FortiSIEM Analyst

Duration: 2 Days

Course Description:

In this course, you will learn how to use FortiSIEM to search, enrich, and analyze events from customers in a managed security service provider (MSSP) organization. You will learn how to perform real-time and historical searches and build advanced queries. You will also learn how to perform analysis and remediation of security incidents.

Target Audience:

Security professionals responsible for the detection, analysis, and remediation of security incidents using FortiSIEM should attend this course.

Prerequisites:

You must have an understanding of the topics covered in the following courses, or have equivalent experience:

- FCF - FortiGate Fundamentals
- FortiSIEM Administrator

Course Objectives:

- Describe how FortiSIEM solves common cybersecurity
- challenges
- Describe the main components and the unique database
- architecture on FortiSIEM
- Perform real-time and historical searches
- Define structured search operators and search conditions
- Reference the CMDB data in structured searches
- Add display fields and columns
- Build queries from search results and events Build nested queries and lookup tables
- Build rule subpatterns and conditions
- Identify critical interfaces and processes
- Create rules using baselines
- Analyze a profile report
- Analyze anomalies against baselines
- Analyze the different incident dashboard views
- Refine and tune incidents
- Clear an incident
- Export an incident report
- Create time-based and pattern-based clear conditions
- Configure automation policies
- Configure remediation scripts and actions
- Differentiate between manual and automatic remediation
- Configure notifications

Course Outline:

- Introduction to FortiSIEM
- Analytics
- Nested Queries and Lookup Tables
- Rules and Subpatterns
- Performance Metrics and Baselines
- Incidents
- Clear Conditions and Remediation