Using Splunk Enterprise Security (USES)

ID USES **Price** CHF 1,650.—(excl. VAT) **Duration** 2 days

This course is part of the following Certifications

Splunk Certified Cybersecurity Defense Analyst (SCCDA)

Prerequisites

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

- What is Splunk? (Retired)
- Intro to Splunk
- Using Fields (SUF)
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- Introduction to Dashboards (ITD)

Course Objectives

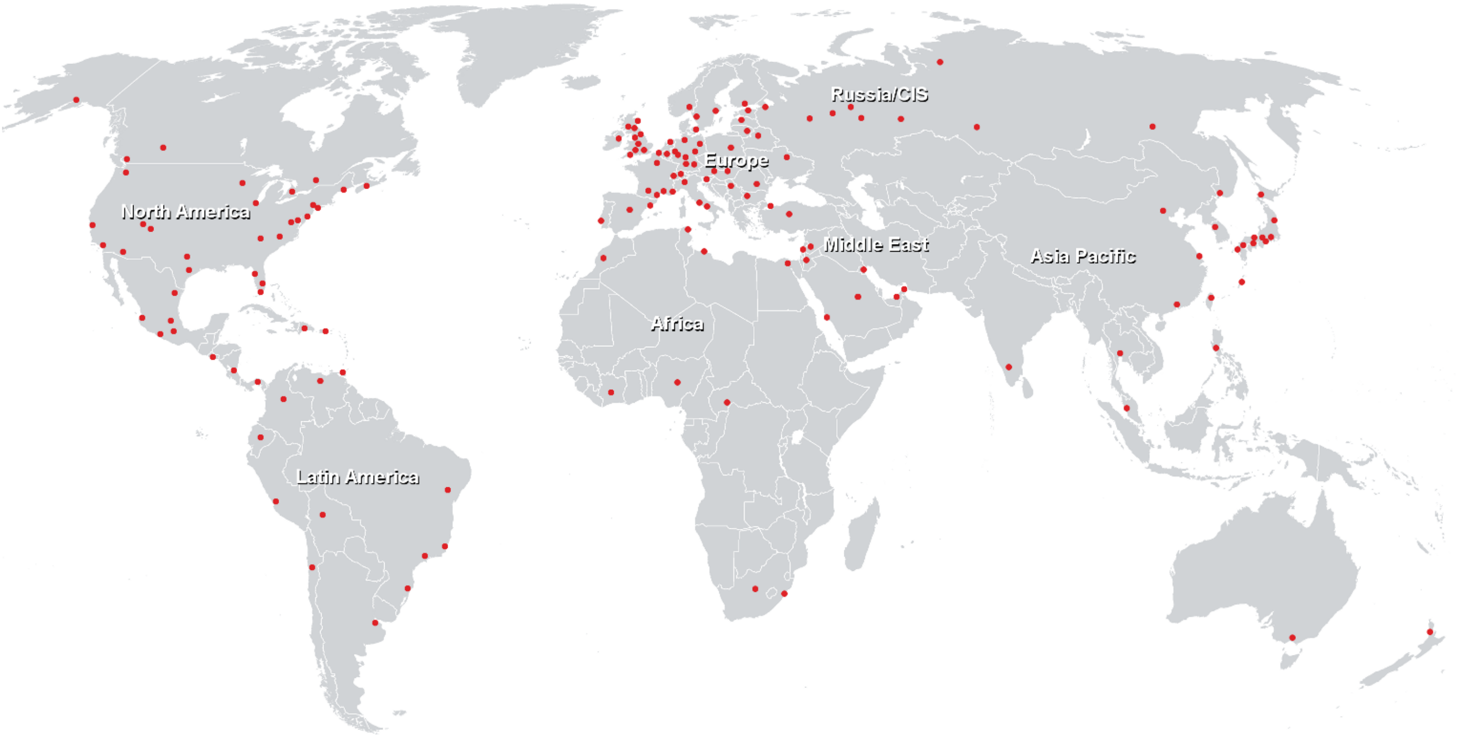
- ES concepts, features, and capabilities
- Security monitoring and Incident investigation
- Use risk-based alerting and risk analysis
- Assets and identities overview
- Creating investigations and using the Investigation Workbench
- Detecting known types of threats
- Monitoring for new types of threats
- Using analytical tools and dashboards
- Analyze user behavior for insider threats
- Use threat intelligence tools
- Use protocol intelligence

Course Content

This 13.5-hour module prepares security practitioners to use Splunk Enterprise Security (ES). Students identify and track incidents, analyze security risks, use predictive analytics, and discover threats.

Please note that this course may run over three days, with 4.5 hour sessions each day.

Training Centres worldwide



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