Imperva Cloud Security Certification

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

Course Overview

The Imperva Cloud Security Certification course is designed to provide IT and security professionals with the expertise to implement, configure, and manage Imperva's cloud-based security solutions. This training focuses on protecting web applications, APIs, and sensitive data across cloud and hybrid environments. It covers essential Imperva services such as Cloud Web Application Firewall (WAF), Distributed Denial of Service (DDoS) protection, API Security, Bot Management, and Cloud Data Security. By the end of the course, participants will have the skills to secure modern cloud workloads against advanced cyber threats while ensuring compliance with industry standards.

What you'll learn?

- Understand Imperva's cloud security architecture and services.
- Deploy and manage Cloud WAF for application and API protection.
- Configure DDoS mitigation strategies for critical workloads.
- Implement API security controls and prevent malicious exploitation.
- Use bot management to detect and block automated threats.
- Protect sensitive data stored and processed in the cloud.
- Monitor, analyze, and respond to cloud security incidents.
- Prepare for the Imperva Cloud Security Certification exam.

Target Audience

Cloud Security Engineers and Architects.

- Application Security Specialists.
- DevOps and SecOps Professionals.
- IT Security Managers and Compliance Officers.
- Anyone responsible for securing applications and data in the cloud.

Pre-Requisites

Basic understanding of cloud computing concepts and platforms (AWS, Azure, GCP).

- Familiarity with networking, web applications, and security fundamentals.
- Prior experience in IT or cybersecurity operations is beneficial.

Course content

Module 1: Introduction to Imperva Cloud Security

- Overview of Imperva's cloud security offerings
- Importance of securing modern cloud environments

Module 2: Cloud Security Architecture and Deployment

- Deployment models for public, private, and hybrid clouds
- Imperva integration with cloud-native services

Module 3: Cloud Web Application Firewall (WAF)

- WAF fundamentals and configuration
- Protecting against OWASP Top 10 threats
- Managing WAF rules and exceptions

Module 4: DDoS Protection

- Understanding DDoS attack vectors

- Implementing Imperva DDoS mitigation strategies
- Testing and validating protection measures

Module 5: API Security

- API threat landscape and vulnerabilities
- Configuring API protection policies
- Securing microservices and serverless APIs

Module 6: Bot Management

- Detecting and classifying bots
- Applying mitigation strategies to prevent bot attacks
- Balancing security with user experience

Module 7: Cloud Data Security

- Data discovery and classification in the cloud
- Encryption, masking, and tokenization techniques
- Ensuring compliance with regulations (GDPR, HIPAA, etc.)

Module 8: Security Monitoring and Incident Response

- Setting up alerts and dashboards
- Investigating and responding to incidents
- Integrating with SIEM and SOAR platforms

Module 9: Exam Preparation

- Certification exam structure and best practices
- Practice questions and scenario-based exercises