Security Operations Analyst

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.

Product Version

- FortiAnalyzer 7.4

Course Duration

- Lecture time (estimated): 4 hours
- Lab time (estimated): 8 hours
- Total course duration (estimated): 12 hours
  - 2 full days or 4 half days

Who Should Attend

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

Certification

This course is intended to help you prepare for the FCSS - *Security Operations 7.4 Analyst* certification exam. This exam is in the Fortinet Certified Solution Specialist - Security Operations certification track.

Prerequisites

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

- FCP - *FortiAnalyzer Analyst*
- FCP - *FortiAnalyzer Administrator*

Agenda

1. SOC Concepts and Security Frameworks
2. FortiAnalyzer Architecture
3. SOC Operations
4. SOC Automation
5. Attack Surface and Vectors
6. Reporting

Objectives

After completing this course, you should be able to:

- 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

Training Delivery Options and SKUs

Instructor-Led Training

Includes standard NSE training content delivered in person onsite, or live online using a virtual classroom application. Training is delivered within public classes or as a private class. Private requests are scoped, quoted, developed, and delivered by Fortinet Training (minimum quantities apply).

Contact your Fortinet Resellers or Authorized Training Partners to purchase this course.

Self-Paced Training

Includes online training videos and resources through the Fortinet Training Institute library, free of charge.

You can purchase on-demand lab access with interactive, hands-on activities using a purchase order (PO) through Fortinet Resellers or Authorized Training Partners.

After you complete the purchase, you receive lab access and the accompanying lab guide within the self-paced course.

For training and lab SKUs, or additional purchasing information, refer to Purchasing Process.

ISC2

- CPE training hours: 4
- CPE lab hours: 8
- CISSP domains: Security Operations

Program Policies and FAQs

For questions about courses, certification, or training products, refer to Program Policy Guidelines or Frequently Asked Questions.