FORTINET
Premier Authorized Training Center

NSE 5 CERTIFIED
SECURITY OPERATIONS
FORTINET

fast lane

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 7.6

Course Duration:

2 Days

Certification:

This course is intended to help you prepare for the Fortinet NSE 5 - FortiAnalyzer 7.6 Analyst 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:

- FortiGate Operator
- FortiAnalyzer Administrator

It is also recommended that you have knowledge of the following topic:

- SQL SELECT statement syntax

Outlines:

1. SOC Concepts and Security Fabric
2. Log Data Flow and Navigation
3. Events, Indicators, and Incidents
4. FortiAI, Threat Hunting, and Troubleshooting
5. Reports
6. Playbooks

Objectives:

After completing this course, you will be able to:

- Describe SOC objectives, responsibilities, and roles
- Describe the role of FortiAnalyzer in a SOC
- Describe FortiAnalyzer Security Fabric integration
- Describe how logging works in a Security Fabric

- Describe FortiAnalyzer Fabric deployments
- Describe FortiAnalyzer operating modes
- Describe how FortiAnalyzer parses and normalizes logs
- Validate log parsers
- Search logs using normalized fields
- View and search for logs in the log view
- Create saved filters and dashboards
- View summary data in FortiView
- View dashboards and widget features
- Configure event handlers
- Manage events
- Configure indicators
- Create incidents
- Analyze incidents
- Configure incident settings
- Describe FortiAI operations and use cases
- Describe threat hunting
- Use the log count chart
- Use the SIEM log analytics table
- Describe outbreak alerts
- Collect log volume statistics
- Configure an automation stitch
- Configure an event handler with an automation stitch enabled
- Run and fine-tune predefined reports
- Customize reports with macros, custom charts, and datasets
- Configure external storage for reports
- Group reports
- Import and export reports and charts
- Attach reports to incidents
- Manage and troubleshoot reports
- Create new playbooks
- Use variables in tasks
- Monitor playbooks
- Export and import playbooks

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.