Web Application Security Version 13.0

SecureSphere Web Application Security Version 13.0

Training Course

Required Training Units: 4 (TR-UNIT) *Training Units are good for 1 year from the time of purchase.*

Length: 4 Days

Overview

In this 4-day hands-on course, students will learn:

- How to configure SecureSphere for an on premises 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.

On the final day of class, students will perform a capstone exercise to reinforce their understanding and ability to apply the concepts learned during class.

Who Should Attend

This course is intended for security administrators, security analysts,security engineers, and Web application developers who are responsible for securing and monitoring Web applications with SecureSphere.

Prerequisites

Before taking this course, you should have the following skills:

- General understanding of application layer security concepts, application layer Web, and/or database protocols.
- Basic understanding of HTML and HTTP.
    - URLs, Parameters, headers, methods, HTTP server response codes, etc.
- Experience implementing or managing data center security or database applications.

Lesson Objectives

Lesson 1: Lab Environment and SecureSphere Web UI

- Review the SecureSphere Architecture

- Become familiar with the presentation of the training materials.

- Learn to use the Imperva training portal to find supplemental course materials.

- Become familiar with the lab environment, topology, and user accounts.

- Become familiar with the SecureSphere Web UI's major components and navigating the Web UI.

Lesson 2: Initial Web UI Configuration

- Set password strength requirements.

- Enable users to enter comments when making changes to security policies.

- Create SecureSphere user accounts and roles.

- Configure Active Directory authentication.

- Update ADC content.

Lesson 3: Sites Tree Configuration

- Create a Site.

- Create a Server Group.

- Create a Service and default Application.

- Discover and secure previously unknown servers on the network.

- Add discovered servers to a Site.

Lesson 4: HTTP Service Configuration

- Configure Forwarded Connections (Load Balanced Traffic)

- Install Protected Web Servers' SSL Keys

- Configure Data Masking

- Configure Web Error Pages

Lesson 5: HTTP Application Configuration

- Create and Configure Web Applications as needed.

- Direct HTTP client traffic to the appropriate Web Application.

- Adjust initial learning thresholds so that SecureSphere more accurately profile web traffic.

Lesson 6: Actions

- Define, compare, and contrast Action Interfaces, Action Sets, and Followed Actions.

- Explain placeholders, and where to find complete details regarding them.

- Create Email, FTP, Syslog, etc., Action Interfaces as needed.

- Create Email, FTP, Syslog, etc., Action Sets as needed.

- Use Followed Actions to implement Action Sets on system administration jobs.

Lesson 7: Security Policies

- Given different types of Web attacks, configure appropriate polices to defend Web applications.

- Implement Followed Actions in Security Policies.

- Configure and apply:

    o   Signature policies to defend Web applications from attacks with easily recognizable signatures.

    o   Protocol policies to defend Web applications from protocol attacks.

    o   Correlation policies to protect against multi-front Web attacks.

    o   Custom Web policies to protect specific application weaknesses.

- 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.

Lesson 8: Web Application Profiling

- Describe the components of the Web Application Profile.

- Explain how the Web Application Profile learns and protects web applications.

- Define and explain how application activity is mapped to the profile application mapping.

- Identify common web application components used in the learning process.

- Define and explain how web application user tracking operates.

- Explain how to select Web Profile Policy rules for the protected web application.

Lesson 9: ThreatRadar

- Identify and configure appropriate ThreatRadar feeds to help secure web applications.

- Identify when to use and how to configure TR Reputation Services.

- Identify when to use and how to configure ThreatRadar Bot Protection.

- Identify when to use and how to configure Intelligence (Community Defense).

Lesson 10: Alerts and Violations

- Use the Monitoring Dashboard to view a summary of current Violations and Alerts.

- Perform detailed analysis of Alerts and Violations to identify false positives, attacks, and tuning opportunities.

- Use the "Add as Exception" and "add to profile" buttons to tune policies and profiles.

- Manage the workflow of Security Monitoring by using SecureSphere's Alert Flags.

Lesson 11: Reporting

- Describe the features of SecureSphere's **Report Settings**.

- Describe how to work with report **Keywords**.

- Create reports of various types, including **System Events**, **Configuration**, and **Alerts** reports.

- Schedule Reports and the **Reports Archive** job.

- Create security-focused reports, such as Daily or Weekly **Top 10** Alert reports.

Lesson 12: Web Application Security Tuning

- Use Reports to identify where to tune SecureSphere.

- Use the Profile Optimization Wizard to help tune Profiles.
- Explain the impact and trade-offs of various Profile tuning options.
- Examine multiple ways to tune Security Policies.

Lesson 13: Active Blocking

- Configure SecureSphere to enforce the tuned configuration.
- Move SecureSphere from Simulation to Active Blocking mode.
- Verify the non-default error page is working.
- Identify and manage Followed Action Block events.
- Configure additional Web Error Page Groups as needed.

Lesson 14: Reverse Proxy

- 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.
- Configure and apply SSL Cipher Suites to inbound and outbound proxy rules.
- 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.

Lesson 15: End of Class Capstone Exercise

The Capstone Exercise challenges students to perform a series of tasks designed to help students reinforce learning by recalling and applying the concepts and skills presented during the class. Tasks include:

- Configure a Site Hierarchy to protect a Web Application.
- Mask sensitive data, such as credit card numbers, so they are not exposed.
- Configure SecureSphere's Web Application profiles and map web traffic to appropriate Web Applications.
- Configure SecureSphere to properly support and inspect traffic that is load balanced or proxied before reaching the protected web servers.
- Automate and archive regular SecureSphere system backups.
- Configure SecureSphere to protect web servers against data leakage.
- Configure SecureSphere to share information with external monitoring servers, such as a syslog server.
- Perform Security Tuning to optimize SecureSphere's configuration.
- Create a variety of reports.
- Find and protect unexpected / rogue servers on the network.

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, you attend class via web conferencing. Class includes: ➢ Electronic Training Materials ➢ Sandbox for hands-on labs	Instructor-Led, in person classes hosted at your facility for 6 to 12 participants. (purchase TR-4-DAY-ONSITE-6 for 6 participants) Class includes: ➢ Electronic Training Materials ➢ Sandbox for hands-on labs

How to Purchase

Purchase Training Units via Purchase Order

Contact your local Imperva sales representative or contact your local Imperva partner for training unit price quote and to submit a Purchase Order for training units. You will receive an **Imperva SRV#** for use in class enrollment. If you do not have a sales contact, please call 1-866-926-4678, or complete our information **form**.

Purchase Classes via Credit Card

Training can be purchased using a major credit card, during the course enrollment process.

How to Enroll

IMPORTANT: Only individuals with an Imperva portal account username and password can enroll in classes. 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**.

To enroll, have your portal username and password available, visit the **Imperva Training website** and register for your class from the Training Calendar. Select either **Credit Card** or **Training Units (Purchase Order)** as your payment option. If you select Training Units, you may be asked to enter an Imperva SRV# (received when Purchase Order is finalized). Note: Company PO#s are not accepted for payment during class enrollment process.

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 training for additional information.