

# Administering Splunk Enterprise Security (ASES)

ID ASES Prix CHF 1 650,- (Hors Taxe) Durée 2 jours

## A qui s'adresse cette formation

- SOC Analyst
- SOC Engineer

## Cette formation prépare à la/aux certifications

Splunk Enterprise Security Certified Admin (SESCA)  
Splunk Certified Cybersecurity Defense Engineer (SCCDE)  
Splunk Certified Cybersecurity Defense Architect (SCDARQ)

## Pré-requis

To be successful, students must have completed the following Splunk Education course:

- [Using Splunk Enterprise Security \(USES\)](#)

Students should also be familiar with the topics covered in the following courses:

- Intro to Splunk
- [Using Fields \(SUF\)](#)
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- [Creating Knowledge Objects \(CKO\)](#)
- [Creating Field Extractions \(CFE\)](#)
- [Enriching Data with Lookups \(EDL\)](#)
- [Data Models \(SDM\)](#)
- [Introduction to Dashboards \(ITD\)](#)
- [Splunk Enterprise System Administration \(SESA\)](#) AND [Splunk Enterprise Data Administration \(SEDA\)](#) OR [Splunk Cloud Administration \(SCA\)](#)

## Contenu

### Module 1 - Introduction to Enterprise Security

- Explain the function of a SIEM
- Give an overview of Splunk's Enterprise Security (ES)
- Describe detections and findings
- Configure ES roles and permissions
- Give an overview of ES navigation

### Module 2 - Customizing the Analyst Queue and findings

- Give an overview of the Analyst Queue
- Create and use Analyst Queue Views
- Customize the Analyst Queue
- Modify Urgency
- Create new Status values
- Add fields to Finding attributes
- Create ad hoc Findings
- Suppress Findings

### Module 3 - Working with Investigations

- Give an overview of an investigation
- Use and create Response Plans
- Add Splunk events to an investigation
- Use Playbooks and Actions

### Module 4 - 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 5 - Data Normalization

- Understand how ES uses accelerated data models
- Verify data is correctly configured for use in ES
- Validate normalization configurations
- Install additional add-ons
- Ingest custom data in ES
- Create an add-on for a custom sourcetype
- Describe add-on troubleshooting

### Module 6 - Detection Engineering

- Give an overview of how to create Event-based detections
- Review the Detection Editor
- Give an overview of how to create Finding-based detections

### Module 7 - Risk-Based Alerting

# Administering Splunk Enterprise Security (ASES)

---

- Give an overview of Risk-Based Alerting (RBA)
- Explain risk scores and how they can be changed by detections or manually
- Review the Risk analysis dashboard
- Understand Finding-based detections
- Describe annotations
- View risk information in Analyst Queue findings

## Module 8 - Managing Threat Intelligence

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

## Module 9 - Post-Deployment Configuration

- Give an overview of general ES install requirements
- Explain the different add-ons and where they are installed
- Provide ES pre-installation requirements
- Describe the Splunk\_TA\_ForIndexers app and where it is installed
- Set general configuration options
- Configure local and cloud domain information
- Work with the Incident Review KV Store
- Customize navigation
- Configure Key Indicator searches

# Administering Splunk Enterprise Security (ASES)

---

## Centres de formation dans le monde entier



### 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>