Forti Sandbox Administrator Course

Course Duration: 16 Hrs. **Course Code: FSB-ADM-7.x**

Course Overview

The **FortiSandbox Administrator** course is designed for security professionals who want to deploy, configure, and manage FortiSandbox for advanced threat detection and malware analysis. This course focuses on identifying zero-day threats, analyzing suspicious files, and integrating FortiSandbox with the Fortinet Security Fabric. Participants will gain practical knowledge to strengthen organizational security posture through advanced threat intelligence and automated response.

What You'll Learn?

By completing this course, you will be able to:

- Understand FortiSandbox architecture and deployment options
- Configure malware analysis and sandboxing policies
- Detect and analyze zero-day and advanced threats
- Integrate FortiSandbox with FortiGate and other Fortinet products
- Use threat intelligence and reporting features
- Automate response actions based on sandbox verdicts
- Troubleshoot and optimize FortiSandbox performance

Target Audience

This course is ideal for:

- Security Engineers and Analysts
- SOC and Incident Response Professionals

- Network and Security Administrators
- Threat Intelligence and Malware Analysts
- Professionals managing advanced threat protection solutions

Pre-Requisites

Participants should have:

- Understanding of cybersecurity fundamentals
- Familiarity with malware and threat concepts
- Experience with Fortinet security products is beneficial

Course Content

Module 1: Introduction to FortiSandbox

- Role of sandboxing in cybersecurity
- FortiSandbox deployment models
- System requirements and interface overview

Module 2: Malware Detection and Analysis

- Static and dynamic malware analysis
- File behavior analysis techniques
- Verdicts and threat scoring

Module 3: Integration with Fortinet Security Fabric

- Integrating FortiSandbox with FortiGate, FortiMail, and FortiClient
- Automated response workflows
- Threat intelligence sharing

Module 4: Advanced Threat Protection Configuration

- Custom policies and analysis profiles
- Zero-day threat detection
- Handling evasive malware techniques

Module 5: Monitoring, Reporting, and Automation

- Threat dashboards and reports
- Alerting and notifications
- Automated remediation actions

Module 6: Maintenance, Troubleshooting, and Best Practices

- System updates and backups
- Performance tuning
- The best operational practices and course wrap-up