NSE 5 FortiEDR 4.2 Course

Course Duration: 16 Hrs. **Course Code: NSE5-FEDR-4.2**

Course Overview

The **NSE 5 FortiEDR 4.2** course is designed for security professionals responsible for endpoint protection and advanced threat detection. This course provides in-depth knowledge of deploying, configuring, and managing FortiEDR 4.2 to detect, prevent, and respond to malware, ransomware, and targeted attacks on endpoints. Participants will gain hands-on experience in monitoring endpoint activity, managing threats, and integrating FortiEDR with the Fortinet Security Fabric, while preparing for the NSE 5 FortiEDR certification.

What You'll Learn?

By completing this course, you will be able to:

- Deploy and configure FortiEDR 4.2 across endpoints
- Implement advanced endpoint protection policies
- Detect, investigate, and remediate malware and ransomware threats
- Monitor endpoint activity and analyze security incidents
- Integrate FortiEDR with FortiGate, FortiAnalyzer, and FortiSIEM
- Automate endpoint threat response workflows
- Troubleshoot and optimize FortiEDR deployments

Target Audience

This course is ideal for:

- Endpoint Security Administrators

- SOC Analysts and Incident Response Teams
- Network and Security Engineers
- IT Security Operations and Threat Hunting Professionals
- Professionals preparing for the NSE 5 FortiEDR certification

Pre-Requisites

Participants should have:

- Understanding of networking and endpoint security concepts
- Familiarity with threat detection and incident response
- Experience with Fortinet products or NSE 4-level knowledge is recommended

Course Content

Module 1: FortiEDR 4.2 Architecture and Deployment

- FortiEDR system components and architecture
- Deployment models and system requirements
- Installation and initial configuration

Module 2: Endpoint Security Policies

- Creating and managing protection policies
- Application control, threat prevention, and exploit protection
- Policy enforcement across endpoints

Module 3: Threat Detection and Response

- Real-time monitoring and alerting
- Investigating incidents and forensic analysis

- Automated and manual remediation actions

Module 4: Integration with Security Fabric

- FortiEDR integration with FortiGate, FortiAnalyzer, and FortiSIEM
- Endpoint telemetry and threat intelligence sharing
- Coordinated response across Fortinet products

Module 5: Monitoring, Reporting, and Analytics

- Dashboards and event monitoring
- Compliance reporting
- Performance and threat metrics

Module 6: Troubleshooting, Maintenance, and Best Practices

- Common FortiEDR issues and resolutions
- System updates, backup, and restore
- Best practices for endpoint security operations