

## Administering Splunk Enterprise Security (ASES)

ID ASES Preis auf Anfrage Dauer 3 Tage

### Zielgruppe

Dieses 13,5-stündige Modul bereitet Architekten und Systemadministratoren auf die Installation und Konfiguration von Splunk Enterprise Security (ES) vor.

### Empfohlenes Training für die Zertifizierung zum

Splunk Enterprise Security Certified Admin (SESCA)

### Voraussetzungen

Um erfolgreich zu sein, sollten die Studierenden ein solides Verständnis des folgenden Moduls haben:

- Splunk Grundlagen 1 und 2 (nicht mehr verfügbar)

Oder die folgenden Ein-Fach-Module:

- [Intro to Splunk \(ITS\)](#)
- [Using Fields \(SUF\)](#)
- [Scheduling Reports & Alerts \(SRA\)](#)
- [Visualizations \(SVZ\)](#)
- [Leveraging Lookups and Subsearches \(LLS\)](#)
- [Search Under the Hood \(SUH\)](#)
- [Intro to Knowledge Objects \(IKO\)](#)
- [Creating Knowledge Objects \(CKO\)](#)
- [Creating Field Extractions \(CFE\)](#)
- [Enriching Data with Lookups \(EDL\)](#)
- [Data Models \(SDM\)](#)
- [Introduction to Dashboards \(ITD\)](#)
- [Dynamic Dashboards \(SDD\)](#)

Die Studierenden sollten ausserdem die folgenden Kurse abgeschlossen haben:

- [Splunk Enterprise System Administration \(SESA\)](#)
- [Splunk Enterprise Data Administration \(SEDA\)](#)

### Kursziele

- Untersuchen Sie die Funktionsweise von ES, einschliesslich Datenmodellen, Korrelationssuchen,

bemerkenswerten Ereignissen und Dashboards.

- Überprüfung der risikobasierten Alarmierung
- Anpassen der Investigation Workbench
- Erfahren Sie, wie Sie ES installieren oder aktualisieren können
- Feinabstimmung der globalen ES-Einstellungen
- Lernen Sie die Schritte zum Einrichten von Eingaben mithilfe von Technologie-Add-ons kennen
- Benutzerdefinierte Korrelationssuche erstellen
- Anpassen von Assets und Identitäten
- Konfigurieren von Bedrohungsdaten

### Kursinhalt

Es behandelt die Verarbeitung und Normalisierung von ES-Ereignissen, Bereitstellungsanforderungen, Technologie-Add-ons, Dashboard-Abhängigkeiten, Datenmodelle, Risikomanagement und die Anpassung von Bedrohungsdaten.

# Administering Splunk Enterprise Security (ASES)

---

## Weltweite Trainingscenter



## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3  
CH-8304 Wallisellen  
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>