Security Operations Analyst (SOC-ANS)

ID SOC-ANS **Price** on request **Duration** 1 day

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 design, deploy, and manage a Fortinet SOC solution using advanced FortiAnalyzer features and functions to detect, investigate, and respond to cyberthreats. You will learn how to analyze and respond to security incidents according to industry best practices for incident handling. You will also learn how threat actors behave, and how to use widely adopted industry frameworks and models to identify and characterize adversary behavior.

This exam is in the FCSS Security Operations certification track.

Who should attend

Security professionals involved in the design, implementation, and monitoring of Fortinet SOC solutions based on FortiAnalyzer should attend this course.

Prerequisites

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

- FortiAnalyzer Analyst (FAZ-ANS)
- FortiAnalyzer Administrator (ANLZR-ADMN)

Course Objectives

After completing this course, you will be able to:

- Describe the main functions and roles within a SOC
- Identify common security challenges that Fortinet SOC solutions address
- Analyze simulated attacks and categorize attacker tactics using industry frameworks
- Analyze and respond to security incidents according to industry best practices for incident handling
- Describe basic FortiAnalyzer SOC concepts, definitions, and features
- Manage administrative domains
- Describe FortiAnalyzer operation modes
- Configure FortiAnalyzer collectors and analyzers
- Design and deploy FortiAnalyzer Fabric deployments
- Manage Fabric groups
- Analyze and manage events, and customize event handlers
- Analyze and create incidents
- Analyze threat hunting dashboards
- Analyze indicators of compromise (IOC) information from compromised hosts
- Manage outbreak alerts
- Identify playbook components
- Describe trigger types and their properties
- Create and customize playbooks from a template
- Create new playbooks from scratch
- Use variables in tasks
- Configure connector actions
- Monitor playbooks
- Export and import playbooks

Detailed Course Outline

- 1. SOC Concepts and Security Frameworks
- 2. FortiAnalyzer Architecture
- 3. SOC Operations
- 4. SOC Automation

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