Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Freistädterstraße 236, A-4040 Linz

Email: education.ecs.at@arrow.com
Phone: +43 1 370 94 40 - 34

FortiSIEM Administrator

CODE:	LÄNGE:	PREIS:
FNT_SIEM	16 Hours (2 Tage)	€2,900.00

Description

After completing this course, you should be able to:
Describe FortiSIEM key features and deployment architectures
Describe FortiSIEM indicators of compromise (IoC) and reputation check
Describe how FortiSIEM receives, collects, normalizes, and enriches logs
Describe event type classifications
Describe customer scaling with FortiSIEM collectors and collector high availability (HA)
Describe FortiSIEM agent architecture for managed security services providers (MSSP)
Describe various Fortinet Security Fabric integrations
Perform initial configurations, and role-based access management (RBAC)
Configure and troubleshoot asset discovery
View performance metrics and perform actions in the configuration management database (CMDB)
Deploy, assign, register, and upgrade collectors for MSSP customers
Configure and manage collector HA
Create and monitor critical business services I Analyze business services dashboards
Install and register FortiSIEM agents
Monitor agent status on the CMDB
Monitor events per second (EPS) usage
Configure event dropping rules
Configure identity and location information in the CMDB
Deploy AI-based user entity behavior analysis (UEBA)
Configure on-net and off-net detection, and FortiInsight watchlists
Configure zero-trust network access (ZTNA) integration
Create custom dashboards
Load, save, schedule, and import reports
Create and run CMDB and UEBA reports
Manage collection jobs
Define maintenance schedules
Monitor system status with FortiSIEM health check scripts
Collect and analyze system logs

Lernziel

In this course, you will learn about FortiSIEM initial configurations and architecture, and the discovery of devices on the network. You will also learn how to collect performance information and aggregate it with syslog data to enrich the overall view of the health of your environment, use the configuration database to greatly facilitate compliance audits, and integrate FortiSIEM into your network awareness infrastructure.
Product Version FortiSIEM 7.2

Zielgruppe

Security professionals involved in the deployment, administration, maintenance, and troubleshooting of FortiSIEM devices should attend this course

Voraussetzungen

You must have an understanding of the topics covered in the following course, or have equivalent experience:
FCF - FortiGate Operator

Inhalt

1. Architecture
2. SIEM and PAM Concepts
3. Discovery
4. Collectors
5. Agents
6. Fortinet Fabric Integration
7. Reports and Dashboards
8. Maintaining and Tuning
9. Troubleshooting

Test und Zertifizierung

Weitere Informationen

ISC2
CPE training hours: 7
CPE lab hours: 8
CISSP domains: Security Operations

Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
15 Mar 2027	München		German	Instructor Led Online		€2,900.00
05 Jul 2027	München		German	Instructor Led Online		€2,900.00
15 Nov 2027	München		German	Instructor Led Online		€2,900.00

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.