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

FCP- FortiAnalyzer

CODE:	**LÄNGE:**	**PREIS:**
FNT_ANALYZER	16 Hours (2 Tage)	€1,790.00

Description

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging and reporting. You will learn how to configure and deploy FortiAnalyzer, and identify threats and attack patterns through logging, analysis, and reporting. Finally, you will examine the management of events, incidents, playbooks, and some helpful troubleshooting techniques.

Lernziel

After completing this course, you will be able to:
l Describe key features and concepts of FortiAnalyzer
l Deploy an appropriate architecture
l Use administrative access controls
l Monitor administrative events and tasks
l Configure high availability
l Understand HA synchronization and load balancing
l Upgrade the firmware of an HA cluster
l Verify the normal operation of an HA cluster
l Manage ADOMs
l Manage RAID
l Register supported devices
l Troubleshoot communication issues
l Manage disk quota
l Manage registered devices
l Protect log information
l View, search, manage, and troubleshoot logs
l Monitor and manage events
l Manage and customize event handlers
l Create and manage incidents
l Explore tools used for threat hunting
l Create, run, and troubleshoot playbooks
l Import and export playbooks
l Generate and customize reports
l Customize charts and datasets
l Manage and troubleshoot reports

Zielgruppe

Anyone who is responsible for the day-to-day management of FortiAnalyzer devices and FortiGate security information.

Voraussetzungen

l Familiarity with all topics presented in the NSE 4 FortiGate Security and NSE 4 FortiGate Infrastructure courses
l Knowledge of SQL SELECT syntax is helpful, but not required

System Requirements
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

1. Introduction and Initial Configuration
2. Administration and Management
3. Device Registration and Communication
4. Logging
5. FortiSoC—Incidents and Events
6. FortiSoC—Playbooks
7. Reports

Test und Zertifizierung

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

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

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