



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

CODE:	LÄNGE:	PREIS:
FNT_FT-FSM-L	16 Hours (2 Tage)	€1,900.00

Description

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
- Add display fields and columns
- Build queries from search results and events
- Build nested queries and lookup tables
- Build rule subpatterns and conditions
- Identify critical interfaces and processes
- Create rules using baselines
- Analyze a profile report
- Analyze anomalies against baselines
- Analyze the different incident dashboard views
- Refine and tune incidents
- Clear an incident
- Export an incident report
- Create time-based and pattern-based clear conditions
- Configure automation policies
- Configure remediation scripts and actions
- Differentiate between manual and automatic remediation
- Configure notifications

Lernziel

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.
Product Version FortiSIEM 7.2

Zielgruppe

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

Voraussetzungen

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

- FCF - FortiGate Fundamentals
- FortiSIEM Administrator

Inhalt

1. Introduction to FortiSIEM
2. Analytics
3. Nested Queries and Lookup Tables
4. Rules and Subpatterns

- 5. Performance Metrics and Baselines
- 6. Incidents
- 7. Clear Conditions and Remediation

Test und Zertifizierung

This course is part of the preparation for the FCP - FortiSIEM 7.2 Analyst certification exam. This exam is part of the Fortinet Certified Professional - Security Operations certification track

Weitere Informationen

ISC2
CPE training hours: 6
CPE lab hours: 5
CISSP domains: Security Operations

Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
07 Apr 2026	Wien	CEDT	German	Classroom		€1,900.00
07 Apr 2026	Wien	CEDT	German	Instructor Led Online		€1,900.00
29 Jun 2026	Wien	CEDT	German	Classroom		€1,900.00
29 Jun 2026	Wien	CEDT	German	Instructor Led Online		€1,900.00
19 Oct 2026	Wien	CEDT	German	Classroom		€1,900.00
19 Oct 2026	Wien	CEDT	German	Instructor Led Online		€1,900.00

Zusätzliche Information

[Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.](#)