



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

<b>CODE:</b>	<b>LÄNGE:</b>	<b>PREIS:</b>
SPL_ASESGE	16 Hours (2 Tage)	€1,790.00

## Description

This 13.5 hour course prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES). It covers ES event processing and normalization, deployment requirements, technology add-ons, dashboard dependencies, data models, managing risk, and customizing threat intelligence

## Lernziel

Examine how ES functions including data models, correlation searches, notable events, and dashboards  
Create custom correlation searches  
Customize the Investigation Workbench  
Learn how to install or upgrade ES  
Learn the steps to setting up inputs using technology add-ons  
Fine tune ES Global Settings  
Customize risk and configure threat intelligence

## Voraussetzungen

To be successful, students should have a solid understanding of the following:

If on-prem:

- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

If on cloud:

- Splunk Cloud Administration
- and
- What is Splunk?
- Creating Knowledge Objects
- Intro to Splunk
- Creating Field Extractions
- Using Fields
- Enriching Data with Lookups
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- Data Models
- Introduction to Dashboards

## Inhalt

Module 1 – Introduction to ES

- Review how ES functions
- Understand how ES uses data models
- Configure ES roles and permissions

Module 2 – Security Monitoring

- Customize the Security Posture and Incident Review dashboards
- Create ad hoc notable events
- Create notable event suppressions

### Module 3 – Risk-Based Alerting

- Explain Risk-Based Alerting
- Explain risk scores
- Review the Risk Analysis dashboard
- Use annotations
- Explain ways to assign risk

### Module 4 – Incident Investigation

- Review the Investigations dashboard
- Customize the Investigation Workbench
- Manage investigations

### Module 5 – Installation

- Prepare a Splunk environment for installation
- Download and install ES on a search head
- Test a new install
- Post-install configuration tasks

### Module 6 – Initial Configuration

- Set general configuration options
- Add external integrations
- Configure local domain information
- Customize navigation
- Configure Key Indicator searches

### Module 7 – Validating ES Data

- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons

### Module 8 – Custom Add-ons

- Design a new add-on for custom data
- Use the Add-on Builder to build a new add-on

### Module 9 – Tuning Correlation Searches

- Configure correlation search scheduling and sensitivity
- Tune ES correlation searches

### Module 11 – Asset & Identity Management

- Review the Asset and Identity Management interface
- Describe Asset and Identity KV Store collections
- Configure and add asset and identity lookups to the interface
- Configure settings and fields for asset and identity lookups
- Explain the asset and identity merge process
- Describe the process for retrieving LDAP data for an asset or identity lookup

### Module 10 – Creating Correlation Searches

- Create a custom correlation search
- Manage adaptive responses
- Export/import content

### Module 12 – Managing Threat Intelligence

- Understand and configure threat intelligence

#### Splunk Education Services

- Use the Threat Intelligence Management interface to configure a new threat list

## Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
12 Jun 2025	Wien	CEDT	German	Instructor Led Online		€1,790.00
03 Dec 2025	Wien	CET	German	Instructor Led Online		€1,790.00

## Zusätzliche Information

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