DSC
Database Security and Compliance Version 13.0

Overview

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

- The key features and benefits of having Imperva's Database Security Solution (DBS)in your environment
- How DBS operates and base functionality
- Hands-on navigation of the DBS Web User interface
- How to evaluate your readiness for a DBS deployment
- How to complete standard database configuration tasks
- How to run DB Database Classification scans
- How to create a Database Security policy
- How to create database profiles and audit the database
- How to troubleshoot basic DBS implementation and configuration issue

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.