Training: Fortinet

FortiSIEM Analyst

Premier Authorized
Training Center

TRANING TERMS

2025-09-15 | 2 days | Kraków / Virtual Classroom
2025-12-01 | 2 days | Warszawa / Virtual Classroom

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.

Objectives

After completing this course, you should be able to:

- Identify business drivers for using SIEM tools
- 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

Who Should Attend

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

CONSPECT:

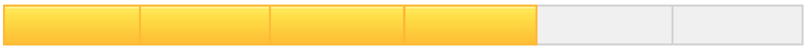
- Introduction to FortiSIEM
- Analytics
- Nested Queries and Lookup Tables
- Rules and Subpatterns
- Performance Metrics and Baselines
- Incidents
- Clear Conditions and Remediation

REQUIREMENTS:

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

- FCF - FortiGate Fundamentals
- FortiSIEM Administrator

Difficulty level



CERTIFICATE:

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

This course prepares you also for the *FCP - FortiSIEM Analyst* exam. By passing this exam, you will be awarded the associated exam badge.

TRAINER:

Fortinet Certified Trainer (FCT)

ADDITIONAL INFORMATION:

ISC2

- CPE training hours: 6
- CPE lab hours: 5
- CISSP domains: Security Operations