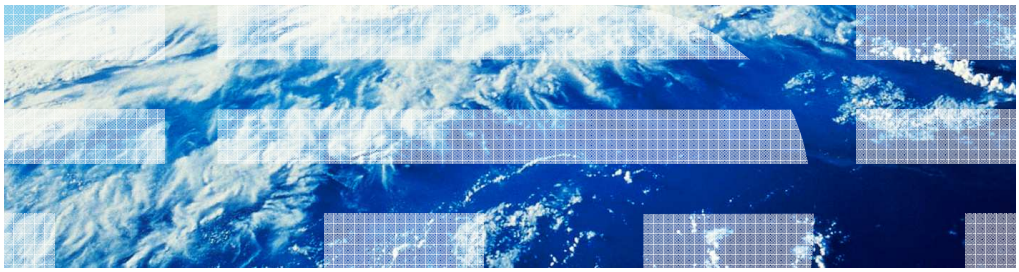
# IBM Security SiteProtector System V2.9

## New features of the SiteProtector console





IBM Security SiteProtector System V2.9: New features of the SiteProtector console.

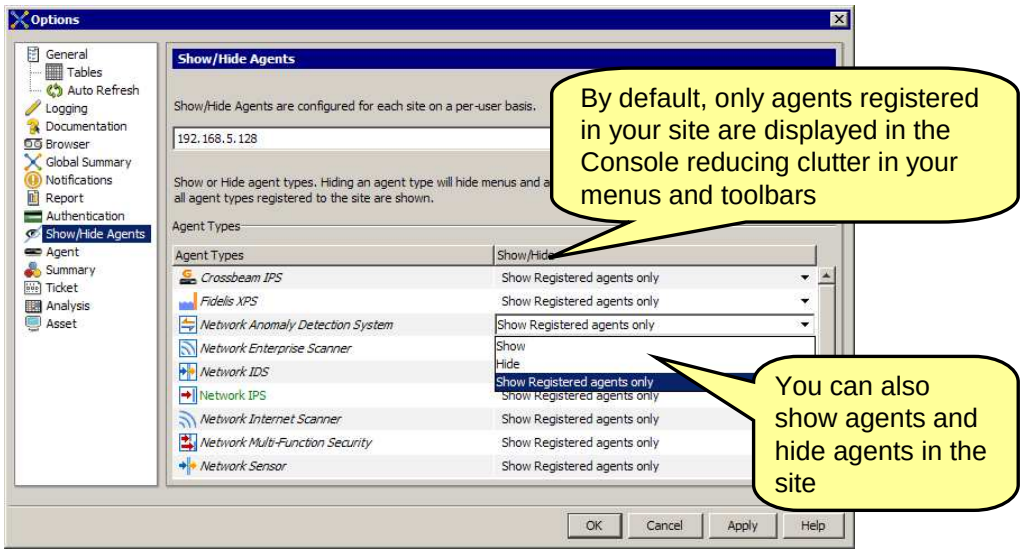
## Objectives

- When you complete this module, you will be able to identify some of the new features in the SiteProtector version 2.9 console




When you complete this module, you will be able to identify some of the new features of the SiteProtector version 2.9 console.

## SiteProtector interface updates




**Note**: To access the Options window, navigate to **Tools > Options**

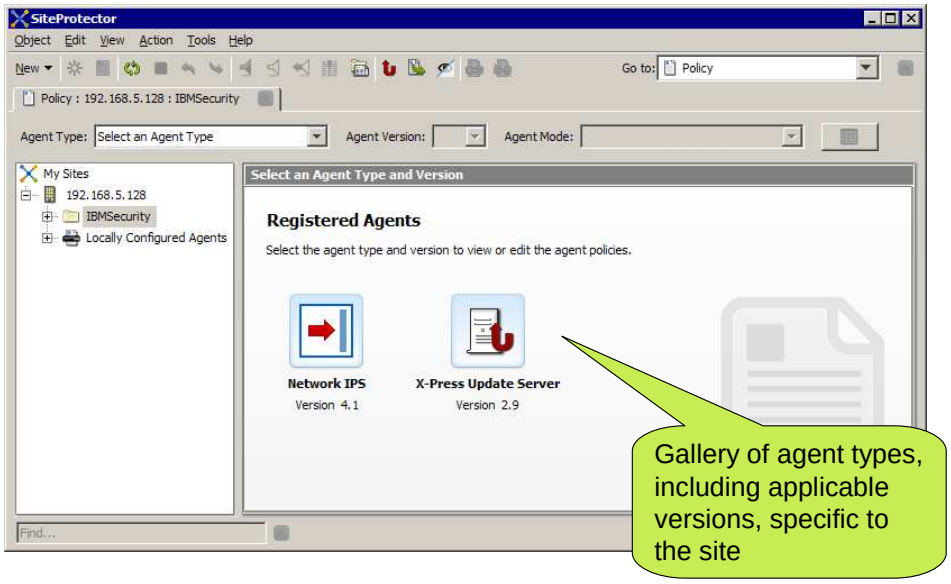
3 New features of the SiteProtector console 

SiteProtector V2.9 uses a solution-specific interface that allows you to focus on information relevant to your tasks. By default, only agents registered in your site are displayed in the SiteProtector Console. You can modify the default settings using the Options window. To access the Options window, navigate to the Tools menu and select **Options**.

You can use the **Show/Hide Agents** option to hide agents that are not necessary in your site. Removing unused agents from the Console reduces the clutter in your working environment allowing you to focus on relevant tasks. For example, if an analyst only monitors Server Protection agents, the analyst can hide other agents he or she does not monitor. This action removes menu and toolbar items that do not apply to the Server Protection products.

You can choose to display unregistered agents in your site. For example, you might want to configure policies that apply to a new agent before it is actually registered in the site.

## New Policy view

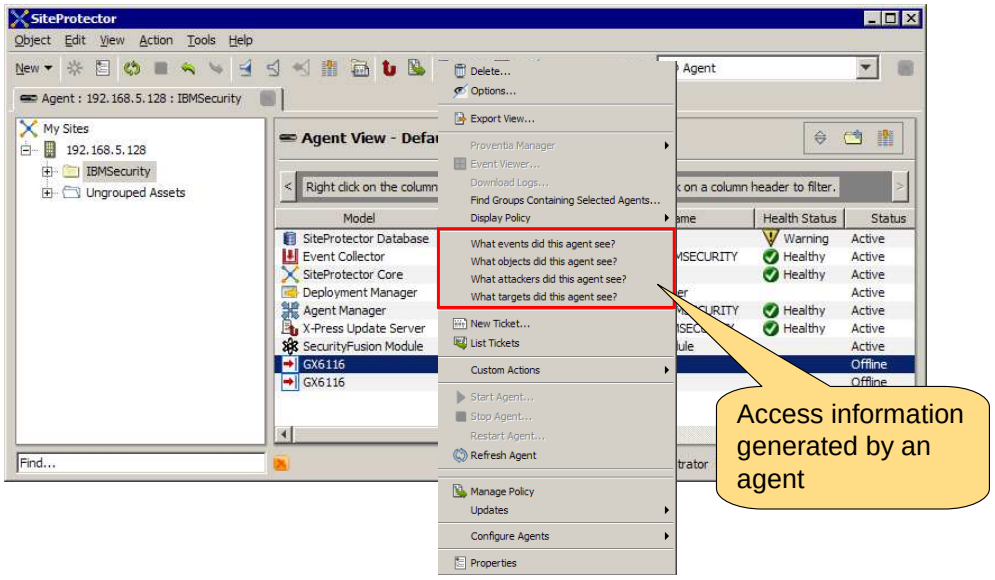






The Policy view in SiteProtector V2.9 displays a gallery view that shows the agents, along with the versions available, that are specific to your site. When you double-click the agent icon, the policies that control the type of security events an agent detects and the agent's response to an event are displayed. The configuration of policies and policy repositories and deployment of the policies remains unchanged.

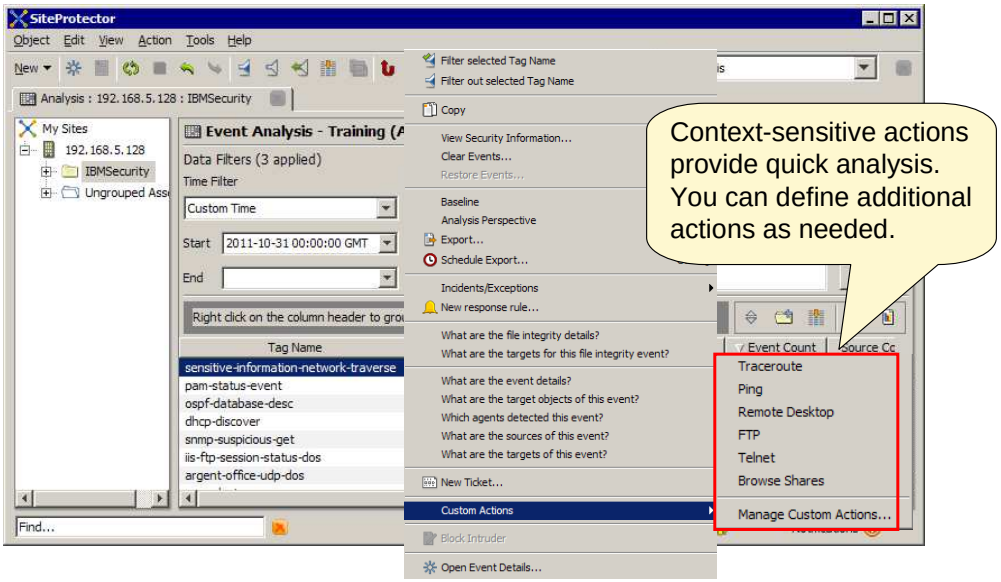
## Access event data from the Agent view



You can now access information detected by an agent from the Agent view. To view the events, objects, attackers, and targets specific to an agent, right-click the agent and select the appropriate option.

## Custom Actions options



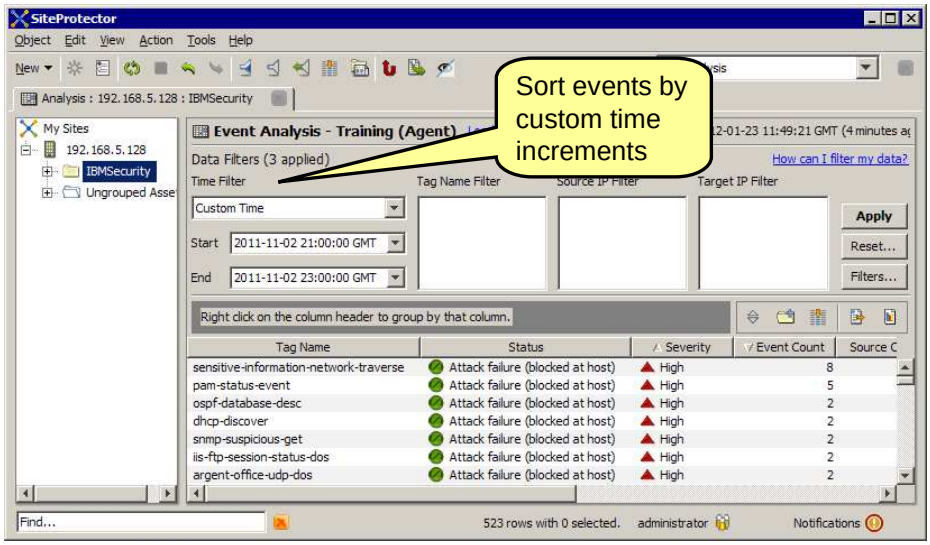

**Note**: You can also access custom actions from the Agent and Asset view




You can analyze events that occur in your network to manage vulnerabilities, investigate attacks, or monitor applications. Custom actions allow you to quickly apply commands and operations on event characteristics such as source IP, agent, tag name, and so on. As seen on the slide, some default actions are included in the Analysis view. Custom actions are also available from the Agent and Asset views. Use the **Manage Custom Actions** menu option to add, edit, and delete custom actions.

Note that the actions performed are local and specific to each SiteProtector Console. These commands are run on the machine where the Console is installed, not on the application server machine.

## Custom time filters



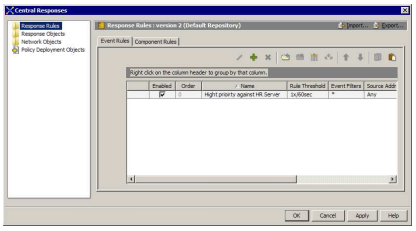




The Analysis view includes customized time filtering. As seen on the slide, you can use the **Custom Time** filter to sort your events by narrow time increments and focus on a specific set of events. The other default time filters include Today, Yesterday, This Week, Last Week, This Month, Last Month, This Year, Last Year, and Relative Time.

## Other features

Updated versions of **IBM Java**, **Apache, and** the **Geronimo** application server



400 Central Response event rules

Database improvements equals better performance when working with large event sets

| Tag Name | Status | Severity | Event Count |
|---|---|---|---|
| sensitive-information-network-traverse | Attack failure (blocked at host) | High | 8 |
| pam-status-event | Attack failure (blocked at host) | High | 5 |

Columns automatically resize to fit the data in the Analysis, Agent, and Asset views




Other miscellaneous new features in the SiteProtector version 2.9 Console are:
- Updated versions of IBM Java, Apache, and the Geronimo application server are included so that you have access to the latest security safeguards.
- The number of Central Response event rules you can create has doubled. You can now create up to 400 rules.
- Because of improvements to the SiteProtector Database, there is better performance when you are working with large event sets in the Analysis view.
- The widths of the columns in the Analysis, Agent, and Asset views automatically resize to accommodate data displayed in the column. You can still save customized settings.

## Further reference

For more information, use the following resources:

- IBM Security SiteProtector System V2.9 announcement
- SiteProtector V2.9 documentation
- IBM Security Systems
- IBM Institute for Advanced Security

For more information about SiteProtector V2.9 and IBM Security Systems, use the resource links listed on the slide.

## Summary

- Now you are able to identify some of the new features in the SiteProtector version 2.9 Console




Now that you have completed the module, take a moment to review the module's objective.

## Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_new_console.ppt

This module is also available in PDF format at: ../new_console.pdf




You can help improve the quality of IBM Education Assistant content by providing feedback.

# Trademarks, disclaimer, and copyright information