



**Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

---

**Sie erreichen uns unter**

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: [training.ecs.de@arrow.com](mailto:training.ecs.de@arrow.com)

Phone: +49 (0)89 930 99 168

**CODE:**

FNT\_FT-SOC-ANS

**LÄNGE:**

8 Hours (1 day)

**PREIS:**

Request Price

## Description

In this course, you will learn how to design, deploy, and manage a Fortinet SOC solution using advanced FortiAnalyzer features and functions to detect, investigate, and respond to cyberthreats. You will learn how to analyze and respond to security incidents according to industry best practices for incident handling. You will also learn how threat actors behave, and how to use widely adopted industry frameworks and models to identify and characterize adversary behavior

## Lernziel

After completing this course, you will be able to:

- Describe the main functions and roles within a SOC
- Identify common security challenges that Fortinet SOC solutions address
- Analyze simulated attacks and categorize attacker tactics using industry frameworks
- Analyze and respond to security incidents according to industry best practices for incident handling
- Describe basic FortiAnalyzer SOC concepts, definitions, and features
- Manage administrative domains
- Describe FortiAnalyzer operation modes
- Configure FortiAnalyzer collectors and analyzers
- Design and deploy FortiAnalyzer Fabric deployments
- Manage Fabric groups
- Analyze and manage events, and customize event handlers
- Analyze and create incidents
- Analyze threat hunting dashboards
- Analyze indicators of compromise (IOC) information from compromised hosts
- Manage outbreak alerts
- Identify playbook components
- Describe trigger types and their properties
- Create and customize playbooks from a template
- Create new playbooks from scratch
- Use variables in tasks
- Configure connector actions
- Monitor playbooks
- Export and import playbooks

## Zielgruppe

Security professionals involved in the design, implementation, and monitoring of Fortinet SOC solutions based on FortiAnalyzer should attend this course

## Voraussetzungen

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

- FCP - FortiAnalyzer Analyst
- FCP - FortiAnalyzer Administrator

## Inhalt

1. SOC Concepts and Security Frameworks

- 2. FortiAnalyzer Architecture
- 3. SOC Operations
- 4. SOC Automation

## Weitere Informationen

This course is intended to help you prepare for the FCSS - Security Operations 7.4 Analyst certification exam. This exam is in the Fortinet Certified Solution Specialist - Security Operations certification track.

## Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
28 Oct 2025	Virtual Classroom	CET	English	Instructor Led Online		Request Price

## Zusätzliche Information

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