NSE 5 Network Security Analyst—FortiAnalyzer 7.0 Course

Course Duration: 16 Hrs. **Course Code: NSE5-FAZ-7.0**

Course Overview

The **NSE 5 Network Security Analyst — FortiAnalyzer 7.0 Course** is designed for security professionals who need centralized visibility, analytics, and reporting across Fortinet security devices. This course focuses on deploying and managing FortiAnalyzer 7.0 to collect, analyze, and correlate logs, generate reports, and support incident investigation. Participants will gain practical knowledge to improve threat detection, compliance, and operational efficiency using FortiAnalyzer in enterprise environments.

What You'll Learn?

By completing this course, you will be able to:

- Understand FortiAnalyzer architecture and features
- Deploy and configure FortiAnalyzer 7.0
- Collect and manage logs from Fortinet devices
- Analyze traffic, threats, and security events
- Create and customize reports and dashboards
- Perform event correlation and incident investigation
- Integrate FortiAnalyzer with Fortinet Security Fabric
- Troubleshoot logging and reporting issues

Target Audience

This course is ideal for:

- Network Security Analysts

- SOC Analysts and Security Operations Teams
- Network and Security Engineers
- IT Administrators responsible for logging and monitoring
- Professionals preparing for NSE 5 certification

Pre-Requisites

Participants should have:

- Basic understanding of networking and security concepts
- Familiarity with FortiGate or Fortinet products
- Experience with logs and monitoring tools is recommended

Course Content

Module 1: Introduction to FortiAnalyzer and Analytics

- FortiAnalyzer role in the Security Fabric
- Key features and use cases
- Architecture and deployment options

Module 2: FortiAnalyzer Deployment and Initial Setup

- FortiAnalyzer 7.0 installation and configuration
- Device registration and management
- Storage and retention policies

Module 3: Log Collection and Management

- Log sources and types
- Log forwarding and filtering
- Log aggregation and optimization

Module 4: Analytics, Dashboards, and Event Monitoring

- Real-time and historical analytics
- Custom dashboards and widgets
- Event views and threat analysis

Module 5: Reporting and Compliance

- Predefined and custom reports
- Scheduling and automation
- Compliance and audit reporting

Module 6: Incident Analysis and Troubleshooting

- Event correlation and investigation
- Alerts and notifications
- Troubleshooting logging and performance issues