NSE 5 FortiSIEM 5.2 Course

Course Duration: 24 Hrs. **Course Code: NSE5-FSIEM-5.2**

Course Overview

The **NSE 5 FortiSIEM 5.2** course is designed for security operations and IT professionals responsible for monitoring, analyzing, and responding to security events using FortiSIEM version 5.2. This course focuses on deploying, configuring, and managing FortiSIEM for centralized log collection, real-time event correlation, and incident response. Participants will gain hands-on experience in SOC workflows, advanced analytics, and reporting while preparing for the NSE 5 FortiSIEM certification.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiSIEM 5.2 in enterprise environments
- Collect and normalize logs from Fortinet and third-party devices
- Create correlation rules and incident workflows
- Monitor security events and performance metrics
- Perform threat analysis and root-cause investigations
- Generate dashboards and compliance reports
- Troubleshoot and optimize FortiSIEM performance

Target Audience

This course is ideal for:

- SOC Analysts and Security Engineers
- Network and System Administrators

- IT Operations and Monitoring Teams
- Incident Response and Threat Hunting Professionals
- Professionals preparing for the NSE 5 FortiSIEM certification

Pre-Requisites

Participants should have:

- Understanding of networking and cybersecurity fundamentals
- Familiarity with log management and SIEM concepts
- Experience with Fortinet products is helpful but not mandatory
- Basic knowledge of SOC operations and incident response

Course Content

Module 1: FortiSIEM 5.2 Architecture and Deployment

- FortiSIEM components and system architecture
- Deployment models and sizing considerations
- Initial setup and configuration

Module 2: Log Collection and Device Integration

- Integrating Fortinet and third-party devices
- Log normalization and parsing
- Agent-based and agentless data collection

Module 3: Event Correlation and Incident Management

- Correlation rules and alerts
- Incident creation and workflow management
- Root cause analysis

Module 4: Monitoring and Dashboards

- Real-time monitoring views
- Custom dashboards and widgets
- Performance and security metrics

Module 5: Reporting and Compliance

- Predefined and custom reports
- Compliance reporting (PCI DSS, ISO, etc.)
- Scheduled and automated reporting

Module 6: Troubleshooting and Optimization

- Diagnosing log and performance issues
- System tuning and optimization
- Best practices for FortiSIEM operations

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