# FortiSIEM Analyst (FORT-SIEM)

**ID** FORT-SIEM **Price** US $ 1,900.—(excl. tax) **Duration** 3 days

This training is provided by our partner Fortinet.

## Important notes for the booking of trainings directly provided by Fortinet

If you are unable to attend the training date you have booked (e.g. illness, etc.) or if Fortinet cancels the course, a credit note is not possible under any circumstances. In both cases of cancellation, the validity of your credit remains for 12 months after the order.

For more information, please refer to the **Fortinet Terms and Conditions**.

## Course Overview

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.

This exam is part of the FCSS Security Operations certification track.

## 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:

- FortiGate Operator
- FortiSIEM Administrator

## 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
- 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

## Detailed Course Outline

- 1. Introduction to FortiSIEM
- 2. Analytics
- 3. Nested Queries and Lookup Tables
- 4. Rules and Subpatterns

- 5. Incidents
- 6. Clear Conditions and Remediation
- 7. Threat Hunting
- 8. Performance Metrics and Baselines
- 9. Machine Learning
- 10. User and Entity Behavior Analytics
- 11. FortiSIEM ZTNA
- 12. Reports and Dashboards

# About Fast Lane

Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

## Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

## Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

## Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

**Worldwide Presence**
with high-end training centers around the globe

**Multiple Awards**
from vendors such as AWS, Microsoft, Cisco, Google, NetApp, VMware

**Experienced SMEs**
with over 19.000 combined certifications


**Germany**
**Fast Lane Institute for Knowledge Transfer GmbH**
Tel. +49 40 25334610
info@flane.de / www.flane.de

**Austria**
**ITLS GmbH**
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

**Switzerland**
**Fast Lane Institute for Knowledge Transfer (Switzerland) AG**
Tel. +41 44 8325080
info@flane.ch / www.flane.ch