Security Operations Analyst (SOC-ANS)

ID SOC-ANS **Prix** sur demande **Durée** 1 jours

A qui s'adresse cette formation

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

Pré-requis

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)

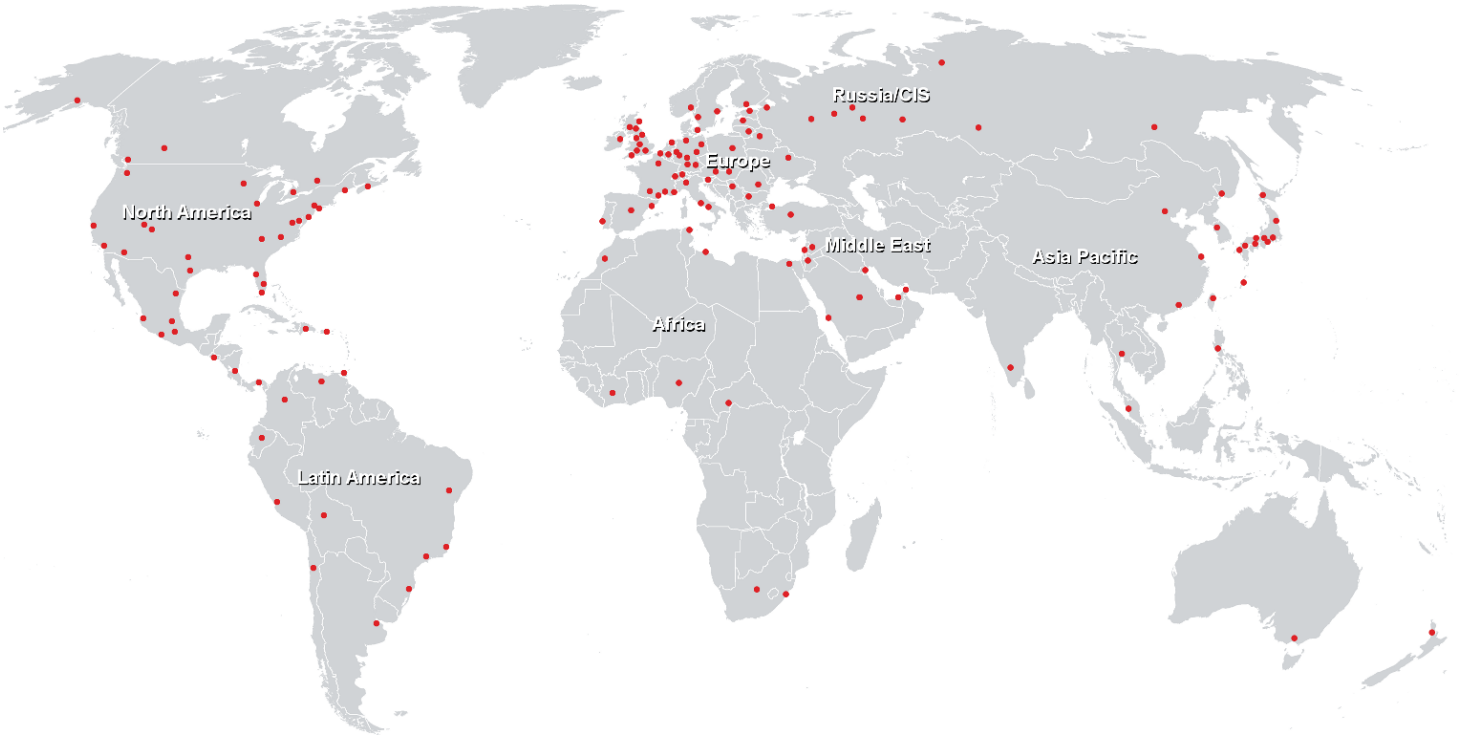
Objectifs

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

Security Operations Analyst (SOC-ANS)

Centres de formation dans le monde entier





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