IMPERVA

Web Application Security Version 12.0

Web Application Security Version 12.0

Training Course

Overview

In this 2 day hands-on course, students will learn:

- How to initially implement and configure SecureSphere for an on premise Web Application Firewall including ThreatRadar subscription services.
- How to evaluate the configuration of the Web Application Firewall to ensure it is monitoring protected assets you have identified.
- How to implement detection and protection controls using Policies and Followed Actions
- How to configure Web Profiling.
- How to analyze Violations and Alerts.
- How to perform best practice tuning tasks.
- How to configure Active Blocking and error pages.
- How to integrate external web scanner data with SecureSphere and manage identified vulnerabilities.
- How and why to configure SecureSphere Web Gateway to work in a Reverse Proxy deployment mode.

Who Should Attend

This course is intended for security administrators, security analysts,security engineers, and Web application developers who are responsible for the implementation and configuration of the SecureSphere Web Application Gateway and for those who are responsible for securing and monitoring Web applications.

Prerequisites

Before taking this course, you should have already completed ***SecureSphere System Administration*** training.

In addition, make sure you have the following skills:

- General understanding of application layer security concepts, application layer Web, and/or database protocols.
- Experience implementing or managing data center security or database applications.

Lesson Objectives

Lesson 1: Web Application Security Admin Setup

- Configure users, roles and permissions for the SecureSphere Web Application Firewall.
- Create additional SecureSphere users with local or external authentication, as needed.

Lesson 2: Verifying the Initial Configuration

- Verify and configure all Web assets for protection by SecureSphere.
- Configure the details of a Web Service object and associated application object in a manner which accurately represents an organization's deployment of a specific web application.
- Verify network traffic from Load Balancers and Proxies will be handled correctly.
- Install SSL keys for the Web applications to be protected.
- Prevent potential compliance issues by configuring Data Masking to prevent sensitive information from being captured by SecureSphere.
- Customize the SecureSphere default error page.

Lesson 3: Web Application Level Preparations

- Create additional Web Application Sites Tree objects, as needed.
- Map an application object by host header and prioritize the mapping rules.
- Adjust the initial learning thresholds based on the protected applications and Imperva best practice recommendations.

Lesson 4: Web Application Security Policies

- Given different types of Web attacks, configure appropriate polices to defend Web applications.
- Create Action Set policies.
- Assign relevant Action Set policy to specify Security Policy Followed Actions.
- Configure and apply signature policies to defend Web applications from attacks with easily recognizable signatures.
- Disable a signature from a signature dictionary.
- Configure and apply protocol policies to defend Web applications from protocol attacks.
- Mitigate and monitor Slow HTTP and Slow HTTPS attacks.
- Configure and apply correlation policies to protect against multi-front web attacks.
- Mitigate SQL injection, cross site scripting attacks and more using Web correlation policies.
- Consider how correlation technology works before disabling policies or policy rules.
- Configure and apply custom Web policies to protect specific application weaknesses.
- Configure and apply ThreatRadar policies to protect against advanced Web attacks, and the latest Web attacks.
- Explain the factors that determine when to use modify a built-in policy, and when to create a copy of a built-in policy and modify it instead.
- Create policy configuration reports.

Lesson 5: Web Application Profiling

- Describe the components of the Web Application Profile.
- Explain how the Web Application Profile learns and protects Web applications.
- View a summary of all the profiles and statistics about them.
- Define and explain how application activity is mapped to the profile with application mapping.
- Identify common Web application components used in the learning process.
- View and edit a profile URL's HTTP methods and URL parameters.
- Display a profile's list of URL patterns defined for the application, learned cookies and their statuses, a list of the application's login action URLs, a list of the hosts on which the application's URLs are located and susceptible directories.
- Monitor the Web profile as it is being built during the learning period.
- Switch a URL from learning mode to protect mode.
- Lock a URL or a URL directory.
- Define and explain how Web application user tracking operates.
- Specify the authentication method to be used for a Web service.
- View, add and edit Action URLs.
- Define a Web Application User Tracking Decision Rule.
- Create a Set of Decision Rules for an Action URL.
- Explain how to select Web Profile Policy rules for the protected Web application.
- Configure appropriate reports to help administrators analyze profiles and profile learning.
- Display graphical representations of profile information.

Lesson 6: ThreatRadar Threat Intelligence

- Identify and configure appropriate ThreatRadar feeds to help secure web applications.
- Configure and use ThreatRadar Reputation Service to identify potentially malicious client activity.
- Protect Applications from Anonymous Proxies, Comment Spam IPs, Malicious IPs, Phishing URLs, and TOR IPs.
- Identify when to use and how to configure ThreatRadar Reputation Services.
- Identify when to use and how to configure ThreatRadar Bot Protection.
- Identify when to use and how to configure Community Defense.
- Identify environments that may benefits from ThreatRadar Fraud Prevention Services.
- Use IP Forensics to investigate and analyze source of traffic SecureSphere alerts.
- Enable and disable ThreatRadar services globally.
- Restrict Access by Country using IP Geo Location.
- Mask data in feeds sent to Community Defense.

Lesson 7: Alerts, Violations and Monitoring

- Monitor alerts using the dashboard view
- Identify Gateways managed by SecureSphere.
- Review the state of Gateways and server groups.

- Analyze traffic, CPU load, and hits.
- Analyze the latest alerts and system events.
- Apply a filter to view alerts generated in a specific date range.
- Identify false positive and attack events.
- Identify tuning opportunities.
- Determine alert severity, action taken in response to the event, and whether the alert information has been aggregated.
- Apply basic, quick, and advanced filters to Alerts and Violations.
- Configure appropriate reports for analysis of Alerts and Violations.
- Configure appropriate reports to identify tuning opportunities.
- Correct false positive events with the “Add as Exception” and “add to profile” buttons.
- Flag Alerts to support an event review workflow.

Lesson 8: SecureSphere Web Application Firewall Tuning

- Tune SecureSphere to minimize false positives, streamline profiles, improve policies and reduce non-essential alerts.
- Explain the impact and trade-offs of the “add to profile” button.
- Explain the impact and trade-offs of Parameter prefixes and URL prefixes.
- Identify impacts of modifying predefined, automatically applied Policies.
- Create custom policy to minimize the impacts of modifications with the predefined, automatically applied Policies.
- Reduce the number of alerts in SecureSphere by preventing the display of false positives and making changes to noisy policies.
- Improve performance of SecureSphere by removing redundant policies and controlling the size and number of profiles.
- Confirm the correct SSL keys have been imported and the encryption ciphers used by the servers.
- Exclude trusted vulnerability scanners from WAF inspection.
- Identify profiling anomalies.
- Determine if a separate web application should be created.
- Determine if web profile plug-ins are needed and configure them.
- Build a report to show how many of what type alerts have occurred.
- Use this report to direct your alert review and give you an agenda for alert tuning.
- Restrict application object monitoring to specific URLs and directories.

Lesson 9: Active Blocking

- Configure SecureSphere to enforce the tuned configuration.
- Move SecureSphere from Simulation to Active Blocking mode.
- Test that blocking is occurring with simulated attack patterns.
- Verify the error page is working and is displaying a non-default error page.
- Define custom error pages and error page policies.
- Configure additional Web Error Page Groups as needed.
- Monitor suspicious, Users/IPs/Sessions and apply extended blocking with Action Sets and Followed Actions.

Lesson 10: Web Scanner Integration

- Integrate external web scanner data with SecureSphere and manage identified vulnerabilities.
- Conduct a web server scan.
- Prepare results from the vulnerability scan for import into SecureSphere.
- Import scanner File.
- Configure a scanner integration policy.
- Apply the policy to the target server where the scan results originated.
- View the results of the Scanner Integration in the Vulnerability Workbench.
- Mitigate vulnerabilities discovered.

Lesson 11: Configuring Reverse Proxies

- Select the appropriate reverse proxy mode based on deployment requirements for URL rewriting, cookie signing, SSL termination, and/or response rewriting.
- Configure Reverse Proxy mode settings.
- Create and configure default and custom web error pages for use in security policies.
- Configure URL rewrite and redirection rules.
- Configure SecureSphere to work with SSL Client Certificates.

Getting Started

Delivery Options

Open Classroom	Virtual Classroom	Private On-site
Instructor-Led, in person classes hosted at an Imperva training facility. Class includes: ➢ Electronic Training Material ➢ Sandbox for hands-on labs	Instructor-Led, in person classes hosted at an Imperva training facility. Class includes: ➢ Electronic Training Materials ➢ Sandbox for hands-on labs ➢ 4 hours of instruction followed by independent lab time ➢ 4 hours of instructor office-hours each class day	Instructor-Led, in person classes hosted at your facility for up to 15 participants. Class includes: ➢ Electronic Training Materials ➢ Sandbox for hands-on labs

Enroll

Visit Imperva Services Training web page to view upcoming classroom and instructor led online events and register today. If you do not have a Customer or Partner portal account, you may request one from our site. If you need assistance with the account request, contact support@imperva.com. Customers and partners can register for training using their Imperva

Service Order number (SRV#) obtained from their Imperva sales representative or local Imperva partner, or buy training using a major credit card* from our training portal.

Purchase

Contact your local Imperva sales representative or contact your local Imperva partner for a price quote and to purchase training. If you do not have a sales contact, please call 1-866-926-4678, or complete our information form. **The purchase by credit card option is only available for purchasers in most select countries in North and South America.*

Schedule

If you purchased onsite training and would like to schedule delivery, please call us at +1-972-887-5922 or email training@imperva.com

Please refer to Imperva **Terms and Conditions** when registering for classes for additional information.