Training: Fortinet

FortiSIEM Analyst

Premier Authorized
Training Center

TRAINING GOALS:

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 using traditional and machine learning (ML)assisted methods.

Objectives

After completing this course, you should be able to:

- 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
- Configure display fields and columns
- Build queries from search results and events
- Build nested queries and lookup tables
- Build rule subpatterns and conditions
- Manage and tune incidents
- Resolve an incident
- Create time-based and pattern-based clear conditions
- Configure automation policies
- Create rules using baselines
- Analyze anomalies against baselines
- Describe the threat hunting workflow
- Analyze threat hunting dashboards
- Describe FortiSIEM ML modes and algorithms
- Describe how to train an ML model perform an analysis using a ML model
- Describe the benefits of deploying FortiSIEM UEBA

- Configure tags, rules, and incidents using UEBA data
- Describe how ZTNA tags affect the FortiSIEM incident and remediation process
- Configure a ZTNA tag using FortiSIEM to remediate incidents
- Generate and export a report
- Create a custom dashboard

Who Should Attend

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

CONSPECT:

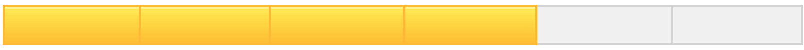
- Introduction to FortiSIEM
- Analytics
- Nested Queries and Lookup Tables
- Rules and Subpatterns
- Incidents
- Clear Conditions and Remediation
- Threat Hunting
- Performance Metrics and Baselines
- Machine Learning
- User and Entity Behavior Analytics
- FortiSIEM ZTNA
- Reports and Dashboards

REQUIREMENTS:

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

- FortiGate Operator
- FortiSIEM Administrator

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Fortinet (course completion).

This course is intended to help you prepare for the Fortinet NSE6 FortiSIEM Analyst exam. This exam is part of the FCSS Security Operations certification track.

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 9
- CPE lab hours: 9
- CISSP domains: Security Operations