FortiAnalyzer Analyst

Duration: 1 Day

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.

Target Audience:

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

Prerequisites:

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

Course Objectives:

- Understand basic FortiAnalyzer concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand SOC 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

Course Outline:

- Introduction and Initial Access
- Logging
- Incidents and Events
- Reports
- Playbooks