



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

<b>CODE:</b>	<b>LÄNGE:</b>	<b>PREIS:</b>
SPL_ASESGE	16 Hours (2 Tage)	€1,500.00

## 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

At the end of this course you should be able to:

- Provide an overview of Splunk Enterprise Security (ES)
- Customize ES dashboards
- Examine the ES Risk framework and Risk-based Alerting (RBA)
- Customize the Investigation Workbench
- Understand initial ES installation and configuration
- Manage data intake and normalization for ES
- Create and tune correlation searches
- Configure ES lookups
- Configure Assets & Identities and Threat Intelligence

## Zielgruppe

SOC Analyst

## Voraussetzungen

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

- Using Splunk Enterprise Security
- What is Splunk?
- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Splunk Enterprise System Administration
- Splunk Enterprise Data Administration

## Inhalt

**Module 1** – Introduction to ES

- Review how ES functions
- Understand how ES uses data models
- Describe correlation searches, adaptive response actions, and notable events
- 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

- Give an overview of Risk-Based Alerting (RBA)
- Explain risk scores and how they can be changed
- Review the Risk Analysis dashboard
- Describe annotations

**Module 4** – Incident Investigation

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

**Module 5** – Installation

- Give an overview of general ES install requirements
- Explain the different add-ons and where they are installed
- Provide ES pre-installation requirements
- Identify steps for downloading and installing ES

**Module 6** – General Configuration

- Set general configuration options
- Configure local and cloud domain information
- Work with the Incident Review KV Store
- 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

- Ingest custom data in ES
- Create an add-on for a custom sourcetype
- Describe add-on troubleshooting

**Module 9** – Tuning Correlation Searches

- Describe correlation search operation
- Customize correlation searches
- Describe numeric vs. conceptual thresholds

**Module 10** – Creating Correlation Searches

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

**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 12** – Managing Threat Intelligence

- Understand and configure threat intelligence
- Use the Threat Intelligence Management interface
- Configure new threat lists

## Module 13 – Supplemental Apps

- Review apps to enhance the capabilities of ES including, Mission Control, SOAR, UBA, Cloud-based Streaming Analytics, PCI Compliance, Fraud Analytics, and Lookup File Editor

## Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
12 Jun 2025	Virtual Classroom	CEDT	German	Instructor Led Online		€1,500.00
03 Dec 2025	Virtual Classroom	CET	German	Instructor Led Online		€1,500.00
23 Apr 2025	Virtual Classroom	BST	English	Instructor Led Online		€1,500.00
07 May 2025	Virtual Classroom	BST	English	Instructor Led Online		€1,500.00
28 May 2025	Virtual Classroom	BST	English	Instructor Led Online		€1,500.00
18 Jun 2025	Virtual Classroom	BST	English	Instructor Led Online		€1,500.00
25 Jun 2025	Virtual Classroom	BST	English	Instructor Led Online		€1,500.00

## Zusätzliche Information

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