FORTINET
Premier Authorized Training Center

FORTINET CERTIFIED SOLUTION SPECIALIST
Security Operations

fast lane

Security Operations Architect

Course Description

In this course, you will learn how to design, deploy, and manage a Fortinet SOC solution using FortiSIEM and FortiSOAR. You will learn how to analyze and respond to security incidents according to industry best practices for incident handling. You will also learn about SOC playbook development, threat hunting, and how to incorporate FortiAI in your workflow.

Product Version:

- FortiSOAR 7.6

Course Duration:

2 days

Certification:

This course is intended to help you prepare for the Fortinet NSE 7 - Security Operations Architect exam. This exam is part of the FCSS Security Operations certification track.

Prerequisites:

You must have an understanding of the topics covered in the FortiSIEM Analyst course, or have equivalent experience.

Outlines:

1. SOC Concepts and Security Frameworks
2. Fortinet SOC with FortiSIEM and FortiSOAR
3. Incident Handling and FortiSIEM
4. Incident Handling and FortiSOAR
5. SOC Playbook Development
6. Threat Hunting

Objectives:

After completing this course, you will be able to:

- Describe the main functions and roles within a SOC
- Identify the challenges that can be solved by the Fortinet SOC
- Describe the MITRE ATT&CK Enterprise Matrix and the Cyber Kill Chain
- Describe how to identify and reduce the attack surface
- Describe common attack vectors
- Describe the benefits of using FortiSIEM and FortiSOAR
- Describe different Fortinet SOC deployment architectures
- Describe the FortiSOAR Content Hub and connectors
- Describe FortiAI features
- Describe FortiAI in FortiSIEM and FortiSOAR
- Describe reactive and proactive threat hunting processes

- Generate threat hunting hypotheses
- Identify and configure data sources
- Configure data ingestion
- Configure FortiSIEM rules
- Execute attack vectors
- Describe the NIST SP 800-61 incident handling process
- Describe the incident handling workflow with FortiSIEM and FortiSOAR
- Analyze, handle, and tune incidents on FortiSIEM
- Ingest FortiSIEM incidents into FortiSOAR for incident handling
- Escalate FortiSOAR alerts into incidents
- Describe automation requirements
- Describe FortiSOAR playbook steps
- Run playbooks to enrich indicators
- Configure a playbook to retrieve a hash rating from FortiSandbox
- Perform containment on FortiGate, Windows Active Directory, and FortiClient EMS using FortiSOAR connectors
- Eradicate artifacts from a compromised host
- Release a compromised host from quarantine after recovery
- Manage playbook history logs

Who should attend

Security professionals involved in the design, implementation, operation, and monitoring of Fortinet SOC solutions using FortiSIEM and FortiSOAR should attend this course.