

FortiSIEM Analyst (FORT-SIEM)

ID FORT-SIEM Price on request Duration 2 days

Who should attend

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

This course is part of the following Certifications

Fortinet Certified Solution Specialist Security Operations (FCSSSO)

Prerequisites

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

- FCF FortiGate Fundamentals
- 1

Course 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
- · 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

FortiSIEM Analyst (FORT-SIEM)

Training Centres worldwide





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3 CH-8304 Wallisellen Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch