FORTINET
Premier Authorized Training Center

fast lane

FORTINET CERTIFIED PROFESSIONAL
Security Operations

FortiAnalyzer Analyst

Course Description

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging. You will also learn how to identify current and potential threats through log analysis. Finally, you will examine the management of events, incidents, reports, and task automation with playbooks. These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.

Product Version:

- FortiAnalyzer 7.2

Course Duration:

1 day

Who should attend?

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Certification:

This course is intended to help you prepare for the Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst exam. This exam is part of the Fortinet Certified Professional - Security Operations certification track.

Prerequisites:

- Familiarity with all topics presented in the FCP - FortiGate Security and FCP - FortiGate Infrastructure courses
- Knowledge of SQL SELECT syntax is helpful

Outlines:

1. Introduction and Initial Access
2. Logging
3. FortiSoC—Events and Incidents
4. Reports
5. FortiSoC—Playbooks

Objectives:

After completing this course, you will be able to:

- Understand basic concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand FortiSoC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents
- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks