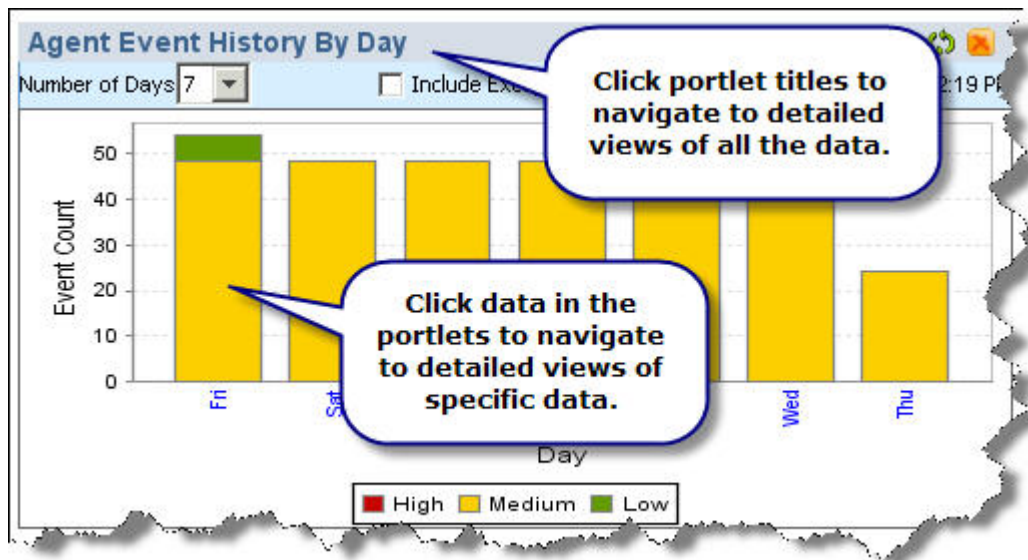
You can navigate from most of the portlets in the Summary view to the source of the data in SiteProtector.

Procedure

Do one of the following in the Summary view:

- Click a portlet title to see a detailed view of all the data in that portlet.

- Click the data (including graphs) in a portlet to see a detailed view of just that specific data.



Example

Examples:

- If you click the **Agent Event History by Day** portlet header, the **Event Analysis-Details** view appears, filtered by the start date.
- If you click a bar in the graph in the **Agent Event History by Day** portlet, the **Event Analysis-Details** view appears, filtered by the data you clicked in the portlet.

What to do next

Notes:

- Due to the specific data displayed in the portlet, you cannot click the portlet titles to navigate from the **System Health**, **Available Updates**, **Scan Progress**, or **Offline / Stopped Agents** portlets. However, you can click the data within those portlets to navigate to the detailed view of that specific data.
- You cannot navigate from the **Site Summary** or **Group Summary** portlets.

Event Name view

The Event Analysis - Event Name view provides a good starting point for determining the types of events detected on your network and for customizing analysis views for specific tasks. Use this view during the early stages of event detection.

What is the Event Name view?

The Event Name view provides the tag name of the event, status (this is most useful if SecurityFusion is enabled), severity, event counts, and date and time.

Example of the Event Name view

The following figure provides an example of the Event Name view. When combined with statuses from the SecurityFusion Module, the Event Name view can provide an accurate snapshot of your network's security:

Event Analysis - Event Name									
Tag Name	Status	Severity	Event Count	Source Count	Target Count	Ob...	Earliest Event	Latest Ever	
SNMP_Long_Field_Length	Failed attack (blocked at host)	Medium	20	1	1	1	09-30 12:00	09-30 13:00	
SNMP_InvalidTag_VarBindList	Failed attack (blocked at host)	Medium	20	1	1	1	09-30 12:00	09-30 13:00	
FTP_Cwd_Root	Failed attack (blocked at host)	Medium	1	1	1	1	09-30 12:00	09-30 12:00	
SNMP_Discovery_Broadcast	Failed attack (blocked at host)	Low	16	1	1	1	09-30 12:00	09-30 13:00	
UDP_Probe_Other	Failed attack (blocked at host)	Low	9	7	1	1	09-30 11:00	09-30 17:00	
synflood	Failed attack (blocked at host)	Low	1	1	1	1	09-30 12:00	09-30 12:00	
Brute_force_login_likely_successful	Failure likely (wrong OS)	Medium	1	1	1	1	09-30 12:00	09-30 12:00	
Brute_force_login_attack	Failure likely (wrong OS)	Medium	1	1	1	1	09-30 12:00	09-30 12:00	
Logon_with_special_privileges	Failure likely (wrong OS)	Medium	1	1	1	1	09-30 12:00	09-30 12:00	
Logon_with_admin_privileges	Failure likely (wrong OS)	Medium	1	1	1	1	09-30 12:00	09-30 12:00	
Log_on_to_account_failed	Failure likely (wrong OS)	Low	24	1	1	1	09-30 12:00	09-30 12:00	
HTTP_Cross_Site_Scripting	Failure likely (wrong OS)	Low	8	1	1	4	09-30 13:00	09-30 13:00	
User_logout	Failure likely (wrong OS)	Low	4	1	1	1	09-30 12:00	09-30 12:00	
Synthesized_Host_Attack_Flood	Failure likely (wrong OS)	Low	2	1	1	1	09-30 12:00	09-30 12:00	
Successful_Network_Login	Failure likely (wrong OS)	Low	2	1	1	1	09-30 12:00	09-30 12:00	
Failed_login-account_disabled	Failure likely (wrong OS)	Low	1	1	1	1	09-30 12:00	09-30 12:00	
Logon_process_registered	Failure likely (wrong OS)	Low	1	1	1	1	09-30 12:00	09-30 12:00	
EventCollector_Error	Unknown impact (no correlation)	High	37	1	1	1	09-02 15:00	09-30 21:00	
DesktopController_Error	Unknown impact (no correlation)	High	17	1	1	1	09-02 21:00	09-25 15:00	
Logon_with_admin_privileges	Unknown impact (no correlation)	High	9	1	1	1	09-30 13:00	10-01 08:00	
Logon_with_special_privileges	Unknown impact (no correlation)	High	9	1	1	1	09-30 13:00	10-01 08:00	
Changes_to_important_files	Unknown impact (no correlation)	High	9	1	1	1	09-30 13:00	09-30 13:00	
Sensor_Error	Unknown impact (no correlation)	High	2	2	2	1	09-25 09:00	10-01 09:00	

Guidelines for viewing the Event Name view

Use the following guidelines to view events in the Event Name view:

- Filtering for specific attacks

If you are monitoring for a specific exploit, the Event Name view can provide a good starting point. For example, if you have determined from your security research that a widespread attack is underway that uses a combination of a Microsoft remote procedure call and an SQL injection attack, you could filter the Event Name view to show only events that trigger these signatures. See “Section C: Filtering Activity from Analysis Views” on page 49.

- Filtering by severity or status

If the SecurityFusion Module is enabled and your vulnerability data is current, sort the view by the degree of vulnerability or severity, with the most vulnerable or most severe events appearing first in the list. This rearranges your view so that the events that will most likely require further action appear first in the list.

Tip: Click the column name while pressing the SHIFT key to sort additional columns in the same view.

- Customizing the Event Name view for greater source correlation

The Event Name offers several possibilities for customization. Consider adding the Sensor Name, SourceIP, and DestinationIP columns to the Event Name view, and sort the view by the Event Name column. Use the Sensor Name column and the SourceIP column to correlate the events by source.

Target view

The Event Analysis - Target view provides a good perspective for determining the hosts that are possible targets of suspicious activity. While these hosts may not be the ultimate target of an attack, they can be an early indicator of the attack's scope.

What is the Target view?

The Target view is a default analysis view that provides information about IP address and DNS names that may be the target of suspicious activity. The Target view provides event counts for the source hosts and tag names that are associated with the activity. It also provides severity counts and the date and time of the event.

Example of the Target view

The following figure provides an example of the Target view:

Event Analysis - Target									
Target IP	Target DNS Name	# High	# Medium	# Low	Tag Count	Source Count	Object Count	Earliest Event	Latest Event
63.210.164.72		0	0	108	7	1	1	09-29 10:00	09-29 10:00
63.210.164.87		3	0	15	7	1	1	09-11 17:00	09-29 10:00
63.210.164.88		0	0	149	7	1	1	09-11 17:00	09-11 17:00
63.211.153.95		0	0	129	7	1	1	09-30 09:00	09-30 09:00
63.211.153.103		1	0	7	5	1	1	09-30 09:00	09-30 09:00
64.124.83.105		2	0	5	5	1	1	09-07 09:00	09-07 09:00
127.0.0.1		0	0	1	1	1	1	09-30 12:00	09-30 12:00
192.168.0.32	hometwo	0	0	1496	10	4	13	09-02 10:00	09-30 21:00
192.168.0.33	homeone	0	0	17	5	3	18	09-02 15:00	09-30 20:00
192.168.0.34	gothops	0	3	309	18	11	273	09-02 15:00	10-01 08:00
192.168.0.62	RSSP2	0	55	5521	48	5	292	09-02 15:00	10-01 08:00
192.168.0.255		0	0	44	1	1	1	09-02 15:00	10-01 08:00
206.112.112.6		2	0	12	7	1	1	09-07 09:00	09-07 09:00
206.112.112.13		1	0	182	8	1	1	09-07 09:00	09-07 09:00
206.112.112.69		0	0	55	7	1	1	09-07 09:00	09-07 09:00
207.46.131.229		2	0	5	5	1	1	09-11 17:00	09-11 17:00
207.46.197.59		0	0	20	4	1	1	09-07 09:00	09-11 17:00
207.46.197.121		0	0	20	4	1	1	09-07 09:00	09-30 09:00
207.46.242.247		0	0	4	4	1	1	09-07 09:00	09-07 09:00
208.172.13.222		2	0	5	5	1	1	09-07 09:00	09-07 09:00
255.255.255.255		24	68	329	7	3	3	09-02 10:00	09-30 21:00

Guideline for viewing the Target view

Use the following guideline when you are viewing events in the Target view:

- External probes and scans

If you are monitoring external events from agents that are located in your DMZ or outside your network (for example, a network appliance outside your external firewall), you may see hundreds of events from the automated probes and scans, many of which can be harmless. If you choose to monitor this activity, consider how you can effectively filter these events. See “Section C: Filtering Activity from Analysis Views” on page 49.

Attacker view

The Event Analysis - Attacker view provides a good starting point for determining the hosts from which suspicious traffic has originated. Use the Attacker view to correlate events with the source IP address.

What is the Attacker view?

The Attacker view is a default analysis view that provides information about the IP address and the DNS name that is the source of suspicious traffic. It also provides dates, event counts, and severity ratings. By default, the High, Medium, and Low columns are sorted by severity.

Example of the Attacker view

The following figure provides an example of the Attacker view:

Event Analysis - Attacker									
Source IP	Source DNS Name	# High	# Medium	# Low	Tag Count	Target Count	Object Count	Earliest Event	Latest Event
192.168.0.34	gothops	14	58	175	8	7	1	09-02 15:00	10-01 08:00
192.168.0.62	RSSP2	0	1	15	2	1	2	09-30 12:00	09-30 12:00
209.86.128.192		0	0	3	1	1	1	09-30 16:00	09-30 16:00
24.158.198.33		0	0	1	1	1	1	09-30 17:00	09-30 17:00
24.190.108.2		0	0	1	1	1	1	09-30 16:00	09-30 16:00
66.69.103.142		0	0	1	1	1	1	09-30 16:00	09-30 16:00
65.34.205.49		0	0	1	1	1	1	09-30 11:00	09-30 11:00
24.198.12.93		0	0	1	1	1	1	09-30 11:00	09-30 11:00
24.73.64.236		0	0	1	1	1	1	09-30 11:00	09-30 11:00
24.161.178.64		0	0	1	1	1	1	09-18 17:00	09-18 17:00

Guidelines for viewing events in the Attacker view

Use the following guidelines when viewing events in the Attacker view:

- Determine the organization that the IP address is registered to
Knowing the company that owns the SourceIP listed in the SourceIP column can help narrow down the search for the attacker. Use the guided question “What is the WhoIs record of this IP address?” to determine the IP address that the SourceIP is registered to. Also consider other Internet sources of this information, such as RIPE, ARIN, and APNIC.
- Consider the source
The IP addresses listed in the SourceIP column of the Attacker view are not always the origin of suspicious traffic. This IP address may be registered to an Internet Service Provider or another institution, and the IP address sending the traffic may reside behind a firewall that uses network address translation (NAT). The IP address may be an internal host that has been hijacked by an attacker who is using this host to try to attack other internal hosts.

Scenarios for using guided questions and Event Analysis views

Guided questions and event analysis views can help you correlate the source of suspicious activity. Use this topic to help familiarize yourself with situations you may encounter.

Reference: See the following topics for procedures on using guided questions and analysis views:

- “Selecting an Analysis view” on page 7
- “Selecting guided questions” on page 12

Scenario 1

The following table describes a process in which an analyst discovers suspicious activity, and then accesses event analysis views for more specific information:

Stage	Description
1	While monitoring the Event Analysis - Event Name view, an analyst detects a sudden increase in events. The tag names do not seem to correlate with a specific category of signatures.
2	The analyst selects the event that is at the top of the list, and then selects “What are the sources of this event?” The Event Analysis - Attacker view appears and shows that a single IP address is the source of all the events associated with this tag name.
3	The analyst selects “Which sensors detected this attacker?” and the Event Analysis - Sensor view appears. The Sensor view shows that all the events coming from the attacker's IP address are detected by a network appliance located in the DMZ. No other agents in the network are reporting events from this attacker.

Stage	Description
4	The analyst concludes that this attacker is starting a series of probes or scans that are targeted at the servers in the network's DMZ. The analyst creates an incident for this event and decides to manually correlate the remaining events.

Section C: Filtering Activity from Analysis Views

To successfully detect suspicious activity, you must eliminate normal activity from the analysis views. This section provides background information and procedures for filtering activity so that you can focus on what is important in your analysis.

The importance of filtering

Filtering is an important part of detecting suspicious activity. On any a given day, you may create dozens of filters. Typically, the filtering you perform at this stage is different from the more targeted filtering you perform when you investigate a confirmed attack or a compromised system.

Creating baselines

A baseline enables you to tell at a glance if the number of events in an analysis view has increased or if a new event has appeared.

For example, if you notice that one IP address or tag name is associated with an unusually high increase in the number of events, you may want to investigate it further.

Important: You can only set one baseline view at a time. Baseline data only appears for event counts. If event count columns do not appear in your view, then you will not see baseline data.

Guidelines for creating baselines

Because baselines exclude data from analysis, you should follow the guidelines for creating baselines:

- Familiarize yourself with the traffic in your environment
You must be familiar with the traffic in your network before a baseline can be effective. You must establish what is normal for your network, and then compare this state with the current state. This is an ongoing process and requires constant attention.
- Understand how the change control process affects baselines
Understand how changes that you are implementing in your network can affect baselines. For example, if you install software patches on a group of servers, this could significantly increase or decrease the number of events that you are seeing.

Items changed in the analysis view

When you create a baseline, the following items are changed in the analysis view:

Item	Description
event counts	If an agent detects a new event, the increase is shown in red in the event count column that applies (source, target, tag, object). Example: 241 (+34). If the change is a decrease, the amount of decrease is shown in blue.
status bar	The status bar displays the baseline icon when a baseline is enabled. Move the pointer over this icon to view the "Baseline [date and time]" information.

Example of baseline view

The following figure provides an example of a baseline created for a the Event Name view. Note that the event counts that show increases are in parentheses:

Event Analysis - Event Name						
Tag Name	Severity ▲	Event Count ▼	Source Count	Target Count	Object Count	Earliest Event
Sensor_Warning	Medium	18 (+18)	2 (+2)	2 (+2)	1 (+1)	2004-06-08 13:00:00 EDT
SMB_Winreg_File	Medium	13 (+9)	2 (+1)	3 (+2)	2 (+1)	2004-06-08 15:00:00 EDT
TCP_Port_Scan	Medium	5 (+5)	1 (+1)	3 (+3)	2 (+2)	2004-06-09 11:00:00 EDT
Email_Vrfy	Medium	1 (+1)	1 (+1)	1 (+1)	1 (+1)	2004-06-09 11:00:00 EDT
LanMan_Share_Enum	Low	2296 (+863)	6	3	1	2004-06-10 14:00:00 EDT
SMB_Filename	Low	1766 (+539)	7	4	2	2004-06-10 14:00:00 EDT
Windows_Null_Session	Low	1437 (+539)	7	4	2	2004-06-10 14:00:00 EDT
Netbios_Session_Granted	Low	1309 (+492)	6	3	1	2004-06-10 14:00:00 EDT
Netbios_Session_Request	Low	1309 (+492)	3	6	606 (+211)	2004-06-10 14:00:00 EDT
SensorStatistics	Low	298 (+113)	1	1	1	2004-06-10 14:00:00 EDT
SensorStatistics_Cumulative	Low	298 (+113)	1	1	1	2004-06-10 14:00:00 EDT
HTTP_User_Agent	Low	184 (+174)	2	9 (+7)	2	2004-06-10 14:00:00 EDT
HTTP_Server_ID	Low	99 (+89)	2	7 (+5)	2	2004-06-10 14:00:00 EDT
Sensor_Info	Low	98 (+98)	4 (+4)	4 (+4)	1 (+1)	2004-06-08 13:00:00 EDT
TCP_Probe_SMTP	Low	75 (+28)	1	1	1	2004-06-10 14:00:00 EDT
iss-host-scan	Low	61 (+61)	1 (+1)	6 (+6)	1 (+1)	2004-06-09 11:00:00 EDT

Creating a baseline

Use the Baseline function to analyze changes in the number of events relative to the events identified at the time of the baseline.

Before you begin

Baseline data appears only with event counts, therefore you must add the **Event Count** column to the Analysis view to see baseline data.

About this task

You can set only one baseline view at a time, and the view applies to the currently selected group.

Procedure

1. Open an **Analysis** tab, and then select a group in the left pane.
2. If the **Event Count** column is not in the current view, either add it or select an Analysis View that includes it.
3. Click **Action > Baseline > Establish**. The Baseline icon appears in the status bar of the Console whenever the baseline is displayed.
4. If event counts change over time or if they change because of changes you make in the view, the **Event Count** column, and other applicable count columns, change as follows:

If the event count...	Then the event count is displayed...
increases	in red, followed by the number of additional events inside parentheses. Example: 45(+4)
decreases	in blue, followed by the number of fewer events inside parentheses. Example: 2(-2)

Modifying the baseline

Restore the baseline to return to your last baseline, or reset the baseline to use current values.

Before you begin

Baseline data appears only with event counts, therefore you must add the **Event Count** column to the Analysis view to see baseline data.

Procedure

1. Open an **Analysis** tab, and then select a group in the left pane.
2. If the **Event Count** column is not in the current view, either add it or select an **Analysis View** that includes it.
3. To the last baseline, click **Action > Baseline > Restore**.
4. To reset the baseline, do one of the following tasks:

If you want to reset...	Then...
the entire baseline	click Action > Baseline > Restore .
selected rows	select the rows to reset and click Action > Baseline > Reset Selected Values .

Creating incidents and exceptions

Incidents and exceptions are event filters that you can use to emphasize or exclude events that meet certain criteria. This topic provides guidelines and procedures for doing the following:

- creating incidents and exceptions
- editing incidents and exceptions
- deleting incidents and exceptions

Reference:

- See “Creating exceptions to filter scan activity” on page 58 for information about how to use exceptions to exclude events generated by authorized vulnerability scans.

When to use incidents and exceptions

The following table describes when to use incidents and exceptions:

If you want to...	Then create an...
emphasize or track certain events in your analysis	incident.
exclude certain events from your analysis	exception.

Information that you can include in an incident or exception

The SiteProtector system automatically associates certain event details with an incident or an exception. If you create an incident or exception by first right-clicking an event or a group of events, the SiteProtector system populates the information in the fields in the New Incident/Exception window with the event details that apply.

Guideline for creating incidents

Use the following guideline for creating incidents:

- Merge incidents with tickets when you confirm that certain activity is a threat
If you determine that an incident should be formally investigated, consider merging the information from the incident into a ticket. Tickets allow you to categorize and track the activity and assign ownership using the SiteProtector system's incident tracking system.

Guidelines for creating exceptions

Use the following guidelines for creating exceptions:

- Create exceptions for activity that fits a specific pattern
Use exceptions to filter events that fit a specific pattern. Typically, an exception should require some future action to be performed by the person or organization responsible for it.
- Configure the SecurityFusion Module to ignore events that are categorized as exceptions
The SecurityFusion Module requires system resources when it analyzes traffic. Because exceptions are by definition not part of your analysis, configure the SecurityFusion Module to ignore events that are categorized as exceptions.
- Do not create exceptions for events of undetermined importance
You may be tempted to categorize events of undetermined importance as exceptions. If you do not know the importance of events you are monitoring, do not categorize these events but continue monitoring and manually correlating these events until you can make a determination.

Defining incidents and exceptions

Use the New Incident/Exception window to define the types of events and SecurityFusion module attack patterns that you want SiteProtector to handle as incidents or as exceptions.

About this task

Note: For incidents or for exceptions that involve SecurityFusion module attack patterns, you can modify only the values in the **Name** and **Description** fields.

Procedure

1. Select an event in an **Analysis** tab, and then click **Action > Incidents/Exceptions > New**.
2. Select **Incident** or select **Exception** for the **Category**, and then complete the following fields as applicable:

Field	Description
Ignore these events in SecurityFusion attack patterns	Whether to exclude the events you specify for this incident or exception from SecurityFusion module attack patterns
Name	A unique name to help you identify this incident or exception
(Optional) Description	A brief description to help you remember the purpose of this incident or exception
Time	The Start and End times and dates for the period of time that you want this incident or exception to be in effect Tip: If you want to change the time and the date, change the time first. Note: Leave the End field empty if you want the incident or exception to remain in effect indefinitely.
Source IP	The range of source IP addresses for which you want the incident or exception to apply. If there is only one IP address, type it in both boxes. Note: You must specify either a source or a target IP address.
Target IP	The range of target IP addresses for which you want the incident or exception to apply Note: You must specify either a source or a target IP address.
Tag Name	The name by which the event to include in the incident or exception is known in the X-Force
Object Name	The types of objects—such as File, Registry Key, or User Group—to include in this incident or exception Tip: The complete list of objects is defined for Object Type in Advanced Filters.

Field	Description
Observance Type	The types of observances—such as Incomplete data, Intrusion detection, or vulnerability—to include in this incident or exception Tip: The complete list of observances is defined in the Observance Type filter.

3. Click **OK**.

Editing incidents and exceptions

Use the Manage Incident/Exception window to edit an incident or exception.

Procedure

1. Select **Action > Incident/Exception > Manage**.
2. In the Incidents/Exceptions area, select the check boxes for the types of incidents and exceptions you want to appear in the list, and then click **Load**.
3. Select the incident or exception you want to edit, and then click **Edit**.
4. Edit the following items as necessary:
 - **Name**
 - **Description**
 - **Source IP Address**
 - **Target IP Address**
 - **Tag Name**
 - **Object Name**
 - **Observance Type**

Note: If you are editing an incident or exception involving attack patterns, you can modify the values only in the **Name** and **Description** boxes.

5. Click **OK**.

Deleting incidents and exceptions

Use the Manage Incident/Exception window to delete an incident or exception

Procedure

1. Select **Action > Incident/Exception > Manage**.
2. In the Incidents/Exceptions area, select the check boxes for the types of incidents and exceptions you want to appear in the list, and then click **Load**.
3. In the Manage Incident/Exception window, select the incident or exception you want to delete, and then click **Delete**. A confirmation window appears.
4. Click **Yes** to delete the incident or exception.
5. Click **OK**.

Chapter 7. Is Suspicious Activity Significant?

To detect suspicious activity efficiently, you must rule out activity that is not significant and do this early in the detection process. This approach helps you filter unimportant events and focus on attacks that are significant. This chapter primarily addresses ruling out suspicious activity that is caused by the following:

- unauthorized activity that according to your security policy does not require an in-depth investigation or response
- authorized or normal activity that appears suspicious but is actually harmless

Quick reference for tasks covered in this chapter

The following table provides a quick reference for tasks that are covered in this chapter. Use this table to help you choose the topic or topics that correspond to specific problems:

If you....	And...	Then...
know when authorized scans are scheduled to run	the SecurityFusion Module is not enabled	before the scan is scheduled to run, create an exception that filters the scan activity from the Console. See “Creating exceptions to filter scan activity” on page 58.
do not know when authorized scans are scheduled to run but suspect that an Internet Scanner scan is running	the SecurityFusion Module is enabled	view Internet Scanner incidents in the Event Analysis-Incidents view. See “Filtering authorized scans using attack patterns” on page 57.
	the SecurityFusion Module is not enabled	identify the authorized scan by analyzing the event details, and then create an exception that filters the activity from your Console. See the following topics: <ul style="list-style-type: none">• “Identifying activity caused by vulnerability scans” on page 56• “Creating exceptions to filter scan activity” on page 58
do not know when authorized scans are scheduled to run but you suspect that a third party scan is running		identify the authorized scan by analyzing the event details, and then create an exception that filters the activity from your Console. See the following topics: <ul style="list-style-type: none">• “Identifying activity caused by vulnerability scans” on page 56• “Creating exceptions to filter scan activity” on page 58
suspect that activity is caused by a misconfigured system		see “Identifying activity caused by misconfigured systems” on page 58.
suspect that activity is caused by authorized activity that is commonly identified as suspicious		See “Identifying normal activity commonly identified as suspicious” on page 59

Identifying the location of an attack

Attack location is the first thing you should consider when you are determining the significance of an attack. Suspicious activity at your Internet firewall is less significant than an attacker who has gained access to your Accounting file server. This topic provides a procedure for identifying an attack location using the Event Analysis - Agent view.

Significance of attack location

The location of the sensor that detected the activity can tell you the general vicinity of an attack. Typically, suspicious activity that is detected outside your network is frequent enough that it cannot be monitored successfully. For example, events that are detected by agents located in your internal network may require more attention than events detected by agents located outside your firewall.

Analyzing the Event Analysis - Agent view

Procedure

1. Select **Analysis** from the **Go to** list.
2. Select the **Event Analysis - Event Name** view.
3. Right-click the event that you are investigating, and then select **Which agents detected this event?** from the menu.

Note: This question is not limited to the Event Name view. This guided question is available in all the Event Analysis views except the **Event Analysis - Agent view**.

4. View the Agent IP and the DNS Name columns to determine where the agent is located in your network.

Note: If the agent that detected this event is located outside your network, in your DMZ, or in a location that you have determined is not vulnerable, consider limiting the time and effort that is directed toward monitoring and tracking this activity.

What to do next

Reference: You can also use guided questions to inquire about vulnerability events. See “Selecting guided questions” on page 12.

Identifying activity caused by vulnerability scans

Important information about vulnerability scans that are running or scheduled to run on your network may not be communicated in a timely fashion to the departments that are affected. If you know or suspect that a vulnerability scan is running on your network, use the information in this topic to help you identify this activity.

Importance of communication and planning

Communication and planning are important in helping you avoid false alarms caused by unexpected vulnerability scans. Maintain close communication with the personnel that perform vulnerability scans on your network so that these scans do not come as a surprise to you.

Unauthorized vulnerability scans

Because vulnerability scans probe hosts similar to the way attackers do, you cannot always distinguish between authorized vulnerability scans and scans that are started by attackers. If you cannot confirm that a vulnerability scan is authorized, it is probably an attack.

Guidelines for identifying scans in the Console

A vulnerability scan may be in progress if you observe one or more of the following:

Note: Exercise caution when using these guidelines because the authorized scan activity is often very similar to attack activity.

- an excessive number of events associated with a single source and a large number of target hosts
- activity that progresses according to some logical internal pattern, such as functional areas or departments
- activity that triggers a wide range of signatures in a short time period

Filtering authorized scans using attack patterns

Authorized vulnerability scans can generate a large volume of suspicious traffic within a short time period. Typically, this traffic is correctly identified as suspicious but is not an attack. This topic provides background information and guidelines for using Internet_Scanner_Scan attack patterns to identify authorized vulnerability scans.

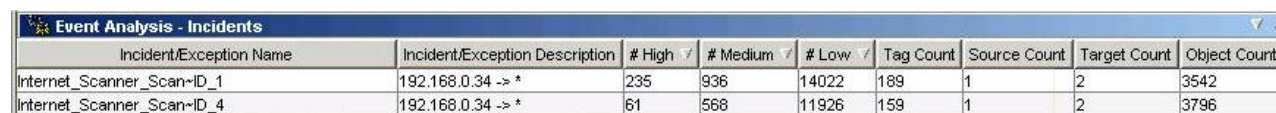
Important: The SecurityFusion Module must be enabled before you can use Internet_Scanner_Scan attack patterns. See “Section E: SecurityFusion Module Impact Analysis” on page 18 for more information.

How does an Internet_Scanner_Scan attack pattern work?

The Internet_Scanner_Scan attack pattern identifies initiation of an IBM Internet Scanner scan from a host followed by other events triggered by the same source host against one or more targeted hosts. Appropriately configured agents and appliances can trigger this attack pattern when they are monitoring a network over which scanning is performed. By default, the Internet_Scanner_Scan attack pattern automatically creates an incident for the events that match this pattern and continues to filter the events accordingly.

Example of Internet_Scanner_Scan attack patterns

The following figure shows two Internet_Scanner_Scan attack patterns in the Event Analysis - Incidents view. These incidents appear only when the SecurityFusion Module is enabled. Note the large event counts that are associated with a single source count (the scanning host) and two target counts (the hosts that are being scanned):



Incident/Exception Name	Incident/Exception Description	# High	# Medium	# Low	Tag Count	Source Count	Target Count	Object Count
Internet_Scanner_Scan-ID_1	192.168.0.34 -> *	235	936	14022	189	1	2	3542
Internet_Scanner_Scan-ID_4	192.168.0.34 -> *	61	568	11926	159	1	2	3796

Guidelines for using Internet_Scanner_Scan attack patterns

Use the following guidelines to analyze Internet_Scanner_Scan attack patterns:

- Attackers use scanners to perform reconnaissance and even begin attacks, so verify that an unauthorized user is not using IBM Internet Scanner to perform these types of scans.
- Because a one-to-one correspondence does not always exist between the scanning host and the target host, the SecurityFusion Module may create more than one incident for a single scan. Conversely, it may also create one incident for multiple scans.

Important: If you think that the SecurityFusion Module is not pairing hosts correctly, you should manually correlate scanning hosts with target hosts.

Creating exceptions to filter scan activity

After you know that a vulnerability scan is running or is scheduled to run on your network, consider creating an exception to filter this traffic from the Console. Use the guidelines and the procedure in this topic to help you create exceptions for filtering scan activity.

When to filter scans

Consider creating exceptions for vulnerability scans in the following situations:

- you or some one in your organization is using a third-party scanning tool (not IBM Internet Scanner) to scan your network
- SecurityFusion Module is not enabled

Important: Exceptions are not global; they apply only to the Console that creates the exception.

Guidelines for creating exceptions

Use the following guidelines to specify criteria for filtering scan activity:

- Use criteria that is unique to the scan so that you do not filter activity that is not related to the scan.
- When in doubt, narrow the scope of the activity you are filtering rather than expand it.
- Limit the target addresses of the scan to IP addresses inside the internal network.

Creating exceptions for filtering scans from the Console

Procedure

1. Perform the procedure in “Defining incidents and exceptions” on page 52.
2. Use the following table to specify information in the New Incidents/Exceptions window:

Field	Description
Start	Specify the time and date the scan is scheduled to begin.
End	Specify the time and date the scan is scheduled to end.
Source IP	Specify the IP address of the scanning host. This is the host where the scanning agent is installed.
Target IP	Specify the range of IP addresses that the scanning is scheduled to scan. Note: You may not be required to specify a Target IP for this exception if you specified a scanning agent in the Source IP field.

Identifying activity caused by misconfigured systems

Misconfigured systems can cause malfunctions and introduce vulnerabilities that are sometimes hard to detect and remediate, and it is not always clear whether the misconfiguration is an honest mistake or malicious. You can use information about misconfigured systems to help troubleshoot problems in your network and identify possible vulnerabilities.

Misconfigured systems

Systems can be misconfigured accidentally by employee misuse, or misconfigured due to poor design. Attackers can sometimes exploit misconfigured system to gain access. The following can cause misconfigurations in your network:

- new or updated software or hardware
- incompatible software or hardware

- systems that are accidentally misconfigured by employees
- backdoors created for legitimate maintenance reasons

Note: If an attacker misconfigures a system to gain access or cause harm, this is considered an attack, not a misconfigured system, and should be investigated.

Examples of events that are caused by misconfigured systems

Misconfigured systems can trigger certain events if the corresponding signatures are enabled in your policies. Use the following examples to help you identify misconfigured systems:

- Subnet masks

Legitimate hosts can sometimes reside on IP addresses that are typically used for broadcast addresses or subnet masks, such as 255.255.255.0. These hosts can sometimes trigger events that identify exploits that use broadcast addresses, such as denial of service attacks or Smurf attack.

- SMB authentication and share events

These events are caused by hosts that freely share data with other hosts or authenticate without requiring a password, or requiring a weak or easily guessable password. Although it is not a best practice, some administrators allow internal hosts to communicate this way. This activity can trigger events that detect host-to-host communication that is weak or out of compliance, such as the Smb_empty_password and Smb_guessable_password events.

- Routing errors

Administrators sometimes neglect to disable IP routing, which is enabled by default on hosts that run the Unix operating system. In most cases, these hosts are typically not configured properly and they can drop a significant number of packets.

Identifying normal activity commonly identified as suspicious

Agent and appliance policies contain hundreds of checks that identify everything from high to low severity activity. One of the biggest challenges in detecting suspicious activity is filtering normal activity that is identified as suspicious. This topic provides information that can help you filter this activity from the Console.

Why is normal activity sometimes identified as suspicious?

Normal activity is typically identified as suspicious if it exceeds certain predefined thresholds, if the protocol that the traffic uses is considered vulnerable, or if it triggers events that are primarily used for auditing purposes. While normal traffic is typically not malformed, it may be prohibited by your security policy or incompatible with the systems that are running in your network. Typically, normal traffic falls into the following categories:

- audit events
- false positives

Events that are typically identified as suspicious

The following table lists events that are typically identified as suspicious:

Important: This information is subject to change.

Events	Description
DHCP ^a	The DHCP protocol dynamically assigns IP addresses to hosts on your network. If this protocol is enabled in your environment, this traffic is probably legitimate.

Events	Description
ftp_*	Administrators use the FTP protocol to transfer files between network devices. This traffic is probably legitimate if it is allowed by your security policy.
http_*	The HTTP protocol is found extensively in networks where Internet traffic is allowed. This is probably legitimate if it is allowed by your security policy. However, if you have certain subnets where Internet traffic is restricted, such as engineering labs, you should monitor for HTTP traffic.
Lanman_share_enum	This event identifies hosts that are trying to enumerate shares on a specified target. If your security policy allows enumeration between hosts in your network, this traffic is probably legitimate.
netbios_session*	NetBIOS allows applications on different computers to communicate within a local area network. This lower layer protocol is used by almost all devices that use the Windows operating system.
Nntp_*	NNTP is a protocol that allows users to post, distribute, and read Usenet messages. This traffic is probably legitimate if it is allowed by your security policy.
Ospf_*	OSPF is a routing protocol that routers use to communicate with other routers. This traffic is probably legitimate if routers on your network are configured to use this protocol.
Smb_*	SMB is a host-to-host communication protocol that allows hosts to access and share information with other hosts. While attackers can use this protocol for reconnaissance, it is probably legitimate if it is allowed by your security policy.
Snmp_community Snmp_activity	SNMP is a network management protocol that allows administrators to remotely monitor and troubleshoot network devices. This traffic is probably legitimate if it is allowed by your security policy.
Tcp_probe_xwindows	X Windows System is a graphical interface protocol that is installed with earlier versions of Windows that allows devices to communicate in distributed environments. This traffic is probably legitimate if it is allowed by your security policy.

a. These events refer to all events in a particular category of signatures.

Chapter 8. Is an Attack a Threat?

After you determine that suspicious activity is an attack, you should decide whether the activity is a threat to your network. This chapter provides information about using the SecurityFusion Module and other SiteProtector system tools to assess whether an attack is a threat.

Combining the SecurityFusion Module and other SiteProtector system tools

SecurityFusion Module information may not always be conclusive, although it can provide a significant amount of data about an attack. Consider combining SecurityFusion Module statuses with other information that is provided in the SiteProtector system analysis views.

Section A: Using the SecurityFusion Module to Assess an Attack

An event's SecurityFusion status is an important factor in determining whether an attack poses a significant threat. This is because it can provide information about several key areas of your investigation that you would otherwise have to gather manually.

Impact analysis

The SecurityFusion Module uses a process called *impact analysis* to determine whether an attack from a single event has succeeded. When an intrusion detection sensor detects an attack, the Module correlates the attack with information about the host—such as operating system, vulnerabilities, and responses taken by host agents—to determine the success or failure of the attack. The Module reports the result of impact analysis as a status that appears in the SiteProtector system.

Topic

“Viewing attack statuses”

Viewing attack statuses

Attack statuses can provide valuable information about an attack. This topic provides information about viewing attack statuses in the SiteProtector System.

Agents and appliances that provide impact analysis

Only certain agents can provide impact analysis information to the SiteProtector system. The following agents and appliances can be configured to provide attack statuses to the SiteProtector system:

- Proventia Network Multi-Function Security (MFS) appliances
- IBM Security Network Intrusion Prevention System (IPS) appliances
- IBM Security Server Protection

Attack statuses

The status of a correlated event describes the impact of an attack or other security event. These statuses appear in the Analysis views when the Status, Reason, and Description columns are enabled. The SecurityFusion module derives the impact by correlating events with vulnerability assessment data and other host information about targeted hosts. The following table describes vulnerability statuses for intrusion detection events from highest to lowest priority:

Status	Reason	Description
Attack Successful	Confirmed by agent	The agent that detected the event determined that the attack was successful.
	File accessed	The agent that detected the event determined that files on the target host were accessed.
Successful attack likely	Vulnerable	A vulnerability assessment scan indicates that the host was vulnerable to this attack, so the attack was probably successful.
Attack detected	No correlation	The impact of the event is unknown because no host data (vulnerability or operating system) corresponds to this event. These events could be audit events, such as "login successful," status events from sensors, or, in some cases, events that SecurityFusion does not correlate.
	SecurityFusion not configured for this host	The SecurityFusion module is not enabled for this Site or for this host.
	SecurityFusion not licensed	Neither the source nor the destination host is licensed for SecurityFusion correlation.
	Vuln not scanned recently	For one of the following reasons, no vulnerability or other host data is available to determine the impact of the attack: <ul style="list-style-type: none"> • This status supersedes other potentially applicable statuses, such as no correlation or not scanned recently. • The host has never been scanned. • The scan data for the host has passed the user-defined expiration date.
	OS check indeterminate	The impact of the attack is unknown because the vulnerability assessment scan could not determine the operating system of the target.
	Simulated block response not enabled	The simulated block response was not configured on the agent that detected this attack.
	Block response not enabled	The block response was not configured on the agent that detected this attack.

Status	Reason	Description
Vulnerable	Attack will be detected and prevented	The scanning agent determined that the target host is vulnerable; however, the agent that is configured to monitor this traffic will block attacks that exploit this vulnerability.
	Attack will be detected and partly blocked	The scanning agent determined that the target host is vulnerable; however, the agent that is configured to monitor this traffic will partly block attacks that exploit this vulnerability.
	Attack will be detected	The scanning agent determined that the target host is vulnerable; however, the agent that is configured to monitor this traffic will detect attacks that exploit this vulnerability.
	Attack will not be detected	The scanning agent determined that the target host is vulnerable; however, the agent that is configured to monitor this traffic will not detect attacks that exploit this vulnerability.
Not Vulnerable	Not applicable	The agent determined that the host was not vulnerable to the attack.
Vuln check indeterminate	Not applicable	The vulnerability status is unknown because the vulnerability assessment scan could not determine whether the target host is vulnerable.
Failure possible	Scanned, vuln not confirmed	IBM Internet Scanner ran the correlating vulnerability check against the target, but the target did not confirm whether the vulnerability exists.

Status	Reason	Description
Attack failure	No vulnerability	A vulnerability assessment scan indicates that the host was not vulnerable to this attack, so the attack probably failed.
	Rolled-back change	A sensor detected an unauthorized change to a protected system object—such as to a registry key or to a share—and reverted the object to its prior state.
	Wrong OS	The host is running an operating system that is not susceptible to this attack.
	Connection reset	The agent or firewall reset the attacker's connection.
	Process terminated	The target process or service was terminated.
	File not accessed	The attacker was not able to access the file on the target host.
	Port not open	The target ports were not open on the target host or firewall.
	Blocked at host	The attack failed because the sensor or agent protecting the host blocked the attack.
	Dynamically blocked at host	The attack failed because the agent protecting the host dynamically blocked the attack.
Failed attack	Blocked by Proventia® or IBM Security appliance	The attack failed because the appliance protecting the host in inline protection mode blocked the attack.
	Attacker quarantined by Proventia or IBM Security appliance	The attack failed because the appliance protecting the host quarantined the attack.
Simulated block	Proventia or IBM Security appliance in simulation mode	An attack was not blocked by an appliance because the appliance was in simulation mode. The appliance would have blocked the attack if it had been in protection mode.
	Protection not enabled	An attack was not blocked by an appliance because protection was not enabled on the appliance.

Status	Reason	Description
Not Compliant	Application access blocked	The agent determined that the host attempting to access the network was not compliant and the host was blocked from accessing applications.
	Corporate access blocked	The agent determined that the host attempting to access the network was not compliant and the host was blocked from accessing the corporate network.
	Network access blocked	The agent determined that the host attempting to access the network was not compliant and the host was blocked from accessing the network.

Viewing the attack status for an event or group of events

This topic describes how to view the attack status for an event or group of events.

Procedure

1. Select **Analysis** from the **Go to** list.
2. Open an **Event Analysis** view that contains the **Status** column.
3. Display the events for a group of assets, and then do the following:

To find...	Look for these statuses in the Status column:
likely successful attacks	Success likely (target vulnerable)
possibly successful attacks	Unknown impact (SecurityFusion not licensed) Failure possible (scanned, vulnerability not confirmed) Unknown impact (no correlation) Unknown impact (OS check indeterminate)
failed and likely failed attacks	Failed attack (blocked at host) Failed attack (blocked by Proventia appliance) Failure likely (no vulnerability) Failure likely (rolled-back change) Failure likely (wrong OS)
problems that prevent correlation	Unknown impact (SecurityFusion not enabled) Unknown impact (not scanned recently)

Section B: Assessing an Attack Manually



















If the SecurityFusion Module is not enabled or impact analysis data provided by the Module is inconclusive, you can use other analysis tools to assess an attack's threat level. Use this section to help you use other SiteProtector system analysis tools to determine whether an attack is a threat.

Determining the X-Force risk level of an attack

The X-Force risk levels provide a quick way for you to determine the severity of an attack without analyzing the details of an event. Use the X-Force risk levels to help you determine whether an attack is a threat.

How to view X-Force risk levels on the Console

X-Force provides a severity level for each event that appears on the Console. The risk level (high, medium, or low) appears in the Severity column of the Analysis views, as follows:

Severity	Event Count	Source Count	T
 Medium	20	1	1
 Medium	20	1	1
 Medium	1	1	1
 Low	16	1	1
 Low	9	7	1
 Low	1	1	1
 Medium	1	1	1
 Medium	1	1	1
 Medium	1	1	1
 Medium	1	1	1
 Low	24	1	1
 Low	8	1	1
 Low	4	1	1
 Low	2	1	1
 Low	2	1	1
 Low	1	1	1
 Low	1	1	1
 High	37	1	1

X-Force risk levels

X-Force assigns risk levels to describe the extent of damage that can be caused by a security issue. The possible risk levels are as follows:

Risk Level	Description
High	Security issues that allow immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges. Examples are most buffer overflows, backdoors, default or no password, and bypassing security on firewalls or other network components.
Medium	Security issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components. Examples are cross-site scripting, man-in-the-middle attacks, SQL injection, denial of service of major applications, and denial of service resulting in system information disclosure (such as core files).
Low	Security issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access. Examples are brute force attacks, non-system information disclosure (configurations, paths, etc.), and denial of service attacks.

Was the attack target vulnerable?

If the target host is not vulnerable, then the attack is probably not a threat. Use the information in this topic to help you determine whether a target host is vulnerable.

Guidelines for determining whether a target is vulnerable

Use the following guidelines to scan an attacked host:

- If you know the specific exploit the attacker is using, and you can run this exploit, then run the exploit from the Console computer.
- If you do not know the specific exploit the attacker is using, then scan the host using an IBM Internet Scanner or IBM Proventia Network Enterprise Scanner policy that has the following checks enabled:
 - Windows: DCOM, LSASS, ASN, and null sessions
 - Unix: default community string for router software, open nfs mounts, and common buffer overflows
- If you know the specific exploit the attacker is using, then scan using an IBM Internet Scanner or Proventia Network Enterprise Scanner policy with only the check or checks that correspond to the exploit the attacker is using.
- Search previous scan data of the target host in which an IBM Internet Scanner or Proventia Network Enterprise Scanner L5 policy was applied.

Running scans against attack targets using IBM Internet Scanner

Use the Remote Scan window to run a vulnerability scan against an attack target for specific exploits using IBM Internet Scanner.

Procedure

1. Select **Asset** from the **Go to** list.
2. Right-click the asset, and then select **Scan** from the pop-up menu. The Remote Scan window appears.
3. Select **Internet Scanner**.
4. Select the scanner you want to use from the **Agent Name** list.
5. In the left pane, select the **Scan Policy** icon.
6. Do you know the exploit the attacker is using?
 - If *yes*, right-click a blank policy from the list in the right pane, select **Derive from new** from the pop-up menu, and then go to Step 7.
 - If *no*, select the IBM Internet Scanner policy that you want to use in the **Policy** box, and then go to Step 9.
7. Type the name of the new policy in the Derive New window. The policy you selected opens in the policy editor.
8. Select the check or checks that correspond to the exploit, and then save the policy.
9. Select the Scan Session icon in the left pane, and then select the session that you want to use with this scan from the list in the right pane.
10. Click **OK**.
11. When the scan is complete, right-click the host in the **Asset** view, and then select **What are the known vulnerabilities** from the menu. The vulnerabilities found on the host appear in the **Vuln Analysis - Vuln Name** view.

Running an ad hoc assessment scan

Use Proventia Network Enterprise Scanner to run an ad hoc assessment scan of an entire group of assets or of one or more selected assets.

Procedure

1. In an **Asset** tab, do one of the following:
 - Select a group in the left pane.
 - Select one or more assets in the right pane.
2. Right-click the group or the assets to scan, and then select **Scan**.

Note: If given a choice of IBM Internet Scanner or Proventia Network Enterprise Scanner, select **Enterprise Scanner**.

3. Click the **Adhoc Scan Control** icon.
4. In the **Ad Hoc Assessment** section, select the **Perform one-time discovery scan of this group** check box.
5. Type a **Job name** to identify the job when it appears in the Command Jobs window.
6. If you want the scan to run only during your scheduled scanning windows, select the **Run only during open discovery windows** check box.
7. Click **Assessment** in the left pane.
8. Configure the policy the same way as you would configure the background Assessment policy.
9. Click **OK**. The ad hoc assessment scan appears in the Command Jobs window.

Running an ad hoc discovery scan

If you want to run a one-time scan that uses ranges of IP addresses to discover devices running on your network, you can configure an ad hoc discovery scan from the IBM Proventia Network Enterprise Scanner agent.

Procedure

1. On the SiteProtector navigation pane, set up a tab with any view except for a Policy view.
2. Expand the Site to see the group you want to scan.
3. Right-click the group to scan; if given a choice of IBM Internet Scanner or IBM Proventia Network Enterprise Scanner, select **Enterprise Scanner**; and then select **Scan** from the pop-up menu.
4. In the **Ad Hoc Discovery** section, select the **Perform one-time discovery scan of this group** check box.
5. Type a **Job name** to identify the job when it appears in the Command Jobs window.
6. If you want the scan to run only during your scheduled scanning windows, select the **Run only during open discovery windows**.
7. Click **Discovery** in the left pane.
8. Type the range, or ranges, of IP addresses to scan in the **IP range(s) to scan** box.
9. Type the IP addresses (in dotted-decimal or CIDR notation) of the assets to exclude in the **IP range(s) to scan** box as follows:
 - Type an IP address, and then press **ENTER**.
 - Type a range of IP addresses, and then press **ENTER**.

Example: 172.1.1.100-172.1.1.200

- Type a series of individual IP addresses and/or ranges of addresses separated by commas.

Note: A red box appears around the **IP range(s) to scan** box until the data is validated.

10. If you want to add newly discovered assets to the group where you have defined the scan—rather than to the Ungrouped Assets group, select the **Add newly discovered assets to group** check box.
11. If you want to add previously known assets (that are not in the group) to the group, select the **Add previously known assets to group** check box.
12. Click **OK**. The ad hoc discovery scan appears in the Command Jobs window.

Was the target service or operating system susceptible?

Even if unauthorized activity is malicious, the target operating system that it is trying to exploit may not be susceptible. Use the information in this topic to help you view security information about the exploit and the targeted asset so that you can determine whether the asset is susceptible.

Task overview

This topic contains the following tasks:

Task	Description
1	Access security information about an event.
2	Determine the operating system running on the target host.
3	Determine the services targeted by the attack

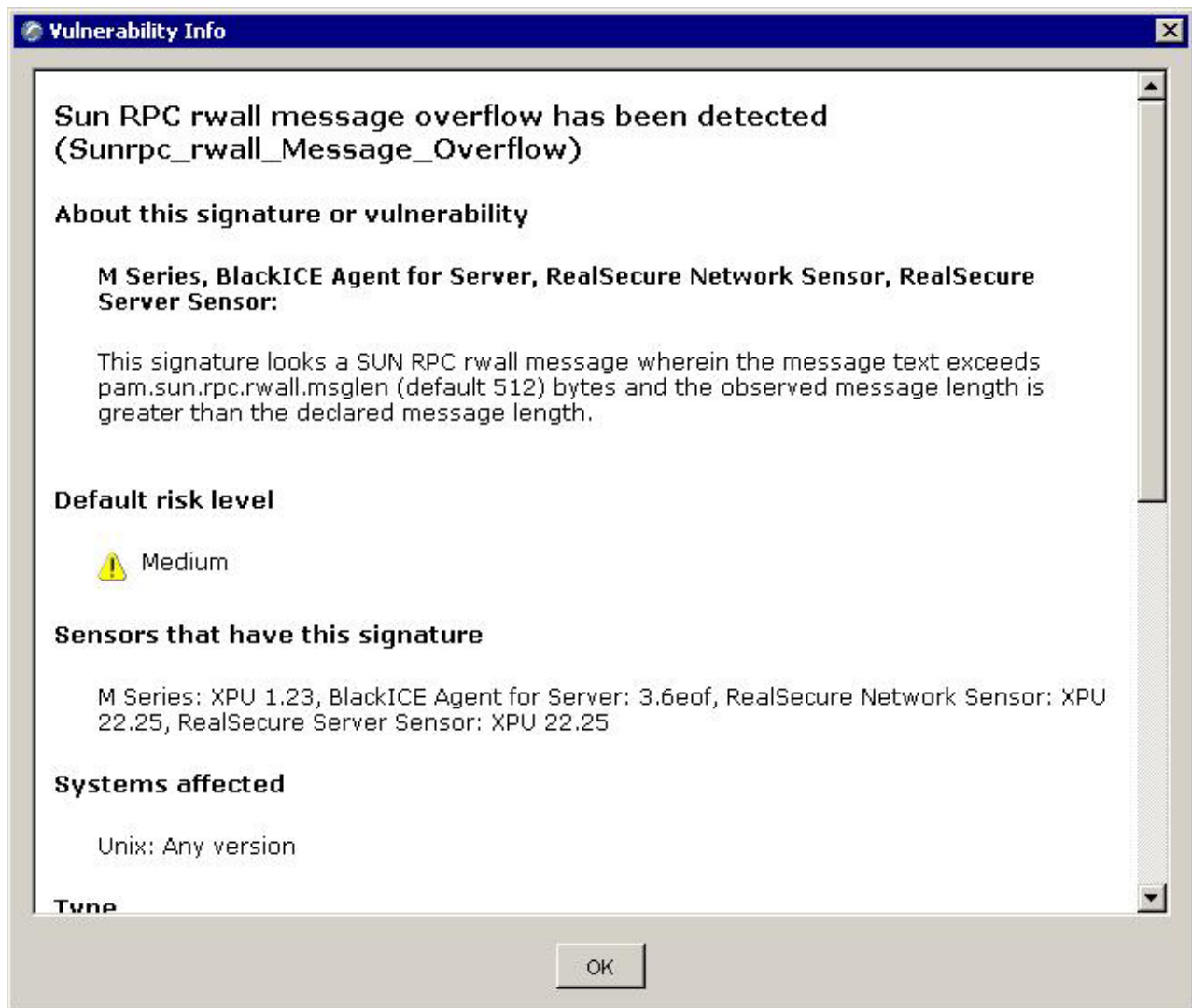
Information about a service or operating system

The completeness of vulnerability data can determine how accurate and detailed information about a target is. For example, detailed information about services running on a host or operating system version may not be available if the target has not been scanned using a policy that checks for this information.

Note: If the target host has not been scanned recently, consider running an ad hoc scan against the target. See “Was the attack target vulnerable?” on page 66.

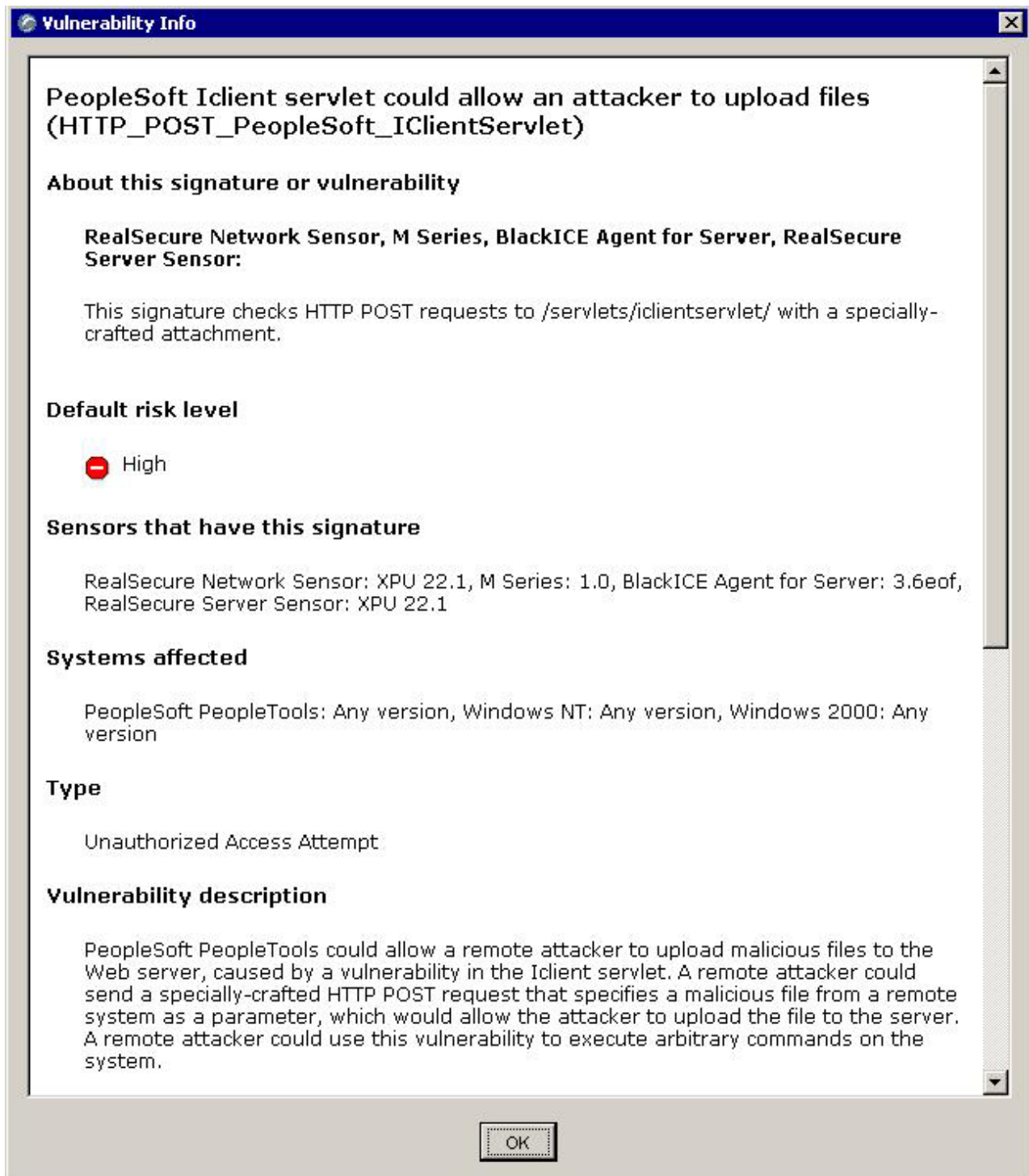
Operating system susceptibility

The following figure shows security information for the Sun RPC rwall message overflow. Note that Unix is the only operating system listed under Systems affected. A Windows host is not susceptible to being attacked by this exploit:



Service susceptibility

The following figure shows security information for the PeopleSoft Iclient servlet. Note that PeopleSoft is the only service that is affected by this exploit:



Accessing security information about an event

Procedure

In the **Event Analysis** view, right-click an event, and then select **Open Event Details** from the pop-up menu.

Security information about the event you selected appears in the right pane.

Determining the operating system of a target asset

This topic describes how to determine the operating system of assets that are targeted by an attack.

Procedure

1. Select **Analysis** from the **Go to** list.
2. Select the **Event Analysis - Event Name** view, right-click the event you want to inquire about, and then select **What are the targets of this event?** The **Event Analysis - Target view** appears that lists one or more IP addresses that are targets of the attack.
3. Select the **Event Analysis - OS** view.

Note: If the SiteProtector system cannot determine the operating system of the selected asset, "Unrecognized OS" appears in the **Target OS** column.

A list of target operating systems appears.

Determining the service that is targeted

This topic describes how to use guided questions to determine the service that is targeted by an attack.

Procedure

1. Select **Analysis** from the **Go to** list.
2. Select the **Event Analysis - Event Name** view, right-click the event you want to inquire about, and then select **What are the targets of this event?** The **Event Analysis - Target view** appears that lists one or more IP addresses that are targets of the attack.
3. Right-click the IP address that you want to inquire about, then select **What objects were targeted on this asset?**

Note: Service information only appears in the **Target Object** and **Object Name** columns if the agent detected and it can report this information to the SiteProtector system. Other information that does not relate to service may also appear in these columns.

If a service was identified by the agent that detected the attack, information about this service appears in the **Target Object** and **Object Name** columns of the **Event Analysis - Target Object** view.

Chapter 9. Tracking and Prioritizing Confirmed Attacks

After you determine that a confirmed attack is a threat to your enterprise, you should start an investigation and begin to track this threat. This chapter contains guidelines and procedures for managing tickets and for exporting incident information to a ticket.

Tickets

A ticket is typically an event that, according to your security policy, requires that you begin an investigation. Typically, you should create a ticket for any confirmed attack that poses a threat to your organization. Tickets are different from the incidents that you create in the Incident/Exception window.

Remedy Action Request System

You can also configure the SiteProtector system to export tickets into the Remedy Action Request System third-party ticketing tool. The Remedy tool lets you add user-defined fields to the ticket. Use the user-defined fields in the Remedy tool to associate additional information with a ticket.

Guidelines for establishing ticket priority

When you create a ticket, you should prioritize the ticket according to the scope and impact of the attack. The priority of a ticket determines the manner in which you conduct your investigation and respond to threats. Use the guidelines in this topic to help you specify a ticket's priority.

Important: The information that you collect before you begin an investigation may be insufficient to fully determine the priority of a ticket. In most cases, you may need to change the priority level as you learn more about the activity.

How to determine the priority of a ticket

Use the guidelines in the following table to specify a value in the Priority box on the Ticketing Setup window. The activity in the table appears from most severe to least severe. Depending on your environment, some or all of these categories may not apply:

Suggested Priority Level	Characteristics
1 (Critical)	<ul style="list-style-type: none">• successful penetration or denial of service attacks detected with significant impact on organization<ul style="list-style-type: none">– very successful, difficult to control or counteract– large number of systems compromised– significant loss of confidential data– loss of critical systems or applications• significant risk of negative financial or public relations impact• significant systems degradation/loss due to a virus or worm outbreak that is not handled by installed antivirus software• a verified widespread attack

Suggested Priority Level	Characteristics
2 (High)	<ul style="list-style-type: none"> • penetration or denial of service attack or attacks detected with limited impact on organization • minimally successful, easy to control or counteract <ul style="list-style-type: none"> – small number of systems compromised – little or no loss of confidential data – no loss of critical systems or applications • widespread instances of a known computer virus or worm that cannot be handled by deployed antivirus software • small risk of negative financial or public relations impact • a verified attack but limited to certain assets
3 (Medium)	<ul style="list-style-type: none"> • significant level of network probes, scans, and similar activities detected indicating a pattern of concentrated reconnaissance • penetration or denial of service attack(s) attempted with no impact to your organization • widespread instances of a known computer virus or worm, easily handled by deployed antivirus software • isolated instances of a new computer virus or worm that cannot be handled by deployed antivirus software • increased risk of attack to limited number of assets

Creating tickets

This topic describes how to create tickets in the SiteProtector System.

The SiteProtector System lets you create tickets, associate tickets with events, agents, and assets, and track the status of the ticket.

Ticket types

The following table describes the types of tickets you can create in the SiteProtector System:

Ticket	Description
Event	Use event tickets when you are investigating an event or a group of events. You create event tickets in the Analysis view.
Asset	Use asset tickets when a particular asset is the target or source of an attack or has been compromised. You create asset tickets in the Asset view.
Agent	Use agent tickets when an agent is the target or source of an attack or requires maintenance or support. You create agent tickets in the Agent view.

Vulnerability auto ticketing

You can set up vulnerability auto ticketing so that the SiteProtector System automatically generates tickets for vulnerable events discovered in a vulnerability assessment scan.

At the group level, you define vulnerability auto ticketing rules to specify the criteria by which SiteProtector generates auto tickets. As part of each rule, you also can configure the ticket priority and the person responsible for addressing the ticket.

Note: Vulnerability Auto Ticketing works for vulnerable events identified by either IBM Proventia Network Enterprise Scanner or IBM Internet Scanner.

Reference: Refer to the *IBM Security SiteProtector System Configuration Guide* for more information about vulnerability auto ticketing.

Remedy users

Remedy users can create tickets in the SiteProtector System, but they must track and manage tickets through Remedy.

Creating tickets

Use the New Ticket tab to create a new ticket in SiteProtector.

Procedure

1. Select **Agent**, **Asset**, or **Analysis** from the **Go to** list.
2. Select the agent, asset, or event, and then select **Object > New > Ticket**.

Note: After you create a ticket, you are not able to continue filtering the activity that is associated with the ticket from the Console.

3. Specify the following options:

Option	Description
Priority	Ticket priority level that categorizes tickets by the amount of time allocated to resolve the ticket Notes: <ul style="list-style-type: none">• SiteProtector creates the Due Date automatically based on the priority you select in this field.• You can change the priorities in the Priority tab on the Ticketing Setup window.
Responsibility	SiteProtector user who is responsible for handling the ticket Note: This field contains Administrators and users populated with Active Directory.
Due Date	SiteProtector creates the Due Date automatically based on the priority you select in the Priority field. If you want to change the due date, select a date by which the ticket must be closed. Note: If a ticket is not resolved by the Due Date, SiteProtector sends an email notification to the ticket's creator.
Category	Category for organizing tickets Note: This field is optional and defaults to the Default category. You can create custom categories in the Custom Category tab on the Ticketing Setup window.
Synopsis	Summary of the issue
Actions	Steps required to resolve the issue

4. Select the **Custom Category** icon, and then type values for any custom categories that apply.
5. Select **Action > Save All**. SiteProtector displays a message that the ticket is created, and provides the ticket ID number.
6. Click **OK** at the prompt to close the New Ticket tab.

Viewing tickets

You can view any tickets you created in the SiteProtector system in the Ticketing view.

If you are using the SiteProtector system native ticketing system, you can edit ticket details in the SiteProtector system. If you are using the Remedy Action Request System, you can view the tickets created in the SiteProtector system, but you must use Remedy to edit ticket details.

Columns in the Ticketing view

Use the Ticketing view to view information about tickets that you have created. The following table lists the columns that are displayed in the Ticketing view:

This Item...	Shows the following...
Ticket ID	A unique identification number associated with the ticket. This number is generated when the ticket is created.
Synopsis	A brief description of the ticket.
Responsibility	The user responsible for handling the ticket.
Time Stamp	The time and date the ticket was created.
Revision ID	Current revision number for the ticket.
Responsibility	The user who is responsible for handling the ticket.
Due Date	Date by which the responsible party must handle the ticket.
Category	The category assigned to the ticket.
Status	The ticket's current status.
Priority	The priority of the ticket.
Creator	The user who created the ticket.

Viewing and editing tickets

Use the Ticket view to view and edit tickets in SiteProtector. If you are using the SiteProtector native ticketing system, you can edit ticket details in SiteProtector. If you are using a third-party ticketing system (such as Remedy), you can view the tickets created in SiteProtector, but you must use the third-party ticketing system to edit tickets.

Procedure

1. Select the group or Site for which you want to view tickets.
2. Select **Ticket** from the **Go to** list.
3. Select the ticket you want to view and select **Object > Open**. The Ticket Detail window appears.

Note: You can also double-click a ticket or a ticket revision at the bottom of the window to view ticket details.

4. Edit the following fields as necessary:

Option	Description
Priority	Specifies the ticket priority level that categorizes tickets by the amount of time allocated to resolve the ticket Notes: <ul style="list-style-type: none">• SiteProtector creates the Due Date automatically based on the priority in this field.• You can change the priorities in the Priority tab on the Ticketing Setup window.
Responsibility	Specifies the SiteProtector user who is responsible for handling the ticket Note: This field contains Administrators and users populated with Active Directory.
Due Date	SiteProtector creates the Due Date automatically based on the priority you select in the Priority field. If you want to change the due date, select a date by which the ticket must be closed. Note: If a ticket is not resolved by the Due Date, SiteProtector sends an email notification to the ticket's creator.
Status	Specifies the level of progress made toward resolving the ticket
Synopsis	Summary of the issue

Option	Description
Actions	Specifies the actions taken to resolve the ticket Tip: Include the dates of the actions taken to help create an action history for the ticket.

5. Select **Action > Save All**. SiteProtector saves the ticket and modifies the RevisionID field.
6. Click **OK**.

What to do next

Note: To view and modify multiple tickets in the Ticket view, press **Shift** and select the tickets you want to modify. Then double-click the selected tickets and modify the fields as necessary. The changes you make to the fields affect all the selected tickets.

Chapter 10. Determining the Scope of Attack

After you determine that an attack is a threat, you should determine the scope of the attack. This chapter introduces concepts and procedures that can help you identify high level indicators of attack scope.

Attack scope

Attack scope refers to the number of systems or applications affected by an incident, the number of attempts by the intruder to access the system or application, or the degree of penetration the attacker has achieved. An attack's scope can provide clues about the skill of the attacker, possible strategies you can use to defend against the attacker, and the degree and promptness of your response.

Attack scope

An attack's scope can provide clues about the skill of the attacker, possible strategies you can use to defend against the attacker, or strategies you can use to defend against future attacks that are similar. The attack scope can also help you assess the degree and promptness of your response. Use the information in this topic to help you determine the degree to which this attack has affected your network.

Attack scope

Attack scope refers to the number of systems or applications affected by an incident, or to the number of attempts by the intruder to access the system or application.

Degree of penetration

An attacker's degree of penetration into your internal network can indicate the level of privileged access the attacker has obtained and the assets the attacker has gained control of. If an attacker has compromised a firewall or has accessed internal file servers, then the attacker has deeply penetrated your network and probably has already obtained confidential information or done considerable damage to assets.

Number of platforms or hosts targeted

Platform scope refers to the diversity of platforms the attacker is targeting. If the attacker is targeting Windows, UNIX, and mainframe platforms, then the attacker is increasing the chances that he will successfully compromise a host.

Sophistication of exploits that are deployed

If the attacker has an overall strategy that he or she is deploying, then the attacker is increasing the chances he will successfully compromise a host. Coordinated attacks and slow and grow attacks are can be highly sophisticated. The strategies deployed in an attack can be a good indicator of the attacker's skill and his or her potential to do more damage in the future.

Goals of typical attackers

Understanding why an attacker is attacking your network can help you to determine the severity of an attack and the lengths to which an attacker may go to compromise your network.

Use the definitions in this topic to help familiarize yourself with the goals of a typical attacker, as follows:

- theft

- vandalism

Theft

The type of theft depends on the assets the attacker wants to acquire:

Asset	Description
System resources	An attacker may want to acquire system resources to attack other hosts and acquire bandwidth or memory that he or she can profit from illegally. In most cases, whether intentionally or not, the attacker may also compromise the confidentiality and integrity of information that resides on these systems.
Confidential information	An attacker may want to acquire confidential information that he or she can profit from illegally, such as trade secrets, payroll data, and bank account numbers. While accessing confidential information, the attacker may also compromise the integrity of this information even if he or she does not intend to acquire it.

Vandalism

Vandalism is the process by which an attacker breaches security for the thrill of it or to cause harm to company. Sabotage is the process by which an attack breaches security to undermine a company's credibility, disable its operations, or force it out of business.

Viewing the number of assets targeted by an attacker

Use the Event Analysis - Event Name view to identify the number of hosts the attacker is targeting.

About this task

The number of assets the attacker is targeting is a good indicator of the topological scope of the attack. For example, if you see high target counts in groups that contain critical assets, this may indicate that an attacker has circumvented several layers of security controls.

Reference: For an illustration and additional guidelines for using the Event Name view, see "Event Name view" on page 45.

Procedure

1. In the left pane, select the entire Site, or the group that includes hosts that are likely targets of the attack you are investigating.

Note: If you grouped your assets by criticality, consider viewing your groups from most critical to least critical.
2. Select **Analysis** from the **Go to** list.
3. Select the **Event Analysis - Event Name** view from the list.
4. Sort the **Target Count** column from highest to lowest.
5. In the **Severity** column, view the severity level of the **Tag Names** that are associated with the highest target counts.
6. Right-click an event with a high target count, and then select the **What agents detected this event?** from the pop-up menu.

Note: Use the **Agent IP Address** column to determine the location of the assets with the highest target counts. If you know where each agent is located, this information can help you understand the extent to which the attacker has penetrated the network.

The **Event Analysis - Agent** view appears.

Viewing the number of platforms targeted by an attacker

Use the information in this topic to customize the Event Analysis - Attacker view so that you can view the platforms that are targeted by an attacker.

About this task

The number of platforms the attacker is targeting is a good indicator of the attacker's skill. For example, if the attacker is targeting Windows, Unix, and mainframe platforms, the attacker probably has a variety of exploits at his or her disposal as well as the skills and knowledge to implement these exploits successfully.

Reference: See “Attacker view” on page 47 for a description and illustration of the Attacker view.

Procedure

1. In the left pane, select the entire Site, or the group that includes assets that are likely targets of the attack you are investigating.

Note: If you grouped your assets by criticality, consider viewing your groups from most critical to least critical.

2. Select **Analysis** from the **Go to** list.
3. Select the **Event Analysis - Attacker** view from the list.
4. Select **View > Add/Remove Columns** The Advanced Filter window appears.
5. Select **Show Columns** in the left pane.
6. Select the following from the **Available** column, and then click **Add** to move them to the **Displayed** column:
 - **Target OS**
 - **Status**
7. Select the **Target OS** column in the left pane, and then drag it to the immediate right of the **Source** column.
8. Add the **Status** column, and then move it to the immediate right of the **Target OS** column.
9. Click **View > Save** to save the customized view.

Notices

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

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

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

IBM Corporation
SiteProtector Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

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

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

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

Trademarks

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Other company, product, or service names may be trademarks or service marks of others.

Index

A

- abuse 42
- access control
 - inappropriate or weak 32
 - scanning with highest level of user access 38
 - vulnerabilities due to improper user activity 32
- action plan for vulnerabilities 34
- activity, authorized versus unauthorized 41
- ad hoc 28, 29
- ad hoc assessment scanning 67
- ad hoc discovery scanning 68
- add-on components, summary 6
- ADS
 - entity information 17
 - event details 17
 - traffic analysis 18
- agent, description 1
- analysis 10
 - events 9
 - export 13, 27, 28
 - filter 9
 - report 27
 - view 9
 - views 12
- Analysis
 - baseline 51
 - perspective 8
 - view 8
- Analysis tab
 - Analysis Views, custom 12
 - baselines 50
 - guided questions 12
 - navigating history 14
- Analysis Views
 - custom 12
- Anomaly Detection
 - entity information 17
 - event details 17
 - traffic analysis 18
- appliance, description 1
- architecture of SiteProtector, illustration 2
- asset criticality, grouping by 43
- assets 80
 - finding assets in a group 19
 - finding groups 18
- attack detected 62
- attack location, significance of 56
- attack patterns 57
- attack scope 79
- attack successful 62
- attacker view 47
- attacks 56, 80
 - target not vulnerable 67
- authorized activity 55
- authorized scans 55

B

- backdoor 32
- baseline
 - creating in Analysis tab 50
 - reset
 - restore 51
- buffer overflow 32
- business function, grouping by 43

C

- change control, affect on baselines 49
- columns 9
- completeness of vulnerability data 69
- components
 - descriptions of 3
- confidential information 80
- critical hosts 38
 - avoiding during peak times 39
 - vulnerabilities that affect 33
- custom 28, 29

D

- data generated by authorized scans 57
- determining the source of 43
- discovery scans 37
- documentation
 - SiteProtector Help iv
 - SiteProtector Installation Guide iii
- domain administrator rights, role in scanning 38
- domain controller hosts, role in scanning 40

E

- Enterprise Scanner 37
 - running an ad hoc assessment scan 67
 - running an ad hoc discovery scan 68
- event data
 - clearing events 11
 - defining exceptions for 52
 - defining incidents for 52
 - exporting 28
 - restoring cleared events 11
 - viewing details 13
 - viewing security information 11
- Event Name view 80
- events 10
- events of undetermined importance 52
- exceptions 34, 52, 58
 - categorizing vulnerabilities as 33
 - defining 52
- exploits, sophistication of 79
- export
 - event data 28
- external probes and scans 47

F

- failed attack 64
- failure likely 64
- failure possible 63
- filtering authorized scans 57
- filtering, importance of 49
- firewalls
 - adjusting rules to prevent access 31, 34
 - blocking scans 38

G

- geography, grouping by 43
- group by 11
- grouping 11
- groups
 - finding 18
 - finding assets 19
- guided questions
 - using 12
- guidelines for creating 52, 58
- guidelines for identifying 57

H

- health
 - health checks 14
 - Health Summary 14
 - Ignore Health Status 14
- Health 15, 16
- Health Summary
 - agent health checks 14
- Help, SiteProtector, content of iv
- hosts
 - availability during scans 38
 - limiting number included in scans 40
- hosts, determining number targeted by an attack 79

I

- ICMP requests 38, 40
- identifying location using Agent view 56
- identifying the source of 48
- identifying the target of 46
- ignoring authorized scans using attack patterns
 - attack patterns 58
- impact analysis 4, 61
- impact analysis, defined 18
- improper configuration, vulnerabilities due to 32
- incidents 34
 - categorizing vulnerabilities as 33
 - defining 52
- Installation Guide, content of iii
- Internet 57

Internet Scanner attack pattern 57
IP address
 determining organization that it is
 registered to 48
iterative process, role in analysis 41

M

malicious activity 42
misconfigured systems 55, 58
misuse 41

N

navigation history
 Analysis tab 14
not compliant 65
not vulnerable 63
Notifications view 15, 16
number attacker is targeting 80
number of platforms targeted 81

P

patches
 role in repairing vulnerabilities 34, 35
penetration, degree of 79
ping responses, role in scanning 40
policy
 maintaining between scans 38
 reducing levels of default scan
 policies 40
portlets
 adding 43
 modifying data displayed in 44
 navigating from 44
 removing 43
 summary view 43, 44
portlets, summary view 43, 44
priority 73

R

Remedy Action Request System 73
repairing vulnerabilities 33
report
 analysis view 28, 29
 create 22
 delete 25
 email 26
 image 26
 sample 26
 schedule 23, 25
 template 14, 21, 24, 25, 27
 permissions 14, 27
reports 21
 finding 26
role in filtering authorized scans
 authorized scans
 attack patterns 57
running an ad hoc assessment scan with
 Enterprise Scanner 67
running an ad hoc discovery scan with
 Enterprise Scanner 68

S

scanner, description 1
scans 57
 scans, guidelines for identifying 56
schedule 29
 delete 25
security information
 viewing 11
SecurityFusion
 defining exceptions for 52
 defining incidents for 52
SecurityFusion module 4
 impact analysis 4
sensitive traffic
 grouping according to 43
sensor location, role in analysis 56
sensor, description 1
simulated block 64
SiteProtector Configuration Guide iii
SiteProtector Configuring Firewalls for
 SiteProtector Traffic iv
SiteProtector Policies and Responses
 Configuration Guide iii
sorting 10
successful attack likely 62
summary view 43, 44
suspicious activity 43, 46
system resources 80

T

target, operating system of 72
target, services running on 72
template 21
 creating 24
 delete 25
 exporting 24
 importing 24
theft 80
ticket 73
tickets 73
 creating 75
 editing 76
 viewing 76
topology, grouping by 42

U

unauthorized activity 55
unauthorized vulnerability scans 56
upgrades
 role in repairing vulnerabilities 35

V

Vandalism 80
vendors
 patches supplied by 34
 vulnerabilities specific to 32
vulnerabilities
 advanced hackers that exploit 33
 categories of 32
 exploited by an outsider 33
 informational 32
 mitigating 33

vulnerabilities (*continued*)
 monitoring 34
 resolving 33
 target of attack not vulnerable 67
 that cannot be resolved
 immediately 34
 worse case scenario if exploited 33
vulnerability assessment scans
 developing a plan 38
vulnerability check indeterminate 63
vulnerability identification and resolution
 process, illus 31
vulnerable, host 63

X

X-Force risk levels 66
X-Press Updates
 maintaining between scans 38



Printed in USA