Using Splunk Enterprise Security (USES)

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

Cette formation prépare à la/aux certifications

Splunk Certified Cybersecurity Defense Analyst (SCCDA)

Pré-requis

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

- Intro to Splunk
- Intro to Splunk (ITS)
- Using Fields (SUF)
- Visualizations (SVZ)
- Search Under the Hood (SUH)
- Intro to Knowledge Objects (IKO)
- Introduction to Dashboards (ITD)

Objectifs

- 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

Contenu

Module 1 - Getting Started with ES

- Describe the features and capabilities of Splunk Enterprise Security (ES)
- Explain how ES helps security practitioners prevent, detect, and respond to threats
- Describe correlation searches, data models and notable events
- Describe user roles in ES
- Log into Splunk Web and access Splunk for Enterprise Security

Module 2 - Security Monitoring and Incident Investigation

- Use the Security Posture dashboard to monitor ES status
- Use the Incident Review dashboard to investigate notable events
- Take ownership of an incident and move it through the investigation workflow
- Create notable events
- Suppress notable events

Module 3 – Risk-Based Alerting

- Give an overview of Risk-Based Alerting
- View Risk Notables and risk information on the Incident Review dashboard
- Explain risk scores and how to change an object's risk score
- Review the Risk Analysis dashboard
- Describe annotations
- Describe the process for retrieving LDAP data for an asset or identity lookup

Module 4 – Assets & Identities

- Give an overview of the ES Assets and Identities framework
- Show examples where asset or identity data is missing from ES dashboards or notable events
- View the Asset & Identity Management Interface
- View the contents of an asset or identity lookup table

Module 5 – Investigations

- Use investigations to manage incident response activity
- Use the investigation workbench to manage, visualize and coordinate incident investigations
- Add various items to investigations (notes, action history, collaborators, events, assets, identities, files and URLs)
- Use investigation timelines, lists and summaries to document and review breach analysis and mitigation efforts

Module 6 – Security Domain Dashboards

- Describe the ES security domains
- Use the Security Domain dashboards to troubleshoot various security threats
- Learn how to launch the Security Domain dashboards from Incidents Review and from a notable event Action menu

Module 7 – User Intelligence

- Understand and use user activity analysis
- Use investigators to analyze events related to an asset or identity
- Use access anomalies to detect suspicious access patterns

Module 8 – Web Intelligence

- Use the web intelligence dashboards to analyze your network environment
- Filter and highlight events

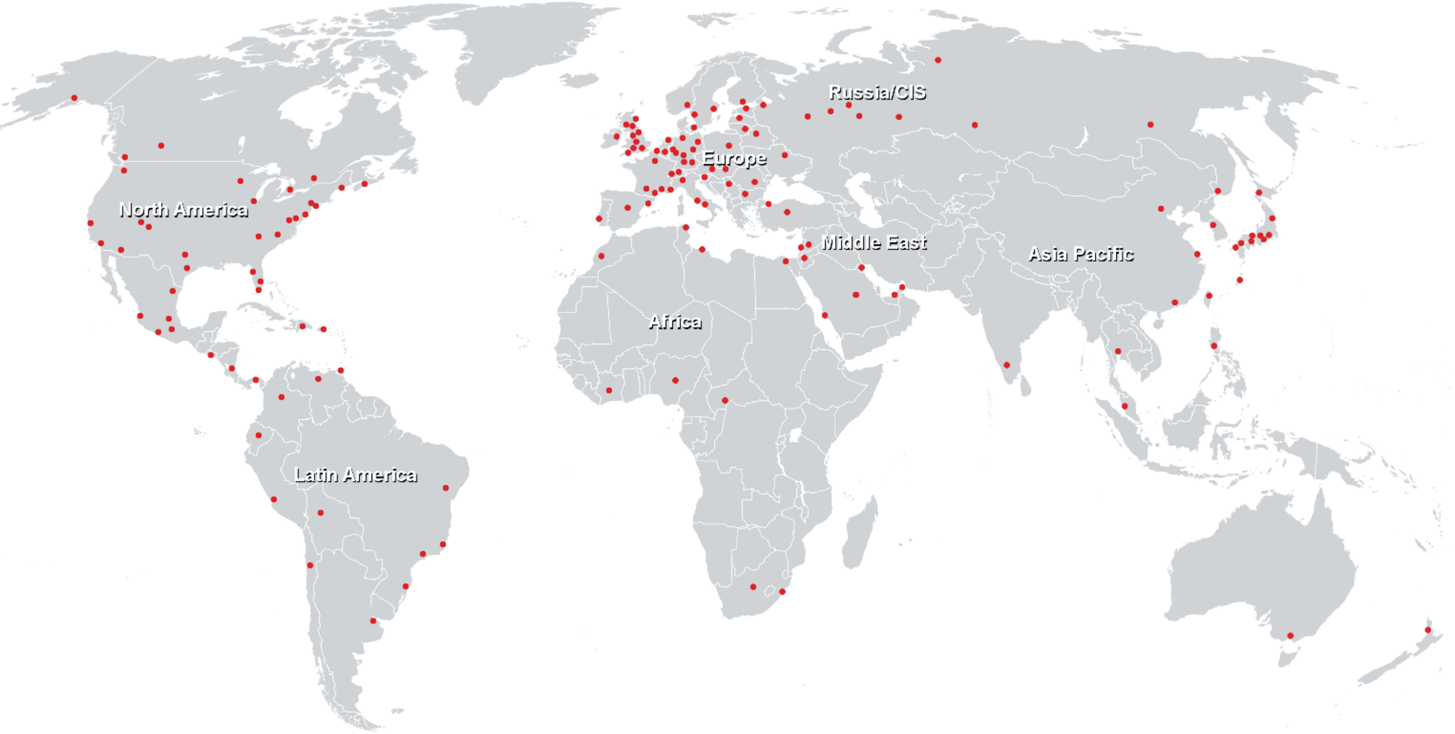
Module 9 – Threat Intelligence

- Give an overview of the Threat Intelligence framework and how threat intel is configured in ES
- Use the Threat Activity dashboard to see which threat sources are interacting with your environment
- Use the Threat Artifacts dashboard to examine the status of threat intelligence information in your environment

Module 10 – Protocol Intelligence

- Explain how network data is input into Splunk events
- Describe stream events
- Give an overview of the Protocol Intelligence dashboards and how they can be used to analyze network data

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