

FortiAnalyzer Analyst (FAZ-ANS)

ID FAZ-ANS Prix sur demande Durée 1 jour

A qui s'adresse cette formation

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Pré-requis

- Familiarity with all topics presented in the [FortiGate Security \(FORT-SECI\)](#) and [FortiGate Infrastructure \(FORT-SECII\)](#) courses
- Knowledge of SQL SELECT syntax is helpful, but not required

Objectifs

- Introduction and Initial Configuration
- Logging
- FortiSoC—Events and Incidents
- Reports
- FortiSoC—Playbooks

Contenu

After completing this course, you should be able to:

- Understand basic concepts and features
- Describe the purpose of collecting and securing logs
- View and search for logs in Log View and FortiView
- Understand FortiSoC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents
- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks

FortiAnalyzer Analyst (FAZ-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>