Training: Fortinet

FortiAnalyzer Analyst 7.4

FORTINET
Premier Authorized
Training Center

TRAINING GOALS:

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.

Objectives

After completing this course, you will be able to:

- Understand basic concepts and features
- Describe the purpose of collecting and securing 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

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.

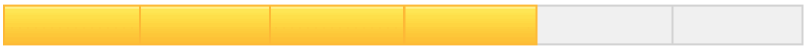
CONSPECT:

- Introduction and Initial Configuration
- Logging
- FortiSoC-Events and Incidents
- Reports
- FortiSoC-Playbooks

REQUIREMENTS:

- Familiarity with all topics presented in the FortiGate Security and FortiGate Infrastructure courses
- Knowledge of SQL SELECT syntax is helpful, but not required

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Fortinet.

This course is also intended to help you prepare for the Fortinet - FortiAnalyzer Analyst certification exam. This exam is part of the FCP Security Operations certification track. More information about Fortinet certification Program on the https://www.fortinet.com/training-certification

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

(ISC)2

- CPE training hours: 3
- CPE lab hours: 4
- CISSP domains: Security Operations