Imperva Application Security Course

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

Course Overview

The Imperva Application Security Certification Course equips IT and security professionals with the skills to configure, manage, and optimize Imperva's application security solutions. This training covers Web Application Firewall (WAF), API security, bot protection, DDoS mitigation, and advanced threat intelligence features. Through hands-on labs and real-world scenarios, participants will learn to secure web applications, APIs, and data against evolving cyber threats while ensuring compliance with industry standards.

What you'll learn?

- Understand the core concepts of Imperva Application Security solutions.
- Configure and deploy Imperva Web Application Firewall (WAF).
- Protect APIs and applications from bots, DDoS, and zero-day attacks.
- Implement custom security policies and rules.
- Monitor, analyze, and respond to security incidents using Imperva dashboards and reports.
- Integrate Imperva security with existing IT infrastructure.
- Prepare for the Imperva Application Security Certification exam.

Target Audience

Application Security Engineers and Analysts.

- Network and Security Administrators.
- Cybersecurity Professionals working with web applications and APIs.
- IT professionals responsible for implementing Imperva solutions.
- Security Architects and Consultants.

Pre-Requisites

Basic understanding of web applications and HTTP/HTTPS protocols.

- Familiarity with cybersecurity fundamentals and threats.
- Experience in network administration or security operations is beneficial.

Course content

Module 1: Introduction to Imperva Application Security

- Overview of Imperva security solutions
- Application security challenges and threat landscape

Module 2: Imperva Web Application Firewall (WAF)

- WAF architecture and deployment options
- Policy configuration and management
- Handling false positives and tuning WAF Rules

Module 3: API Security

- Securing APIs against injection, authentication, and data exposure attacks
- API discovery and monitoring
- Policy enforcement for API Protection

Module 4: Bot Management

- Detecting and mitigating malicious bot traffic
- Custom bot policies and behavioral analysis
- Real-time bot reporting and analytics

Module 5: DDoS Protection

- Types of DDoS attacks and mitigation strategies
- Configuring Imperva DDoS protection
- Incident response for large-scale attacks

Module 6: Threat Intelligence & Incident Management

- Leveraging Imperva threat intelligence feeds
- Logging, monitoring, and alerting
- Reporting for compliance and auditing

Module 7: Integration & Automation

- Integrating Imperva with SIEM, SOAR, and other security tools
- Automation using APIs and scripts
- Best practices for enterprise security integration

Module 8: Hands-on Labs & Case Studies

- Real-world attack simulation and mitigation
- Troubleshooting common issues
- Performance optimization techniques

Module 9: Exam Preparation

- Certification exam structure and requirements
- Practice questions and review of key concepts