



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com

Phone: +49 (0)89 930 99 168

CODE:	LÄNGE:	PREIS:
FNT_SIEM	24 Hours (3 Tage)	€1,990.00

Description

In this course, you will learn about FortiSIEM initial configurations, 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, how to use the configuration database to greatly facilitate compliance audits, and how to integrate FortiSIEM into your network awareness infrastructure.

Lernziel

After completing this course, you should be able to:

- Identify business drivers for using SIEM tools
- Describe SIEM and PAM concepts
- Describe key features of FortiSIEM
- Understand how collectors, workers, and supervisors work together
- Configure notifications
- Create new users and custom roles
- Describe and enable devices for discovery
- Understand when to use agents
- Perform real-time, historic structured searches
- Group and aggregate search results
- Examine performance metrics
- Create custom incident rules
- Edit existing, or create new, reports
- Configure and customize the dashboards
- Export CMDB information
- Identify Windows agent components
- Describe the purpose of Windows agents
- Understand how the Windows agent manager works in various deployment models
- Identify reports that relate to Windows agents
- Understand the FortiSIEM Linux file monitoring agent
- Understand agent registration
- Monitor agent communications after deployment
- Troubleshoot FortiSIEM issues

Zielgruppe

Anyone who is responsible for the day-to-day management of FortiSIEM should attend this course.

Voraussetzungen

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

NSE 4 FortiGate Security **System Requirements**

NSE 4 FortiGate Infrastructure If you take the online format of this class, you must use a computer that has the following:

A high-speed Internet connection
An up-to-date web browser
A PDF viewer
Speakers or headphones
One of the following:
HTML 5 support
An up-to-date Java Runtime Environment (JRE) with Java Plugin enabled on your web browser
You should use a wired Ethernet connection, not a WiFi connection. Firewalls, including Windows Firewall or FortiClient, must allow connections to the online labs.

Inhalt

Introduction
SIEM and PAM Concepts
Discovery and FortiSIEM Agents
FortiSIEM Analytics
CMDB Lookups and Filters
Group By and Data Aggregation
Rules and MITRE ATT&CK
Incidents and Notification Policies
Reports and Dashboards
Maintaining and Tuning
Troubleshooting

Test und Zertifizierung

This course prepares you for the NSE 5 FortiSIEM certification exam.

Weitere Informationen

- E-BOOK - Die Original-Herstellerunterlage zu diesem Kurs erhalten Sie als [digitale Kursunterlage](#)

Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
03 Sep 2024	Virtual Classroom		German	Instructor Led Online		€1,990.00
03 Dec 2024	Virtual Classroom	GMT	German	Instructor Led Online		€1,990.00

Zusätzliche Information

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