Imperva Data Security Fabric – Data Gateway

Overview

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

- _How to initially configure SecureSphere for a Database Security

deployment

- _How to run DB Data Classification Scans to find sensitive data
- _How to implement Database Security Policies and Database Auditing.
- _How to configure DB Profiling
- _How to analyze Database Violations and Alerts
- _How to perform best practice tuning tasks
- _How to configure Active Blocking
- _How to configure Assessment Scans and manage risk scores
- _How to configure Database User Rights Management Scan and analyze

the results

Course Length

4 days

Who Should Attend

This course is intended for database administrators, security administrators, security engineers responsible for configuring, securing and monitoring their database applications with Imperva Database Security and Compliance.

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.
- _Experience implementing or managing data center security or database applications.
- _Imperva Security Administration is recommended

Lesson Objectives

Lab Environment and Imperva Data Protection Web UI

- _Review the Imperva Data Protection Architecture
- _Become familiar with the presentation of the training materials.
- _Learn to use the Imperva training portal.
- _Become familiar with the lab environment, topology, and user accounts.
- _Become familiar with the Imperva Data Protection Web UI's major components and navigating the Web UI.

Initial Web User Interface Configuration

- _Set password strength requirements.
- _Enable users to enter comments when making changes to security policies.
- _Create Imperva Data Security user accounts and roles.
- _Configure Active Directory authentication.
- _Update ADC content.

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.

Initial Database Security Configuration

- _Verify existing Site objects, making any necessary corrections.
- _Install Database Agent.
- _Configure additional Agent settings.
- _Configure Database Connections on the Database Service.
- _Create Stored Procedure Groups and apply them to their database applications.
- _Add the protected DB server's SSL key to the Database Service.
- _Apply Data Masking to the Database Service.
- _Enable and configure Personal Information Masking.
- _Create Imperva Data Security Users and Roles.

DB Data Classification Scans

- _Define sensitive data.
- _Identify Imperva Data Security's predefined data types.
- _Create Custom DB Data Types.
- _Create Scan Profiles.
- _Create and run DB Data Discovery Scans.
- _Analyze DB Data Discovery Scan Results.
- _Accept and Reject DB Discovery Scan Results.
- _Review the effect of Accepting DB Discovery Scan Results.

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.

Reporting

- _Describe the features of Imperva Data Security'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.

DB Security Policies

- _Explain Predefined Policies and Default Policies.
- _Summarize the each of the Default DB Security Policies applied to the SuperVeda Site.
- _Explain performance differences between Signatures and Dictionaries.
- _Add Followed Actions to SuperVeda's Default DB Security Policies.
- _Create Custom DB Security Policies.
- _Create a DB Security Policy Configuration Report.

Database Profiling

- _Explain how Imperva Data Security's Dynamic Profiling works.
- _Explain the structure of Database Profiles and their place in the Sites Tree.
- _Explain Profile Modes and Thresholds.
- _Explain the components of DB Profiles.
- _Explain the benefit of creating User Groups for profiles.
- _Configure the SQL Profile Policy.
- _Disable profiling for a specific database.
- _Configure DB Profile Reports.

DB Violations and Alerts

- _Define Violations, Alerts, and Alert Aggregation.
- _Explain the components of Violations and Alerts.
- _Use Imperva Data Security's Alert Flags to manage alerts.
- _Use the Dashboard to quickly monitor Imperva Data Security's current overall state.
- _Configure and run Alert Reports to help analyze the Top Ten attacks against a protected application.

Database Auditing

- _Explain Imperva Data Security's Database Auditing process.
- _Explain the Fast Viewing process.
- _Explain Imperva Data Security's Audit Archiving and Purging process.
- _Identify the data collected by the Default Rule – All Events Audit policy.
- _Create Audit Policies.
- _Explain how to share DB Audit Data information with SIEM systems.
- _Explain how DB Audit Data Views help administrators analyze audit data.
- _Create Reports directly from the DB Audit Data Views.

Tuning
- _Resolve Connected User and Hashed User when observed in the DB Audit Data.
- _Configure SSL and Kerberos Keys.
- _Tune Security Policies and Profiles.
- _Tune Audit Policies.
- _Configure Agent Exclude from Monitoring Rules.
- _Become familiar with Imperva Data Security's Audit Management Statistics.

Active Blocking
- _Review Imperva Data Security's traffic blocking capabilities.
- _Explain the Server Group Operation Modes.
- _List and explain Imperva Data Security's Blocking Followed Actions for Database Traffic.
- _Explain the DB Agent's Modes and how they relate to blocking DB traffic.
- _Describe Imperva's recommended practices to enable DB traffic blocking.

Assessment Scans and Risk
- _Describe the structure of DB Assessment Policies.
- _Configure DB Assessment Scans that implement DB Assessment Policies.
- _Review DB Assessment Scan results.
- _Explain how SecureSphere evaluates Risk.
- _Create DB Assessment Scan Result Reports.

Database User Rights Management
- _Configure and run DB User Rights Scans.
- _Analyze the Effective Permissions found by the DB User Rights Scan.
- _Manage Role and Permission Grants.
- _Create a DB User Rights Report that informs the DBA team which permissions should be corrected.