Using Splunk Enterprise Security (USES)

ID USES **Price** on request **Duration** 3 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 modules:

- Splunk Fundamentals 1 (Retired)
- Splunk Fundamentals 2 (Retired)

Or the following single-subject modules:

- What is Splunk? (Retired)
- 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)
- Enriching Data with Lookups (EDL)
- Data Models (SDM)
- 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

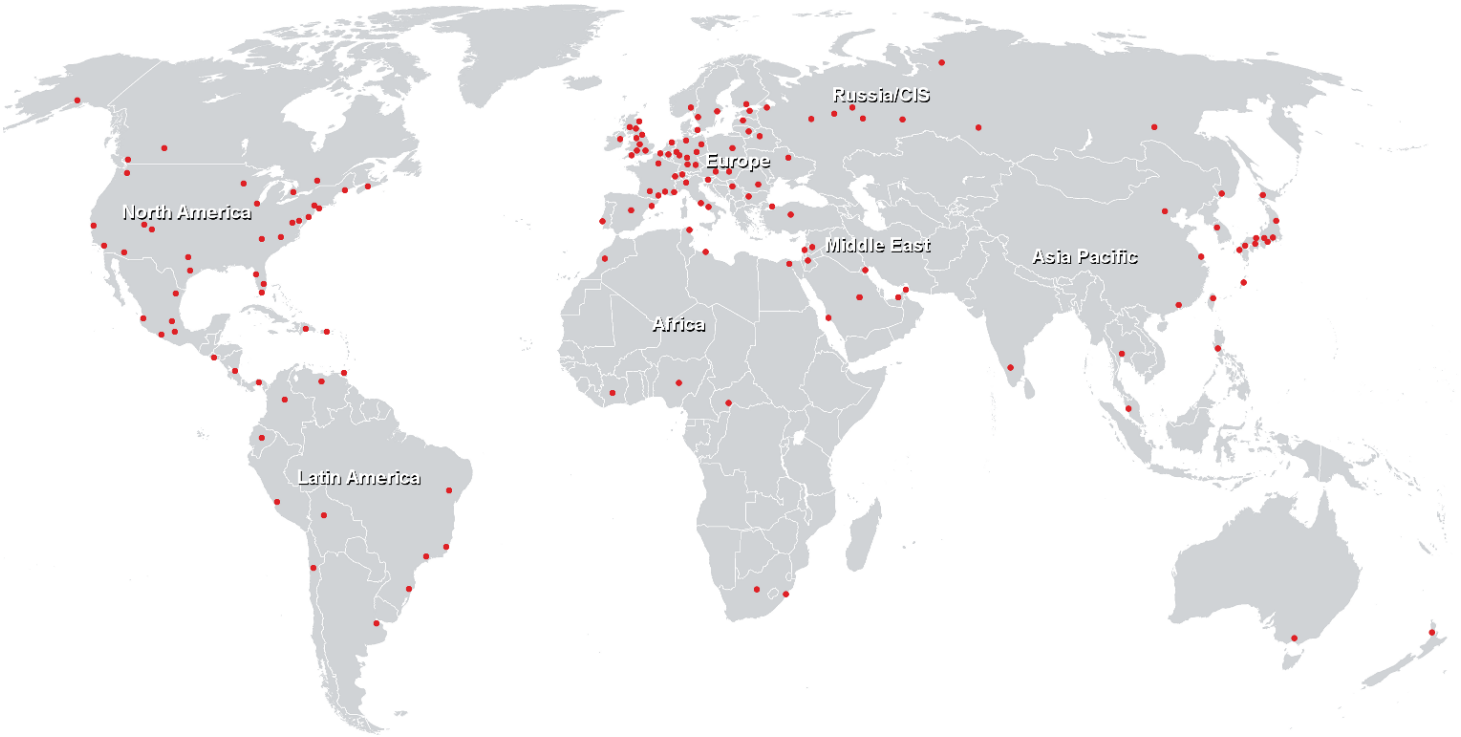
Course Content

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.

Using Splunk Enterprise Security (USES)

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