Using Splunk Enterprise Security (USES)

ID USES **Preis** CHF 1'650.– (exkl. MwSt.) **Dauer** 2 Tage

Zielgruppe

SOC Analysts.

Empfohlenes Training für die Zertifizierung zum

Splunk Certified Cybersecurity Defense Analyst (SCCDA)
Splunk Certified Cybersecurity Defense Engineer (SCCDE)

Voraussetzungen

To be successful, students should have a working understanding of the topics covered in the following Splunk courses:

- Intro to Splunk (eLearning)
- Using Fields (SUF)
- Visualizations
- Search Under the Hood
- Intro to Knowledge Objects
- Introduction to Dashboards (ITD)

Kursinhalt

Module 1 - ES Fundamentals

- Explain the function of a SIEM
- Give an overview of Splunk Enterprise Security (ES)
- Understand how ES uses data models
- Describe detections and findings
- Identify ES roles and permissions
- Give an overview of ES navigation

Module 2 - Exploring the Analyst Queue

- Explore the Analyst Queue
- Filtering
- Triage Findings and Finding Groups
- Create ad hoc Findings
- Suppress Findings from the Analyst Queue

Module 3 - Working with Investigations

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

Module 4 - Risk-based Alerting

- Give an overview of risk and Risk-Based Alerting (RBA)
- Explain risk scores and how to change an entity's risk score
- Review the Risk Analysis dashboard
- Describe annotations
- View risk information in Analyst Queue findings

Module 5 - Assets & Identities

- Give an overview of the ES Assets and Identities (A&I) framework
- Show where asset or identity data is missing from ES findings or dashboards
- View the A&I Management Interface
- View the contents of an asset or identity lookup table
- Identify A&I field matching criteria

Module 6 - Adaptive Responses

- Describe Adaptive Responses
- Identify the default ES Adaptive Responses
- Discuss Adaptive Response invocation methods
- Troubleshoot Adaptive Response issues

Module 7 - Security Domain Dashboards

- Use ES to inspect events containing information relevant to active or past incident investigation
- Identify ES Security Domains
- Use the Security Domain dashboards
- Launch Security Domain dashboards from the Analyst Queue and from field action menus in search results

Module 8 - Intelligence Dashboards

- Use the Web Intelligence dashboards to analyze your network environment
- Filter and highlight events
- Understand and use User Intelligence dashboards
- Use Investigators to analyze events related to an asset or identity
- Use Access Anomalies to detect suspicious access patterns

Using Splunk Enterprise Security (USES)

Module 9 - Threat Intelligence

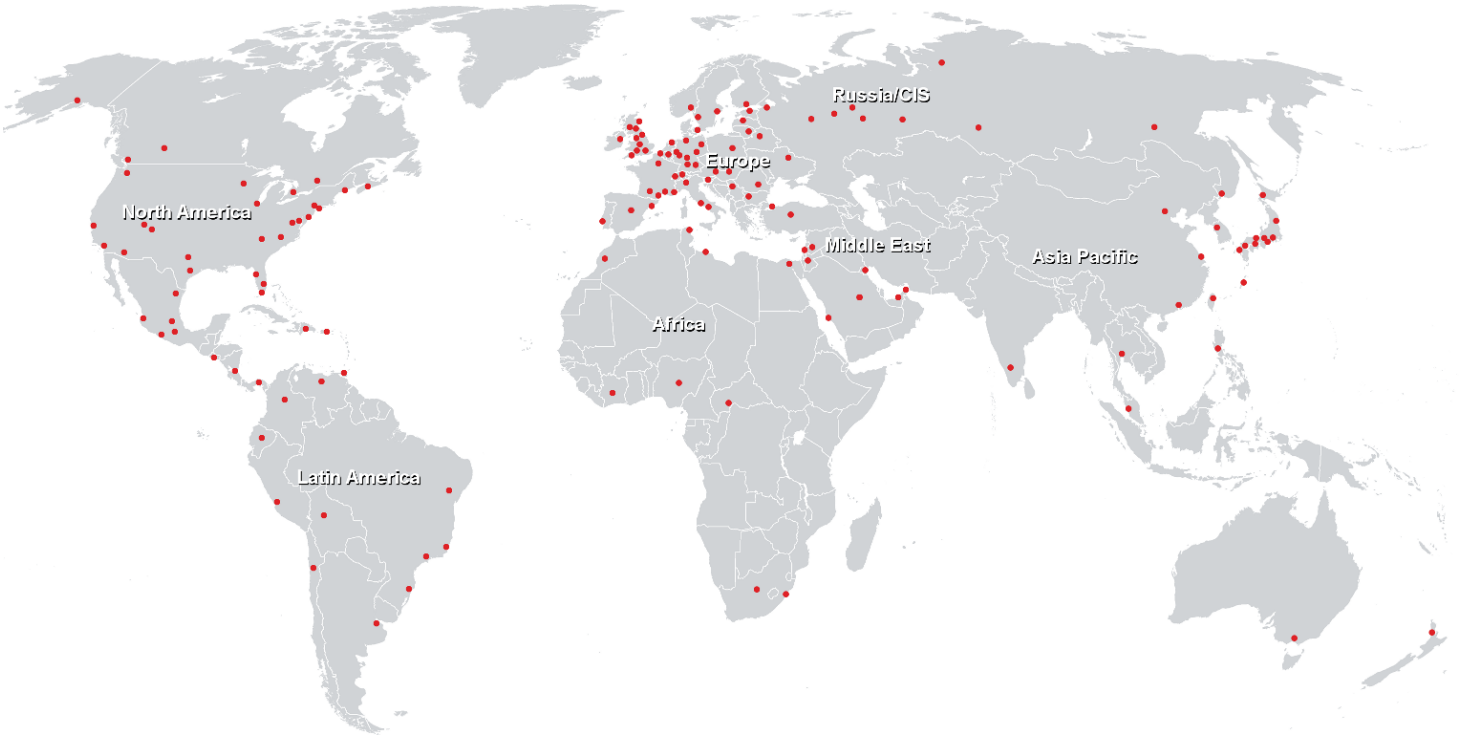
- Give an overview of the Threat Intelligence framework
- Identify where Threat Intelligence is configured
- Observe Threat Findings
- View downloaded Threat Indicators
- Troubleshooting Threat Intelligence

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

Using Splunk Enterprise Security (USES)

Weltweite Trainingscenter





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