Security Operations Architect (SECOP-ARCH)

ID SECOP-ARCH **Preis** US $ 1.900,– (exkl. MwSt.) **Dauer** 2 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 design, deploy, and manage a Fortinet SOC solution using FortiSIEM and FortiSOAR. You will learn how to analyze and respond to security incidents according to industry best practices for incident handling. You will also learn about SOC playbook development, threat hunting, and how to incorporate FortiAI in your workflow.

This course is intended to help you prepare for the Fortinet NSE 7 - Security Operations Architect exam. This exam is part of the FCSS Security Operations certification track.

Zielgruppe

Security professionals involved in the design, implementation, operation, and monitoring of Fortinet SOC solutions using FortiSIEM and FortiSOAR 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 FortiSIEM Analyst course, or have equivalent experience.

Kursziele

After completing this course, you will be able to:

- Describe the main functions and roles within a SOC
- Identify the challenges that can be solved by the Fortinet SOC
- Describe the MITRE ATT&CK Enterprise Matrix and the Cyber Kill Chain
- Describe how to identify and reduce the attack surface
- Describe common attack vectors
- Describe the benefits of using FortiSIEM and FortiSOAR
- Describe different Fortinet SOC deployment architectures
- Describe the FortiSOAR Content Hub and connectors
- Describe FortiAI features
- Describe FortiAI in FortiSIEM and FortiSOAR
- Describe reactive and proactive threat hunting processes
- Generate threat hunting hypotheses
- Identify and configure data sources
- Configure data ingestion
- Configure FortiSIEM rules
- Execute attack vectors
- Describe the NIST SP 800-61 incident handling process
- Describe the incident handling workflow with FortiSIEM and FortiSOAR
- Analyze, handle, and tune incidents on FortiSIEM
- Ingest FortiSIEM incidents into FortiSOAR for incident handling
- Escalate FortiSOAR alerts into incidents
- Describe automation requirements
- Describe FortiSOAR playbook steps
- Run playbooks to enrich indicators
- Configure a playbook to retrieve a hash rating from FortiSandbox
- Perform containment on FortiGate, Windows Active Directory, and FortiClient EMS using FortiSOAR connectors
- Eradicate artifacts from a compromised host
- Release a compromised host from quarantine after recovery
- Manage playbook history logs

Detaillierter Kursinhalt

- SOC Concepts and Security Frameworks
- Fortinet SOC with FortiSIEM and FortiSOAR
- Incident Handling and FortiSIEM
- Incident Handling and FortiSOAR
- SOC Playbook Development
- Threat Hunting

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter 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