



**Enterprise Computing Solutions - Education Services**

## **TRAINING OFFERING**

---

**Sie erreichen uns hier**

Freistädterstraße 236, A-4040 Linz

Email: [education.ecs.at@arrow.com](mailto:education.ecs.at@arrow.com)

Phone: +43 1 370 94 40 - 34

CODE:	LÄNGE:	PREIS:
FNT_FT-ADA	24 Hours (3 Tage)	€2,900.00

## Description

In this course, you will learn how to use FortiSIEM in a multi-tenant environment. You will learn about rules and their architecture, how incidents are generated, how baseline calculations are performed, the different methods of remediation available, and how the MITRE ATT&CK framework integrates with FortiSIEM. You will also learn how to integrate FortiSOAR with FortiSIEM.

## Lernziel

After completing this course, you should be able to:

- Identify various implementation requirements for a multi-tenant FortiSIEM deployment
- Deploy FortiSIEM in a hybrid environment with and without collectors
- Design multi-tenant solutions with FortiSIEM
- Deploy collectors in a multi-tenant environment
- Manage EPS assignment and restrictions on FortiSIEM
- Manage resource utilization of a multi-tenant FortiSIEM cluster
- Maintain and troubleshoot a collector installation
- Deploy and manage Windows and Linux agents
- Create rules by evaluating security events
- Define actions for a single pattern security rule
- Identify the incident attributes that trigger an incident
- Identify multiple pattern security rules and define conditions and actions for them
- Differentiate between a standard and baseline report
- Create your own baseline profiles
- Examine the MITRE ATT&CK framework integration on FortiSIEM and FortiSOAR
- Deploy FortiSIEM UEBA agents
- Examine UEBA rules, reports, event types, and windows template
- Configure clear conditions on FortiSIEM
- Analyze some out-of-the-box remediation scripts
- Configure various remediation methods on FortiSIEM
- Integrate FortiSOAR with FortiSIEM
- Remediate incidents from FortiSOAR

## Zielgruppe

Security professionals involved in the management, configuration, administration, and monitoring of FortiSIEM and FortiSOAR devices in an enterprise or service provider deployment used to monitor and secure the networks of customer organizations.

## Voraussetzungen

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

- NSE 4 FortiGate Security
- NSE 4 FortiGate Infrastructure
- NSE 5 FortiSIEM

It is also highly recommended that you have an understanding, or equivalent experience with, Python programming, Jinja2 template language for Python, Linux systems, and SOAR technologies.

### 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**

Introduction to Multi-Tenancy

Defining Collectors and Agents

Operating Collectors

Windows and Linux Agents

Rules

Single Subpattern Security Rule

Multiple Subpattern Rules

Introduction to Baseline

Baseline

UEBA

MITRE ATT&CK

Clear Conditions

Remediation

## **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.](#)