NSE 7 Advanced Analytics Course

Course Duration: 16 Hrs. **Course Code: NSE7-AA-7.x**

Course Overview

The **NSE 7 Advanced Analytics** course is designed for security professionals and SOC analysts responsible for leveraging Fortinet's advanced analytics tools to enhance threat detection, incident response, and security operations. This course focuses on deploying, configuring, and using Fortinet Security Fabric analytics, FortiAnalyzer, and FortiSIEM to gain actionable insights into network and security events. Participants will gain hands-on experience in advanced data correlation, reporting, and automated threat response, preparing for the NSE 7 Advanced Analytics certification.

What You'll Learn?

By completing this course, you will be able to:

- Understand Fortinet Security Fabric analytics capabilities
- Configure and deploy FortiAnalyzer and FortiSIEM for advanced analytics
- Collect, correlate, and analyze security events from multiple sources
- Generate actionable reports and dashboards for SOC operations
- Automate threat detection and response workflows
- Implement best practices for security monitoring and incident response
- Troubleshoot and optimize analytics deployments for maximum efficiency

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

Target Audience

This course is ideal for:

- SOC Analysts and Engineers
- Network and Security Administrators
- IT and Security Operations Teams
- Fortinet Security Fabric Administrators
- Professionals preparing for the NSE 7 Advanced Analytics certification

Pre-Requisites

Participants should have:

- Understanding of networking and cybersecurity fundamentals
- Familiarity with Fortinet products such as FortiGate, FortiAnalyzer, and FortiSIEM
- Experience with SOC operations, logging, and incident response
- Knowledge of SIEM and analytics concepts is recommended

Course Content

Module 1: Advanced Analytics Overview

- Introduction to Fortinet Security Fabric analytics
- FortiAnalyzer and FortiSIEM capabilities
- Use cases for advanced analytics in SOC operations

Module 2: Data Collection and Event Correlation

- Configuring log collection from Fortinet and third-party devices

- Correlation rules and event management
- Identifying patterns and anomalies

Module 3: Dashboard and Reporting

- Creating actionable dashboards
- Generating automated reports for compliance and monitoring
- Customizing views for different stakeholders

Module 4: Automated Threat Detection and Response

- Threat intelligence integration
- Creating automated workflows and alerts
- Incident prioritization and response

Module 5: Troubleshooting and Optimization

- Diagnosing data collection and correlation issues
- Performance tuning for analytics platforms
- Best practices for operational efficiency

Module 6: Use Cases and Real-World Scenarios

- Advanced analytics for enterprise networks
- Security incident investigation
- Case studies and practical applications