

IBM Proventia[®] Management SiteProtector System[™]

User Guide for Security Analysts

Version 2.0, Service Pack 7.0

© Copyright IBM Corporation 1994, 2008.
IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

All Rights Reserved.

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. ADDME, Ahead of the threat, BlackICE, Internet Scanner, Proventia, RealSecure, SecurePartner, SecurityFusion, SiteProtector, System Scanner, Virtual Patch, X-Force and X-Press Update are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

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

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

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than IBM Internet Security Systems (IBM ISS). Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. IBM Internet Security Systems disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall IBM ISS be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if IBM Internet Security Systems has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by IBM Internet Security Systems. The views and opinions of authors expressed herein do not necessarily state or reflect those of IBM Internet Security Systems, and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents IBM Internet Security Systems, Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.

June 4, 2008

Contents

Preface

Overview	7
How to Use SiteProtector System Documentation	8
Getting Technical Support	10

Chapter 1: Introduction to the SiteProtector System

Overview	11
What is the SiteProtector System?	12
SiteProtector System Architecture	13
SiteProtector System Components and Features	14
SiteProtector System Web Console	15
Add-on Components	16

Chapter 2: Before You Begin

Overview	17
SiteProtector System Configuration Requirements and Recommendations	18
Threat Analysis and Vulnerability Assessment Planning	19
Vulnerability Assessment and Remediation Checklist	20
Threat Investigation and Analysis Checklist	21

Part I: Monitoring and Report Tasks

Chapter 3: Monitoring Your Network

Overview	25
Section A: SiteProtector System Analysis Components	27
Overview	27
Section B: Analysis Views and Modes	29
Overview	29
Selecting Default Analysis Views	30
Customizing Analysis Views	33
Selecting Analysis Perspectives	36
Selecting Guided Questions	37
Section C: Refreshing and Clearing Event Data	39
Overview	39
Refreshing the Console	40
Clearing and Unclearing Events	41
Section D: Viewing Anomaly Detection Content	43
Overview	43
Accessing ADS Content	44
Viewing ADS Entity Information	45
Section E: SecurityFusion Module Impact Analysis	47
Overview	47
SecurityFusion Module Attack Patterns	48

Section F: Locating Assets and Agents	51
Overview	51
Locating a Group That Contains a Selected Agent or Asset	52
Locating an Asset or Agent That is Contained in a Group	53
Chapter 4: Running Reports	
Overview	55
Section A: Before You Begin	57
Overview	57
Guidelines for Running Reports	58
Section B: Common Report Tasks	59
Overview	59
Viewing and Saving Reports	60
Configuring the Report Name and Format	61
Specifying Report Frequency	62
Filtering Reports By Date	63
Distributing Report Results in Email Messages	64
Working with Email Addresses in the SiteProtector System Users List	65
Section C: Options for Specific Reports	67
Overview	67
Assessment Reports	68
Asset Reports: Event Details and Summary	71
Asset Reports: Protection	74
Asset Reports: Asset Risk Report	75
Attack Activity Reports	79
Audit Reports: Audit Detail Report	83
Audit Reports: Audit User to Group Report	84
Content Filtering Reports	85
Mail Filtering Reports	87
Management Reports	89
Permission Reports	93
Ticket Reports	94
Virus Activity Reports	96

Part II: Vulnerability Assessment and Remediation

Chapter 5: Identifying and Resolving Network Vulnerabilities

Overview	103
Developing Vulnerability Assessment Plans	104
Vulnerability Data Generated by the SiteProtector System	105
Gathering Information About Vulnerability Events	106
Deciding Whether to Resolve Vulnerabilities	107
Repairing and Mitigating Vulnerabilities	108
Creating a Plan of Action	110
Implementing Upgrades and Patches	111

Chapter 6: Managing Scans

Overview	113
Identifying Hosts on Your Network	114
Ensuring That Vulnerability Data is Complete and Accurate	115
Scheduling Vulnerability Scans	116
Running Background Scans	117

Reducing the Time Required to Run Scans	118
---	-----

Part III: Threat Investigation and Analysis

Chapter 7: Detecting Suspicious Activity

Overview	121
Section A: Suspicious Activity.	123
Overview	123
Section B: Monitoring Event Analysis Views.	125
Overview	125
Choosing the Traffic to Monitor and Correlate	126
Summary View	127
Event Name View.	129
Target View	131
Attacker View	132
Scenarios for Using Guided Questions and Event Analysis Views	133
Section C: Filtering Activity from Analysis Views	135
Overview	135
Creating Baselines.	136
Creating Incidents and Exceptions	138

Chapter 8: Is Suspicious Activity Significant?

Overview	141
Identifying the Location of an Attack	143
Identifying Activity Caused by Vulnerability Scans	144
Filtering Authorized Scans Using Attack Patterns	145
Creating Exceptions to Filter Scan Activity	146
Identifying Activity Caused by Misconfigured Systems.	147
Identifying Normal Activity Commonly Identified as Suspicious	148

Chapter 9: Is an Attack a Threat?

Overview	151
Section A: Using the SecurityFusion Module to Assess an Attack	153
Overview	153
Viewing Attack Statuses	154
Section B: Assessing an Attack Manually	159
Overview	159
Determining the X-Force Risk Level of an Attack.	160
Was the Attack Target Vulnerable?	162
Was the Target Service or Operating System Susceptible?	165

Chapter 10: Tracking and Prioritizing Confirmed Attacks

Overview	169
Guidelines for Establishing Ticket Priority	170
Creating Tickets	172
Viewing Tickets	174

Chapter 11: Determining the Scope of Attack

Overview	175
Attack Scope	176
Goals of Typical Attackers.	177
Viewing the Number of Assets Targeted by an Attacker	178

Viewing the Number of Platforms Targeted by an Attacker.	179
Chapter 12: Identifying Compromised Systems	
Overview	181
Section A: SecurityFusion Module Attack Patterns	183
Overview	183
How Attack Patterns Work	184
Host Patterns	185
Viewing Attack Patterns	186
Incidents, Exceptions, and Attack Patterns	188
Section B: Identifying Information Gathering Activities	189
Overview	189
Information Gathering Attack Patterns	190
Section C: Identifying Log On Activities	193
Overview	193
Logon Activities Between Compromised Hosts	194
Logon Failures	196
Logon Activities From a Spoofed Source	197
Section D: Identifying Break-In Activities	199
Overview	199
Network Break-In Attempts	200
Targeted Break-In Attempts	201
Program Startups	202
Program Shutdowns	203
Section E: Identifying Evasion Activity	205
Overview	205
Targeted Probing and Evasion	206
Targeted Break-In Attempt and Evasion	207
Section F: Identifying Denial of Service Attacks	209
Overview	209
Targeted DoS Attacks	210
Targeted DoS Successful	211
Attacking DDoS Agent	212
Index	213

Preface

Overview

Introduction	The <i>SiteProtector System User Guide for Security Analysts</i> provides background information, procedures, and recommendations for using the SiteProtector system to assess vulnerabilities and monitor and analyze suspicious activity on your network.
Scope	This guide provides guidelines for analyzing event data from a variety of IBM ISS agents, including Network Intrusion Prevention System (IPS) appliances, Network Multi-Function Security appliances, Server Sensor, and Network Internet Scanner. This guide does not provide guidelines for analyzing data from Network Enterprise Scanner or from third-party products.
Audience	The intended audience for the <i>SiteProtector System User Guide for Security Analysts</i> 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.

How to Use SiteProtector System Documentation

Using this guide This topic explains how the information in the *SiteProtector System User Guide for Security Analysts* is organized and lists other documents in the SiteProtector system documentation suite.

Document organization This document is organized into logical units, as described in Table 1:

Part	Description
I	Monitoring and Report Tasks Part I provides background information and procedures for performing basic monitoring and report tasks in the SiteProtector system. Use this information to familiarize yourself with these tasks if you have not done so already.
II	Vulnerability Assessment and Remediation Part II provides guidelines for using Network Internet Scanner to identify and resolve vulnerabilities and manage scans. Use this information to help you implement vulnerability assessment and remediation best practices with the SiteProtector system.
III	Threat Investigation and Analysis Part III provides background information, procedures, and guidelines for using the SiteProtector system to monitor, investigate, and analyze suspicious activity and confirmed attacks. Use this information to help you implement threat investigation and analysis best practices with the SiteProtector system.

Table 1: *Parts of the User Guide for Security Analysts*

Where to get SiteProtector system documents

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

- the IBM ISS Web site at <http://www.iss.net/support/documentation>
- the Deployment Manager
- the IBM ISS product CD in the \Docs folder

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

- the SiteProtector system box
- the IBM ISS product CD
- the IBM ISS Web site at <http://www.iss.net/support/documentation>

Related publications The following table describes other SiteProtector system documents:

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

Table 2: *Descriptions of SiteProtector system user documents*

Document	Contents
<i>SiteProtector System Help</i>	Contains many of the procedures that you need to use the SiteProtector system.

Table 2: *Descriptions of SiteProtector system user documents (Continued)***Licensing
agreement**

For licensing information on IBM Internet Security System products, download the IBM Licensing Agreement from: http://www-935.ibm.com/services/us/iss/html/contracts_landing.html

Getting Technical Support

Introduction

IBM Internet Security Systems provides technical support through its Web site and by email or telephone.

The IBM ISS Web site

The Customer Support Web page (<http://www-935.ibm.com/services/us/index.wss/offerfamily/iss/a1029129>) provides direct access to online user documentation, current versions listings, detailed product literature, white papers, and the Technical Support Knowledgebase.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding IBM ISS published holidays Note: If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 3: *Hours for technical support*

Contact information

For contact information, go to the Contact Technical Support Web page at <http://www-935.ibm.com/services/us/index.wss/offering/iss/a1029178>.

Chapter 1

Introduction to the SiteProtector System

Overview

Introduction

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

Terms to know

Table 4 describes the terms used for security products in this document:

Term	Description
agent	The generic term for all sensors, scanners, and Desktop 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.

Table 4: *Terms for security products*

In this chapter

This chapter contains the following topics:

Topic	Page
What is the SiteProtector System?	12
SiteProtector System Architecture	13
SiteProtector System Components and Features	14
SiteProtector System Web Console	15
Add-on Components	16

What is the SiteProtector System?

Introduction

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

Reference: Refer to the *SiteProtector - Supported Agents and Appliances* document available at <http://www.iss.net/support/documentation/> 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 security and management 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

Table 5 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	SiteProtector system	sensors
Console	Reporting Module	scanners
Site Database	SiteProtector system	appliances
System Scanner Databridge	SecurityFusion Module	Desktop agents
Deployment Manager	SiteProtector system	
Event Archiver	Third Party Module	
Event Collector	SiteProtector system	
Event Viewer	SecureSync Integrated Failover System	
SP Core (includes the application server and sensor controller)		
X-Press Update Server		
Web Console		

Table 5: SiteProtector system components and agents

SiteProtector System Architecture

Introduction

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 component

Figure 1 illustrates the components in a standard instance of the SiteProtector system that uses three computers:

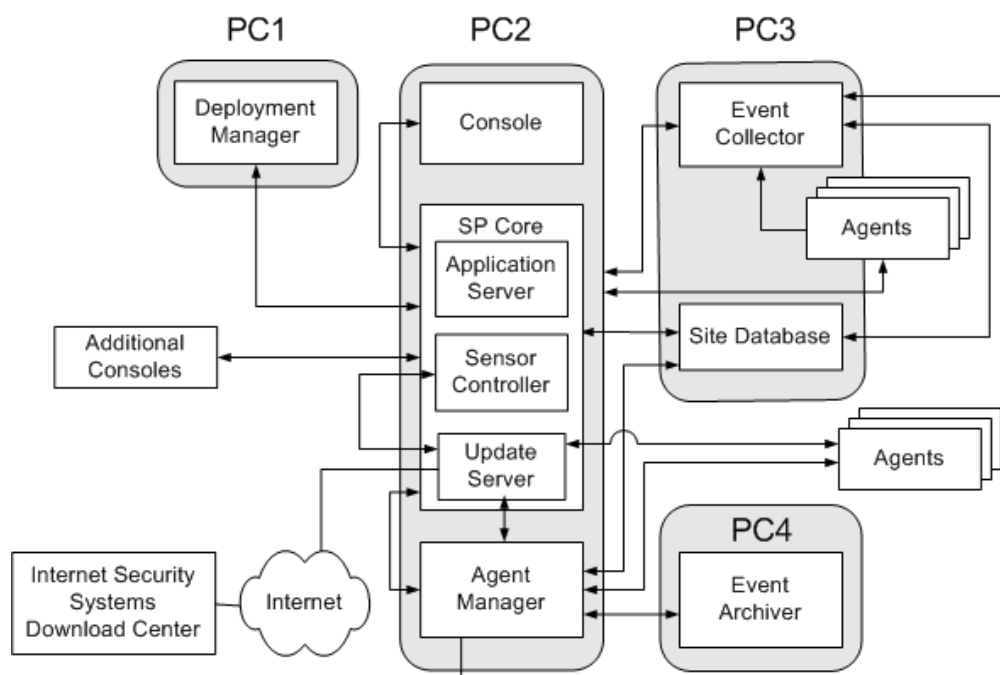


Figure 1: Components in a typical Site

SiteProtector System Components and Features

Introduction

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

Component descriptions

Table 6 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, Proventia G and M appliances, Event Archiver, and X-Press Update Server; and it facilitates data transfer from agents to the Event Collector.
Console	The SiteProtector system Console is the main interface to the SiteProtector system where you can perform most SiteProtector system functions, such as monitoring events, scheduling scans, generating reports, and configuring agents.
System Scanner Databridge	The System Scanner Databridge accepts data from earlier versions of agents and sends them to the Event Collector in the proper format.
Deployment Manager	The Deployment Manager is a Web server that lets you install any of the SiteProtector system components and agents on computers on your network.
Event Archiver	The Event Archiver provides the capability to archive security events to a remote location.
Event Collector	The event collector manages real-time events from sensors and vulnerability data from scanners.
Event Viewer	The SiteProtector system Event Viewer receives unprocessed events from the Event Collector to provide near real time access to security data for troubleshooting.
Site database	The SiteProtector system 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 (XPUs).
SP Core	The SP core includes the following components: <ul style="list-style-type: none"> The application server enables communication between the SiteProtector system Console and the SiteProtector system 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 (XPUs) from the IBM ISS 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.

Table 6: *Description of the core components of the SiteProtector system*

SiteProtector System Web Console

Introduction

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
- create reports

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 *SiteProtector - System Requirements* available at <http://www.iss.net/support/documentation/> for specific information about Web Console requirements.

Logging on to the Web Console

To log on to the Web Console:

1. Type the address of the SiteProtector system application server in the **Address** box of your Web browser, using the following format:
`https://computer name or IP address:3994/siteprotector/`
The Login window appears.
2. Type the SiteProtector system **Username** and **Password** for the Site you want to access.
3. If you need to retype the user name or password, click **Reset** to start over.
4. Click **Submit**.

Note: Some functions of the SiteProtector system Web Console may require you to add the Site server to your "trusted sites" in Internet Explorer before you can use them.

Downloading the Java runtime environment (JRE)

To download the JRE:

1. Contact the following Web site: <http://java.sun.com/j2se/index.jsp>
2. Select Core Java.
3. Select the installation package for J2SE.
4. Download J2SE JRE.
5. Accept the license agreement.
6. Under Windows Platform, select **Windows Offline Installation, Multi-language**.

Caution: If you choose **Windows Installation, Multi-language**, the installation will fail.

Add-on Components

Introduction	The add-on components for the SiteProtector system provide additional protection and functionality that go beyond the base protection of the SiteProtector system.
SecurityFusion Module	<p>The SiteProtector system 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> <p>Attack pattern recognition—The Module recognizes patterns of events that may indicate specific types of attacks, such as unauthorized scans, break-in attempts, and activity from a compromised host.</p>
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.
Third Party Module	The SiteProtector system Third Party Module retrieves data from third-party firewalls, enabling you to view firewall activity and to associate security events with specific firewalls.
Reporting Module	Graphical summary and compliance reports provide the information managers need to assess the state of their security. Reports cover vulnerability assessment, attack activities, auditing, content filtering, Desktop, SecurityFusion and virus activity.

Chapter 2

Before You Begin

Overview

Introduction

This chapter provides requirements and considerations that you should review before you implement the practices in this guide, and provides checklists that can help you perform the tasks in this guide.

In this chapter

This chapter contains the following topics:

Topic	Page
SiteProtector System Configuration Requirements and Recommendations	18
Threat Analysis and Vulnerability Assessment Planning	19
Vulnerability Assessment and Remediation Checklist	20

SiteProtector System Configuration Requirements and Recommendations

Introduction

This topic provides prerequisites and recommendations that apply to the guidelines and procedures that are addressed in this guide.

Prerequisite checklist

Table 7 provides a checklist of the prerequisites that you must meet before you can use the information in this guide:

✓	Prerequisite Task	Reference
<input type="checkbox"/>	1. Install the SiteProtector system.	<i>SiteProtector System Installation Guide</i> available at http://www.iss.net/support/documentation/
<input type="checkbox"/>	2. Configure the SiteProtector system.	<i>SiteProtector System Configuration Guide</i> available at http://www.iss.net/support/documentation/

Table 7: *Prerequisites for installing the SiteProtector system*

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 purchased and 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.

Threat Analysis and Vulnerability Assessment Planning

Introduction	Effective planning is crucial to assessing risk and protecting your enterprise against threats. This guide makes certain assumptions about the manner in which you implement security planning in your organization.
Asset valuation and risk	This guide assumes that your organization has determined the value of its assets and has analyzed the risk associated with them. This guide does not provide guidelines for evaluating assets or risk.
Incidence response plan	The guide assumes that your organization has developed and implemented a detailed incident response plan.
Vulnerability assessment and remediation plan	This guide assumes that your organization has developed and implemented a vulnerability assessment and remediation plan.

Vulnerability Assessment and Remediation Checklist

Introduction This topic provides a checklist for assessing and remediating vulnerabilities using the SiteProtector system. These tasks are covered in “Part II: Vulnerability Assessment and Remediation.”

Checklist Table 8 provides a checklist of the tasks you should complete when you perform vulnerability assessment and remediation:

✓	Task	Threat Assessment Checklist
<input type="checkbox"/>	1	Gather information about vulnerability events. See “Gathering Information About Vulnerability Events” on page 106.
<input type="checkbox"/>	2	Determine whether to resolve vulnerabilities. See “Deciding Whether to Resolve Vulnerabilities” on page 107
<input type="checkbox"/>	3	Resolve vulnerabilities. See “Repairing and Mitigating Vulnerabilities” on page 108.
<input type="checkbox"/>	4	Create an action plan to resolve vulnerabilities. See “Creating a Plan of Action” on page 110.
<input type="checkbox"/>	5	Implement fixes. See “Implementing Upgrades and Patches” on page 111.

Table 8: *Checklist of threat assessment tasks*

Threat Investigation and Analysis Checklist

Introduction

This topic provides a checklist for investigating and analyzing threats. These tasks are covered in "Part III: Threat Investigation and Analysis."

Checklist

Table 9 provides a checklist of the tasks you should complete when you perform vulnerability assessment and remediation:

✓	Task	Threat Assessment Checklist
<input type="checkbox"/>	1	Monitor and detect suspicious activity. See Chapter 7, "Detecting Suspicious Activity" on page 121.
<input type="checkbox"/>	2	Determine whether suspicious activity is significant. See Chapter 8, "Is Suspicious Activity Significant?" on page 141
<input type="checkbox"/>	3	Determine whether an attack is a threat. See Chapter 9, "Is an Attack a Threat?" on page 151.
<input type="checkbox"/>	4	Track and prioritize confirmed attacks. See Chapter 10, "Tracking and Prioritizing Confirmed Attacks" on page 169.
<input type="checkbox"/>	5	Determine the scope of an attack. See Chapter 11, "Determining the Scope of Attack" on page 175.

Table 9: Checklist of threat investigation and analysis tasks

Monitoring and Report Tasks

Chapter 3

Monitoring Your Network

Overview

Introduction

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.

In this chapter

This chapter contains the following sections:

Section	Page
Section A, "SiteProtector System Analysis Components"	27
Section B, "Analysis Views and Modes"	36
Section C, "Refreshing and Clearing Event Data"	39
Section D, "Viewing Anomaly Detection Content"	43
Section E, "SecurityFusion Module Impact Analysis"	47
Section F, "Locating Assets and Agents"	51

SECTION A: SiteProtector System Analysis Components

Overview

Introduction

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

Table 10 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.

Table 10: *SiteProtector System Analysis Components*

SECTION B: Analysis Views and Modes

Overview

Introduction

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

In this section

This section contains the following topics:

Topic	Page
Selecting Default Analysis Views	30
Customizing Analysis Views	33
Selecting Analysis Perspectives	36
Selecting Guided Questions	37

Selecting Default Analysis Views

- Introduction

The default analysis views are most commonly used for monitoring data in the SiteProtector system. Use analysis views as a starting point for event detection and for creating customized reports.
- What are analysis views?

Default analysis views appear in the Analysis View list on the Analysis tab. When you select a view from the list, event data appears in a table in the view pane. The events are filtered with the default filters that are enabled for that view. Analysis views are divided into categories:

 - event
 - vulnerability
 - application monitoring (only enabled with IBM Proventia® Desktop Endpoint Security)
 - anomaly detection (only enabled with the IBM Proventia® Network Anomaly Detection System (ADS))

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 may vary because the SiteProtector system chooses the Analysis Perspective based on the Analysis view. See “Selecting Analysis Perspectives” on page 36.
- Tasks you can perform with analysis views

You can use these views as part of your standard event analysis and as the basis for customizing your own views. Analysis views let you perform the following tasks:

 - refresh the event data
 - move backward or forward through the analysis history
 - open the Filters window
 - sort columns
- Event analysis views

Use event analysis views to analyze intrusion detection events and track incidents that are created. Table 11 describes each event analysis view displayed in the SiteProtector system:

Analysis View	Description
Event Analysis—Agent	Provides information about sensors that have detected events.
Event Analysis—Attacker	Displays information about the IP address that is the source of attacks against your assets. Depending the filters used, the sources may be internal, external, or both.
Event Analysis—Detail Time	Provides timestamp information about an event, but does not display associated event details, such as a MAC address, that are available with the Event Analysis—Details view.
Event Analysis—Details	Displays additional information about the source and targets of an attack.
Event Analysis—Event Name	Displays information about the type and number of events detected by sensors.

Table 11: Event analysis view descriptions

Analysis View	Description
Event Analysis—Incidents	Displays information about events matching criteria that you consider important and need to track. A view that provides information only about incidents lets you concentrate on critical events.
Event Analysis—OS	Provides information about the operating system of the host that is the target of attack.
Event Analysis—Target Object	Displays information about IP addresses that may be the target of an attack. Depending on the filters used, the sources may be internal, external, or both.
Event Analysis—Target	Displays information about IP addresses that may be the target of an attack. Depending on the filters used, the sources may be internal, external, or both.

Table 11: Event analysis view descriptions

Vulnerability analysis views

Use the vulnerability analysis views to perform vulnerability assessments and to manually correlate vulnerabilities with hosts that you are monitoring. Table 12 lists a description of the vulnerability analysis views that are displayed in the SiteProtector system:

Analysis View	Description
Vuln Analysis—Asset	Displays for the time period you specify: <ul style="list-style-type: none"> IP address of the affected hosts priority level of the vulnerabilities objects affected most recent event Important: You should set the time period of this view to the time of your most recent scan. Otherwise, the view displays vulnerability events for previous scans.
Vuln Analysis—Detail	Adds more information to the “Attacked Vuln (Fusion)—Overview” view.
Vuln Analysis—Object	Displays objects on your network or desktop computers that are a source of vulnerabilities.
Vuln Analysis—Target OS	Displays events with emphasis on information related to the OS of the target
Vuln Analysis—Vuln Name	Displays the name of vulnerabilities affecting your network or desktop computers.

Table 12: Vulnerability analysis view descriptions

Application monitoring views

The application monitoring views are only enabled if Proventia Desktop is configured to report to the SiteProtector system. Use the application monitoring views to track Proventia Desktop events and to determine if applications have been allowed to run:

Analysis View	Description
Application Monitoring—Detail	Displays detailed information about the application that Desktop is monitoring, including the user name, directory path of the application, and source and target IP addresses.
Application Monitoring—Summary	Enables you to track trends in the way certain applications are used on your network.
Application Monitoring—Target	Displays information about the IP addresses that the applications that are being monitored are using.
Application Monitoring—User	Displays information about users that may be the source or target of an attack.

Table 13: Appliance monitoring view descriptions

Procedure

To select a default analysis view:

1. In the left pane, select an asset or group of assets for which you want to examine event data.
2. Select **Analysis** from the **Go to** list.
The Event-Analysis view appears in the **Analysis** tab.
3. Select a view from the **Analysis View** list.

Customizing Analysis Views

Introduction

The SiteProtector system lets you change the column and filter settings that are applied to default analysis views, and then save the changes in separate analysis files. Use customized analysis views to create views and reports that are tailored to your specific needs.

Important: If you define a filter or customize a view and do not save the settings in a new analysis file, the settings are not saved when you close the Console. If you want to reuse the filters and column settings, you must save the analysis file, which is stored on the client computer (not the Site database).

Filters window

Use the Filters window to specify values for filters you want to apply and to select columns that you want to add, remove, or reorder. The Filters window is divided into the following sections:

Section	Description
Filter list	The left pane lists the filters that are available. When you enable a filter, a check appears next to the filter. The Show Column option, which lets you customize columns, also appears in this list.
Parameters	The upper right pane lists the parameters. The parameters let you specify values that vary according to the filter you select in the filter list.
Description	The lower right pane contains information that describes the filter's purpose and a procedure that explains how to use it.

Table 14: *Sections in the Filters window*

Columns

You can add columns to view more detailed information, and remove them to see higher-level information. You can select from four categories:

- count columns
- event columns
- target and source columns
- time columns

Filters

Although most of the default analysis views have filters, you may need to change a filter setting when you analyze an event. For example, you might want to see events from only one IP address that you suspect is a source of malicious activity. The Filters window lets you change and apply a number of different filters.

Identifying active filters

To identify active filters:

1. On an **Analysis** tab, find the **Filters Applied** link.
2. Notice the number in parentheses that indicates the number of filters applied.
3. To see which filters are applied, place your cursor over the link.
The list of applied filters appears.
4. To see the details about the filters, click the link.

Rearrange columns To rearrange columns in the Analysis views:

1. Select **Analysis** from the **Go to** list.
2. Select the view to which you want to add, remove, or reorder columns from the **Analysis View** list.
3. Select **View→Add/Remove Columns**

The Filters window appears with the **Show Columns** filter selected in the left pane.

Note: The parameter window appears in the right pane. The information in the bottom right pane describes the filter and explains how to change the settings.

4. Do one or more of the following:

To...	Select a column in the right pane from the...
add columns	Available list, and then click Add.
remove columns	Displayed list, and then click Remove.
reorder columns	Displayed list, and then use the Up and Down buttons.

5. Click **OK**.

The Analysis tab changes according to the options you selected.

Sort column data To sort the data in columns:

1. Select **Analysis** from the **Go to** list.
2. Select the view that you want to sort from the **Analysis View** list.
3. In the **Analysis** view you selected, click the column name you want to sort.
An arrow appears next to the column name, and the data in that column is sorted according to the direction of the arrow (up or down).
4. Click the column again to change the sort order (up or down).
5. If you want to sort data in additional columns, click the column you want to sort while pressing the **SHIFT** key.

Defining filters To define filters in the Analysis views:

1. Select **Analysis** from the **Go to** list.
2. Select the view for which you want to define a filter from the **Analysis View** list.
3. Select **View→Filter**.

The Filters window appears.

Tip: To define filters for certain columns in the Analysis views, right-click on the column you want edit, and then select **Add/Edit [column name] Filter(s)**.

4. In the left pane, select the filter you want to edit.
The parameter window appears in the right pane.
5. Use the fields in the parameter pane on the right to change specific settings, which vary according to the filter you selected.
6. Click **OK**.

7. If you want to save the filters you have applied in a customized view, then select **View→Save**.
8. Type the name of the customized view in the **Save Analysis View** window, and then click **Save**.

Selecting Analysis Perspectives

Introduction

Analysis perspectives let you manually change the focus of data that is associated with a selected asset. Use the analysis perspectives in combination with analysis views to determine the extent to which one or more assets are involved in event activity.

Procedure

To select an analysis perspective:

1. In the left pane, select an asset or group of assets for which you want to examine event data.
2. Select **Analysis** from the **Go to** list.
3. Select **Action** → **Analysis Perspective**, and then use the following table to select one of the options from the submenu:

Select this option...	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.

The **Analysis** tab changes based on the analysis perspective you select, and the perspective you selected appears in the title bar.

Selecting Guided Questions

Introduction

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.

Examples of guided questions

Table 15 lists examples of guided questions that are displayed in the SiteProtector system and in the corresponding analysis views:

If you select one of these questions...	This analysis view appears...
Who attacked this target? What are the sources of this event? What attackers did this sensor see? Who attacked this object?	Event Analysis—Attacker
What attacks came from this target? What events were against this target? What events were generated by this attacker? What attacks were against this target? What events did this sensor see? What events were against this object?	Event Analysis—Event Name
What are the event details?	Event Analysis—Details
Which sensors detected this target? Which sensors detected this attacker? Which sensors detected this event? What sensor detected this object being attacked?	Event Analysis—Sensor
What objects were targeted on this host? What are the target objects of this attacker? What are the target objects of this event? What objects did this sensor see?	Event Analysis—Target Object
What are the targets of this attacker? What are the targets of this event? What targets did this sensor see? What target host had this object attacked?	Event Analysis—Target
What is the 'whois' record of this target? What is the 'whois' record of this attacker?	Displays American Registry for Internet Numbers (ARIN) search results for the IP address of the host

Table 15: Examples of guided questions and the corresponding analysis views

Procedure

To select a guided question:

1. In the left pane, select the group or host for which you want to view information.
2. Select **Analysis** from the **Go to** list.
3. Right-click an event, and then select the most relevant question from the pop-up menu.

An analysis view appears with different columns and filters.

Important: Certain columns must appear in the Analysis view you selected; otherwise, the guided questions do not appear.

4. To move to an earlier view, click the Back icon in the toolbar until you reach the event data you want to see.
5. Use the filter panel to focus the event data more narrowly, if necessary.

SECTION C: Refreshing and Clearing Event Data

Overview

Introduction

Ensuring that information about your network is up-to-date is crucial when you are detecting and investigating events. You can configure the SiteProtector system to refresh event data automatically and to clear events that are not relevant to your inquiry.

In this section

This section contains the following topics:

Topic	Page
Refreshing the Console	40
Clearing and Unclearing Events	41

Refreshing the Console

Introduction

You can configure the Console to update itself at a predefined frequency using the Auto-Refresh option. You can also refresh the Console manually.

Auto Refresh settings

When you select the Auto-Refresh option, the Console is updated according to the frequency that you specify in Tools→Options→General→Auto Refresh. You can also configure whether to automatically refresh only active consoles or all consoles.

Caution: Exercise caution when you use the Auto-Refresh option, because it can negatively impact Console performance if the refresh interval is too short.

Configuring the Console to refresh data automatically

To configure the Console to refresh automatically:

- Select **View→Auto-Refresh**.
A check appears next to the **Auto-Refresh** option.
Note: To disable **Auto-Refresh**, re-select the option.

Refreshing the Console manually

To refresh the Console manually:

1. To refresh the data in a tab that you have selected, do one of the following:
 - Select **View→Refresh**.
 - Press F5.

The option updates the view with any events received since the last time the view was refreshed.

2. To refresh a pane in the **Summary** view, click the **Refresh** icon on the title bar.

Reloading the current view

To reload the current view:

1. On an **Analysis** tab, click **View→Reload Current View**.
2. Click **Yes**.

The option removes any changes you made to filters or to columns in the currently selected view.

Clearing and Unclearing Events

Introduction	Ensuring that information about your network is relevant is crucial when you are monitoring and detecting events. You can configure the SiteProtector system to clear events that are not relevant to your inquiry and to restore previously cleared events.
What is event clearing?	The SiteProtector system lets you clear events from the Analysis views that you no longer need. This makes it easier for you to identify events that are potential threats.
Clearing events	<p>To clear events from the SiteProtector system Console:</p> <ol style="list-style-type: none">1. On an Analysis tab, select the events you want to clear.2. Click Action→Clear Events. The Clear/Unclear Event(s) window appears.3. Click Yes to confirm that you want to clear the event. The events that you selected are cleared from the Console.
Restoring cleared events	<p>To restore cleared events from the Site Protector system Console:</p> <ol style="list-style-type: none">1. On an Analysis tab, select the Analysis View for which you want to clear events.2. Select View→Filter. The Filters window appears.3. In the left pane, select Show Columns. The parameter window appears in the right pane.4. Select Cleared Count from the Available column, and then click Add.5. Click OK.6. Select the event or events you want to unclear, and then select Action→Restore Events. Note: If you have cleared all of the events in the view, the view is empty, and the right-click menu will not appear to enable you to unclear events.7. Click Yes. The events that you selected are restored.

SECTION D: Viewing Anomaly Detection Content

Overview

Introduction 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.

In this section This section contains the following topics:

Topic	Page
Accessing ADS Content	44
Viewing ADS Entity Information	45

Accessing ADS Content

Introduction

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

To start the ADS Web Console:

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

To access ADS content:

- 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

Introduction	This topic provides procedures for viewing ADS entity information, ADS event details, and viewing Traffic Analysis.
Viewing ADS entity information	<p>To view ADS entity information:</p> <ol style="list-style-type: none">1. In the left pane of the Console, select a group or an asset for which you want to view content.2. Select to display agents, assets, or events from the Agents, Event Analysis - Details, or Assets view.3. Highlight the agents, assets, or event(s) you want to investigate from the list.4. To view ADS entity information, do one of the following:<ul style="list-style-type: none">■ Right-click the agent, asset, or event, and then select Network Behavior.■ Select Actions → Network Behavior, and then select the ADS information you want to review. <p>Note: 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.</p>
Viewing ADS event details	<p>To view ADS event details:</p> <ol style="list-style-type: none">1. In the left pane of the Console, select a group or an asset for which you want to view events.2. Select Analysis from the drop-down list, or click an open Analysis tab.3. Select Event Analysis - Details from the list, and then select the event.4. To select the ADS event details, do one of the following:<ul style="list-style-type: none">■ Right-click the agent, and then select What are the ADS Event Details?■ Select Action, and then select What are the ADS Event Details? <p>The ADS Alert Details for the selected event appear.</p>
Analyzing traffic	<p>To view ADS events using the Traffic Analysis option:</p> <ol style="list-style-type: none">1. Select the group for which you want to view Traffic Analysis.2. Select Traffic Analysis from the Go to list. <p>The Traffic Analysis embedded tab appears, displaying the ADS traffic content for the selected group. The system displays traffic content from the last 24 hours.</p>

SECTION E: SecurityFusion Module Impact Analysis

Overview

Introduction

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.

In this section

This section contains the following topics:

Topic	Page
SecurityFusion Module Attack Patterns	48

SecurityFusion Module Attack Patterns

Introduction

The Module recognizes patterns of event activity that indicate serious security incidents, such as targeted and network break-in attempts or attack activity from compromised hosts. These patterns of attack are consolidated into a single incident, which makes dealing with streaming event data much more manageable. You can easily get to the details of incidents in a few quick clicks of the mouse.

How attack patterns work

The Module saves attack pattern correlations to the SiteProtector system database, making them available in the Console, only after all the events and other criteria for the attack pattern are satisfied. The Module continues to monitor and update existing attack pattern correlations until the time limits for the attack patterns are reached. The time span for an attack pattern is determined by time-related options for each attack pattern as well as system-related variables. The types of attack patterns are as follows:

- information gathering
- break-in attempts
- denial of service attacks
- evasion

Data columns that appear for attack patterns

The following table describes the data columns that appear for attack patterns correlations in the Console and the Event Analysis-Incidents view:

Column	Description
Incident/Exception Name	The name of the attack pattern, followed by a sequentially assigned, numeric identifier, in the following format: Attack_Pattern_Name~ID_n
Incident/Exception Description	A shorthand explanation of the hosts involved in the attack: <ul style="list-style-type: none"> • a visual description of the hosts involved. • a column that you can update with tracking or other useful information
# High	The number of High Severity events in the attack pattern correlation.
# Medium	The number of Medium Severity events in the attack pattern correlation.
# Low	The number of Low Severity events in the attack pattern correlation.
Tag Count	The number of different types of events, identified by Tag Name, in the attack pattern correlation. An attack pattern correlation, such as a worm attack, could contain several instances of the same type of event, so the Tag Count may be less than the total number of events.
Source Count	The number of different IP addresses that are sources for events in the attack pattern correlation.
Target Count	The number of different IP addresses that are targets for events in the attack pattern correlation.

Table 16: Data columns that appear for attack patterns

Column	Description
Object Count	The number of different objects targeted in the attack pattern correlation.
Earliest Event	The date and time of the earliest event in the attack pattern correlation.
Latest Event	The date and time of the latest event in the attack pattern correlation.

Table 16: *Data columns that appear for attack patterns (Continued)*

SECTION F: Locating Assets and Agents

Overview

Introduction 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.

In this section This section contains the following topics

Topic	Page
Locating a Group That Contains a Selected Agent or Asset	52
Locating an Asset or Agent That is Contained in a Group	53

Locating a Group That Contains a Selected Agent or Asset

Introduction

As you monitor your Site, you may need to locate a group that an agent or an asset belongs to. This topic provides a procedure for using the Find option to locate the group that an agent or asset belongs to.

Procedure

To locate a group that contains a selected asset or agent:

1. In the **Agent** or **Asset** view, select an agent or asset in the right pane.
2. Select **Edit→Find**.
The Find Group window appears with the parent group of the agent or asset selected.
3. Use the **Expand** and **Collapse** options to view the groups in the tree.
4. Select a group, and then click **OK** to navigate to that group.

Locating an Asset or Agent That is Contained in a Group

Introduction

The SiteProtector system lets you search a selected group to locate an asset or an agent. This topic provides a procedure for searching groups using keywords or patterns.

Procedure

To locate an asset or agent that is contained in a group:

1. Select a group in the left pane.
2. Select **Edit→Find**.

The Find Asset in Group window appears.

3. Type a keyword in the **Pattern** box, and then click **Find**.

If the pattern you typed matches an asset, the asset's host name and the asset's parent group appear in the pane below.

4. Use the **Expand** and **Collapse** options to view the groups in the tree.
5. Select a group, and then click **OK** to navigate to that group.

Chapter 4

Running Reports

Overview

Introduction

Important: This chapter provides guidelines and procedures for running SiteProtector system reports.

In this chapter

This chapter contains the following sections:

Section	Page
Section A, "Before You Begin"	57
Section B, "Common Report Tasks"	59
Section C, "Options for Specific Reports"	67

SECTION A: Before You Begin

Overview

Introduction This section provides background information and guidelines for running reports. Review this section before you perform the procedures in this chapter.

In this section This section contains the following topic:

Topic	Page
Guidelines for Running Reports	58

Guidelines for Running Reports

Introduction	This topic provides guidelines for scheduling report jobs, formatting large reports, and sending reports through email.
Scheduling report jobs	Do not schedule more than 11 jobs at the same time. While the first job is processing, a maximum of 10 jobs can be queued, and then any additional jobs fail.
Formatting large reports	Some reports may be longer than 30 pages. If so, the HTML format can cause the text in the report to overlap and become unreadable. If you think that a report may be longer than 30 pages, use the PDF or CSV formats. If you print the HTML version of a report, you may notice that the report content extends past the edge of the paper. Use the PDF format for better quality when you print a report.

SECTION B: Common Report Tasks

Overview

Introduction

This section provides procedures that apply to all reporting tasks. Use the information in this section to view reports, configure report format, frequency, and date, and use email to distribute report results.

In this section

This section contains the following topics:

Topic	Page
Viewing and Saving Reports	60
Configuring the Report Name and Format	61
Specifying Report Frequency	62
Filtering Reports By Date	63
Distributing Report Results in Email Messages	64
Working with Email Addresses in the SiteProtector System Users List	65

Viewing and Saving Reports

Introduction

Use the procedure in this topic to view report instances that the SiteProtector system generates and to save these instances locally.

How are reports saved?

By default, when you save a report's configuration settings, the SiteProtector system saves an instance of this report in the following folder on the Application Server:

```
ApplicationServer\deployed-apps\iss\SiteProtector.ear\webconsole.war\reports
```

Note: You must have the required permissions to access reports on the Application Server. Typically, these permissions vary depending on the Application Server's configuration.

Running report instances at specified intervals

The Recurrence tab lets you control the frequency with which the SiteProtector system runs report instances. See "Specifying Report Frequency" on page 62.

Procedure

To view and save reports:

1. Select **Report** from the **Go To** list.
2. Right-click the report that you want to generate, and then select **New Report** from the pop-up menu.
A window appears that displays the report's configuration options.
3. Enter the name of the report, specify additional configuration options, and then click **OK**.
4. Right-click the report template again, and then select **Properties** from the pop-up menu.
5. Right-click the report instance you want to view in the list, and then select **Open Report** from the pop-up menu.
6. To save the report to a local drive, right-click the report, and then select **Save As** from the pop-up menu.
7. Browse to the location where you want to save the report, select it, and then click **OK**.

Configuring the Report Name and Format

Introduction

The SiteProtector system lets you run reports in several formats. This topic provides a procedure for configuring report formats. The Report Specification tab contains general options that apply to all SiteProtector system reports.

Report format types

You can generate reports using the following file formats:

- PDF
- CSV
- HTML

Note: The default and recommended file format is PDF.

Procedure

To configure the Report Specification tab:

1. Select **Report** from the **Go To** list.
A list of reports appears in the right pane.
2. Right-click the report you want to generate, and then select **New Report** from the pop-up menu.
3. In the Report Specification tab, specify the following:

In this box...	Do the following...
Report Filename	Type a unique name for the report.
Report Comments	Type optional comments.
Report Type	Select the report format (PDF, CSV, HTML).

4. Click **OK**.

Specifying Report Frequency

Introduction

By default, the SiteProtector system generates a report only once. However, if you want the SiteProtector system to run a report at specified intervals, you can specify the frequency on the Recurrence tab.

Prerequisite

You must specify a report name and a report type on the Report Specification tab before you can save changes that you specify on other report tabs.

Reference: See “Configuring the Report Name and Format” on page 61.

Procedure

To specify report frequency:

1. Select **Report** from the **Go To** list.
A list of reports appears in the right pane.
2. Right-click the report you want to generate, and then select **New Report** from the pop-up menu.
3. Select the **Recurrence** tab.
4. In the **Recurrence pattern** section, select the frequency that you want the SiteProtector system to use to automatically generate this report.
5. Select the time that you want this report to be generated in the **Start** box.
Note: The current time is selected by default.
6. In the **Range of recurrence** section specify one of the following:
 - Select the **No end date** option.
 - Select the **End by** option, and then select a date from the list.**Note:** If the **Run Once** option is selected in the **Recurrence Pattern** section, then the **Range of recurrence** options are unavailable.
7. Click **OK**.

Filtering Reports By Date

Introduction

In most cases, you want to limit the data in a report to a specific time period. The SiteProtector system lets you create reports that filter data by standard and custom time periods. Use the background information and procedures in this topic to filter reports by time and date.

Prerequisite

You must specify a report name and a report type on the Report Specification tab before you can save changes that you specify on other report tabs.

Reference: See “Specifying Report Frequency” on page 62.

Procedure

To filter reports by date and time:

1. Select **Report** from the **Go To** list.
A list of reports appears in the right pane.
2. Right-click the report you want to generate, and then select **New Report** from the pop-up menu.
3. Select the **Report Period** tab.
4. Do you want to limit the data for this report to a specific time period?
 - If *yes*, select the **Custom** option.
 - If *no*, select the **Standard Time Period** option, and then go to Step 7.
5. Select one of the following time formats:
 - *SiteProtector system Console Time Zone*
 - **GMT** (Greenwich Mean Time)
6. Type the report period start and end times in the boxes provided, or click the arrow to select dates from the pop-up calendar, and then go to Step 8.
7. In the **Standard Time Period** section, do one of the following:

To include...	Select this option from the first list...	And then do this...
the current time period only	This	select the time unit (day, week, month, or year) from the third list.
previous time periods	Previous	<ul style="list-style-type: none">• select the number of time periods to include from the second list.• select the time unit (day, week, month, or year) from the third list.

8. Click **OK**.

Distributing Report Results in Email Messages

Introduction

This topic provides a procedure to send report results in an email message to various individuals. The Email Distribution tab applies to all SiteProtector system users for which an email address is configured. Use the procedure in this topic to send reports in email messages to other SiteProtector system users.

Procedure

To email report results:

1. Select **Report** from the **Go to** list.
2. Right-click the report you want to send, and then select **New Report** from the pop-up menu.
3. Select the **Email Distribution** tab.
4. To e-mail the report as an attachment, select the **Email report as attachment for PDF report type** check box.

Note: If you select this option, you must select **PDF** as the **Report Type**.

5. Do one of the following:
 - To e-mail the report to all the SiteProtector system users that appear in the box, select the **Select All** check box.
 - To e-mail the report to specific SiteProtector system users, select the check boxes next to the individual users.
6. To add email addresses for non-SiteProtector system users who should receive the report, type the email addresses in the **Configure other email addresses separated by semicolons below** box.
7. Click **OK** to exit.

Note: The SiteProtector system sends an email message containing a hyperlink to the recipient. You must be authenticated with the SiteProtector system to view the report.

Working with Email Addresses in the SiteProtector System Users List

Introduction

You can add or edit email addresses to the current SiteProtector system Users List so that users can send or receive report results from other users through email.

Task overview

Adding email addresses to the SiteProtector system Users List is a three-task process:

Task	Description
1	Add new users to the current user list.
2	Enter the email server address to tell the SiteProtector system which email server to use to send the email.
3	Add email addresses to the users list.

Table 17: Adding email address to the SiteProtector system Users List

Adding users to current user list

To add new users:

1. Select **Report** from the **Go to** list.
2. Select **Tools → User Groups**.
3. In the left pane, choose the desired User Group, and then select **Add**.
Note: This step is optional. You do not have to choose a User Group in order to add a user to an email distribution list.
4. In the Members Search section, click **Add**.
5. In the Search Users/Groups to Add window, type the individual name in the Members Search window, and then click **Check Names**.
6. Select the desired member from the list, and then click **OK**.
Note: You can select more than one user.
7. In the Search Users/Groups to Add window, click **OK**.
8. In the User Groups window, click **OK**.

Entering the email server address

To enter the email server address:

1. Select **Tools → User Email Addresses**.
2. Type the email server address in the Email Server Address window.
3. Click **OK**.

Adding or editing email addresses to users

To add or edit email addresses:

1. Select **Tools → User Email Addresses**.
2. Select the user from the list, and then complete the settings as indicated in the following table:

Setting	Description
Adding an email address	<p>Do one of the following:</p> <ul style="list-style-type: none">• Click the Update with AD. <p>Note: You can select more than one user.</p> <ul style="list-style-type: none">• Select the user to add the email address to, and then click Edit email address to manually enter the email address. <p>Note: When you select Update with AD, the SiteProtector system automatically updates the email address with information obtained from the Active Directory.</p>
Edit email address	<p>Do the following:</p> <ol style="list-style-type: none">1. Select the user from the list, and then click Edit email address.2. Enter the email address, and then click OK.

3. Click **OK**.

SECTION C: Options for Specific Reports

Overview

Introduction This section provides descriptions for the options that apply to each report category. These categories are organized by category on the Report tab.

In this section This section contains the following topics:

Topic	Page
Assessment Reports	68
Asset Reports: Event Details and Summary	71
Asset Reports: Protection	74
Asset Reports: Asset Risk Report	75
Attack Activity Reports	79
Audit Reports: Audit Detail Report	83
Audit Reports: Audit User to Group Report	84
Content Filtering Reports	85
Mail Filtering Reports	87
Management Reports	89
Permission Reports	93
Ticket Reports	94
Virus Activity Reports	96

Assessment Reports

Introduction

This topic describes the options that you can configure for Assessment reports. The options that appear vary according to the report that you are configuring.

Assessment reports

Table 18 lists the Assessment reports that appear on the Report tab:

Function	Assessment Reports
Asset	<ul style="list-style-type: none">Asset Assessment DetailAsset Assessment Summary
Operating System	<ul style="list-style-type: none">Operating System SummaryOperating System Summary By Asset
Payment Card Industry (PCI)	<ul style="list-style-type: none">PCI DetailPCI Summary
Service	<ul style="list-style-type: none">Service SummaryService Summary By Asset
Vulnerability	<ul style="list-style-type: none">Top VulnerabilitiesVulnerability By AssetVulnerability By GroupVulnerability By OSVulnerability CountsVulnerability Counts By AssetVulnerability Detail By AssetVulnerability DifferentialVulnerability Names By AssetVulnerability Remedies By AssetVulnerability Summary By AssetVulnerable Assets

Table 18: Assessment Reports on the Report tab

Sorting options

Table 19 lists the sorting options for Assessment reports. These options appear in the Sort Results By list:

Reports	Options in the Sort Results By list
Top Vulnerabilities	<ul style="list-style-type: none">CountVulnerability Name
Vulnerability By Group	<ul style="list-style-type: none">Group NameHigh SeverityMedium SeverityLow SeverityTotal Vulnerabilities

Table 19: Sorting options for Assessment Reports

Reports	Options in the Sort Results By list
Asset Assessment Detail Asset Assessment Summary Operating System Summary Operating System Summary By Asset Service Summary By Asset Vulnerability Counts By Asset Vulnerability Detail By Asset Vulnerability Remedies By Asset	<ul style="list-style-type: none"> DNS Name IP Address Operating System
Vulnerability Name By Asset Vulnerability Summary By Asset	<ul style="list-style-type: none"> DNS Name IP Address
Vulnerable Assets	<ul style="list-style-type: none"> Asset Criticality Asset Name DNS Name IP Address
Vulnerability By OS	<ul style="list-style-type: none"> High Severity Medium Severity Low Severity Total Vulnerabilities OS Name

Table 19: *Sorting options for Assessment Reports (Continued)*

Assessment report options

Table 20 describes the options for Assessment reports and the tabs that they appear on. Not all options are available on every report:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option if to give other SiteProtector system users the option to view this report.
Available and Displayed	Display	Use the Add or Remove option to select which columns appear on the Vulnerability By Group report. Use the Up or Down option to adjust the order in which they appear in the report.
Include Exceptions	Filters	Select this option to include exceptions in the report that you are running.
Asset Value	Filters	Select one of the following to determine the asset name to use for the IP addresses that are displayed in the report: <ul style="list-style-type: none"> Best Name (defined by NetBios, then DNS, then IP) IP (IP address) DNS (Domain Name System) NB (NetBios) Note: Select Best Name to prevent blank asset names from appearing in the report, especially in environments where asset names are not populated consistently.

Table 20: *Assessment report options*

Option	Tab	Description
Sort Results By	Report Format	Select an option to sort the report by. See Table 19 for the list of options.
Sort Order	Report Format	Select one of the following options: <ul style="list-style-type: none"> Ascending Descending
Show Asset Details	Report Format	Select this option to view the asset details.
Group by	Report Format	Select one of the following options to sort the report by: <ul style="list-style-type: none"> Severity Status
Number of Records	Report Format	Select one of the following options: <ul style="list-style-type: none"> 5 10 25 50 100
Show Graph	Report Format	Select this option to display a graph on the report. This option only appears on the reports listed in Table 19.
Graph Style	Report Format	Select a graph style for the graph you enabled in the Show Graph box: <ul style="list-style-type: none"> Pie chart Bar chart
Show vulnerability fix details	Report Format	Select this option to display fix details for each vulnerability.
Standard Time Period	Report Period	Select one of the following time periods: <ul style="list-style-type: none"> Previous and This Number Day Week Month Year
Custom	Report Period	Select a date within the month to run the first day of the report, and then select one of the following to determine the time of the report: <ul style="list-style-type: none"> <i>SiteProtector system Console Time Zone</i> Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console. GMT
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none"> Select All Individual email addresses

Table 20: Assessment report options (Continued)

Asset Reports: Event Details and Summary

Introduction This topic describes the options that you can configure for Asset reports. The options that appear vary depending upon the type of Asset report you are configuring.

Asset reports The following Asset reports appear on the Report tab:

- Asset Event Details
- Asset Event Summary

Sorting options Table 21 lists the sorting options for the Asset Event Details report that appear in the Sort Results By list on the Report Format tab:

Report	Options in the Sort Results By list
Asset Event Details	<ul style="list-style-type: none"> • Event/Vulnerability Name • Asset Owner • Inventory Tag • Asset Function • Asset Criticality

Table 21: *Sorting options in the Asset Event Detail report*

Asset Report options Table 22 describes the options that appear on Asset reports and the tabs that they appear on. Not all options are available on every report:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Choose Assets to include	General	Select one the following: <ul style="list-style-type: none"> • All assets • Desktops Only • No desktops
Observance types to include	General	Select one of the following to include in the report: <ul style="list-style-type: none"> • Events • Vulnerabilities • Events and Vulnerabilities
Display summary by	General	Select one of the following to choose how to sort summary information in the Asset Event Summary report: <ul style="list-style-type: none"> • Criticality • Function • Owner

Table 22: *Asset report options*

Option	Tab	Description
Available	Filters	<p>Select one of the following to choose how to filter information to be sorted in the Asset Event Summary and the Asset Event Detail:</p> <ul style="list-style-type: none"> • Incomplete data • Vulnerability • Informational Only • Web Filter • Anti-Spam • Application Compliance
Displayed	Filters	<p>Select one of the following to choose how to filter information to be displayed in the Asset Event Summary and the Asset Event Detail:</p> <ul style="list-style-type: none"> • Intrusion Detection • AntiVirus • Firewall • Network Anomaly Detection
Owners	Filters	Select the owners that correspond to the assets that you want to appear in the report. If no owners are defined, no options will appear.
Criticality	Filters	Select the criticality levels that correspond to the assets that you want to appear in the report.
Functions	Filters	Select the functions that correspond to the assets that you want to appear in the report. If no functions are defined, no options will appear.
Include Exceptions	Filters	Select this option to include exceptions in the report that you are running.
Sort Results By	Report Format	Select an option to sort the report by. See Table 21 for the list of options.
Sort Order	Report Format	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Ascending • Descending
Show Graph	Report Format	Select this option to display a graph on the report.
Graph Style	Report Format	<p>Select a graph style for the graph you enabled in the Show Graph box:</p> <ul style="list-style-type: none"> • Pie chart • Bar chart
Number of Records	Report Format	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100

Table 22: Asset report options (Continued)

Option	Tab	Description
Standard Time Period	Report Period	<p>Select one of the following time periods:</p> <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	<p>Select a date within the month to run the first day of the report, and then select one of the following to determine the time of the report:</p> <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> <p>Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console.</p> <ul style="list-style-type: none"> • GMT
Select All	Email Distribution	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 22: Asset report options (Continued)

Asset Reports: Protection

Introduction

This topic describes the options that you can configure for Asset Protection reports. The following is a list of Asset Protection reports that appear on the Report tab:

- Desktop Protection Report
- Server Protection Report

Desktop Protection report options

Table 23 describes the options for the Protection reports and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the permission to view this report.
Display Version As	Display	Select one of the following to determine the type of version to display in the report: <ul style="list-style-type: none"> • Agent Version • Intrusion Detection and Prevention Version • Virus Protection Version • Combined Version
Display Assets By	Report Format	Select one of the following to determine the asset name to use for the IP addresses that are displayed in the report. <ul style="list-style-type: none"> • Best Name (defined by NetBios, then DNS, then IP) • IP (IP address) • DNS (Domain Name System) • NB (NetBios) Note: Select Best Name to avoid blank host names from appearing in the report, especially in environments where host names are inconsistently used.
Sort Results By	Report Format	Select an option to sort the results by: <ul style="list-style-type: none"> • Status • Version
Show Graph	Report Format	Select this option to display a graph on the report.
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 23: Protection report options

Asset Reports: Asset Risk Report

Introduction

This topic describes the options that you can configure in the Asset Risk report. Use this report to assess the risk associated with vulnerabilities on any assets on your Site. The report includes a graph of the risk trend for the specified reporting period, along with a risk score report for each asset group.

How the SiteProtector system determines risk score

The SiteProtector system combines risk factors with weighting and asset criticality to determine risk scores for each asset. Risk factors include attacks that are not blocked, vulnerabilities found on the assets, no asset protection (such as Proventia Server or Desktop), and no recent vulnerability scans (Internet Scanner or Enterprise Scanner). The SiteProtector system assigns risk score between 0 and 100 for each asset every day, as well as a total score for the entire Site.

Each risk factor has a value between one and 10, except Criticality, which has a value between 40 and 100. The SiteProtector system also assigns a weight to each factor, and the risk score is calculated by the sum of each factor multiplied by its weight, multiplied by the Asset Criticality weight, divided by the total of weights times 10.

Example: Asset Criticality x ((Factor 2 x weight 2)+(Factor 3 x weight 3)+... (Factor 10 x weight 10))/(Total of weights x 10)

Risk factors

Table 24 lists factors that determine risk score and their default weight values:

Risk Factor	Weight
Asset criticality	This is a raw score, determined as follows: <ul style="list-style-type: none"> • Low or unassigned: 40 • Medium: 50 • High: 70 • Critical: 100
High-severity, non-blocked attacks	10
Medium-severity, non-blocked attacks	3
Low-severity, non-blocked attacks	1
High-severity vulnerabilities	10
Medium-severity vulnerabilities	3
Low-severity vulnerabilities	1
Vulnerability on X-Force Hot List	10
Host not protected (Desktop or Server protection agent)	5
Host not scanned (Internet Scanner or Enterprise Scanner agent)	24

Table 24: Risk factors that determine an asset's risk score

Sample Risk Score Calculation 1

Asset 1 has a criticality of “Medium.” It is not protected by a Desktop or Server agent, which means no attacks have been detected. And since it has not been scanned within the past 90 days, there have been no vulnerabilities detected. Table 25 shows the risk scores and weights used in the calculation:

Risk Factor	Description	Raw Score	Weight
Criticality	Medium	50	N/A
High-severity, non-blocked attacks	None	0	10
Medium-severity, non-blocked attacks	None	0	3
Low-severity, non-blocked attacks	None	0	1
High-severity vulnerabilities	None	0	10
Medium-severity vulnerabilities	None	0	3
Low-severity vulnerabilities	None	0	1
Vulnerability on X-Force Hot List	None	0	10
Host not protected (Desktop or Server protection agent)	No protection	10	5
Host not scanned (Internet Scanner or Enterprise Scanner agent)	Not scanned	10	24

Table 25: Risk factors used to calculate risk score for Asset 1

The Risk Score calculation would look like this:

$$50 \times ((0 \times 10) + (0 \times 3) + (0 \times 1) + (0 \times 10) + (0 \times 3) + (0 \times 1) + (0 \times 10) + (10 \times 5) + (10 \times 24)) / 670 = 21.6$$

The report would show a risk score of **22**.

Sample Risk Score Calculation 2

Asset 2 has a criticality of “High.” It is protected by Proventia Desktop, which has detected 12 medium-severity (non-blocked) attacks and 25 low-severity (non-blocked) attacks. It was recently scanned by a IBM Proventia® Network Enterprise Scanner, which detected 2 medium-severity vulnerabilities, one of which is on the X-Force Hot List, and 5 low-severity vulnerabilities. Table 26 shows the risk scores and weights used in the calculation:

Risk Factor	Description	Raw Score	Weight
Criticality	High	70	N/A
High-severity, non-blocked attacks	None	0	10
Medium-severity, non-blocked attacks	12	8	3
Low-severity, non-blocked attacks	25	8	1
High-severity vulnerabilities	None	0	10
Medium-severity vulnerabilities	2	4	3
Low-severity vulnerabilities	5	5	1
Vulnerability on X-Force Hot List	1	1	10

Table 26: Risk factors used to calculate risk score for Asset 1

Risk Factor	Description	Raw Score	Weight
Host not protected (Desktop or Server protection agent)	Proventia Desktop 9.0	0	5
Host not scanned (Internet Scanner or Enterprise Scanner agent)	Scanned 5 days ago	0	24

Table 26: Risk factors used to calculate risk score for Asset 1

The Risk Score calculation would look like this:

$$70 \times ((0 \times 10) + (8 \times 3) + (8 \times 1) + (0 \times 10) + (4 \times 3) + (5 \times 1) + (1 \times 10) + (0 \times 5) + (0 \times 24)) / 670 = 61.64$$

The report would show a risk score of **62**.

Risk Scores

Risk scores below 15 will appear on the graph in **Green**. Risk scores from 15-35 appear **Yellow**, and scores above 35 appear **Red**.

Risk report options

Table 27 describes the options that appear on the Asset Risk report:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option if you want to give other SiteProtector system users permissions to view this report.
Display Assets by	Display	Select one of the following options to identify assets in the report: <ul style="list-style-type: none"> Best Name (defined by NetBios, then DNS, then IP) IP (IP address) DNS (Domain Name System) NB (NetBios) Note: Select Best Name to prevent blank asset names from appearing in the report, especially in environments where asset names are not populated consistently.
Standard Time Period	Report Period	Select this option to run a report covering a specified number of days, weeks, or months.
Custom Time Period	Report Period	Select this option to run a report covering a specific date range. Important: Reporting on future dates is not supported and will result in a risk score of 0.
Show Graph	Report Format	Select this option if you want the graphs to appear on the report.
Show Each Asset	Report Format	Select this option to display individual scores for each asset in the report.

Table 27: Options for the Asset Risk report

Option	Tab	Description
Sort Results by	Report Format	Select one of the following options to sort asset details by: <ul style="list-style-type: none">• Score• Asset• Operating System
Report Period Divided Into	Report Format	Select this option to display risk results in periods of days, weeks, months, quarters, or years.
Maximum Depth of Subgroups	Report Format	Select this option to define the depth of subgroups (1 through 9, or “all”) to display. Example: “1” would hide any subgroups.

Table 27: *Options for the Asset Risk report*

Attack Activity Reports

Introduction

This topic describes the options that you can configure for Attack Activity reports. The options that appear vary depending upon the type of Attack Activity report you are configuring.

Attack Activity reports

The following Attack Activity reports appear on the Report tab:

- Attacks By Group
- Attacks By Protection Domain
- Security Events By Category
- Top Attacks
- Top Attacks By Severity
- Top Sources of Attack
- Top Targets of Attack
- Top Targets of Attack By Severity

Sorting options

Table 28 lists the Attack Activity reports that you can sort and the sorting options for them. These options appear on the Report Format tab in the Sort Results By list:

Report	Options
Top Attacks	<ul style="list-style-type: none"> • Attack Name
Top Attacks By Severity	<ul style="list-style-type: none"> • Count
Top Targets of Attack By Severity	<ul style="list-style-type: none"> • Target Value
Attacks By Group	<ul style="list-style-type: none"> • Total Attacks
Attacks By Protection Domain	<ul style="list-style-type: none"> • High Severity
Top Sources of Attack	<ul style="list-style-type: none"> • Medium Severity
Top Targets of Attack	<ul style="list-style-type: none"> • Low Severity • Group Name • Source Value

Table 28: *Sorting options for the Attack Activity reports*

Attack activity report options

Table 29 describes the options for Attack Activity reports and the tabs that they appear on. Not all options are available on every report:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.

Table 29: *Attack Activity report options*

Option	Tab	Description
Choose Assets to include	General	Select one the following: <ul style="list-style-type: none"> • All assets • Desktops only • No Desktops
Add/Remove	Display	Add or remove the following: <ul style="list-style-type: none"> • High Severity • Medium Severity • Low Severity
Up/Down	Filters	Reorder the columns that you specified in the Add or Remove boxes.
Include Exceptions	Filters	Select this option to include exceptions in the report that you are running.
Source Value	Filters	Select one of the following to determine the asset name to use for the source addresses that are displayed in the report: <ul style="list-style-type: none"> • Best Name (defined by NetBios, then DNS, then IP) • IP (IP address) • DNS (Domain Name System) • NB (NetBios) Note: Select Best Name to avoid blank host names from appearing in the report, especially in environments where host names are not populated consistently.
Target Value	Filters	Select one of the following to determine the asset name to use for the target addresses that are displayed in the report: <ul style="list-style-type: none"> • Best Name (defined by NetBios, then DNS, then IP) • IP (IP address) • DNS (Domain Name System) • NB (NetBios) Note: Select Best Name to avoid blank host names from appearing in the report, especially in environments where host names are not populated consistently.
Available/Displayed	Filters	Add or remove the following from the report: <ul style="list-style-type: none"> • Incomplete data • Vulnerability • Informational Only • Web Filter • Anti-Spam • Application Compliance • Intrusion Detection • AntiVirus • Firewall • Network Anomaly Detection

Table 29: Attack Activity report options (Continued)

Option	Tab	Description
Status	Filters	<p>Select one of the following to filter by statuses:</p> <ul style="list-style-type: none"> • Select All (Event Statuses) • Blocked • Not Blocked, Not Vuln • Not Blocked, Vuln • Not Blocked, Vuln status unknown • Not Vulnerable • Unassigned • Unknown • Vulnerable
Standard Time Period	Report Period	<p>Select one of the following time periods:</p> <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	<p>Select a date within the month to run the first day of the report, and then select one of the following options to determine the time of the report:</p> <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> <p>Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console.</p> <ul style="list-style-type: none"> • GMT
Sort Results By	Report Format	Select an option to sort the report by. See Table 28 for the list of options.
Sort Order	Report Format	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Ascending • Descending
Number of Records	Report Format	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100
Show Graph	Report Format	Select this option to display a graph on the report.
Graph Style	Report Format	<p>Select a graph style for the graph you enabled in the Show Graph box:</p> <ul style="list-style-type: none"> • Pie chart • Bar chart

Table 29: Attack Activity report options (Continued)

Option	Tab	Description
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none">• Select All• Individual email addresses

Table 29: *Attack Activity report options (Continued)*

Audit Reports: Audit Detail Report

Introduction

This topic describes the options that you can configure for the Audit Detail report. Use this report to track the tasks users perform in the SiteProtector system.

Audit Detail report options

Table 30 describes the options for the Audit Detail report and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
User Name	Filters	Select this option to specify a user name(s) by which to filter data in the report. Note: Select All selects all users.
Activity Type	Filters	Select this option to specify the types of user actions you want the report to display.
Standard Time Period	Report Period	Select one of the following time periods: <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	Select a date within the month to run the first day of the report, and then select one of the following to determine the time of the report: <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console. • GMT
Sort Results By	Report Format	Select an option to sort the report by: <ul style="list-style-type: none"> • User Name • Activity Type
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 30: *Audit Detail report options*

Audit Reports: Audit User to Group Report

Introduction

This topic describes the options that you can configure in the User to Group report. Use this report to determine which SiteProtector system users belong to each User Group on your Site.

User to Group report options

Table 31 describes the options for the User to Group report and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Group Results by	Email Distribution	Select one of the following: <ul style="list-style-type: none">• User: sorts results by user name, displaying groups each user belongs to• Group: sorts results by User Group, displaying all users in each User Group

Table 31: *User to Group report options*

Content Filtering Reports

Introduction This topic describes the options that you can configure for Content Filtering reports.

Content Filtering reports The following Content Filtering reports appear on the Report tab:

- Top Web Categories
- Web Requests

Sorting options Table 32 lists the Content Filtering reports that you can sort and the sorting options. These options appear on the Report Format tab in the Sort Results By list:

Report	Options
Top Web Categories	<ul style="list-style-type: none"> • Asset Count • Request Count • Category
Web Requests	<ul style="list-style-type: none"> • Category • Asset Name

Table 32: *Sorting options for the Content Filtering reports*

Content Filtering report options Table 33 describes the options for the Content Filtering reports and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Include Exceptions	Filters	Select this option to include exceptions in the report that you are running.
Asset Name	Filters	<p>Select one of the following to determine the asset name to use for the IP addresses that are displayed in the report:</p> <ul style="list-style-type: none"> • Best Name (defined by NetBios, then DNS, then IP) • IP (IP address) • DNS (Domain Name System) • NB (NetBios) <p>Note: Select Best Name to avoid blank asset names from appearing in the report, especially in environments where asset names are not populated consistently.</p>
Choose Assets to include	Filters	<p>Select one the following:</p> <ul style="list-style-type: none"> • All assets • Desktops only • No Desktops

Table 33: *Content Filtering report options*

Option	Tab	Description
Standard Time Period	Report Period	<p>Select one of the following time periods:</p> <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	<p>Select a date within the month to run the first day of the report, and then select one of the following to determine the time of the report:</p> <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> <p>Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console.</p> <ul style="list-style-type: none"> • GMT
Sort Results By	Report Format	Select an option to sort the report by. See Table 32 for the list of options.
Sort Order	Report Format	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Ascending • Descending
Number of Records	Report Format	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100
Show Graph	Report Format	Select this option to display a graph on the report.
Select All	Email Distribution	<p>Select one of the following:</p> <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 33: Content Filtering report options (Continued)

Mail Filtering Reports

Introduction

This topic describes the options that you can configure for Mail Filtering reports. The options that appear vary depending upon the type of Email report you are configuring.

Email reports

The following Mail Filtering reports that appear on the Report tab:

- Executive Summary
- Top Analysis Modules
- Top Recipients
- Top Responses
- Top Senders
- Traffic Report

Email report options

Table 34 describes the options for Email reports and the tabs that they appear on. Not all options are available on every report:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Standard Time Period	Report Period	Select one of the following time periods: <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	Select a date within the month to run the first day of the report, and then select one of the following to determine the time of the report: <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> <p>Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console.</p> <ul style="list-style-type: none"> • GMT
Number of Records	Report Format	Select one of the following options: <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100

Table 34: *Email report options*

Option	Tab	Description
Sort Order	Report Format	Select one of the following options: <ul style="list-style-type: none">• Ascending• Descending
Sort Results By	Report Format	Select an option to sort the report by: <ul style="list-style-type: none">• Count• Total Size
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none">• Select All• Individual email addresses

Table 34: *Email report options (Continued)*

Management Reports

Introduction

This topic describes the options that you can configure for Management reports.

Management reports

The following Management reports appear on the Report tab:

- Attack Incidents
- Attack Status Summary
- Attack Trend
- Virus Activity Trend
- Vulnerability Trend

Column options

Table 35 lists the columns that you can include in Management reports. These options appear on the Display tab:

Report	Columns
Attack Incidents	<ul style="list-style-type: none"> • Description • High Severity • Medium Severity • Low Severity
Attack Status Summary	<ul style="list-style-type: none"> • Target Count • Source Count • Object Count • High Severity • Medium Severity • Low Severity
Attack Trend	<ul style="list-style-type: none"> • High Severity • Medium Severity • Low Severity
Virus Activity Trend	<ul style="list-style-type: none"> • High Severity • Medium Severity • Low Severity
Vulnerability Trend	<ul style="list-style-type: none"> • High Severity • Medium Severity • Low Severity

Table 35: Columns that you can include in the Management reports

Sorting options

Table 36 lists the criteria by which you can sort the columns in the Management reports. These options appear on the Report Format tab in the Sort Results By list:

Report	Options
Attack Incidents	<ul style="list-style-type: none"> • Date • Incident Name • High Severity • Medium Severity • Low Severity • Source Count • Target Count
Attack Status Summary	<ul style="list-style-type: none"> • Target Count • Source Count • Object Count • High Severity • Medium Severity • Low Severity
Attack Trend	<ul style="list-style-type: none"> • Units • High Severity • Medium Severity • Low Severity • Total Attacks
Vulnerability Trend	<ul style="list-style-type: none"> • Units • High Severity • Medium Severity • Low Severity • Total Attacks

Table 36: *Sorting options for the Management reports*

Management report options

Table 37 describes the options for the Management reports and the tabs that they appear on. Not all options appear on every report:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Available/Displayed	Display	Select the columns to appear in the report. See Table 35 for a list of the columns that you can configure for each report.
Up/Down	Display	Reorder the columns that you specified in the Add or Remove boxes.
Include Exceptions	Filter	Select this option to include exceptions in the report that you are running.

Table 37: *Management report options*

Option	Tab	Description
Include Fusion Incidents	Filter	Select this option to include Fusion incidents in the report that you are running.
Units	Filter	Select one of the following to filter the report by a specified time period: <ul style="list-style-type: none"> • Day • Week • Month • Quarter • Year
Available/Displayed	Filter	Add or remove the following from the report: <ul style="list-style-type: none"> • Incomplete data • Vulnerability • Informational Only • Web Filter • Anti-Spam • Application Compliance • Intrusion Detection • AntiVirus • Firewall • Network Anomaly Detection
Compare 2 Consecutive	Filter	Select from the following to filter the report by two specified time periods: <ul style="list-style-type: none"> • Day • Week • Month • Quarter • Year
Sort Results By	Report Format	Select an option to sort the report by. See Table 36 for the list of options.
Sort Order	Report Format	Select one of the following options: <ul style="list-style-type: none"> • Ascending • Descending
Number of Records	Report Format	Select one of the following options: <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100
Show Graph	Report Format	Select this option to display a graph on the report.

Table 37: Management report options (Continued)

Option	Tab	Description
Graph Style	Report Format	Select a graph style for the graph you enabled in the Show Graph box: <ul style="list-style-type: none"> • Pie chart • Bar chart
Maximum Number of Dates	Report Format	Specify the maximum number of dates to run the report.
Show Asset Details	Report Format	Select this option to view the asset details.
Group by	Report Format	Select one of the following options to sort the report by: <ul style="list-style-type: none"> • Severity • Status
Report Period Divided into	Report Format	Select one of the following to filter the report by a specified time period: <ul style="list-style-type: none"> • Day • Week • Month • Quarter • Year
Standard Time Period	Report Period	Select one of the following time periods: <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	Select a date within the month to run the first day of the report, and then select one of the following options to determine the time of the report: <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console. • GMT
First day of First Period	Report Period	Select a date within the month to run the first day of the report, and then select one of the options to determine time of the report: <ul style="list-style-type: none"> • Eastern Standard Time • GMT
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 37: Management report options (Continued)

Permission Reports

Introduction

This topic describes the options that you can configure for the Permission Detail report.

Permission Detail report options

Table 38 describes the options for the Permission Detail report and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Sort By	Report Format	Select one of the following columns by which to sort the report. Columns are sorted from the highest to the lowest event count: <ul style="list-style-type: none">• User• Group• Permission
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none">• Select All• Individual email addresses

Table 38: *Permission Detail report options*

Ticket Reports

Introduction

This topic describes the options that you can configure for Ticket reports.

Ticketing reports

The following is a list of Ticket reports that appear on the Report tab:

- Ticket Activity Summary
- Ticket Time Tracking
- Ticket Trend

Ticketing report options

Table 39 describes the options for the Ticket reports and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.
Display assigned users	Display	Select this option to display users that have been assigned tickets in the report.
Display category	Display	Select this option to display custom categories that are assigned to tickets in the report.
Display status	Display	Select this option to display the ticketing statuses (New, Open, In Progress, and so on) in the report.
Display priority	Display	Select this option to display the ticket's priority (Critical, High, Medium, Low) in the report.
Assigned Users	Filters	Select the individual users to display in the report. These users will appear in the report only if you selected the Display assigned users option on the Display tab.
Category	Filters	Select the categories to display in the report. These categories will appear in the report only if you selected the Display category option on the Display tab.
Status	Filters	Select the statuses to display in the report. These statuses will appear in the report only if you selected the Display status option on the Display tab.
Priority	Filters	Select the priority values to display in the report. These values will appear in the report only if you selected the Display priority option on the Display tab.
Number of Records	Report Format	Select one of the following options: <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100
Show Graph	Report Format	Select this option to display a graph on the report.

Table 39: *Ticket report options*

Option	Tab	Description
Graph Style	Report Format	Select a graph style for the graph you enabled in the Show Graph box: <ul style="list-style-type: none"> • Pie chart • Bar chart
Report Period Divided into	Report Format	Select one of the following to filter the report by a specified time period: <ul style="list-style-type: none"> • Day • Week • Month • Quarter • Year
Maximum Number of Dates	Report Format	Specify the maximum number of dates to run the report.
Standard Time Period	Report Period	Select one of the following time periods: <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	Select a date within the month to run the first day of the report, and then select one of the following to determine the time of the report: <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> <p>Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console.</p> <ul style="list-style-type: none"> • GMT
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 39: Ticket report options (Continued)

Virus Activity Reports

Introduction

This topic describes the options that you can configure for Virus Activity reports.

Virus Activity reports

The following is a list of Virus Activity reports that appear on the Report tab:

- Top Virus Activity
- Virus Activity By Asset
- Virus Activity By Group
- Virus Prevention Benefits
- Virus Trend Details

Sorting options

Table 40 lists the criteria by which you can sort the columns in the Management reports. These options appear in the Sort Results By list:

Report	Tab	Options
Top Virus Activity	Display	<ul style="list-style-type: none"> • Attack Name • Count
Virus Activity By Asset	Report Format	<ul style="list-style-type: none"> • Asset Value • High Severity • Medium Severity • Low Severity • Total Count
Virus Activity By Group	Report Format	<ul style="list-style-type: none"> • Asset Value • High Severity • Medium Severity • Low Severity • Total Count
Virus Trend Details	Report Format	<ul style="list-style-type: none"> • Asset Name • Virus Name • Total Count • Severity • Status • Time

Table 40: *Sorting options for the Management reports*

Virus Activity report options

Table 41 describes the options for the Virus Activity reports and the tabs that they appear on:

Option	Tab	Description
Share report with other SiteProtector system users	General	Select this option to give other SiteProtector system users the option to view this report.

Table 41: *Virus Activity report options*

Option	Tab	Description
Choose Assets to include	General	Select one the following from the list: <ul style="list-style-type: none"> • All assets • Desktops only • No Desktops
Sort Results By	Display	Select an option to sort the report by: <ul style="list-style-type: none"> • Attack Name • Count
Sort Order	Display	Select one of the following options: <ul style="list-style-type: none"> • Ascending • Descending
Number of Records	Display	Select one of the following options: <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100
Show Graph	Display	Select this option to display a graph on the report.
Available/Displayed	Display	Select the columns to appear in the report according to event severity, as follows: <ul style="list-style-type: none"> • High Severity • Medium Severity • Low Severity
Up/Down	Display	Reorder the columns that you specified in the Add or Remove boxes.
Display Assets By	Display	Select one of the following to determine the asset name to use for the IP addresses that are displayed in the report: <ul style="list-style-type: none"> • Best Name (defined by NetBios, then DNS, then IP) • IP (IP address) • DNS (Domain Name System) • NB (NetBios) <p>Note: Select Best Name to avoid blank host names from appearing in the report, especially in environments where host names are inconsistently used.</p>
Include Exceptions	Filters	Select this option to include exceptions in the report that you are running.

Table 41: *Virus Activity report options (Continued)*

Option	Tab	Description
Asset Value	Filters	<p>Select one of the following to determine the host name to use for the hosts that are displayed in the report:</p> <ul style="list-style-type: none"> • Best Name (defined by NetBios, then DNS, then IP) • IP (IP address) • DNS (Domain Name System) • NB (NetBios) <p>Note: Select Best Name to prevent blank host names from appearing in the report, especially in environments where host names are not populated consistently.</p>
Choose Assets to include	Filters	<p>Select one of the following to determine which assets to include:</p> <ul style="list-style-type: none"> • All Assets • No desktops • Desktops Only
Standard Time Period	Report Period	<p>Select one of the following time periods:</p> <ul style="list-style-type: none"> • Previous and This • Number • Day • Week • Month • Year
Custom	Report Period	<p>Select a date within the month to run the first day of the report, and then select one of the following options to determine the time of the report:</p> <ul style="list-style-type: none"> • <i>SiteProtector system Console Time Zone</i> <p>Note: The time zone that appears on your system is the time zone that is set on the SiteProtector system Console.</p> <ul style="list-style-type: none"> • GMT
Graph Style	Report Format	<p>Select a graph style for the graph you enabled in the Show Graph box:</p> <ul style="list-style-type: none"> • Pie chart • Bar chart
Report Period Divided into	Report Format	<p>Select one of the following to filter the report by a specified time period:</p> <ul style="list-style-type: none"> • Day • Week • Month • Quarter • Year

Table 41: Virus Activity report options (Continued)

Option	Tab	Description
Sort Results By	Report Format	Select an option to sort the report by: <ul style="list-style-type: none"> • Group Name • High Severity • Medium Severity • Low Severity • Total Count
Sort Order	Report Format	Select one of the following options: <ul style="list-style-type: none"> • Ascending • Descending
Number of Records	Report Format	Select one of the following options: <ul style="list-style-type: none"> • 5 • 10 • 25 • 50 • 100
Avg infection cost per asset	Report Format	Select this option to evaluate what kind of cost return you are receiving on virus prevention.
Show Graph	Report Format	Select this option to display a graph on the report.
Select All	Email Distribution	Select one of the following: <ul style="list-style-type: none"> • Select All • Individual email addresses

Table 41: *Virus Activity report options (Continued)*

Vulnerability Assessment and Remediation

Chapter 5

Identifying and Resolving Network Vulnerabilities

Overview

Introduction

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 ISS.

Before you continue

Review the following topic to be sure that you are following the correct process for vulnerability assessment and remediation:

- “Vulnerability Assessment and Remediation Checklist” on page 20

In this chapter

This chapter contains the following topics:

Topic	Page
Developing Vulnerability Assessment Plans	104
Vulnerability Data Generated by the SiteProtector System	105
Gathering Information About Vulnerability Events	106
Deciding Whether to Resolve Vulnerabilities	107
Repairing and Mitigating Vulnerabilities	108
Creating a Plan of Action	110
Implementing Upgrades and Patches	111

Developing Vulnerability Assessment Plans

Introduction 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 ISS 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

Figure 2 illustrates the vulnerability identification and resolution process:

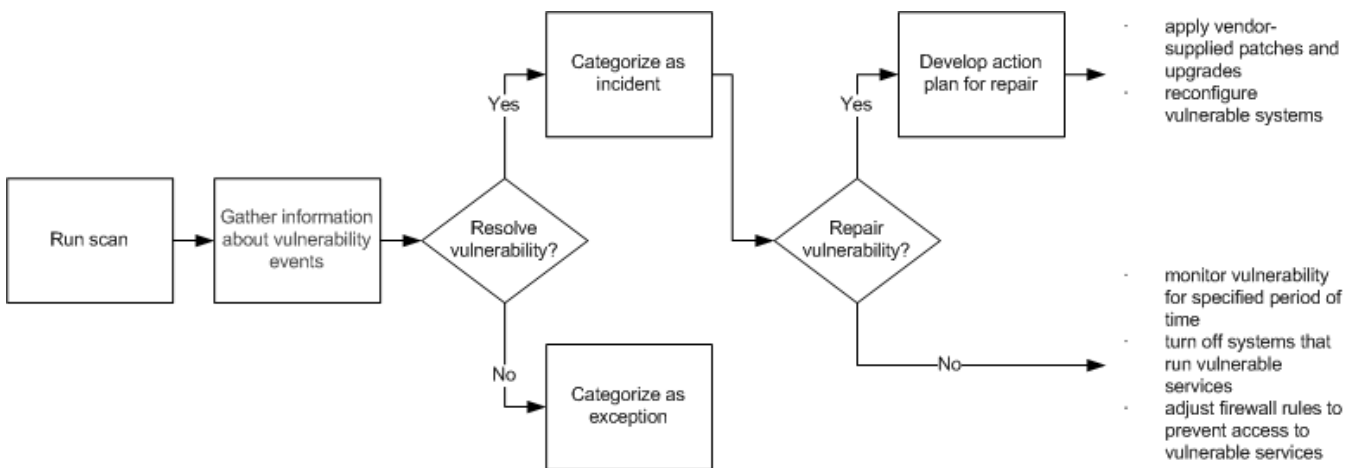


Figure 2: Diagram of vulnerability identification and resolution process

Vulnerability Data Generated by the SiteProtector System

Introduction 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—Information generated by Internet Scanner instances. 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—Information detected by the System Scanner application. 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 Table 42 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.

Table 42: *Vulnerabilities associated with specific attacks*

Gathering Information About Vulnerability Events

Introduction

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 Vulnerability analysis, refer to Table 12, “Vulnerability analysis view descriptions” on page 31.

Deciding Whether to Resolve Vulnerabilities

Introduction

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

Introduction	<p>When you decide to resolve a vulnerability, do one of the following:</p> <ul style="list-style-type: none">● repair the vulnerability● mitigate the risk of the vulnerability
Repairing	<p>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.</p>
Mitigating	<p>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.</p>
Exceptions and incidents	<p>The SiteProtector system provides a simple way to categorize vulnerabilities, as follows:</p> <ul style="list-style-type: none">● 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	<p>Consider using the baseline feature to track vulnerabilities that have been repaired or mitigated.</p>
If a vulnerability cannot be resolved immediately	<p>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.</p>
Resolving vulnerabilities	<p>Use Table 43 as a guide when resolving vulnerabilities:</p>

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.

Table 43: Resolving vulnerabilities

Methods	Task	Incident or Exception
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.

Table 43: *Resolving vulnerabilities (Continued)*

Reference: For more information on repairing vulnerabilities, refer to “Implementing Upgrades and Patches” on page 111.

Creating a Plan of Action

Introduction

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

Introduction	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	<p>To implement upgrades and patches successfully, you must do the following:</p> <ul style="list-style-type: none">● 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	<p>Use the following questions as a guide when implementing upgrades and patches:</p> <ul style="list-style-type: none">● 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 6

Managing Scans

Overview

Introduction

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

In this chapter

This chapter contains the following topics:

Topic	Page
Identifying Hosts on Your Network	114
Ensuring That Vulnerability Data is Complete and Accurate	115
Scheduling Vulnerability Scans	116
Running Background Scans	117
Reducing the Time Required to Run Scans	118

Identifying Hosts on Your Network

Introduction

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 Internet Scanner or 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 Internet Scanner or 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 Internet Scanner or Enterprise Scanner connection requests, it will not be added to the host table.

Ensuring That Vulnerability Data is Complete and Accurate

Introduction

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 Internet Scanner or Enterprise Scanner uses to establish connections with hosts, such as the following:

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

Note: You can achieve best performance if the Internet Scanner or 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 ISS 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

Introduction 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 Table 44 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

Table 44: *When to scan certain hosts*

Running Background Scans

Introduction 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 Table 45 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.
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.

Table 45: *Background scanning process overview*

Reference: For detailed information on background scanning, refer to the *IBM Proventia Network Enterprise Scanner User Guide* available at <http://www.iss.net/support/documentation/>.

Reducing the Time Required to Run Scans

Introduction

Network scans can generate large amounts of data. They can also be time consuming and can impact the performance of the Internet Scanner or 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 ISS 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.

Threat Investigation and Analysis

Chapter 7

Detecting Suspicious Activity

Overview

Introduction

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

In this chapter

This chapter contains the following sections:

Section	Page
Section A, "Suspicious Activity"	123
Section B, "Monitoring Event Analysis Views"	125
Section C, "Filtering Activity from Analysis Views"	135

SECTION A: Suspicious Activity

Overview

Introduction

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. The terms in this section are referred to often in “Part III: Threat Investigation and Analysis.”

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 “Filtering Activity from Analysis Views” on page 135.

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. Unauthorized activity is usually cause for concern; however, and it may require further investigation and remediation. Table 46 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.
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. The types of malicious activity are discussed in more detail on page 177.

Table 46: *Descriptions of unauthorized activity*

SECTION B: Monitoring Event Analysis Views

Overview

Introduction 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 “Analysis Views and Modes” on page 29 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.

In this section This section contains the following topics:

Topic	Page
Choosing the Traffic to Monitor and Correlate	126
Summary View	127
Event Name View	129
Target View	131
Attacker View	132
Scenarios for Using Guided Questions and Event Analysis Views	133

Choosing the Traffic to Monitor and Correlate

Introduction 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 Table 47 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.
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.

Table 47: *Descriptions of grouping structures*

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

Introduction	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?	<p>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.</p> <p>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.</p>
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 from the Summary view	<p>To add or remove portlets from the Summary view:</p> <ol style="list-style-type: none">1. Select Summary from the Go to list.2. Do one of the following:<ul style="list-style-type: none">■ Right-click the title bar on the portlets Summary tab, and then select or clear a portlet option from the pop-up menu.■ Select Action, then select or clear a portlet option from the menu. <p>Note: Check marks appear next to portlets that are enabled for a particular view.</p>
Modifying portlets in the Summary view	<p>To modify data displayed in portlets in the Summary view:</p> <ol style="list-style-type: none">1. Select Summary from the Go to list.2. 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.<p>The data in the portlet immediately refreshes based on the new time frame you selected.</p>3. To include events that are exceptions in the data displayed in a portlet, select the Include Exceptions check box in the portlet.<p>The data in the portlet immediately refreshes to include the event exceptions.</p> <p>Note: You cannot modify the data displayed in the System Health, Site Summary, Group Summary, Scan Progress, Ticket Status, and Offline / Stopped Agents portlets.</p>
Navigating from portlets in the Summary view	<p>To navigate from the portlets in the Summary view to the source of the data in the SiteProtector system:</p> <ol style="list-style-type: none">1. Select Summary from the Go to list.2. Do one of the following:<ul style="list-style-type: none">■ 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.

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.

Event Name View

Introduction

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

Figure 3 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	
System_Error	Unknown impact (no correlation)	High	2	2	2	4	09-30 08:00	10-01 08:00	

Figure 3: Event Name view with the SecurityFusion Module enabled

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 135.

- 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

Introduction

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

Figure 4 provides an example of the Target view:

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

Figure 4: Target view

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 "Filtering Activity from Analysis Views" on page 135.

Attacker View

Introduction

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

Figure 5 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

Figure 5: Attacker view

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

Introduction

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 the event analysis views:

- “Selecting Default Analysis Views” on page 30
- “Selecting Guided Questions” on page 37

Scenario 1

Table 48 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.
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.

Table 48: *Example of using guided questions to correlate by source*

SECTION C: Filtering Activity from Analysis Views

Overview

Introduction

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.

In this section

This section includes the following topics:

Topic	Page
Creating Baselines	136
Creating Incidents and Exceptions	138

Creating Baselines

Introduction 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.

Table 49: *Items changed in an Analysis view when you create a baseline*

Example of baseline view

Figure 6 provides an example of a baseline created for 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_Varning	Medium	18 (+18)	2 (+2)	2 (+2)	1 (+1)	2004-06-08 13:00:00 EDT
SMB_Vinreg_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_Vrty	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
WWindows_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

Figure 6: Example of a baseline created for the Event Analysis - Event Name view

Procedure

To create a baseline:

1. Select **Analysis** from the **Go to** list.
2. On the **Analysis** tab, select the view for which you want to define a baseline.

Tip: If the **Event Count** column is not in the current view, either add it or select an Analysis View that includes it.
3. Select **Action** → **Baseline** → **Establish**.

The current view is the baseline view.
4. If you have expanded items to examine event details, added columns or filters, or selected another group, and want to return to the baseline view, select **Action** → **Baseline** → **Restore**.
5. If you want to reset the event counts in selected rows but not the entire view, right-click the row or rows that you want to reset, and then select **Reset Selected Values** from the pop-up menu.

Creating Incidents and Exceptions

Introduction

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 146 for information about how to use exceptions to exclude events generated by authorized vulnerability scans.
- See “Incidents, Exceptions, and Attack Patterns” on page 188 for information about how to manage incidents and exceptions that are associated with SecurityFusion attack patterns.

When to use incidents and exceptions

Table 50 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.

Table 50: *When to use incidents and exceptions*

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.

Creating incidents and exceptions

To create an incident or an exception:

1. Do one of the following:

If you want to derive an incident or exception from...	Do the following...
a selected event or group of events	right-click an event or group of events in an analysis view, and then select Incident/Exception → New from the pop-up menu.
scratch	select Action → Incident/Exception → Manage , and then click Create .

Note: If you want to create an exception that is derived from selected events, you can include only one event at a time.

The New Incident/Exception window appears.

2. Select one of the following options:

- **Incident**
- **Exception**

3. If the SecurityFusion Module is enabled, and you want the Module to ignore the incident or exception, then select the **Ignore these events in SecurityFusion attack patterns** check box.
4. In the **Name** box, type a name for the incident or exception.
5. (Optional) Type helpful information about the incident or exception in the **Description** box.
6. Are you creating an incident or exception that is associated with an attack pattern?
 - If *yes*, then go to Step 13.
 - If *no*, then go to Step 7.
7. Click the **Start** and **End** arrows to set the time and select start and end dates for events that you want to include in the incident or exception.

Note: If you are creating an incident or exception that is derived from selected events, the fields in the New Incident/Exception window may be populated with the event information that applies. You can edit or delete this information as needed.
8. In the **Source** section, type an IP address in the **Start** and **End** boxes, if applicable.

Note: If there is only one IP address, type it in both boxes.

9. In the **Target** section, type an IP address in the **Start** and **End** boxes, if applicable.
10. In the **Tag Name** box, type the name of the event.
11. In the **Object Name** box, type the objects that are associated with this event.
12. In the **Observance Type** list, select the category that applies.
13. Click **OK**.

Editing incidents and exceptions

To edit an incident or exception:

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

To delete an incident or exception:

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 8

Is Suspicious Activity Significant?

Overview

Introduction

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

In this chapter

This chapter contains the following topics:

Topic	Page
Identifying the Location of an Attack	143
Identifying Activity Caused by Vulnerability Scans	144
Filtering Authorized Scans Using Attack Patterns	145
Creating Exceptions to Filter Scan Activity	146
Identifying Activity Caused by Misconfigured Systems	147
Identifying Normal Activity Commonly Identified as Suspicious	148

Quick reference for tasks covered in this chapter

Table 51 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 146.
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 145.
	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 144 • “Creating Exceptions to Filter Scan Activity” on page 146
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 144 • “Creating Exceptions to Filter Scan Activity” on page 146
suspect that activity is caused by a misconfigured system		see “Identifying Activity Caused by Misconfigured Systems” on page 147.
suspect that activity is caused by authorized activity that is commonly identified as suspicious		see “Identifying Normal Activity Commonly Identified as Suspicious” on page 148.

Table 51: *How to use the information in this chapter*

Identifying the Location of an Attack

Introduction

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

The best way to determine attack location is to use the Event Analysis - Agent view. To analyze the Event Analysis - Agent view for a particular event:

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.

Reference: You can also use guided questions to inquire about vulnerability events. See “Selecting Guided Questions” on page 37 for more information.

Identifying Activity Caused by Vulnerability Scans

Introduction	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	<p>A vulnerability scan may be in progress if you observe one or more of the following:</p> <p>Note: Exercise caution when using these guidelines because the authorized scan activity is often very similar to attack activity.</p> <ul style="list-style-type: none">● 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

Introduction

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 “SecurityFusion Module Impact Analysis” on page 47 for more information.

How does an Internet_Scanner_Scan attack pattern work?

The Internet_Scanner_Scan attack pattern identifies initiation of an 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

Figure 7 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):

Event Analysis - Incidents								
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

Figure 7: Example of Internet_Scanner_Scan attack patterns in the Event Analysis - Incidents view

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 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

Introduction

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 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.

Procedure

To create exceptions for filtering scans from the Console:

1. Perform the procedure in “Creating Incidents and Exceptions” on page 138.
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

Introduction

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. See Table 52 on page 148.
- 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

Introduction 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 Table 52 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.
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 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.
Nnntp_*	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.

Table 52: Events that typically flag legitimate traffic that exceeds predefined thresholds

Events	Description
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.

Table 52: *Events that typically flag legitimate traffic that exceeds predefined thresholds*

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

Chapter 9

Is an Attack a Threat?

Overview

Introduction

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.

In this section

This chapter contains the following topics:

Section	Page
Section A, "Using the SecurityFusion Module to Assess an Attack"	153
Section B, "Assessing an Attack Manually"	159

SECTION A: Using the SecurityFusion Module to Assess an Attack

Overview

Introduction

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.

In this section

This section contains the following topics:

Topic	Page
Viewing Attack Statuses	154

Viewing Attack Statuses

- Introduction**
- 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:

 - network multi-function security appliances
 - network intrusion prevention appliances
 - server sensor

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.

Table 53: *Statuses for intrusion detection events*

Status	Reason	Description
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.
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.

Table 53: Statuses for intrusion detection events (Continued)

Status	Reason	Description
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	Internet Scanner ran the correlating vulnerability check against the target, but the target did not confirm whether the vulnerability exists.
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 appliance	The attack failed because the appliance protecting the host in inline protection mode blocked the attack.
	Attacker quarantined by Proventia appliance	The attack failed because the appliance protecting the host quarantined the attack.
Simulated block	Proventia 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.

Table 53: Statuses for intrusion detection events (Continued)

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.

Table 53: *Statuses for intrusion detection events (Continued)*

Procedure

To view the attack status for an event or group of events:

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, vuln 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**

Overview

Introduction

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.

In this section

This section contains the following topics:

Topic	Page
Determining the X-Force Risk Level of an Attack	160
Was the Attack Target Vulnerable?	162
Was the Target Service or Operating System Susceptible?	165

Determining the X-Force Risk Level of an Attack

Introduction 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

Figure 8: Viewing X-Force risk levels on the Console

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).

Table 54: Descriptions of X-Force risk levels

Risk Level	Description
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.

Table 54: *Descriptions of X-Force risk levels (Continued)*

Was the Attack Target Vulnerable?

Introduction

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 Internet Scanner or 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 Internet Scanner or 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 Internet Scanner or Enterprise Scanner L5 policy was applied.

Running scans against attack targets using Internet Scanner

To run a vulnerability scan against an attack target for specific exploits using Internet Scanner:

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 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 using Enterprise Scanner

To run an ad hoc assessment scan of an entire group of assets or of one or more selected assets using Enterprise Scanner:

1. Select **Asset** from the **Go to** list.
2. Do one of the following:
 - Select a group in the left pane.
 - Select one or more assets in the right pane.
3. Right-click the group or the assets to scan, and then select **Scan**.
The Remote Scan window appears.
4. Select **Enterprise Scanner**.
5. Click the **Adhoc Scan Control** icon.
6. In the Ad Hoc Assessment section, select the **Perform one-time discovery scan of this group** check box.
7. Type a **Job name** to identify the job when it appears in the Command Jobs window.
8. If you want the scan to run only during your scheduled scanning windows, select the **Run only during open discovery windows** check box.
9. Click **Assessment** in the left pane.
10. Configure the policy the same way as you would configure the background Assessment policy.
11. Click **OK**.

The ad hoc assessment scan appears in the Command Jobs window.

Running an ad hoc discovery scan using Enterprise Scanner

To run a one-time ad hoc discovery scan from Enterprise Scanner that uses ranges of IP addresses to discover devices running on your network:

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, and then select **Scan**.
The Remote Scan window appears.
4. Select **Enterprise Scanner**.
5. In the Ad Hoc Assessment section, select the **Perform one-time discovery scan of this group** check box.
6. Type a **Job name** to identify the job when it appears in the Command Jobs window.
7. If you want the scan to run only during your scheduled scanning windows, select the **Run only during open discovery windows** check box.
8. Click **Discovery** in the left pane.
9. Type the range, or ranges, of IP addresses to scan in the **IP range(s) to scan** box.
10. 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.

11. 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.
12. Click **OK**.

The ad hoc assessment scan appears in the Command Jobs window.

Was the Target Service or Operating System Susceptible?

Introduction

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

Table 55: *Task overview*

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 162.

Operating system
susceptibility

Figure 9 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:

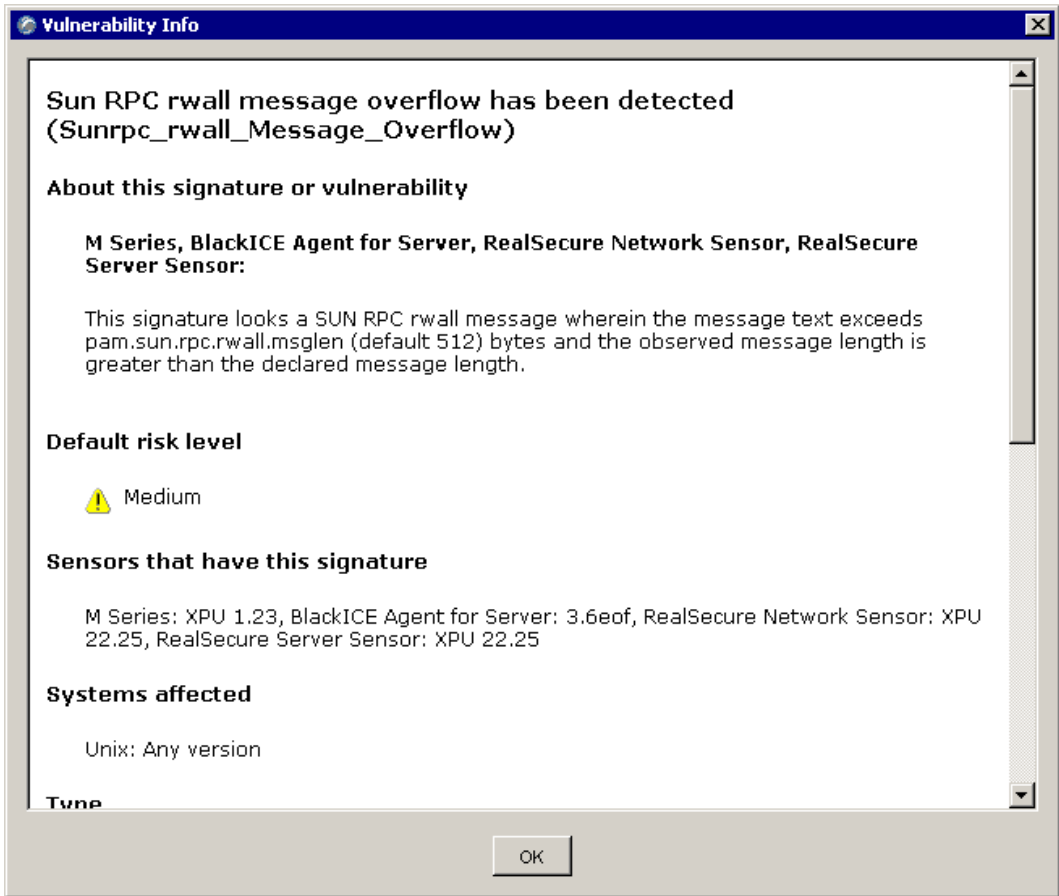


Figure 9: Example of an exploit that only affects Unix operating systems

**Service
susceptibility**

Figure 10 shows security information for the PeopleSoft Iclient servlet. Note that PeopleSoft is the only service that is affected by this exploit:

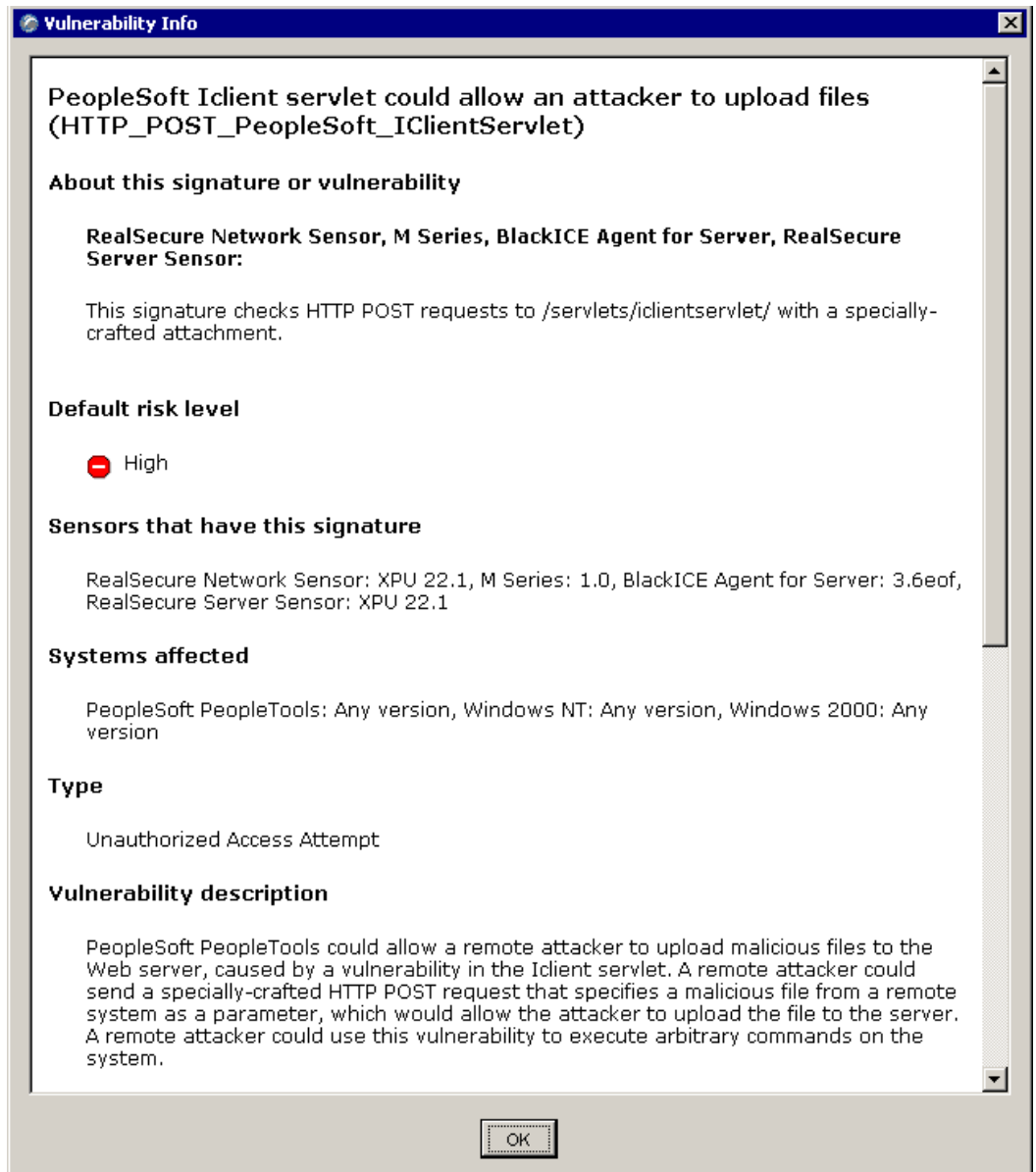


Figure 10: Example of an exploit that only affects PeopleSoft services

**Accessing security
information about
an event**

To access security information about an event:

- 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.

Determine the operating system of a target asset

To determine the operating system of assets that are targeted by an attack:

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.

A list of target operating systems appears.

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

Determining the service that is targeted

To use guided questions to determine the service that is targeted by an attack:

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 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?**

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.

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.

Chapter 10

Tracking and Prioritizing Confirmed Attacks

Overview

Introduction

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.

In this chapter

This chapter contains the following topics:

Topic	Page
Guidelines for Establishing Ticket Priority	170
Creating Tickets	172
Viewing Tickets	174

Guidelines for Establishing Ticket Priority

Introduction

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 Table 56 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
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

Table 56: *How to determine the severity of an incident*

Suggested Priority Level	Characteristics
4	<ul style="list-style-type: none"> • small numbers of system probes, scans and similar activities detected on internal systems • intelligence received concerning threats to which your organization may be vulnerable • increased risk of attack in general
5 (Low)	<ul style="list-style-type: none"> • small numbers of system probes, scans and similar activities detected on internal systems • isolated instances of known computer viruses or worms easily handled by deployed antivirus software

Table 56: *How to determine the severity of an incident (Continued)*

Creating Tickets

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

Ticket types Table 57 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.

Table 57: *Description of ticket types*

Vulnerability auto ticketing You can set up vulnerability auto ticketing so that the SiteProtector system will automatically generate 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 Proventia Network Enterprise Scanner or Internet Scanner.

Reference: Refer to the *SiteProtector System Configuration Guide* available at <http://www.iss.net/support/documentation/> 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.

Procedure To create a ticket:

1. In the left pane, select the group or host that you want to associate with a ticket.
2. Select one of the following from the **Go to** list:
 - **Asset**
 - **Agent**
 - **Analysis**
3. Right-click the asset, agent, or event for which you want to create the ticket, and then select **New Ticket** on the pop-up menu.

The New Ticket tab appears.

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

4. Provide the following general information as necessary to create the ticket:

In this field...	Do the following...
Priority	Select a value from the list. Use the priority levels specified in Table 56 on page 170 as a guide.
Responsibility	Select a SiteProtector system user from the list.
Due Date	The Priority you select automatically determines the due date. If you want to change the due date, select a date by which the ticket must be closed.
Category	Type information in the custom fields that are created by the Site Administrator.
Synopsis	Type a brief description of the issue you want to track. Provide enough information so that you can easily distinguish it from other tickets that are listed in the Ticketing view.
Actions	Type a description of the actions that were performed. For example, you could specify the following: <ul style="list-style-type: none"> the parties that were notified the actions taken to remove or remediate the attack the preventative measures to prevent future attacks

5. Select the **Custom Category** tab, and then type values for any custom categories that apply.

Note: SiteProtector system Administrators must create custom categories before you can enter this information.

6. Select **Action** → **Save All**.
7. Click **OK**.

Viewing Tickets

Introduction

In the Ticketing view, you can view any tickets you created in the SiteProtector system. 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. Table 58 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.

Table 58: *Items that are displayed in the Ticketing view*

Procedure

To view or edit tickets:

1. Select the group or Site for which you want to view tickets.
2. Select **Ticketing** from the **Go to** list.
A list of all active tickets appears.
Note: You can click on any column header to sort tickets by that column.
3. Double-click the ticket you want to view.
The **Ticket Detail** window appears.
4. In the top area of the window, you can view or edit the following items:
Note: The bottom area shows revisions of the ticket. Double-click a revision to see details for that revision.

Chapter 11

Determining the Scope of Attack

Overview

Introduction 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.

In this chapter This chapter contains the following topics:

Topic	Page
Attack Scope	176
Goals of Typical Attackers	177
Viewing the Number of Assets Targeted by an Attacker	178
Viewing the Number of Platforms Targeted by an Attacker	179

Attack Scope

Introduction

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 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

Introduction

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.

Table 59: *Attacker theft goals*

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

Introduction

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. Use this topic to help you identify the number of hosts the attacker is targeting using the Event Analysis - Event Name view.

Reference: For an illustration and additional guidelines for using the Event Name view, see page 129.

Procedure

To view the number of assets targeted by an attacker:

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.

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

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.

Viewing the Number of Platforms Targeted by an Attacker

Introduction

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. 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.

Reference: See page 132 for a description and illustration of the Attacker view.

Procedure

To customize the Attacker view:

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.

Chapter 12

Identifying Compromised Systems

Overview

Introduction

After you begin to track and investigate a confirmed attack, you should determine if the systems on your network have been compromised, and then determine the degree to which they have been compromised. Use the background information and examples in this chapter to identify compromised systems using the SecurityFusion Module attack patterns.

Goals of identifying compromised systems

The goals of identifying compromised systems are as follows:

- to correlate the incident activity with other disparate events that may originate from the same attacker or group of attackers
- to reconstruct the path of the attacker—from the point at which the attacker began gathering information to the last asset the attacker compromised
- to identify systems where you should collect forensic evidence

Degree of penetration

The location and number of compromised systems that are involved in a particular attack can help you determine the attacker's degree of penetration into your internal network or, more specifically, 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 compromised the integrity of your assets.

In this chapter

This chapter contains the following sections:

Section	Page
Section A, "SecurityFusion Module Attack Patterns"	183
Section B, "Identifying Information Gathering Activities"	189
Section C, "Identifying Log On Activities"	193
Section D, "Identifying Break-In Activities"	199
Section E, "Identifying Evasion Activity"	205
Section F, "Identifying Denial of Service Attacks"	209

SECTION A: SecurityFusion Module Attack Patterns

Overview

Introduction

The SecurityFusion Module attack patterns provide a quick and easy way to identify compromised systems in the SiteProtector system. Use the background information and procedures in this section to familiarize yourself with attack patterns and how to use them.

In this section

This section contains the following topics:

Topic	Page
How Attack Patterns Work	184
Host Patterns	185
Viewing Attack Patterns	186
Incidents, Exceptions, and Attack Patterns	188

How Attack Patterns Work

Introduction

The SecurityFusion Module searches for patterns of events to identify attack patterns—attacks that involve more than one event. The SecurityFusion Module can eliminate the manual task of searching a long list of events to determine which ones are related to the same attack.

Correlation rules

The SecurityFusion Module correlates related events to identify attack patterns. Some attack patterns are enabled by default; other patterns you must enable manually. The correlation rules consider many factors, including the following:

- types of events
- number of a specific types of events
- order in which different types of events occur
- number of source and target hosts
- time between required events
- status of the event based on impact analysis

Examples of attack pattern activity

Consider the following examples:

- You may be concerned about certain types of events only if they occur repeatedly and frequently. A single information-gathering event, for example, might not indicate a problem, but a number of those events over a short time period could indicate threatening activity.
- Some attacks involve more than a single type of event. To recognize a compromised host, for example, an attack pattern must include two types of events:
 - events that could compromise a host
 - events from a host indicating that it was compromised

False negatives or positives

Some common types of harmless network activity, such as what you see with proxy and email servers, can cause false positives that trigger attack pattern correlations. To avoid correlations in these situations, you can create an exception for the false positive events in the SiteProtector system and select the option that causes the Module to ignore those events in SecurityFusion attack patterns.

Host Patterns

Introduction

Attack patterns use visual identifiers referred to as *host patterns* to represent the relationship between source, target, and attacked assets. These patterns can help you identify the type of attack, the number of assets at risk, and intermediate assets that are also targeted. Use the descriptions in this topic to familiarize yourself with the following host patterns:

- many-to-one-to-many
- many-to-one
- one-to-many
- one-to-one

Host patterns

Table 60 describes the meaning of the host patterns in the Incident/Exception Description column in the Event Analysis - Incidents view:

Host Pattern	This attack pattern contains events where...
* -> x.x.x.x -> *	multiple sources target a single host, identified by IP address, and the identified host targets multiple hosts (many-to-one-to-many).
* -> x.x.x.x	multiple sources target a single host that is identified by IP address (many-to-one).
x.x.x.x -> *	a single host, identified by IP address, targets multiple hosts (one-to-many).
x.x.x.x -> y.y.y.y	a single host targets a single host, and both hosts are identified by IP address (one-to-one).

Table 60: *Host pattern descriptions*

Host pattern legend

Table 61 describes the meaning of the symbols in Table 60:

Symbol	Description
* (asterisk)	At least one, but potentially more than one, host IP address.
x.x.x.x	A specific host, which is specifically identified by IP address in the Incident/Exception Description.
y.y.y.y	A specific host, which is specifically identified by IP address in the Incident/Exception Description.
->	Events whose sources and targets are identified by *, x.x.x.x, and y.y.y.y.

Table 61: *Host pattern legend*

Viewing Attack Patterns

Introduction

By default, attack pattern correlations appear with Incidents in the Incidents view. You can do the following with attack patterns:

- use guided questions to view details of underlying events
- document your analysis and responses to an attack pattern correlation
- create incidents and exceptions
- create spreadsheets

When does an attack pattern appear

The SecurityFusion Module saves attack pattern correlations to the SiteProtector system database, making them available from the Console, only after all the events and other criteria for the attack pattern are satisfied. The Module continues to monitor and update existing attack pattern correlations until the time limits for the attack patterns are reached.

Information that appears in the Event Analysis - Incidents view

Table 62 describes the data columns that appear for attack pattern correlations in the Event Analysis - Incidents view:

Column	Description
Incident/Exception Name	The name of the attack pattern, followed by a sequentially assigned, numeric identifier, in the following format: Attack_Pattern_Name~ID_n Note: You can change the Incident/Exception Name to follow your Site conventions.
Incident/Exception Description	A shorthand explanation and visual description of the hosts involved in the attack.
# High	The number of High Severity events in the attack pattern correlation.
# Medium	The number of Medium Severity events in the attack pattern correlation.
# Low	The number of Low Severity events in the attack pattern correlation.
Tag Count	The number of different types of events, identified by Tag Name, in the attack pattern correlation. An attack pattern correlation, such as a worm attack, could contain several instances of the same type of event, so the Tag Count may be smaller than the total number of events.
Source Count	The number of different IP addresses that are sources for events in the attack pattern correlation.
Target Count	The number of different IP addresses that are targets for events in the attack pattern correlation.
Object Count	The number of different objects targeted in the attack pattern correlation.
Earliest Event	The date and time of the earliest event in the attack pattern correlation.

Table 62: Information about attack patterns

Column	Description
Latest Event	The date and time of the latest event in the attack pattern correlation.

Table 62: *Information about attack patterns (Continued)*

Procedure

To see attack pattern correlations:

1. Select **Analysis** from the **Go to** list.
2. Select **Event Analysis - Incidents** view.
Active attack patterns appear in the right pane.

Incidents, Exceptions, and Attack Patterns

- Introduction

You can create incidents and exceptions from attack pattern correlations just as you can for events. The reasons for creating incidents and exceptions and how they work are slightly different, however, when you are dealing with attack patterns.

Reference: See for “Creating Incidents and Exceptions” on page 138 information about creating incidents and exceptions.
- Restriction

An exception for an attack pattern correlation applies to just that instance of the attack pattern—not to future instances. Therefore, you cannot use exceptions for attack patterns to manage false positives. This restriction is due to attack patterns being defined by a combination of filters.
- When to create an exception

If you determine that an attack pattern correlation either was never a threat or is no longer a threat, you can remove it from your view by creating an exception. To make an exception for similar attack pattern correlations, however, consider whether you can identify a false positive event that may trigger another attack pattern. You may want to create an exception for that event.
- When to create an incident

The analysis view that displays incidents also displays attack patterns. If you prefer, you can set up your view to display attack patterns separately from incidents. If you make that your permanent default view, you could use incidents to escalate attack patterns that are either verified attacks or attack patterns that you want to continue to monitor.
- Guidelines for creating incidents or exceptions

Note the following guidelines for creating incident or exceptions for attack pattern correlation in the New Incident/Exception window:

 - When you create an incident or an exception for an attack pattern, you can only modify the **Name** and **Description** fields.
 - The fields in the New Incident/Exception window correlate with the attack pattern fields as follows:
- | This field in the New Incident/Exception window... | Is the same as this field in the attack pattern... |
|--|--|
| Name | Incident/Exception Name. |
| Description | Incident/Exception Description. |
- 188

IBM Internet Security Systems

SECTION B: Identifying Information Gathering Activities

Overview

Introduction

Attackers use a wide variety of methods to gather information before they attack. Some methods are benign, such as performing Whois queries or reverse lookups on target systems. Other methods are more intrusive, such as active probing of network resources for detailed information about hosts, operating systems, network topology, and access points.

Information gathering activity can occur at any stage of an attack. It may precede or follow penetration of your network.

In this section

This section contains the following topic:

Topic	Page
Information Gathering Attack Patterns	190

Information Gathering Attack Patterns

Introduction This topic provides descriptions and examples of SecurityFusion Module attack patterns that identify information gathering activities.

Types of information gathering Table 63 describes attack pattern categories that are associated with information gathering:

Pattern Category	Description
Network probing	<ul style="list-style-type: none">• These patterns identify attackers who are probing a host for preliminary information.• Attackers perform these types of probes early in an attack so that they can gain information about how to perform more targeted reconnaissance or break-ins.• For example, to identify potential attack targets, attackers often sweep entire subnets using information gathering tools, such as ping or Nmap, to determine which hosts are active.
Targeted probing	<ul style="list-style-type: none">• These patterns identify attackers who are probing for information about specific services, protocols, or applications running on a host.• The objective is to narrow the inquiry to a handful of vulnerabilities that attackers can successfully exploit.• For example, attackers often scan firewalls for port 53 (UDP) to identify where DNS servers are monitoring so that they can attempt to access valuable host information contained on these servers or, worse, redirect trusted communication to an untrusted host.

Table 63: Attack pattern categories associated with information gathering

Information gathering and compromised hosts Information gathering activities by themselves do not typically compromise hosts, but they often precede these compromises. Attackers can glean valuable clues about systems using information gathering activities that can assist them in gaining access to hosts.

Information gathering attack patterns Table 64 provides descriptions of the information gathering attack patterns:

Attack Pattern	Description
Network_Probing	This correlated attack pattern uses the (x.x.x.x-*) format and detects information gathering attempts against multiple hosts from a single source.
Targeted_Probing	<p>This correlated attack pattern detects targeted attempts to gather information about a specific host.</p> <p>Important: You may see this attack pattern in conjunction with a Network_Break_In attack pattern from the same source if the attacker first launches an attack against this target, and then attempts to break in to other hosts on the network.</p>

Table 64: Descriptions of attack patterns that identify information gathering activities

Example of a Network_Probing attack pattern

The attacking host at IP address 1.1.1.1 scans the ports of the host at IP address 2.2.2.2. Host 1.1.1.1 first, and then attempts to get the DNS name and IP address of the host at IP address 4.4.4.4. Table 65 shows the sequence of events in this example:

Event Type	Event	Source	Target	Time
Info gathering	Port_Scan	1.1.1.1	2.2.2.2	2002-10-31 22:23:30 EST
Info gathering	DNS_All	1.1.1.1	4.4.4.4	2002-10-31 22:23:34 EST

Table 65: *Example of a Network_Probing attack pattern*

Example of a Targeted_Probing attack pattern

The attacking host at IP address 1.1.1.1 attempts first to gather information about the ports on the targeted host at IP address 2.2.2.2 first, and then to retrieve the version of Berkeley Internet Name Domain (BIND) server on that host. Table 66 shows the sequence of events:

Event Type	Event	Source	Target	Time
Info gathering	UDP_Port_Scan	1.1.1.1	2.2.2.2	2002-10-31 17:20:00 EST
Info gathering	Bind_Version_Request	1.1.1.1	4.4.4.4	2002-10-31 17:25:00 EST

Table 66: *Example of a Targeted_Probing attack pattern*

SECTION C: Identifying Log On Activities

Overview

Introduction

Attackers repeatedly log onto hosts usually within a short time period. Because many points of access exist, attackers attempt to log on to a range of services, applications, and operating systems, including database, email, and instant messaging programs.

In this section

This section contains the following topics.

Topic	Page
Logon Activities Between Compromised Hosts	194
Logon Failures	196
Logon Activities From a Spoofed Source	197

Logon Activities Between Compromised Hosts

Introduction Use the descriptions and examples in this topic to help you use attack patterns to identify logon activities between compromised hosts.

Host pattern The logons between compromised hosts attack patterns display the following host pattern in the Incidents/Exceptions description:

- * -> x.x.x.x -> *

Attack patterns Table 67 describes the attack patterns that identify logon activities between compromised hosts.

Attack Pattern	Description
Logon_To_Compromised_Host	This correlated attack pattern detects a compromised host by detecting a host that is attacked followed by a successful logon to the compromised host. This correlated attack consists of the following sequence of events: <ol style="list-style-type: none">1. Break-in attempts from one source (IP address) against a host.2. Successful remote logon(s) from the attacking host to the targeted host.
Logon_From_Compromised_Host	This correlated attack pattern detects targeted attempts to gather information about a specific host. This correlated attack consists of the following sequence of events: <ol style="list-style-type: none">1. Break-in attempts from one or more source hosts against one or more targeted hosts.2. Remote logons from one of the hosts targeted in the break-in attempts to one or more other hosts.

Table 67: Descriptions of attack patterns that identify log on activities

Example of a Logon_To_Compromised_Host attack pattern The user at IP address 1.1.1.1 makes several unsuccessful attempts to log on to the attacked host at IP address 2.2.2.2 over a short time interval, and then successfully logs on to that host. Table 68 shows the sequence of events:

Event Type	Event	Source	Target	Time
Compromise attack	IMAP_Overflow	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Remote logon	Successful_Login	1.1.1.1	2.2.2.2	2002-10-31 09:22:00 EST

Table 68: Example of a Logon_To_Compromised_Host attack pattern

Example of a Logon_From_Compromised_Host attack pattern

After several unsuccessful attempts, the attacking host at IP address 1.1.1.1 logs on to the host at IP address 2.2.2.2. Host 2.2.2.2 then successfully logs on to IP address 3.3.3.3. Table 69 shows the sequence of events:

Event Type	Event	Source	Target	Time
Compromise attack	Brute_force_login_attack	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Remote logon	Successful_login	2.2.2.2	3.3.3.3	2002-10-31 09:22:00 EST

Table 69: *Example of a Logon_From_Compromised_Host attack pattern*

Logon Failures

Introduction

The Logon_Failures_Against_Multiple_Hosts attack pattern consists of failed logon attempts from one source host against two or more targeted hosts. Use the descriptions and examples in this topic to help you use attack patterns to identify logon activities between compromised hosts.

Important: This attack pattern can be triggered by logon errors of legitimate users but still should be considered suspicious activity.

Host pattern

The Logon_Failures_Against_Multiple_Hosts attack pattern displays the following host pattern in the Incidents and Exceptions description:

- x.x.x.x -> *

Example of a Logon_Failures_Against_Multiple_Hosts attack pattern

The user at IP address 1.1.1.1 attempts to log on to two different IP addresses—2.2.2.2 and 4.4.4.4—and fails both times. Table 70 shows the sequence of events.

Event Type	Event	Source	Target	Time
Logon attempt	Failed_login-account_disabled	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Logon attempt	SQLServer_login_failed	1.1.1.1	4.4.4.4	2002-10-31 09:25:00 EST

Table 70: Example of a Logon_Failures_Against_Multiple_Hosts attack pattern

Logon Activities From a Spoofed Source

Introduction

The Logon_From_Spoofed_Source correlated attack pattern detects an attempt to exploit a trust relationship between two hosts on the network. Use the description, scenario, and example in this topic to help you identify logon activities from a spoofed host using attack patterns.

Host pattern

The Logon_From_Spoofed_Source attack pattern uses the following host pattern in the Incidents and Exceptions description:

- * -> x.x.x.x -> *

Logon_From_Spoofed_Source attack pattern

The Logon_From_Spoofed_Source attack pattern consists of the following sequence of attacks:

1. DoS attacks from one or more source hosts against a host
2. Remote logon attempts that appear to originate from the host that is the target of the DoS attack(s)

Reference: For more information about denial of service attacks, see Section F, "Identifying Denial of Service Attacks" on page 209.

Scenario

In the following scenario, Host A is trusted to log on to Host B:

1. The attacker executes a DoS attack against Host A to disable it from responding to log on response messages from other hosts.
2. The attacker then masquerades as Host A and attempts to log on to Host B (if B is known to trust A) or tries to log on to several hosts trying to find one that trusts A.
3. This attack cannot succeed unless the masquerading host is either on the same network as A or B, or on an intermediate network through which traffic between hosts A and B is routed.
4. If successful, the attacker logs on to Host B as Host A and is not detected as an intruder.

Example

While the targeted host at IP address 2.2.2.2 is under a denial of service attack, a remote logon originates from that address to IP address 4.4.4.4. This could indicate that an attacker on another host is attempting to masquerade as 2.2.2.2 to exploit trust relationships and to gain access to another host. Table 71 shows the sequence of events:

Event Type	Event	Source	Target	Time
DoS attack	Finger_Bomb	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Remote logon	Rlogin_Login	2.2.2.2	4.4.4.4	2002-10-31 09:21:00 EST

Table 71: Example of a Logon_From_Spoofed_Source attack pattern

SECTION D: Identifying Break-In Activities

Overview

Introduction

Break-in activities are attempts to obtain unauthorized access using techniques such as buffer overflows and brute force attacks. Attackers often use break-in attempts in combination with other types of exploits, such as denial of service and evasion attacks.

Targeted break-in attempts

These patterns identify attackers who launch a combination of attacks from a single source address so that they can gain control of a host. These patterns often include an unauthorized logon attempt followed or preceded by the following:

- unauthorized execution of malicious code that enables systems to run on the target host
- evasion or denial of service attacks

In this section

This section contains the following topics:

Topic	Page
Network Break-In Attempts	200
Targeted Break-In Attempts	201
Program Startups	202
Program Shutdowns	203

Network Break-In Attempts

Introduction The Network_Break_In_Attempt attack pattern detects break-in attempts against multiple hosts on your network. Use the description and example in this topic to help you use attack patterns to identify network break-in attempts.

Host pattern The Network_Break_In_Attempt attack pattern uses the following host pattern in the Incidents/Exceptions description:

- x.x.x.x -> *

Network_Break-In_Attempt attack pattern The Network_Break_In_Attempt attack pattern consists of at least two different types of break-in attacks from a single source host against two or more targeted hosts on your network.

Example After several unsuccessful attempts, the attacking host at IP address 1.1.1.1 logs on to the host at IP address 3.3.3.3. Host 1.1.1.1 then attempts a generic Intel overflow attack against the host at IP address 4.4.4.4. The attacking host may be randomly looking for a vulnerable target. Table 72 shows the sequence of events:

Event Type	Event	Source	Target	Time
Compromise attack	Brute_force_login_attack	1.1.1.1	3.3.3.3	2002-10-31 23:05:00 EST
Compromise attack	Generic_Intel_Overflow	1.1.1.1	4.4.4.4	2002-10-31 23:15:00 EST

Table 72: Example of a Network_Break_In_Attempt attack pattern

Targeted Break-In Attempts

Introduction

The Targeted_Break_In_Attempt attack pattern detects break-in attempts targeted against a specific host. This correlated attack consists of at least two types of break-in attempts from a single source host against a single targeted host. Use the description and example in this topic to help you use attack patterns to identify targeted break-in attempts.

Important: You may see this attack pattern in conjunction with a Network_Break_In attack pattern from the same source if the attacker first launches an attack against this target, and then attempts to break in to other hosts on the network

Host pattern

The Targeted_Break_In_Attempt attack pattern uses the following host pattern in the Incidents/Exceptions description:

- x.x.x.x -> y.y.y.y

Example of a Targeted_Break_In_Attempt attack pattern

After several unsuccessful attempts, the attacking host at IP address 1.1.1.1 logs on to the host at IP address 2.2.2.2. Host 1.1.1.1 then attempts a generic Intel overflow attack against host 2.2.2.2. Table 73 shows the sequence of events:

Event Type	Event	Source	Target	Time
Compromise attack	Brute_force_login_attack	1.1.1.1	2.2.2.2	2002/11/01 13:45:00 EST
Compromise attack	Generic_Intel_Overflow	1.1.1.1	2.2.2.2	2002/11/01 13:55:00 EST

Table 73: Example of a Targeted_Break_In_Attempt attack pattern

Program Startups

Introduction The Targeted_Break_In_Then_Program_Startup attack pattern recognizes a compromised host by detecting the start of a program on a host soon after a break-in attempt against that host. Use the description and example in this topic to help you use attack patterns to identify program startup attempts.

Host pattern The Targeted_Break_In_Then_Program_Startup attack pattern uses the following host pattern:

- * -> y.y.y.y

Targeted_Break_In_Then_Program_Startup attack pattern This correlated attack consists of the following sequence of events:

1. Break-in attempts from one or more sources (IP addresses) against a single host on your network
2. One or more programs shut down on the attacked host soon after the break-in attempts

Example After several unsuccessful attempts, the attacking host at IP address 1.1.1.1 logs on to the host at IP address 2.2.2.2. Soon after, Oracle starts on Host 2.2.2.2. Table 74 shows the sequence of events:

Event Type	Event	Source	Target	Time
Break-in attack	Brute_force_login_attack	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Start of program	Oracle_Startup	2.2.2.2	2.2.2.2	2002-10-31 09:22:00 EST

Table 74: Example of a Targeted_Break_In_Then_Program_Startup attack pattern

Program Shutdowns

Introduction

The Targeted_Break_In_Then_Program_Shutdown attack pattern recognizes a compromised host by detecting the shutting down of a program on a host soon after a break-in attempt against that host. Use the description and example in this topic to help you use attack patterns to identify program shutdown attempts.

Host pattern

The Targeted_Break_In_Then_Program_Shutdown attack pattern uses the following host pattern:

- * -> y.y.y.y

Targeted_Break_In_Then_Program_Shutdown attack pattern

This correlated attack consists of the following sequence of events:

1. Break-in attempts from one or more sources (IP addresses) against a single host on your network
2. One or more programs shut down on the attacked host soon after the break-in attempts

Example

The attacking host at IP address 1.1.1.1 makes several unsuccessful attempts to log on to the attacked host over a short time interval, then the Oracle database server process is shut down. Table 75 shows the sequence of events:

Event Type	Event	Source	Target	Time
Compromise attack	Brute_force_login_attack	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Shutdown of program	Oracle_Shutdown	2.2.2.2	2.2.2.2	2002-10-31 09:22:00 EST

Table 75: Example of a Targeted_Break_In_Then_Program_Shutdown attack pattern

SECTION E: Identifying Evasion Activity

Overview

Introduction

Evasion occurs when attackers attempt to impersonate trusted hosts or services or hide their attacks by fragmenting them in such a way that network monitoring tools cannot determine that they are malicious. A TCP overlap exploit is a good example of evasion because it constructs connections with overlapping data, which causes network monitoring tools to misinterpret the intent of the connection and erroneously accept the traffic. ICMP overlap exploits function similarly but are less likely to successfully be filtered by network monitoring tools because ICMP traffic is often required for network attacks.

In this section

This section contains the following topics:

Topic	Page
Targeted Probing and Evasion	206
Targeted Break-In Attempt and Evasion	207

Targeted Probing and Evasion

Introduction The Targeted_Probing_And_Evasion attack pattern detects attempts to gather information about a host while also attempting to avoid detection. Use the description and example in this topic to help you use attack patterns to identify targeted probing and evasion attempts.

Host pattern The Targeted_Probing_And_Evasion attack pattern uses the following host pattern in the Incidents/Exceptions description:

- x.x.x.x -> y.y.y.y

Targeted_Probing_And_Evasion attack pattern This correlated attack consists of the following events, in any order, from a single host against a single host:

- one or more information gathering events
- one or more evasion events

Example The attacking host at IP address 1.1.1.1 first attempts to gather information about the ports on the targeted host at IP address 2.2.2.2, and then sends a URL request that contains encoded escape sequences. The attacker may be using encoded escape sequences in an attempt to bypass intrusion detection systems. Table 76 shows the sequence of events:

Event Type	Event	Source	Target	Time
information gathering	UDP_Port_Scan	1.1.1.1	2.2.2.2	2002-10-31 09:21:00 EST
IDS evasion	HTTP_IIS_Double_Eval_Evasion	1.1.1.1	2.2.2.2	2002-10-31 09:23:00 EST

Table 76: Example of a Targeted_Probing_And_Evasion attack pattern

Targeted Break-In Attempt and Evasion

Introduction The Targeted_Break_In_Attempt_And_Evasion attack pattern detects break-in attempts along with attempts to avoid detection. Use the description and example in this topic to help you use attack patterns to identify targeted break-in and evasion attempts.

Host pattern The Targeted_Break_In_Attempt_And_Evasion attack pattern uses the following host pattern:

- x.x.x.x -> y.y.y.y

Targeted_Break_In_Attempt_And_Evasion attack pattern This correlated attack consists of the following attacks, in any order, from a single source host against a single targeted host:

- one or more break-in attempts
- one or more evasion events

Example The user at IP address 1.1.1.1 sends packets with overlapping data to the target at IP address 2.2.2.2, which may be an attempt to cause a problem for the intrusion detection system. The same attacker then makes several unsuccessful attempts to log on to the attacked host over a short period of time. Table 77 shows the sequence of events:

Event Type	Event	Source	Target	Time
IDS evasion	TCP_Overlap_Data	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
Compromise attack	Brute_force_login_attack	1.1.1.1	2.2.2.2	2002-10-31 09:21:00 EST

Table 77: Example of a Targeted_Break_In_Attempt_And_Evasion attack pattern

SECTION F: Identifying Denial of Service Attacks

Overview

Introduction

Denial of service attacks (DoSs) prevent systems or applications from functioning properly. The objectives of these attacks are as follows:

- perform acts of vandalism
- disable communication between hosts

Distributed denial of service attacks

A distributed denial of service attack (DDoS) is a more malicious kind of DOS attack. The DDoS launches a series of attacks from several compromised hosts against a target host. The target host usually accepts the requests because they are seen as routine traffic. The high volume of requests quickly consumes 100 percent of the host's CPU resources.

In this section

This section contains the following topics:

Topic	Page
Targeted DoS Attacks	210
Targeted DoS Successful	211
Attacking DDoS Agent	212

Targeted DoS Attacks

Introduction The Targeted_DoS attack pattern detects a denial of service (DoS) attack targeted against a specific host. This attack consists of at least two types of DoS attacks from a single host against a single host. Use the description and example in this topic to help you use attack patterns to identify targeted DoS attacks.

Host pattern The Targeted_DoS attack pattern uses the following host pattern in the Incidents/Exceptions description:

- x.x.x.x -> y.y.y.y

Example The attacking host at IP address 1.1.1.1 attempts a number of DoS attacks against the targeted host at IP address 2.2.2.2. Table 78 shows the sequence of events:

Event Type	Event	Source	Target	Time
DoS attack	Finger_Bomb	1.1.1.1	2.2.2.2	2002-10-31 14:41:00 EST
DoS attack	HTTP_ECware_DoS	1.1.1.1	2.2.2.2	2002-10-31 14:42:00 EST

Table 78: Example of a Targeted_DoS attack pattern

Targeted DoS Successful

Introduction The Targeted_DoS_Successful attack pattern recognizes a compromised host by detecting a successful DoS attack against a host. Use the description and example in this topic to help you use attack patterns to identify successful targeted DoS attacks.

Host pattern The Targeted_DoS_Successful attack pattern uses the following host pattern in the Incidents/Exceptions description:

- * -> y.y.y.y

Targeted_DoS_Successful attack pattern The Targeted_DoS_Successful attack pattern consists of the following sequence of events:

1. DoS attacks from one or more source hosts against a single targeted host, which is the target IP address in the events
2. An event from the attacked host confirming that the DoS attack was successful, such as 100 percent memory or CPU utilization

Example The attacking host at IP address 1.1.1.1 generates a DoS attack against the targeted host at IP address 2.2.2.2. The success of the attack is confirmed when an event indicates that the targeted host is out of memory. Table 79 shows the sequence of events:

Event Type	Event	Source	Target	Time
DoS attack	Finger_Bomb	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
DoS confirmation	Out_of_virtual_memory	2.2.2.2	2.2.2.2	2002-10-31 09:22:00 EST

Table 79: *Example of a Targeted_DoS_Successful attack pattern*

Attacking DDoS Agent

Introduction The Attack_DDoS_Agent attack pattern recognizes a compromised host that acts as a distributed denial of service (DDoS) agent in a DDoS attack. Use the description, scenario, and example in this topic to help you use attack patterns to identify an attacking DDoS agent.

Host pattern The Attack_DDoS_Agent attack pattern uses the following host pattern:

- * -> x.x.x.x -> *

Attack_DDoS_Agent attack pattern This correlated attack pattern consists of the following sequences of events:

1. One or more DDoS agent commands or responses to or from a single host
2. One or more DoS attack events against one or more hosts originating from the host that engaged in DDoS agent activity

Scenario Because a system may be able to sustain a single DoS attack, attackers may launch a DDoS attack in which several compromised hosts launch simultaneous DoS attacks against a network asset. The following scenario provides an example:

1. An attacker breaks in to (compromises) one or more hosts on your network.
2. The attacker plants a backdoor agent, which serves as the daemon, on the compromised hosts, which serves as the DoS attack daemon.
3. At a particular point in time, the daemons on all hosts simultaneously launch DoS attacks against other hosts.

Example The attacking host at IP address 1.1.1.1 installed a DDoS backdoor agent on the targeted host at IP address 2.2.2.2. The targeted host then became the source host for a DoS attack against the host at IP address 3.3.3.3. Table 80 shows the sequence of events:

Event Type	Event	Source	Target	Time
DDoS Backdoor	TFN2000	1.1.1.1	2.2.2.2	2002-10-31 09:20:00 EST
DoS attack	SYNFlood	2.2.2.2	3.3.3.3	2002-10-31 09:22:00 EST

Table 80: Example of an Attack_DDoS_Agent attack pattern

Index

a

- abuse 123
- access control
 - inappropriate or weak 105
 - scanning with highest level of user access 115
 - vulnerabilities due to improper user activity 105
- action plan for vulnerabilities 110
- activity, authorized versus unauthorized 123
- add-on components, summary 16
- agent view 30
- agent, description 11
- appliance, description 11
- application monitoring views 32
- architecture of SiteProtector, *illus* 13
- asset criticality, grouping by 126
- asset view 31
- assets 178
- attack detected 155
- attack location, significance of 143
- attack pattern recognition 16
- attack patterns 144–145
- attack scope 175–176
- attack successful 154
- attacker view 30, 132
- attacks 143, 178
 - target not vulnerable 162
- authorized activity 141
- authorized scans 142

b

- backdoor 105
- Best Name 69
- buffer overflow 105
- business function, grouping by 126

c

- change control, affect on baselines 136
- completeness of vulnerability data 165
- components

- descriptions of 14
- confidential information 177
- critical hosts 115
 - avoiding during peak times 116
 - vulnerabilities that affect 107

d

- detail view 31
- details view 30
- determining the source of 126
- discovery scans 114
- domain administrator rights, role in scanning 115
- domain controller hosts, role in scanning 118

e

- Enterprise 163
- Enterprise Scanner 113, 163
- Event Name view 178
- event name view 30
- events of undetermined importance 139
- exceptions 108, 138, 146
 - 108
 - categorizing vulnerabilities as 108
- exploits, sophistication of 176
- external probes and scans 131

f

- failed attack 156
- failure likely 156
- failure possible 156
- filtering authorized scans 145
- filtering, importance of 135
- firewalls
 - adjusting rules to prevent access 104, 109
 - blocking scans 115

g

- geography, grouping by 126
- guidelines for creating 138, 146
- guidelines for formatting 58
- guidelines for identifying 144
- guidelines for sending through email 59

h

- hosts
 - availability during scans 115
 - limiting number included in scans 118
- hosts, determining number targeted by an attack 176

i

- IBM Internet Security Systems
 - technical support 10
 - Web site 10
- IBM ISS Technical Support 10
- ICMP requests 115, 118
- identifying location using Agent view 143
- identifying the source of 132
- identifying the target of 131
- ignoring authorized scans using attack patterns
 - attack patterns 147
- impact analysis 16, 153
- impact analysis, defined 47
- improper configuration, vulnerabilities due to 105
- incidents 108
 - categorizing vulnerabilities as 108
- incidents view 31
- Internet Scanner 147
- Internet Scanner attack pattern 145
- Internet Scanner Scan 147
- IP address
 - determining organization that it is registered to 132
- iterative process, role in analysis 123

m

- malicious activity 123
- misconfigured systems 142, 147
- misuse 123

n

- not compliant 157
- not vulnerable 155
- nternet 145
- number attacker is targeting 178
- number of platforms targeted 178

o

- object view 31
- OS view 31

p

- patches
 - role in repairing vulnerabilities 108, 111
- penetration, degree of 176
- ping responses, role in scanning 118
- policy
 - maintaining between scans 115
 - reducing levels of default scan policies 118
- portlets, adding or removing from summary view 127
- priority 170
- probing
 - network 190

r

- Remedy Action Request System 169
- repairing vulnerabilities 108
- reports 58–59
- role in filtering authorized scans
 - authorized scans
 - attack patterns 144

s

- scanner, description 11
- scans 144, 165
- scans, guidelines for identifying 143
- scheduling report jobs, guidelines for 58
- SecurityFusion Module 16
 - attack pattern recognition 16
 - impact analysis 16
- sensitive traffic

- grouping according to 126
- sensor location, role in analysis 143
- sensor, description 11
- simulated block 156
- successful attack likely 154
- suspicious activity 126, 131–132
- system resources 177

t

- target object view 31
- target view 31
- target, operating system of 168
- target, services running on 168
- technical support, IBM Internet Security Systems 10
- theft 177
- Third Party Module
 - description 16
- ticket 169
- tickets 170
- topology, grouping by 126

u

- unauthorized activity 141
- unauthorized vulnerability scans 144
- upgrades
 - role in repairing vulnerabilities 111

v

- Vandalism 177
- vendors
 - patches supplied by 108
 - vulnerabilities specific to 105
- vuln name view 31
- vulnerabilities
 - advanced hackers that exploit 107
 - categories of 105
 - data generated by authorized scans 145
 - exploited by an outsider 107
 - informational 105
 - mitigating 108–109
 - monitoring 109
 - resolving 108
 - target of attack not vulnerable 162
 - that cannot be resolved immediately 108
 - worse case scenario if exploited 107
- vulnerability assessment scans
 - developing a plan 116

- managing large scans 118
- vulnerability check indeterminate 156
- vulnerability identification and resolution process, *illus* 104
- vulnerable, host 155

W

- Web site, IBM Internet Security Systems 10

X

- X-Force risk levels 160
- X-Press Updates
 - maintaining between scans 115

