Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Arrow ECS Internet Security AG, Richtistrasse 11, CH-8304 Wallisellen

Email: trainings.ecs.ch@arrow.com
Phone: +41 43 222 80 00

FortiSIEM Administrator

CODE:	LENGTH:	PRICE:
FNT_FT-FSM-ADM	24 Hours (3 days)	CHf3,900.00

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 l 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

Objectives

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

Audience

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

Prerequisites

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

Programme

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 and Certification

N/A

Further Information

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

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
16 Nov 2026	Virtual Classroom	CET	German	Instructor Led Online		CHf3,900.00

Zusätzliche Information

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