NSE 5 FortiSIEM 6.3 Course

Course Duration: 24 Hrs. **Course Code: NSE5-FSIEM-6.3**

Course Overview

The **NSE 5 FortiSIEM 6.3** course is designed for security professionals who are responsible for monitoring, analyzing, and responding to security events across complex IT environments. This course provides in-depth knowledge of FortiSIEM 6.3, focusing on real-time threat detection, log correlation, incident response, and compliance reporting. Learners will gain hands-on skills to deploy, configure, and operate FortiSIEM as part of the Fortinet Security Fabric and prepare for the NSE 5 certification exam.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiSIEM 6.3 architecture
- Collect, normalize, and analyze logs and events
- Build correlation rules and security analytics
- Monitor network, server, and application performance
- Detect threats and investigate security incidents
- Create dashboards, alerts, and compliance reports
- Troubleshoot FortiSIEM components and data flows

Target Audience

This course is ideal for:

- Security Operations Center (SOC) Analysts
- Network Security Analysts

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

- SIEM Administrator
- Incident Response and Threat Monitoring Teams
- Professionals preparing for the NSE 5 FortiSIEM certification

Pre-Requisites

Participants should have:

- Strong understanding of networking and security concepts
- Experience with log management and monitoring tools
- Familiarity with Fortinet security products is recommended
- NSE 4-level knowledge is helpful

Course Content

Module 1: FortiSIEM 6.3 Architecture and Deployment

- FortiSIEM components and system architecture
- Deployment models and sizing
- Installation and initial setup

Module 2: Data Collection and Normalization

- Log sources and collectors
- Event parsing and normalization
- Performance and availability monitoring

Module 3: Event Correlation and Analytics

- Correlation rules and policies
- Behavioral and anomaly detection
- Threat intelligence integration

Module 4: Incident Monitoring and Response

- Alerts, incidents, and workflows
- Incident investigation and root cause analysis
- Automated responses and remediation

Module 5: Dashboards, Reporting, and Compliance

- Custom dashboards and visualizations
- Compliance and audit reporting
- Data retention and optimization

Module 6: Troubleshooting and Best Practices

- Common FortiSIEM issues and resolutions
- Performance tuning and scaling
- Operational best practices and exam preparation