# FortiAnalyzer Analyst (FAZ-ANS)

**ID** FAZ-ANS **Price** CHF 1,000.—(excl. VAT) **Duration** 1 day

## Who should attend

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

## This course is part of the following Certifications

Fortinet Certified Professional Security Operations (FCPSO)

## Prerequisites

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

- FortiGate Operator
- FortiAnalyzer Administrator (ANLZR-ADMN)

It is also recommended that you have knowledge of the following topic:

- SQL SELECT statement syntax

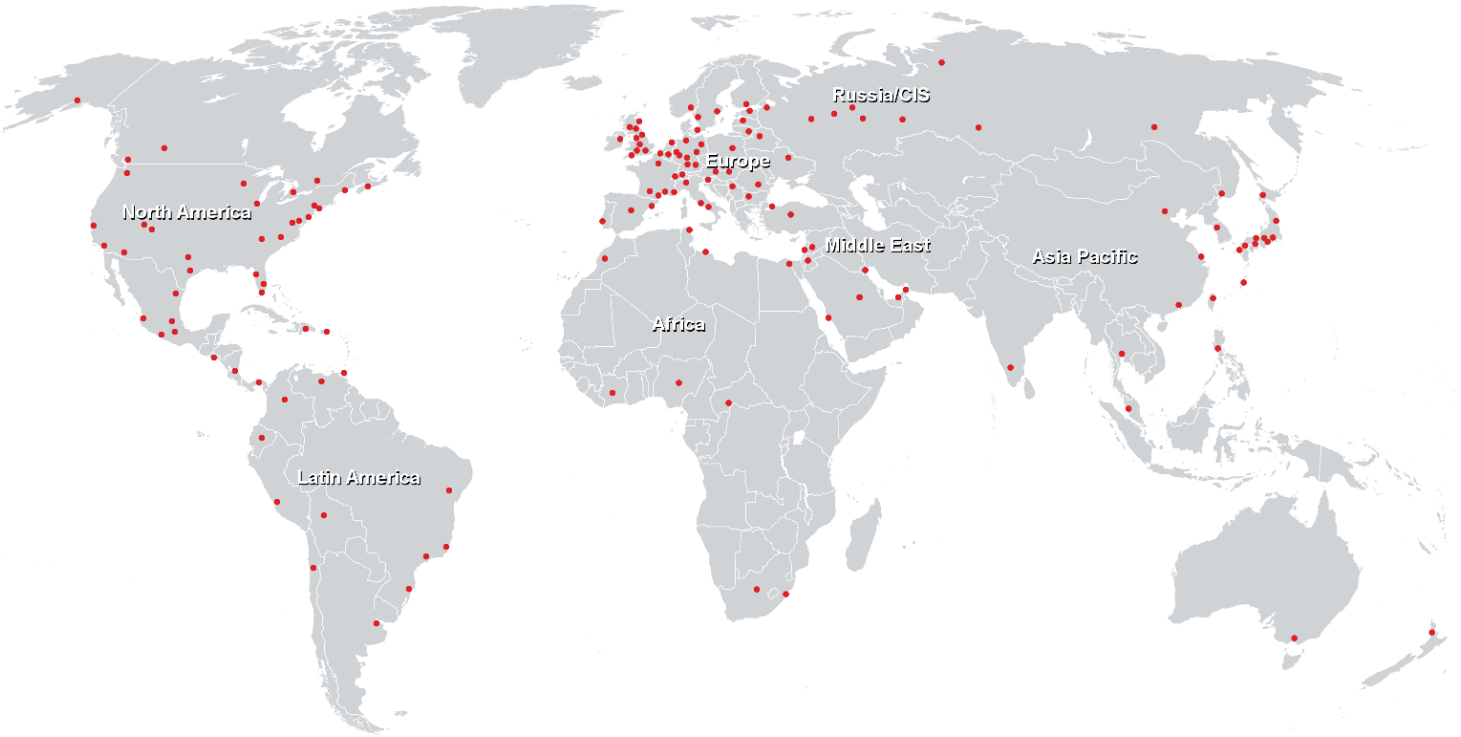
## Course Objectives

After completing this course, you should be able to:

- Describe SOC objectives, responsibilities, and roles
- Describe the role of FortiAnalyzer in a SOC
- Describe FortiAnalyzer Security Fabric integration
- Describe how logging works in a Security Fabric
- Describe FortiAnalyzer Fabric deployments
- Describe FortiAnalyzer operating modes
- Describe how FortiAnalyzer parses and normalizes logs
- Validate log parsers
- Search logs using normalized fields
- View and search for logs in the log view
- Create saved filters and dashboards
- View summary data in FortiView
- View dashboards and widget features
- Configure event handlers
- Manage events
- Configure indicators
- Create incidents
- Analyze incidents
- Configure incident settings
- Describe FortiAI operations and use cases
- Describe threat hunting
- Use the log count chart
- Use the SIEM log analytics table
- Describe outbreak alerts
- Collect log volume statistics
- Configure an automation stitch
- Configure an event handler with an automation stitch enabled
- Run and fine-tune predefined reports
- Customize reports with macros, custom charts, and datasets
- Configure external storage for reports
- Group reports
- Import and export reports and charts
- Attach reports to incidents
- Manage and troubleshoot reports
- Create new playbooks
- Use variables in tasks
- Monitor playbooks
- Export and import 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**