# Imperva Data Security Certification

**Course Duration: 8 Hrs.** **Course code: IDSC**

## Course Overview

The Imperva Data Security Certification Course equips IT and security professionals with the knowledge and skills to implement, configure, and manage Imperva's data security solutions. It covers the complete suite of Imperva tools, including Database Activity Monitoring (DAM), Data Risk Analytics (DRA), Web Application Firewall (WAF), and Cloud Data Security capabilities. Participants will learn how to safeguard sensitive data, maintain compliance, and mitigate risks in on-premises, cloud, and hybrid environments. This certification validates expertise in protecting data assets against evolving cyber threats.

## What you'll learn?

- Understand Imperva's data security architecture and key components.
- Configure and manage Imperva solutions for database and application security.
- Implement Database Activity Monitoring (DAM) for real-time threat detection.
- Use Data Risk Analytics (DRA) to identify anomalies and reduce risks.
- Deploy and configure Web Application Firewall (WAF) for application protection.
- Manage policies, alerts, and incident responses effectively.
- Integrate Imperva solutions with SIEM and security workflows.
- Prepare for the Imperva Data Security Certification exam.

## Target Audience

Security Engineers and Analysts.

- Database Administrators (DBAs) and Data Protection Specialists.
- IT Security Managers and Compliance Officers.
- Network and Application Security Professionals.
- Anyone responsible for safeguarding organizational data assets.

## Pre-Requisites

Basic knowledge of cybersecurity concepts and data protection principles.

- Familiarity with databases, applications, and networking fundamentals.
- Experience in IT security operations is beneficial but not mandatory.

## Course content

Module 1: Introduction to Imperva Data Security

- Overview of Imperva solutions and capabilities
- Data security challenges and compliance requirements

Module 2: Imperva Architecture and Deployment Models

- On-premises, cloud, and hybrid deployment options
- System components and integration points

Module 3: Database Activity Monitoring (DAM)

- DAM architecture and components
- Configuring database monitoring and auditing
- Detecting and responding to threats in real time

Module 4: Data Risk Analytics (DRA)

- Introduction to DRA and its role in data protection

- Identifying anomalies and suspicious activities
- Using analytics for compliance and risk reduction

Module 5: Web Application Firewall (WAF)

- WAF fundamentals and benefits
- Configuring WAF policies for application protection
- Preventing OWASP Top 10 vulnerabilities

Module 6: Cloud Data Security

- Protecting sensitive data in cloud environments
- Integrating Imperva with cloud-native services

Module 7: Policy Management and Incident Response

- Creating, managing, and testing security policies
- Alert configuration and incident workflow management

Module 8: Integrations and Advanced Configurations

- Integrating with SIEM and third-party security tools
- Advanced reporting and audit features

Module 9: Exam Preparation

- Imperva Data Security Certification exam format and tips
- Practice scenarios and sample questions