

Advanced Analytics (FORT-ADVANALYTICS)

ID FORT-ADVANALYTICS Preis 2.900,- € (exkl. MwSt.) Dauer 3 Tage

Dieses Training wird von Fortinet direkt durchgeführt.

Wichtige Hinweise für die Buchung von durch Fortinet direkt durchgeführten Trainings

Sollten Sie den von Ihnen gebuchten Schulungstermin nicht wahrnehmen können (z. B. Krankheit etc.) oder bei Kursabsage durch Fortinet ist eine Gutschrift unter keinen Umständen möglich. In beiden Stornierungsfällen bleibt die Gültigkeit Ihrer Credits für 12 Monate nach Bestellung bestehen.

Weitere Informationen entnehmen Sie bitte den [AGB von Fortinet](#)

...

Kursüberblick

In this course, you will learn how to use FortiSIEM in a multi-tenant environment. You will learn about rules and their architecture, how incidents are generated, how baseline calculations are performed, the different methods of remediation available, and how the MITRE ATT&CK framework integrates with FortiSIEM. You will also learn how to integrate FortiSOAR with FortiSIEM.

Certification - This course is intended to help you prepare for the Fortinet NSE 7 - Advanced Analytics 6.7 certification exam. This exam is in the Fortinet Certified Solution Specialist - Security Operations certification track.

Zielgruppe

Security professionals involved in the management, configuration, administration, and monitoring of FortiSIEM and FortiSOAR devices in an enterprise or service provider deployment used to monitor and secure the networks of customer organizations.

Voraussetzungen

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

- [FortiGate Security \(FORT-SECI\)](#)
- [FortiGate Infrastructure \(FORT-SECII\)](#)
- [FortiSIEM Analyst \(FORT-SIEM\)](#)

It is also highly recommended that you have an understanding of the following topics, or equivalent experience:

- Python programming
- Jinja2 template language for Python
- Linux systems
- SOAR technologies

Kursziele

After completing this course, candidates will be able to:

- Identify various implementation requirements for a multi-tenant FortiSIEM deployment
- Deploy FortiSIEM in a hybrid environment with and without collectors
- Design multi-tenant solutions with FortiSIEM
- Deploy collectors in a multi-tenant environment
- Manage EPS assignment and restrictions on FortiSIEM
- Manage resource utilization of a multi-tenant FortiSIEM cluster
- Maintain and troubleshoot a collector installation
- Deploy and manage Windows and Linux agents
- Create rules by evaluating security events
- Define actions for a single pattern security rule
- Identify multiple pattern security rules and define conditions and actions for them
- Differentiate between a standard and baseline report
- Create your own baseline profiles
- Deploy FortiSIEM UEBA agents
- Examine log-based UEBA rules
- Examine nested queries for advanced analytics
- Configure lookup tables for advanced analytics
- Configure clear conditions on FortiSIEM
- Analyze some out-of-the-box remediation scripts
- Configure various remediation methods on FortiSIEM
- Integrate FortiSOAR with FortiSIEM
- Remediate incidents from FortiSOAR

Detaillierter Kursinhalt

- Introduction to Multi-tenancy
- Defining FortiSIEM Collectors and FortiSOAR Connectors
- Operating Collectors
- Windows and Linux Agents
- Rules
- Single Subpattern Security Rule
- Multiple Subpattern Rules
- Baselines
- Baseline Rules
- FortiSIEM UEBA
- Nested Queries and Lookup Tables
- Clear Conditions
- Remediation

Über Fast Lane



Fast Lane ist weltweiter, mehrfach ausgezeichnete Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

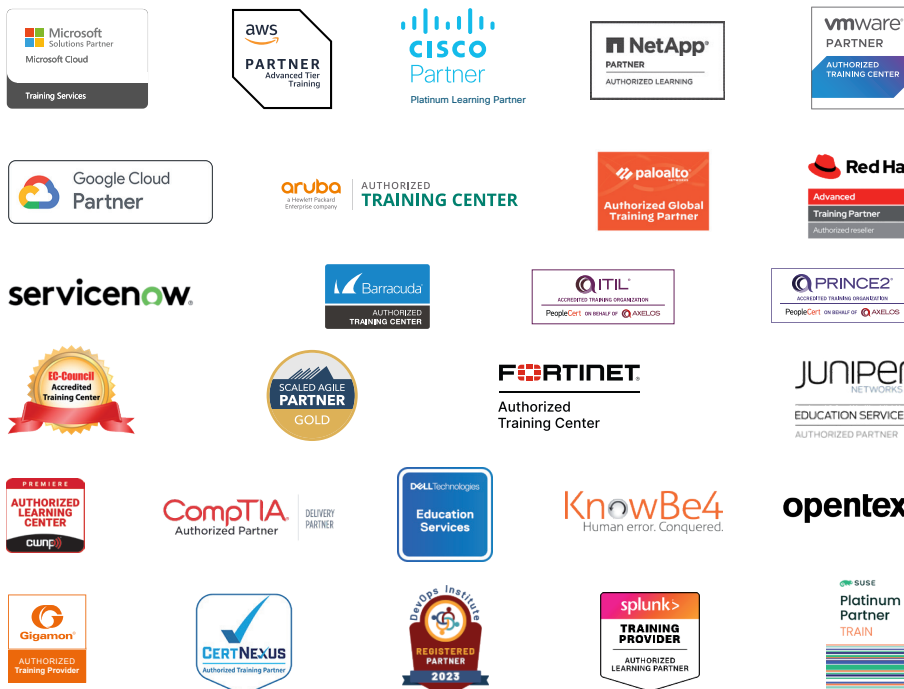
- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center



Weltweit vertreten
mit High-End-Trainingszentren
rund um den Globus



Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft,
Cisco, Google, NetApp, VMware



Praxiserfahrene Experten
mit insgesamt mehr als
19.000 Zertifizierungen

Deutschland

**Fast Lane Institute for Knowledge
Transfer GmbH**

Tel. +49 40 25334610

info@flane.de / www.flane.de

Österreich

ITLS GmbH

(ITLS ist ein Partner von Fast Lane)

Tel. +43 1 6000 8800

info@itls.at / www.itls.at

Schweiz

**Fast Lane Institute for Knowledge
Transfer (Switzerland) AG**

Tel. +41 44 8325080

info@flane.ch / www.flane.ch