FortiAnalyzer Analyst (FAZ-ANS)

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

Who should attend

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

Prerequisites

- Familiarity with all topics presented in the FortiGate Security (FORT-SECI) and FortiGate Infrastructure (FORT-INFRA) courses
- Knowledge of SQL SELECT syntax is helpful

Course Content

After completing this course, you will be able to:

- Understand basic FortiAnalyzer concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand SOC 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)

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