

SecurityFusion Module Guide

Version 2.1, September 4, 2008

Overview

Introduction This guide provides information about installing and configuring SecurityFusion module 2.1 to work with SiteProtector 2.0, Service Pack 6.1 and 7.0.

Audience This guide is primarily for IT/security administrators, security managers, and implementation analysts who are responsible for the installation and configuration of the SecurityFusion module with Site Protector.

In this document This document contains the following sections:

Section	Page
Section A, "Introduction to the SecurityFusion Module"	3
Section B, "Installing the SecurityFusion Module"	7
Section C, "Configuring Policies"	13
Section D, "Configuring Responses"	25
Section E, "Additional Configuration Tasks"	33

SECTION A: Introduction to the SecurityFusion Module

Overview

Introduction This section provides an introduction to the SecurityFusion module.

In this section This section contains the following topics:

Topic	Page
What is the SecurityFusion Module?	4
The SecurityFusion Module Setup Process	5

What is the SecurityFusion Module?

Introduction

The *SecurityFusion module* is a separately purchased product for SiteProtector that provides additional security functionality. The SecurityFusion module increases your ability to quickly identify and respond to critical threats at your Site. Using advanced analysis techniques, the SecurityFusion module escalates high-impact attacks to help you focus on the most important attack activity.

How it works

When an intrusion detection agent detects an attack, the SecurityFusion module does the following:

- increases your ability to quickly identify and respond to critical threats at your Site
- escalates high impact attacks to help you focus on the most important attack activity
- analyses events from intrusion detection/prevention agents and scanning agents
- compares attack information 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
- consolidates the patterns into single incidents, which makes dealing with streaming event data much more manageable

Impact Analysis component

The Impact Analysis component compares intrusion detection events with vulnerability assessment, operating system, and sensor-blocking messages, so that it can immediately estimate the impact of the an individual event.

The SecurityFusion Module Setup Process

Introduction

This topic provides an overview of the stages of the SecurityFusion module process.

Requirement

Before you install and configure the SecurityFusion module, you must complete the tasks for setting up SiteProtector and the agents that work with SiteProtector. For information about this process, see the *SiteProtector Configuration Guide*.

Process

Table 1 describes the stages of the SecurityFusion module setup process:

Stage	Description
1	Installation: Install the SecurityFusion module on a dedicated computer that does not include any other SiteProtector software. See "Installing the SecurityFusion Module" on page 7.
2	Configuration: • Configure a custom policy for the SecurityFusion module that includes the assets monitored by the SecurityFusion module. See "Configuring Policies" on page 13. • Configure a custom response for the SecurityFusion module. See "Configuring Responses" on page 25. • Configure additional parameters for the SecurityFusion module. See "Additional Configuration Tasks" on page 33.

Table 1: *Stages of the SecurityFusion module setup process*

SECTION B: Installing the SecurityFusion Module

Overview

Introduction This section explains how to install the SecurityFusion module.

In this chapter This chapter contains the following topics:

Topic	Page
Before You Begin	8
SecurityFusion Module Licenses	9
Installing from the Deployment Manager	10
Installing the SecurityFusion Module from Separate Installation Packages	11

Evaluating the SecurityFusion module You can install the SecurityFusion module for evaluation purposes and operate without purchasing a license agreement, as follows:

- The evaluation period is 90 days.
- The full functionality of the SecurityFusion module is available.
- The SecurityFusion module generates periodic messages indicating the number of days left in the evaluation period.
- At the end of the evaluation period, you must purchase a license agreement to continue using the SecurityFusion module.

Before You Begin

Introduction

This topic defines the information you must obtain and the tasks you must perform before you install the SecurityFusion module.

Prerequisites

Before you install SecurityFusion module, you must complete the following tasks:

- Install and configure SiteProtector.
See the *SiteProtector Installation Guide* and *SiteProtector Configuration Guide*.
- Verify that you have administrative rights to the SiteProtector Database and Application Server.
- Choose a computer for the SecurityFusion module. You must install the SecurityFusion module on a separate, dedicated computer that does *not* include other SiteProtector software.
- Verify that the computer where you are installing the SecurityFusion module meets the system requirements.
See the *SiteProtector System Requirements*.
- Obtain a license for the SecurityFusion module. If you do not have a license for the SecurityFusion module, then you can run the program in evaluation mode until you obtain a license.
- Determine whether to use Windows or SQL Authentication to the SiteProtector Database.

Note: If you choose Windows Authentication, you must install the SecurityFusion module with the separate installation package; if you choose SQL Authentication, you may install from the Deployment Manager or the installation package.

Installation methods

Table 2 describes the methods for installing the SecurityFusion module:

Method	Description
Deployment Manager	To install the product from the Internet, start Internet Explorer, and then go to the Deployment Manager. Example: <code>https://ip_address_or_server_name:3994/deploymentmanager/</code>
Separate Installation Package	You can obtain the installation package from the following locations: • the IBM ISS Web site http://www.iss.net/download/ • the SecurityFusion folder on the IBM ISS product CD.

Table 2: *Methods for installing SecurityFusion module*

SecurityFusion Module Licenses

Introduction

Your license agreement for the SecurityFusion module allows you to protect a specific number of hosts with SecurityFusion. You must specify which assets can use SecurityFusion module licenses in the SecurityFusion module policy.

Important: The SecurityFusion module will not analyze events until you specify hosts.

How the SecurityFusion module allocates licenses

The SecurityFusion module allocates licenses at startup based on the following:

- the order in which hosts are specified for licensing in the SecurityFusion module policy
- SiteProtector knows of the host because of one of the following:
 - The host belongs to a group in Site Manager.
 - A scan performed by the Network Internet Scanner and Network Enterprise Scanner identified the host.
 - SiteProtector received an event for which the host was either the source or the target.

Guidelines for proxy servers

If you use a proxy server for internet access, you should not include the IP address of the server in your list of hosts. If you do, you may see the following false alarms:

- Traffic into the proxy may be interpreted as incoming attacks directed at the proxy.
- Traffic out of the proxy may be interpreted as outgoing attacks originating at the proxy.

Including a proxy for SecurityFusion module analysis can cause false alarms in either of the following cases:

- The proxy is both the source and the target of the attack.
- The source of the attack is a licensed IP address, and the target of the attack is the proxy.

Using DHCP addresses

When you use DHCP, IP addresses are assigned randomly and a host may use different IP addresses for each network log on. Random assignment of IP addresses may affect your use of licenses. The exact impact at your Site depends on the size of the range and the number of hosts that use the range.

IBM ISS recommends that you use static IP addresses for critical hosts and purchase enough licenses to cover all IP addresses in the range used by DHCP.

Installing from the Deployment Manager

Introduction This topic explains how to install the SecurityFusion module with Deployment Manager.

Procedure To install the SecurityFusion module with Deployment Manager:

1. On the computer where you want to install the SecurityFusion module, start Internet Explorer, and then go to the Deployment Manager.

Example:

`https://ip_address_or_server_name:3994/deploymentmanager/`

The Deployment Manager Main Menu appears.

2. Click **Install the SiteProtector Security Fusion Module**.

The Prerequisites page appears.

3. Verify that the computer meets the prerequisites, and then click **Next**.

The SQL Server Information page appears.

4. Provide connection information for the SQL Server instance running the SiteProtector database, and then click **Next**.

The Prepare to Install page appears.

5. Review the information on the Prepare to Install page, and then click **Install**.

The File Download window appears.

6. Select the **Run this program from its current location** option, and then click **OK**.

The Security Fusion module installation begins.

7. You must complete at least the minimum configuration tasks to make the SecurityFusion module function.

Installing the SecurityFusion Module from Separate Installation Packages

Introduction This topic explains how to install the SecurityFusion module from a separate installation package.

Obtaining the package You can obtain a separate installation package for the SecurityFusion module from the following locations:

- the IBM Internet Security Systems Web site:
<http://www.iss.net/download/>
- the IBM ISS product CD in the \SecurityFusion folder.

Procedure To install the SecurityFusion module from a separate installation package:

1. On the computer where you want to install the product, start the installation program.
The InstallShield Wizard appears.
2. Follow the instructions on the screen to complete the installation process.
3. You must complete at least the minimum configuration tasks to make the SecurityFusion module function.

SECTION C: Configuring Policies

Overview

Introduction

This section provides information about configuring SecurityFusion module policies, including how to define assets in the policy.

Requirement

You must configure and apply a custom policy for SecurityFusion module before the SecurityFusion module will function properly. The policy must include the following information:

- the assets protected by the SecurityFusion module
See “Defining Assets in SecurityFusion Module Policies” on page 15.
- response policies
See “Configuring Responses” on page 25.

Task overview

Table 3 describes the tasks for configuring the SecurityFusion module policies:

Task	Description
1	Configure the custom SecurityFusion module policy. See “Configuring and Applying Custom Policies” on page 14.
2	Define assets in the custom policy. See “Defining Assets in SecurityFusion Module Policies” on page 15.
3	Apply the custom policy. See “Configuring and Applying Custom Policies” on page 14.
4	Verify that the SecurityFusion module is working.

Table 3: *Tasks for configuring SecurityFusion module policies*

In this section

This section contains the following topics:

Topic	Page
Configuring and Applying Custom Policies	14
Defining Assets in SecurityFusion Module Policies	15
Verifying that the SecurityFusion Module is Working	19

Configuring and Applying Custom Policies

Introduction	This topic provides instructions for configuring custom policies based on the existing, predefined policies included with SiteProtector. Important: You cannot change the original, predefined policy.
Environments	SiteProtector provides predefined policies for the Windows environment.
Before you begin	Before you configure and apply custom policies for the SecurityFusion module, make sure the SecurityFusion module appears in the SiteProtector Console with a status of <i>Active</i>.
Configuring custom policies	To configure a custom policy for the SecurityFusion module: 1. In the left pane, right-click the Site Node that contains the SecurityFusion module, and then select Manage Policy from the pop-up menu. The Policy tab appears. 2. Right-click the SecurityFusion module policy, and then select Derive New from the pop-up menu. The Derive New Item window appears. 3. Type the name for the custom policy, and then click OK. 4. Edit the policy in the Common Policy Editor. 5. Save the policy. The policy is available for you to apply to the SecurityFusion module.
Applying policies	To apply a policy to SecurityFusion module: 1. In the left pane, select the group that contains the SecurityFusion module. 2. In the View list, select Agent. 3. In the right pane, right-click the agent, and then select Apply→Policy from the pop-up menu. The Apply Policy window appears. The Command Details section lists the Action (Apply Policy), the Asset where the agent is installed, and the Agent Type. 4. Click the Policy icon, and then select a policy from the list. 5. Click the Schedule icon, and then select Run Once to apply the policy immediately or schedule a job to apply the policy. 6. Click OK.

Defining Assets in SecurityFusion Module Policies

Introduction

This topic provides information about defining assets in the SecurityFusion module policy, including the following tasks:

- defining assets with single addresses
- defining assets with multiple IP addresses
- importing assets from host files

Methods

Table 4 describes the methods for defining assets in the SecurityFusion module policy:

Method	Description
Manual	Use this method to type asset information in the policy manually. You must follow strict format requirements for IP address and host names. You can use this method to define assets with multiple IP addresses in the policy.
Automatic	Use this method to import asset information into the policy automatically from a host file (.hst). The information in the host file must meet format requirements.

Table 4: *Methods for defining assets in the SecurityFusion module policy*

IP address requirements

IP addresses must meet the following requirements:

- Each IP address must be valid, otherwise the SecurityFusion module generates an error message. For example, if the user enters a DNS name for a computer that cannot be resolved to an IP address, the user will get an error message.

Note: Each IP address does not have to be in use. As long as there is a record in the DNS internal or external network, the SecurityFusion module will be able to resolve the IP address correctly.

Allowed formats and examples

Table 5 describes the allowed formats for IP addresses and provides examples:

Type	Allowed Formats	Examples
single IP address	IP address in dotted decimal notation	1.1.1.1
	IP address that includes a wild card (*)	1.1.1.*
	IP address in CIDR format	1.1.1.1/24
	DNS name	host-a.example.microsoft.com
	computer name ^a	MailServer01
	Web address ^b	www.iss.net
range of IP addresses	the first and last IP address separated by a hyphen	1.1.1.1-1.1.1.100 1.1.2.1-1.1.3.1

Table 5: Allowed formats for IP addresses and examples

- a.The SecurityFusion module translates the computer name into an IP address.
- b.The SecurityFusion module translates the Web address into an IP address.

Defining assets manually

To define an asset in the SecurityFusion module policy manually:

1. Open the custom SecurityFusion module policy for editing.
2. In the left pane, select **Host Configuration**.
3. In the right pane, type the names and addresses of your assets in the **Enter IP addresses and/or Host names to validate** box.
Important: The format of the addresses must meet the requirements as defined in this topic.
4. Click **Validate IPs**.
The valid IP addresses move to the **The following hosts are available for SecurityFusion analysis** box.
5. If there were any errors in your IP addresses, correct those errors, and then repeat Step 4.

Assets with multiple IP addresses

The SecurityFusion Impact Analysis Component can analyze events that occur on multi-homed systems, or systems that have more than one network interface card. By default, SecurityFusion module treats each IP address as a separate host, but you can configure SecurityFusion module to treat multiple IP addresses as a single host to analyze events that occur on those IP addresses.

Defining assets with multiple IP addresses

To define an asset with multiple IP addresses:

1. Open your custom SecurityFusion module policy for editing.
2. In the left pane, select **Host Configuration**.
3. In the right pane, scroll to the **Multi-Homed Systems (MHS) Configuration** box.
4. Click **Add**.
5. On the **MHS Configuration** dialog, type a host **Name**.
6. Type two or more **IP Addresses**, separated by commas or hard returns, and then click **OK**.
7. Repeat Steps 4 through 6 to add more multi-homed systems.
8. On the **File** menu, select **Save**, and then click the **Close** button.

Note: If you did not modify the active policy, you must manually apply the policy to make it active.

Host files

If you already have a Host File (.hst) available, then you can import lists of assets from the file into SecurityFusion module. You can generate a host file with Internet Scanner or create one yourself. For either method, use the formats for host names and addresses as explained earlier.

Importing assets from host files

To import assets from a host file:

1. Open your custom SecurityFusion module policy for editing.
2. In the left pane, select **Host Configuration**.
3. In the right pane, click **Import Host File**.
4. Locate the host file (.hst), and then click **Import**.
The content of the file appears in the **Enter IP addresses and/or Host names to validate** box.
5. Click **Validate Hosts**.
The valid IP addresses move to the **The following hosts are available for SecurityFusion analysis** box.
6. If there were any errors in your IP addresses, correct those errors, and then go to Step 5.
7. On the **File** menu, select **Save**, and then click the **Close** button.
Note: If you did not modify the active policy, you must manually apply the policy to make it active.
8. On the **File** menu, select **Save**, and then click the **Close** button.
Note: If you did not modify the active policy, then you must manually apply the policy to make it active.

Deleting assets from the policy

To delete assets from the SecurityFusion module policy:

1. Open your custom SecurityFusion module policy for editing.
2. In the left pane, select **Host Configuration**.
3. In the right pane, select the host(s) that you want to delete in the **The following Hosts are available for SecurityFusion analysis** box, and then click **Delete**.

The host(s) is deleted.

Note: You can only delete a line of hosts. If the line contains hosts that you do not want to delete, you must delete the line, and then add back the hosts to keep.

Tip: Use the CTRL and SHIFT keys to select multiple lines or a range.

4. On the **File** menu, select **Save**, and then click the **Close** button.

Note: If you did not modify the active policy, you must manually apply the policy to make it active.

Verifying that the SecurityFusion Module is Working

Introduction

To verify that the SecurityFusion module is working, you can check the status, and then look for specific SecurityFusion module event statuses in the Status column of the Analysis tab.

Prerequisites

If the SecurityFusion module does not appear to be working, make sure that you have met the following requirements:

- You must have specified hosts for the SecurityFusion module to analyze.
- You must have enabled impact analysis in the SecurityFusion module policy.
Note: All SecurityFusion module functions are enabled by default at installation.
- SiteProtector must be collecting the vulnerability and IDS data for the specified hosts.

Procedure

To verify that the SecurityFusion module is working:

1. In the left pane, select the group that contains the SecurityFusion module.
2. In the View list, select Agent.
3. In the right pane, verify that the Status column for the SecurityFusion module indicates *Active*.

Note: The Status column can indicate an *Active*, *Stopped*, or *Offline* status for the SecurityFusion module.

4. In the View list, select Analysis.
5. Verify that statuses appear in the Status column:

Note: The following status are determined by agents and may appear regardless of whether the SecurityFusion module is working:

- Failed attack (blocked by Proventia appliance)
- Failure likely (rolled-back change)
- Simulated block (Proventia appliance in simulation mode) statuses

Monitoring vulnerability status

Vulnerability Statuses

Table 6 includes a list of statuses and descriptions that might appear in the Status column, based on the most recent vulnerability information from Enterprise Scanner, Internet Scanner, Proventia Desktop, and the Proventia appliances.

Status	Definition
Allowed network access	An application was allowed network access on the host.
Allowed to run	An application was allowed to run on the host.
Attack failure (attacker quarantined by Proventia appliance)	The attack failed because the appliance protecting the host quarantined the attack.
Attack failure (blocked at host)	The attack failed because the agent protecting the host blocked the attack.
Attack failure (blocked by Proventia appliance)	The attack failed because the appliance protecting the host blocked the attack.
Attack failure (blocked packets)	The agent protecting the host blocked some of the attack packets, but the SecurityFusion Module could not determine with 100% accuracy that the attack failed.
Attack failure (confirmed by agent)	The agent detected traffic from the attacked host that confirms the failure of the attack.
Attack failure (dynamically blocked at host)	The agent used dynamic blocking to prevent the attack.
Attack likely successful (vulnerable)	Based on current vulnerability data, the targeted host appears to be vulnerable to the detected event, and the attack was probably successful.
Attack successful (file accessed)	An important system file was accessed and the event detected by a host-based agent.
Blocked application	An application was blocked or not allowed to run on the host.
Blocked network access	An application was denied network access on the host.
Compliant	The virus scanner and/or vulnerability signatures on the host are up to date.
Compliant (blocked app)	The local agent protecting the host blocked the application.
Compliant (expiring soon)	The virus scanner and/or signatures on the host are about to expire.
Deleted	Files were deleted on the host because it was infected with a worm or virus.
Detected attack (block response not enabled)	An attack was not blocked by an appliance because the block response was not enabled.

Table 6: *SecurityFusion module statuses*

Status	Definition
Detected attack (BOEP in Alert Only mode)	An attack was not blocked by Proventia Server because the agent was in simulation mode. The agent would have blocked the attack had it been in protection mode.
Detected attack (IPS in Alert Only Mode)	An attack was not blocked by an IPS appliance because the appliance was in simulation mode. The appliance would have blocked the attack had it been in protection mode.
Detected attack (OS check indeterminate)	The vulnerability assessment scan was not able to identify the host's operating system.
Detected attack (SecurityFusion not configured)	Neither the source nor the destination host is included in the License options of the SecurityFusion Module policy. Note: This status supersedes other applicable statuses such as (no analysis) or (not scanned recently).
Detected attack (vuln not scanned recently)	For one of the following reasons, no vulnerability or other host data information is available: - The host was never scanned. - The host's vulnerability data is older than the user defined expiration.
Detected event	An agent(s) detected an event.
Detected event (SecurityFusion not enabled)	The SecurityFusion Module is not enabled for this site or host.
Failed attack (blocked by firewall)	An attack was blocked by the agent's firewall.
Failed attack (connection reset)	A TCP reset was sent to the both the source and destination of the event resetting the connection.
Failed attack (file not accessed)	An attack attempted to access an important system file but access was prevented by a host-based agent.
Failed attack (port not open)	The port used to facilitate the attack is not open on the target host.
Failed attack (process terminated)	A suspect malicious process was terminated by a host-based agent.
Failed attack (rolled back change)	An agent detected an unauthorized change to a protected system object and reverted the object to its prior state.
Failed attack likely (no vulnerability)	A vulnerability assessment scan indicates that the host was not vulnerable to this attack, so the attack probably failed.
Failed attack likely (scanned, vuln not confirmed)	The host has been scanned, but the scanner was not able to confirm that the vulnerability exists.
Failed attack likely (wrong OS)	The targeted host's operating system is not vulnerable to the detected event.
File Cleaned	The file on the host contained a virus or worm but was cleaned by Proventia Desktop.

Table 6: SecurityFusion module statuses

Status	Definition
Matching traffic pattern detected	A Proventia Anomaly Detection appliance detected matching traffic patterns.
Not compliant	The scanner and/or virus signatures on the host are out of date or there is no scanner present. Proventia Desktop takes no action.
Not compliant (application access blocked)	The scanner and/or virus signatures on the host are out of date or there is no scanner present. Access to the application listed in the Event Source was blocked.
Not compliant (corporate access blocked)	The scanner and/or virus signatures on the host are out of date or there is no scanner present. Access to the corporate network was blocked.
Not compliant (network access blocked)	The scanner and/or virus signatures on the host are out of date or there is no scanner present. All network access was blocked.
Not Vulnerable	The scanned host is not susceptible to the specified exploit.
Policy violation detected	A Proventia Anomaly Detection appliance detected a violation of the current policy.
Propagation behavior detected	A Proventia Anomaly Detection appliance detected suspicious propagation behavior.
Quarantined	The file was isolated by an agent because it was infected by a worm or virus.
Scanning behavior detected	A Proventia Anomaly Detection appliance detected unauthorized scanning behavior.
Simulated block (blocking not enabled)	An attack was not blocked by an appliance because the appliance was in simulation mode and the block response was not enabled.
Successful attack (confirmed by agent)	The agent detected traffic from the attacked host that confirms the success of the attack.
Traffic anomaly detected	A Proventia Anomaly Detection appliance detected a deviation from typical network traffic patterns.
Vuln check indeterminate	The vulnerability was not conclusively identified by a scanner; therefore, it may exist on the scanned host.
Vulnerable	The scanned host is susceptible to the specified exploit.
Vulnerable (attack will be detected and partly blocked)	The agent was able to block some, but not all of, the suspected attack.
Vulnerable (attack will be detected and prevented)	The host is vulnerable to the attack, however the agent prevented the attack from occurring.
Vulnerable (attack will be detected)	The attack will be detected by the agent but not prevented.

Table 6: SecurityFusion module statuses

Status	Definition
Vulnerable (attack will not be detected)	The attack will not be detected and the system or host most likely will be compromised.

Table 6: *SecurityFusion module statuses*

Note: If Unknown impact (SecurityFusion module not enabled) appears in the Status column, then Event Collector is not configured correctly; or, in a multi-Event Collector environment, at least one Event Collector is not configured correctly.

SECTION D: Configuring Responses

Overview

Introduction This section provides information about configuring response policies for the SecurityFusion module.

Note: The Event Collector generates responses for the SecurityFusion module.

Before you begin Before you can configure e-mail, SNMP, or user-specified responses for SecurityFusion module, you must complete the following tasks:

- create a Event Collector response file
- apply the Event Collector response file to each Event Collector

Reference: For information about these tasks, see the *SiteProtector Help*.

In this section This section contains the following topics:

Topic	Page
Adjusting Severity Based on Event Impact	26
Displaying Events in the Console	27
Logging Events to the SiteProtector Database	28
Configuring E-mail and SNMP Responses	29
Configuring User-Specified Responses	31
Responding to Server Sensor Events	32

Adjusting Severity Based on Event Impact

Introduction

You can configure the SecurityFusion module to change the severity of events as follows:

- to reduce false alarms, lower the severity
- to emphasize an attack, raise the severity

Default response

The default is to use the response set by the sensor policy.

Attacks that fail or failure is likely

Table 7 describes the severity adjustment options (in the **Adjust severity to** list) for events that fail or are likely to fail:

Option	Description
Low	Sets the severity of the event to Low.
Medium	Sets the severity of the event to Medium.
(One level lower)	Sets the severity of the event to one level lower than the original severity.
(Do not adjust)	Does not change the severity of the event. Note: This is the default response.

Table 7: *Severity options for events likely to fail*

Attacks that succeed or success is likely

Table 8 describes the severity adjustment options (in the **Adjust severity to** list) for events that succeed or are likely to succeed:

Option	Description
High	Sets the severity of the event to High.
Medium	Sets the severity of the event to Medium.
(One level lower)	Sets the severity of the event to one level lower than the original severity.
(Do not adjust)	Does not change the severity of the event. Note: This is the default response.

Table 8: *Severity options for events likely to succeed*

Displaying Events in the Console

Introduction You can configure the SecurityFusion module to display or not display events in Console as follows:

- to reduce false alarms, do not display the event
- to emphasize an attack, display the event

Default response The default is to use the response set by the sensor policy.

Display options Table 9 describes the options (in the **Modify DISPLAY to** list) for displaying events:

Option	Description
Off	Does not display the event in Site Protector.
On	Displays the event in Site Protector. Important: You must turn on DISPLAY and LOGDB before Site Protector can display events.
(Do not adjust)	Uses the response that is set for the sensor in the sensor policy.

Table 9: *Display Options for events*

Logging Events to the SiteProtector Database

Introduction You can configure whether or not to save events in the SiteProtector Database (LOGDB). Use this response to ensure that you save only important events—regardless of the sensor response.

Default response The default is to use the response set by the sensor policy.

Logging options Table 10 describes the options (in the **Modify LOGDB to** list) for saving events in the Site DB:

Option	Description
Off	Does not log the event to the Site DB.
On	Logs the event to the Site DB. Important: You must turn on both DISPLAY and LOGDB before SiteProtector can display events in the Site Manager.
(Do not adjust)	Uses the response that is set for the sensor in the sensor policy.

Table 10: *Logging options for events*

Configuring E-mail and SNMP Responses

Introduction	You can configure the SecurityFusion module to emphasize events by sending mail and SNMP responses.
Default response	Email and SNMP responses are not sent unless you configure them.
Prerequisites	To send email and SNMP responses, you must have already performed the following: ● created a custom policy file for the SecurityFusion module ● created a custom response file for the Event Collector and sent to the Event Collector ● specified in the SecurityFusion module custom policy the response from the Event Collector's response file ● applied the SecurityFusion module custom policy to the SecurityFusion module Note: The name of the default SecurityFusion module response file is <code>Event Collector Response.Policy</code>.
Procedure	To configure an email or an SNMP response: 1. Open your custom SecurityFusion module policy for editing. 2. In the left pane, expand Impact Analysis Component Settings. 3. Do one of the following: ■ To change the response for failed attacks, select Responses for Failed Attacks. ■ To change the response for successful attacks, select Responses for Successful Attacks. 4. Select the check box next to the type or response you want to send: ■ EMAIL ■ SNMP 5. Does an arrow appear in the Response Name column? ■ If <i>yes</i>, go to Step 6. ■ If <i>no</i>, go to Step 7. 6. If you want to choose a different response, click the arrow, and then select another response. The name of the response you chose appears in the Response Name column. 7. If you want to make additional policy changes, refer to the following topics in the <i>SiteProtector Help</i>: ■ Overview: SecurityFusion Module Licensing ■ Overview: Managing Vulnerability Data ■ Overview: Responses Based on Event Impact

8. On the **File** menu, select **Save**, and then click the **Close** button.

One of the following occurs:

- If you modified the active policy, either a job automatically starts to apply the policy or a prompt appears for you to choose whether to apply the policy.
- If you did not modify the active policy, you must apply the policy manually to make it active.

Configuring User-Specified Responses

Introduction	You can configure the SecurityFusion module to run system commands or your own programs in response to events.
Default response	User-specified responses are not taken unless you configure them.
Prerequisite	You must copy the custom program file to the sensors you want to run the program from.
Procedure	To configure a user-specified response: 1. Open your custom SecurityFusion policy for editing. 2. In the left pane, expand Impact Analysis Component Settings. 3. Do one of the following: ■ To change the response for failed attacks, select Responses for Failed Attacks. ■ To change the response for successful attacks, select Responses for Successful Attacks. 4. Select the check box next to the USER-SPECIFIED list. 5. Does an arrow appear in the USER-SPECIFIED list? ■ If yes, go to Step 6. ■ If no, go to Step 7. 6. If you want to choose a different response, click the arrow, and then select another response. The name of the response you chose appears in the Response Name column. 7. Click the Save button, and then click the Close button. One of the following occurs: ■ If you modified the active policy, either a job automatically starts to apply the policy or a prompt appears for you to choose whether to apply the policy. ■ If you did not modify the active policy, you must apply the policy manually to make it active.

Responding to Server Sensor Events

Introduction

For a small number of events, server sensor automatically compares the event with host vulnerability data. By default, the SecurityFusion module applies its responses to these events.

Background

In a small number of server sensor signatures (starting with version 6.5), the server sensor compares events with host vulnerability data and determines a vulnerability status. In the server sensor policy, however, you cannot configure different responses based on host vulnerability. Consequently, the responses for these events may not be consistent with those applied by the SecurityFusion module for events with the same vulnerability status.

Procedure

To apply SecurityFusion module responses to events analyzed by server sensor:

1. Open your custom SecurityFusion module policy for editing.
2. In the left pane, expand **Impact Analysis Component Settings**.
3. Select **Options**.
4. Select the **Apply SecurityFusion logic to server sensor alerts that analyze vulnerability information at the server** check box.
5. On the **File** menu, select **Save**, and then click the **Close** button.

Note: If you did not modify the active policy, you must manually apply the policy to make it active.

SECTION E: Additional Configuration Tasks

Overview

Introduction The SecurityFusion module provides additional settings that you can configure based on your Site needs.

In this section This section contains the following topics:

Topic	Page
Configuring Vulnerability Data	34
Encrypting Communications with the Site Protector Database	35

Configuring Vulnerability Data

Introduction

The SecurityFusion module requires current host vulnerability assessment data to accurately estimate the impact of events. Depending on your requirements, you can configure how the SecurityFusion module uses vulnerability assessment data and how long the SecurityFusion module considers it as current.

Task overview

Table 11 describes the tasks for configuring vulnerability assessment data:

Task	Description
1	Limit how long the SecurityFusion module considers scanned vulnerability assessment data as up-to-date and uses it to analyze events.
2	For Sites that use both network- and host-based scanners, choose whether to use the most recent scan data or the data from either the network- or host-based scanner when both are available.
3	Scan the hosts that you want to protect with the SecurityFusion module.

Table 11: *Tasks for configuring vulnerability assessment data*

Ensuring current assessment data

To ensure that your vulnerability data is current, you can set up the SecurityFusion module to ignore data that is older than a certain age in your Site. Then you should set up your scanning schedule to scan your hosts before vulnerability data expires. The default setting is 60 days.

How this option works—impact on event status

The SecurityFusion module checks the age of the vulnerability and operating system data for each event, and then does one of the following:

- If the data has not expired, the SecurityFusion module analyzes the event.
- If the data has expired, the SecurityFusion module returns the status of Detected Attack (vuln not scanned recently) and does not analyze the event.

Choosing a default vulnerability data source

By default, the SecurityFusion module uses the most recent vulnerability data available (on a check-by-check basis), whether the data is from a network-based or host-based scanner. You can, however, configure the SecurityFusion module to use one source of data over the other if both are available and current.

Encrypting Communications with the Site Protector Database

Introduction

The SecurityFusion module exchanges data with the SiteProtector database. By default, attack data is always encrypted; vulnerability analysis and other miscellaneous administrative data is not.

If required at your Site, you can set up encryption to include all types of data. You can use either Multiprotocol or SSL (Secure Sockets Layer) methods.

Important prerequisite

Before you encrypt communications for the SecurityFusion module, read the relevant documentation:

- For Multiprotocol, see the *SiteProtector Installation Guide*.
- For SSL, see “How do I set up Site Protector to use encryption for database communication?” in the *Internet Security Systems Knowledgebase* (<http://iss.custhelp.com>)

To find the article:

- Type 1824 in the **Search Text** box, and then select **Answer ID** in the **Search by** list.

© Copyright IBM Corporation 1994, 2008

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.