Administering Splunk Enterprise Security (ASES)

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

A qui s'adresse cette formation

This 13.5-hour course prepares architects and systems administrators to install and configure Splunk Enterprise Security (ES).

Cette formation prépare à la/aux certifications

Splunk Enterprise Security Certified Admin (SESCA)

Pré-requis

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

- Using Splunk Enterprise Security (USES)
- Intro to Splunk
- Using Fields (SUF)
- Intro to Knowledge Objects
- Creating Knowledge Objects (CKO)
- Creating Field Extractions (CFE)
- Enriching Data with Lookups (EDL)
- Data Models (SDM)
- Splunk Enterprise System Administration (SESA)
- Splunk Enterprise Data Administration (SEDA)

Objectifs

- 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

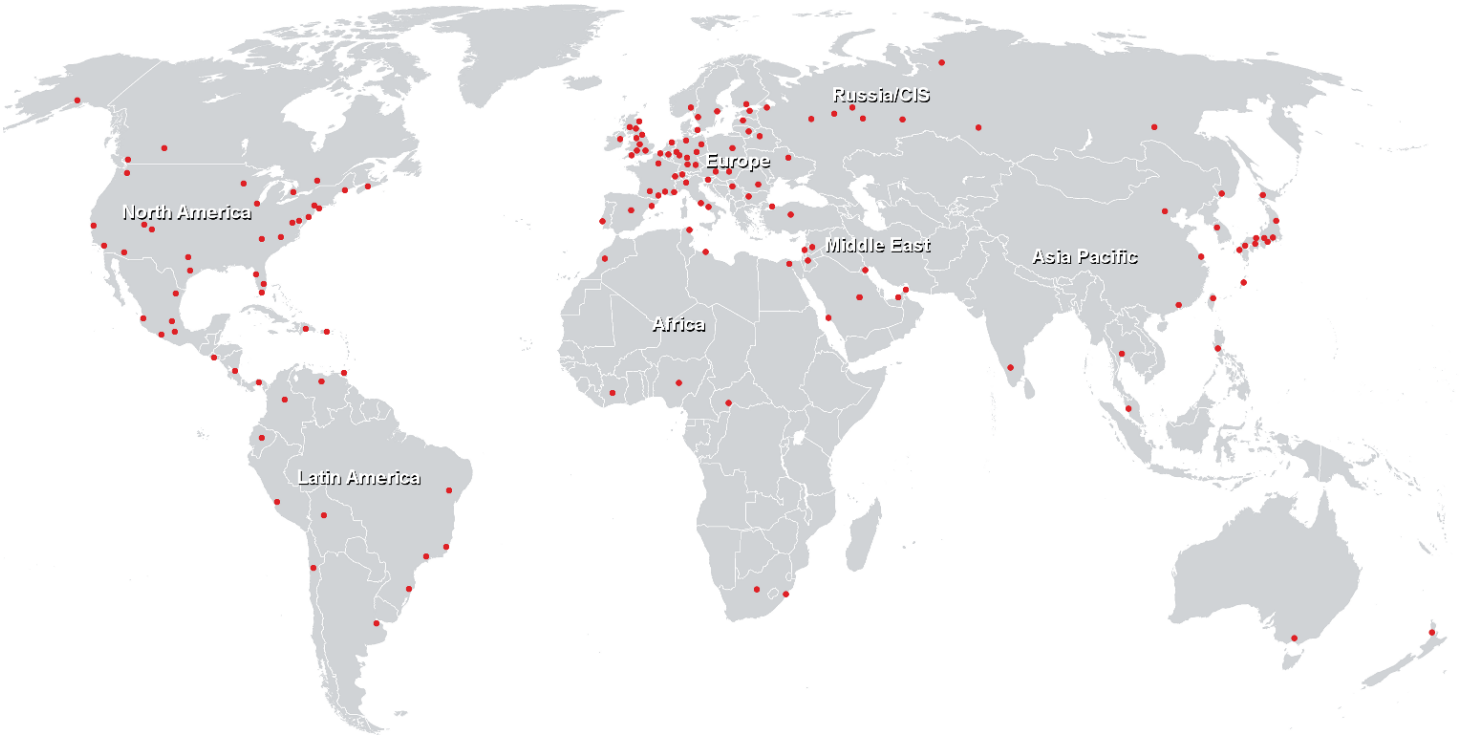
Contenu

The course covers ES event processing and normalization, deployment requirements, technology add-ons, dashboard dependencies, data models, managing risk, and customizing threat intelligence.

Please note that this class may run over three days, with 4.5 hour sessions each day, to achieve the full 13.5 hours of course content.

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