Using Splunk Enterprise Security (USES)

ID USES **Preis** auf Anfrage **Dauer** 3 Tage

Empfohlenes Training für die Zertifizierung zum

Splunk Certified Cybersecurity Defense Analyst (SCCDA)

Voraussetzungen

Um erfolgreich zu sein, sollten die Teilnehmer ein solides Verständnis der folgenden Module haben:

- Splunk Grundlagen 1 (nicht mehr verfügbar)
- Splunk Grundlagen 2 (nicht mehr verfügbar)

Oder die folgenden Ein-Fach-Module:

- 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)

Kursziele

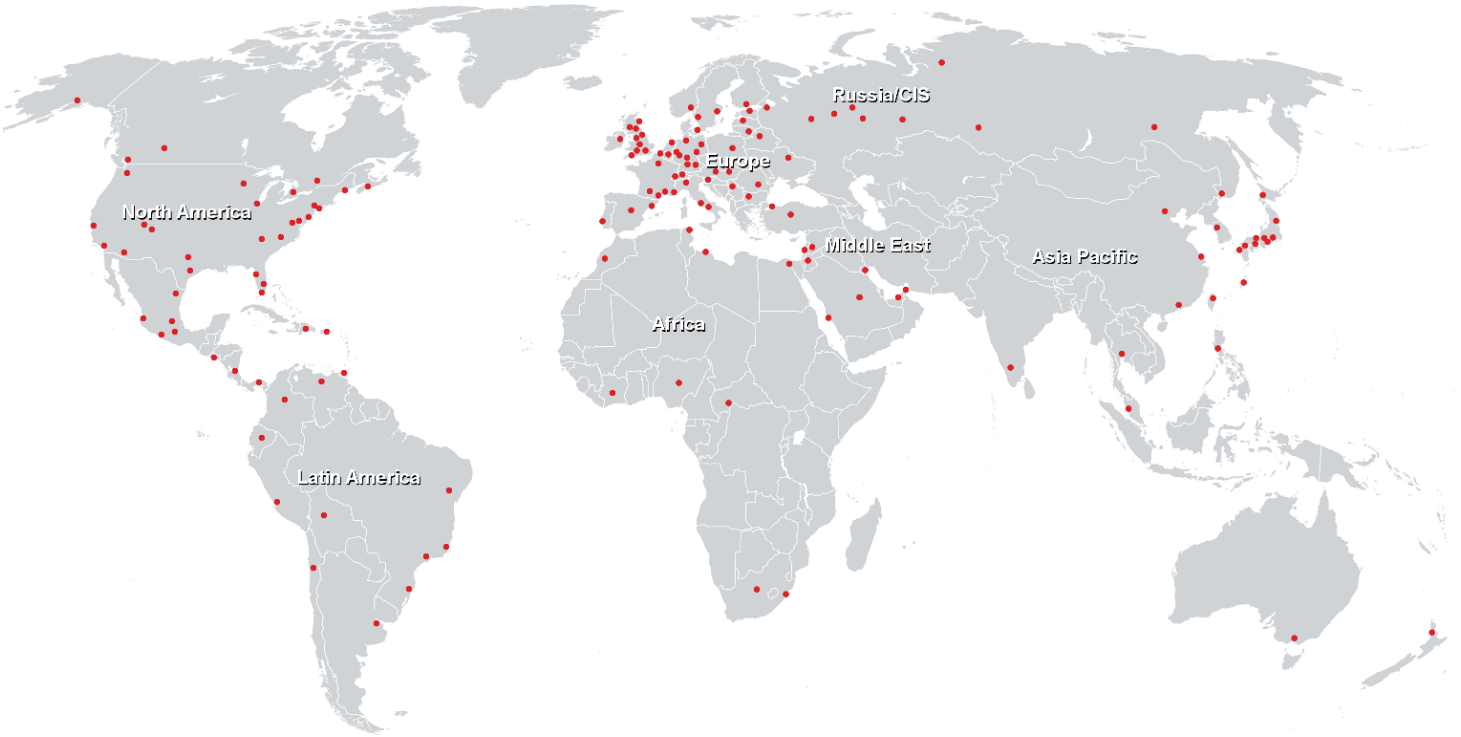
- ES-Konzepte, -Merkmale und -Fähigkeiten
- Vermögenswerte und Identitäten
- Sicherheitsüberwachung und Untersuchung von Vorfällen
- Risikobasierte Warnmeldungen und Risikoanalysen verwenden
- Verwendung von Untersuchungsworkbench, Zeitleisten, Listen und Zusammenfassungswerkzeugen
- Erkennung bekannter Arten von Bedrohungen
- Überwachung neuer Arten von Bedrohungen
- Verwendung von Analyseinstrumenten
- Analysieren Sie das Benutzerverhalten auf Insider-Bedrohungen
- Tools zur Bedrohungsanalyse verwenden
- Verwendung von Protokollinformationen und Live-Stream-Daten

Kursinhalt

Dieses 13,5-stündige Modul bereitet Sicherheitspraktiker auf die Verwendung von Splunk Enterprise Security (ES) vor. Die Teilnehmer identifizieren und verfolgen Vorfälle, analysieren Sicherheitsrisiken, nutzen prädiktive Analysen und entdecken Bedrohungen.

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