FortiWeb Course

Course Duration: 24 Hrs. **Course Code: FWEB-ADMIN-7.x**

Course Overview

The **FortiWeb** course is designed for security professionals responsible for protecting web applications from modern cyber threats. This course focuses on deploying, configuring, and managing FortiWeb Web Application Firewall (WAF) solutions to secure web applications against attacks such as SQL injection, cross-site scripting (XSS), and OWASP Top 10 vulnerabilities. Participants will gain hands-on experience in implementing web application security policies, monitoring threats, and ensuring compliance using FortiWeb.

What You'll Learn?

By completing this course, you will be able to:

- Understand web application security threats and attack vectors
- Deploy and configure FortiWeb in enterprise environments
- Implement WAF policies to protect web applications
- Secure applications against OWASP Top 10 vulnerabilities
- Configure SSL/TLS inspection and certificate management
- Monitor web traffic, logs, and security events
- Troubleshoot and optimize FortiWeb deployments

Target Audience

This course is ideal for:

- Web Application Security Engineers
- Network and Security Administrators

- DevSecOps and Application Security Teams
- SOC Analysts monitoring web application threats
- Professionals preparing for FortiWeb administration roles

Pre-Requisites

Participants should have:

- Basic understanding of web technologies (HTTP/HTTPS, APIs)
- Familiarity with networking and security fundamentals
- Experience with firewalls or web servers is recommended

Course Content

Module 1: FortiWeb Overview and Architecture

- FortiWeb features and deployment modes
- Reverse proxy, transparent, and offline modes
- Initial setup and system configuration

Module 2: Web Application Security Fundamentals

- OWASP Top 10 vulnerabilities
- Web application attack techniques
- Security policy concepts

Module 3: WAF Policies and Protection Profiles

- Creating and managing protection profiles
- Signature-based and behavior-based protection
- Bot mitigation and API security basics

Module 4: SSL Inspection and Certificate Management

- SSL/TLS inspection methods
- Certificate deployment and management
- Performance considerations

Module 5: Monitoring, Logging, and Reporting

- Traffic analysis and threat monitoring
- Logs, alerts, and reports
- Integration with FortiAnalyzer

Module 6: Troubleshooting and Best Practices

- Common FortiWeb deployment issues
- Policy tuning and optimization
- Best practices for web application protection

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