FORTINET
Premier Authorized Training Center

fast lane

FORTINET CERTIFIED PROFESSIONAL
Security Operations

FortiSIEM

Course Description

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:

3 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

Outlines:

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