Security Operations Analyst

Duration: 2 Days

Course Description:

In this course, you will learn how to design, deploy, and manage a Fortinet SOC solution using advanced FortiAnalyzer features and functions to detect, investigate, and respond to cyberthreats. You will learn how to analyze and respond to security incidents according to industry best practices for incident handling. You will also learn how threat actors behave, how to identify and reduce your organization's attack surface, and how to use widely adopted industry frameworks and models to identify and characterize adversary behavior.

Target Audience:

Security professionals involved in the design, implementation, and monitoring of Fortinet SOC solutions based on FortiAnalyzer should attend this course.

Prerequisites:

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- FCP - FortiAnalyzer Analyst
- FCP - FortiAnalyzer Administrator

Course Objectives:

- Describe the main functions and roles within a SOC
- Identify common security challenges that Fortinet SOC solutions address
- Analyze simulated attacks and categorize attacker tactics using industry frameworks
- Analyze and respond to security incidents according to industry best practices for incident handling
- Describe basic FortiAnalyzer SOC concepts, definitions, and features
- Manage administrative domains (ADOM)
- Describe FortiAnalyzer operation modes
- Configure FortiAnalyzer collectors and analyzers
- Design and deploy FortiAnalyzer Fabric deployments
- Manage Fabric groups
- Analyze and manage events, and customize event handlers
- Analyze and create incidents
- Analyze threat hunting dashboards
- Analyze indicators of compromise (IOCs) information from compromised hosts
- Manage outbreak alerts
- Identify playbook components
- Describe trigger types and their properties
- Create and customize playbooks from a template
- Create new playbooks
- Use variables in tasks
- Configure connector actions
- Monitor playbooks
- Export and import playbooks
- Configure automation stitch integrations between FortiAnalyzer and FortiGate
- Identify the attack surface
- Describe how to reduce the attack surface
- Identify common attack vectors
- Capture traffic flows
- Configure new reports
- Customize reports

Course Outlines:

- SOC Concepts and Security Frameworks
- FortiAnalyzer Architecture
- SOC Operations
- SOC Automation
- Attack Surface and Vectors
- Reporting