Data Security Fabric Course

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

Course Overview

The Imperva Web Application Firewall (WAF) course provides in-depth knowledge and practical skills to deploy, configure, and manage Imperva's industry-leading WAF solution. Participants will learn how to protect web applications from common and advanced cyber threats, including OWASP Top 10 vulnerabilities, zero-day attacks, and bot traffic. This course combines theory with hands-on exercises to ensure learners can implement robust application security in on-premises, cloud, and hybrid environments while maintaining performance and compliance.

What you'll learn?

- Understand the architecture and components of Imperva WAF.
- Deploy Imperva WAF on-premises, cloud, or hybrid setups.
- Configure security policies to protect against web-based threats.
- Mitigate OWASP Top 10 vulnerabilities and other common exploits.
- Use advanced features like bot protection, DDoS mitigation, and threat intelligence.
- Monitor, analyze, and respond to WAF alerts and incidents.
- Integrate WAF with SIEM and security automation tools.

Target Audience

Web and Application Security Engineers.

- Network Security Professionals.
- DevOps and Cloud Security Specialists.

- Security Operations Center (SOC) Analysts.
- IT administrators are responsible for web application protection.

Pre-Requisites

Basic understanding of web applications and HTTP/HTTPS protocols.

- Familiarity with cybersecurity concepts and network security principles.
- Experience with firewalls or intrusion prevention systems is beneficial.

Course content

Module 1: Introduction to Imperva WAF

- Overview of web application security challenges
- Imperva WAF features and benefits
- Deployment options and use cases

Module 2: WAF Architecture and Deployment

- Components of Imperva WAF
- On-premises, cloud, and hybrid deployment models
- Initial configuration and setup

Module 3: Security Policy Configuration

- Creating and managing WAF security policies
- Protecting against OWASP Top 10 vulnerabilities
- Custom rules and signatures

Module 4: Advanced Protection Features

- Bot mitigation and API security
- DDoS protection strategies

- Threat intelligence integration

Module 5: Monitoring, Reporting, and Incident Response

- Analyzing logs and alerts
- Investigating and responding to security incidents
- Generating compliance and performance reports

Phone: +91-999-911-1686 **Mail Us:** info@ssdntech.com