

FortiSIEM Analyst (FORT-SIEM)

ID FORT-SIEM Preis US \$ 1.900,- (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 to search, enrich, and analyze events from customers in a managed security service provider (MSSP) organization. You will learn how to perform real-time and historical searches, and build advanced queries. You will also learn how to perform analysis and remediation of security incidents using traditional and machine learning (ML) assisted methods.

This exam is part of the FCSS Security Operations certification track.

Zielgruppe

Security professionals responsible for the detection, analysis, and remediation of security incidents using FortiSIEM should attend this course.

Empfohlenes Training für die Zertifizierung zum

Fortinet Certified Solution Specialist Security Operations (FCSSSO)

Voraussetzungen

You must have an understanding of the topics covered in the

following courses, or have equivalent experience:

- FortiGate Operator
- FortiSIEM Administrator

Kursziele

After completing this course, you should be able to:

- Describe how FortiSIEM solves common cybersecurity challenges
- Describe the main components and the unique database architecture on FortiSIEM
- Perform real-time and historical searches
- Define structured search operators and search conditions
- Reference the CMDB data in structured searches
- Configure display fields and columns
- Build queries from search results and events
- Build nested queries and lookup tables
- Build rule subpatterns and conditions
- Manage and tune incidents
- Resolve an incident
- Create time-based and pattern-based clear conditions
- Configure automation policies
- Create rules using baselines
- Analyze anomalies against baselines
- Describe the threat hunting workflow
- Analyze threat hunting dashboards
- Describe FortiSIEM ML modes and algorithms
- Describe how to train an ML model perform an analysis using a ML model
- Describe the benefits of deploying FortiSIEM UEBA
- Configure tags, rules, and incidents using UEBA data
- Describe how ZTNA tags affect the FortiSIEM incident and remediation process
- Configure a ZTNA tag using FortiSIEM to remediate incidents
- Generate and export a report
- Create a custom dashboard

Detaillierter Kursinhalt

1. Introduction to FortiSIEM
2. Analytics

- 3. Nested Queries and Lookup Tables
- 4. Rules and Subpatterns
- 5. Incidents
- 6. Clear Conditions and Remediation
- 7. Threat Hunting
- 8. Performance Metrics and Baselines
- 9. Machine Learning
- 10. User and Entity Behavior Analytics
- 11. FortiSIEM ZTNA
- 12. Reports and Dashboards

Über Fast Lane



Fast Lane ist weltweit, mehrfach ausgezeichnete(r) 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