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

NSE 5 - FortiAnalyzer Analyst

CODE:	LÄNGE:	PREIS:
FNT_FT-FAZ-ANS	8 Hours (1 day)	€950.00

Description

In this course, you will learn the fundamentals of using FortiAnalyzer for centralized logging. You will also learn how to identify current and potential threats through log analysis. Finally, you will examine the management of events, incidents, reports, and task automation with playbooks. These skills will provide you with a solid foundation for becoming a SOC analyst in an environment using Fortinet products.
Product version:

- FortiAnalyzer 7.4.1

Lernziel

1. Introduction and Initial Access
2. Logging
3. Incidents and Events
4. Reports
5. Playbooks

Zielgruppe

Anyone who is responsible for Fortinet Security Fabric analytics and automating tasks to detect and respond to cyberattacks using FortiAnalyzer should attend this course.

Voraussetzungen

- Familiarity with all topics presented in the FCP - FortiGate Security and FCP - FortiGate Infrastructure courses
- Knowledge of SQL SELECT syntax is helpful

Inhalt

After completing this course, you should be able to:

- Understand basic FortiAnalyzer concepts and features
- Describe the purpose of collecting and storing logs
- View and search for logs in Log View and FortiView
- Understand SOC features
- Manage events and event handlers
- Configure and analyze incidents
- Perform threat hunting tasks
- Understand outbreak alerts
- Describe how reports function within ADOMs
- Customize and create charts and datasets
- Customize and run reports
- Configure external storage for reports
- Attach reports to incidents

- Troubleshoot reports
- Understand playbook concepts
- Create and monitor playbooks

Test und Zertifizierung

Exam:
This course prepares you for the FCP - FortiAnalyzer 7.4 Analyst exam. By passing this exam, you will be awarded the associated exam badge.

Certification:
This exam is part of the FCP Security Operations certification track.

Weitere Informationen

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.

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.