

## FortiAnalyzer Analyst (FAZ-ANS)

ID FAZ-ANS Preis CHF 1'000.— (exkl. MwSt.) Dauer 1 Tag

#### **Zielgruppe**

Jeder, der für die Analyse von Fortinet Security Fabric und die Automatisierung von Aufgaben zur Erkennung von und Reaktion auf Cyberangriffe mit FortiAnalyzer verantwortlich ist, sollte diesen Kurs besuchen.

#### Empfohlenes Training für die Zertifizierung zum

Fortinet Certified Professional Security Operations (FCPSO)

#### Voraussetzungen

- Vertrautheit mit allen Themen, die in den Kursen FortiGate Security (FORT-SECI) und FortiGate Infrastructure (FORT-INFRA) behandelt werden
- Kenntnisse der SQL SELECT-Syntax sind hilfreich

#### Kursinhalt

Nach Abschluss dieses Kurses werden Sie in der Lage sein:

- Verstehen grundlegender FortiAnalyzer-Konzepte und -Funktionen
- Beschreiben Sie den Zweck der Erfassung und Speicherung von Protokollen
- Anzeigen und Suchen von Protokollen in Log View und FortiView
- Verstehen der SOC-Merkmale
- Verwalten von Ereignissen und Ereignisbehandlern
- Konfigurieren und Analysieren von Vorfällen
- Durchführung von Aufgaben zur Bedrohungssuche
- Verstehen von Ausbruchswarnungen
- Beschreiben Sie, wie Berichte innerhalb von ADOMs funktionieren
- Anpassen und Erstellen von Diagrammen und Datasets
- Anpassen und Ausführen von Berichten
- Externen Speicher für Berichte konfigurieren
- Berichte an Vorfälle anhängen
- Fehlerbehebung bei Berichten
- Verstehen von Playbook-Konzepten
- Playbooks erstellen und überwachen

.

# FortiAnalyzer Analyst (FAZ-ANS)

## **Weltweite Trainingscenter**





## 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