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 Analyst

CODE:	LÄNGE:	PREIS:
FNT_FT-FSM-ANS	24 Hours (3 Tage)	€1,900.00

Description

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.
Product Version
FortiSIEM 7.4

Lernziel

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

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:
FortiGate Operator
FortiSIEM Administrator

Inhalt

Introduction to FortiSIEM
Analytics
Nested Queries and Lookup Tables
Rules and Subpatterns
Incidents
Clear Conditions and Remediation
Threat Hunting
Performance Metrics and Baselines
Machine Learning
User and Entity Behavior Analytics
FortiSIEM ZTNA
Reports and Dashboards

Test und Zertifizierung

This course is intended to help you prepare for the Fortinet NSE 6 - FortiSIEM Analyst exam. This exam is part of the FCSS Security Operations certification track.

Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
17 Mar 2027	Wien	CET	German	Instructor Led Online		€1,900.00
07 Jul 2027	Wien	CEDT	German	Instructor Led Online		€1,900.00
17 Nov 2027	Wien	CET	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.