NSE 7 Advanced Threat Protection Course

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

Course Overview

The **NSE 7 Advanced Threat Protection** course is designed for experienced network and security professionals who are responsible for defending enterprise environments against sophisticated and advanced cyber threats. This course focuses on advanced threat detection, prevention, and response techniques using Fortinet's Security Fabric. Participants will learn how to identify advanced persistent threats (APTs), zero-day attacks, and complex malware using integrated Fortinet solutions such as FortiGate, FortiSandbox, FortiAnalyzer, and FortiSIEM, while preparing for the NSE 7 Advanced Threat Protection certification.

What You'll Learn?

By completing this course, you will be able to:

- Understand advanced threat landscapes and attack methodologies
- Detect and mitigate zero-day threats and advanced malware
- Configure Fortinet solutions for advanced threat protection
- Implement sandboxing, threat intelligence, and behavior analysis
- Correlate security events for faster threat identification
- Automate threat response using Fortinet Security Fabric
- Apply best practices for proactive and reactive threat defense

Target Audience

This course is ideal for:

- Senior Network and Security Engineers
- SOC Analysts and Incident Response Teams
- Cybersecurity Architects and Consultants
- IT Security Operations Professionals
- Professionals preparing for the NSE 7 Advanced Threat Protection certification

Pre-Requisites

Participants should have:

- Strong knowledge of networking and cybersecurity fundamentals
- Experience with FortiGate firewall configuration
- Familiarity with Fortinet Security Fabric concepts
- NSE 4 or equivalent Fortinet experience is strongly recommended

Course Content

Module 1: Advanced Threat Landscape

- Overview of advanced cyber threats and attack vectors
- Advanced Persistent Threats (APTs) and zero-day attacks
- Threat intelligence and attacker methodologies

Module 2: Fortinet Advanced Threat Protection Architecture

- Fortinet Security Fabric for ATP
- Integration of FortiGate, FortiSandbox, FortiAnalyzer, and FortiSIEM
- Deployment models and best practices

Module 3: Advanced Malware Detection and Sandboxing

- FortiSandbox architecture and configuration
- Behavior-based analysis and threat scoring
- Automated malware detection and response

Module 4: Threat Intelligence and Correlation

- Threat intelligence feeds and IOC management
- Event correlation and advanced analytics
- Identifying hidden and lateral threats

Module 5: Automated Response and Incident Handling

- Security orchestration and automated response
- Threat containment and remediation
- Incident investigation and reporting

Module 6: Optimization, Monitoring, and Best Practices

- Tuning ATP policies and performance optimization
- Monitoring dashboards and alerts
- Best practices for enterprise-scale threat protection

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