FORTINET CERTIFIED PROFESSIONAL
Security Operations

FORTINET
Authorized
Premier Training Center

FortiSIEM

In this course, you will learn about FortiSIEM initial configurations, architecture, and the discovery of devices on the network. You will also learn how to collect performance information and aggregate it with syslog data to enrich the overall view of the health of your environment, how to use the configuration database to greatly facilitate compliance audits, and how to integrate FortiSIEM into your network awareness infrastructure.

Product Version

FortiSIEM 6.3

Course Duration

- Lecture time (estimated): 11 hours
- Lab time (estimated): 9 hours
- Total course duration (estimated): 20 hours
  - 3 full days or 5 half days

Who Should Attend

Anyone who is responsible for the day-to-day management of FortiSIEM should attend this course.

Certification

This course is part of the preparation for the *Fortinet NSE 5 - FortiSIEM 6.3* certification exam. This exam is part of the Fortinet Certified Professional - Security Operations certification track.

Prerequisites

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

- *FCP - FortiGate Security*
- *FCP - FortiGate Infrastructure*

Agenda

1. Introduction
2. SIEM and PAM Concepts
3. Discovery and FortiSIEM Agents
4. FortiSIEM Analytics
5. CMDB Lookups and Filters
6. Group By and Data Aggregation
7. Rules and MITRE ATT&CK
8. Incidents and Notification Policies
9. Reports and Dashboards
10. Maintaining and Tuning
11. Troubleshooting

Objectives

After completing this course, you will be able to:

- Identify business drivers for using SIEM tools
- Describe SIEM and PAM concepts
- Describe key features of FortiSIEM
- Understand how collectors, workers, and supervisors work together
- Configure notifications
- Create new users and custom roles
- Describe and enable devices for discovery
- Understand when to use agents
- Perform real-time, historic structured searches
- Group and aggregate search results
- Examine performance metrics
- Create custom incident rules
- Edit existing, or create new, reports
- Configure and customize the dashboards
- Export CMDB information
- Identify Windows agent components
- Describe the purpose of Windows agents
- Understand how the Windows agent manager works in various deployment models
- Identify reports that relate to Windows agents
- Understand the FortiSIEM Linux file monitoring agent
- Understand agent registration
- Monitor agent communications after deployment
- Troubleshoot FortiSIEM issues

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).

Use the following ILT Training SKU to purchase scheduled public classes of this course through Fortinet Resellers or Authorized Training Partners:

FT-FSM

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.

Use the following on-demand lab training SKU to purchase lab access using a PO:

FT-FSM-LAB

See Purchasing Process for more information about purchasing Fortinet training products.

(ISC)²

- CPE training hours: 11
- CPE lab hours: 9
- 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.