Advanced SOAR Implementation (ASOARI)

ID ASOARI **Preis** auf Anfrage **Dauer** 14 Stunden

Zielgruppe

Erfahrene SOAR-Berater, die für die Entwicklung komplexer SOAR-Lösungen verantwortlich sind.

Empfohlenes Training für die Zertifizierung zum

Splunk SOAR Certified Automation Developer (SOAR)

Voraussetzungen

Die Teilnehmer an diesem Kurs müssen sicherstellen, dass sie alle Kursvoraussetzungen erfüllen. Es handelt sich um einen anspruchsvollen Kurs für Fortgeschrittene, der technisches Wissen aus vielen Bereichen von Splunk und SOAR voraussetzt, und die anspruchsvollen Übungen und der Kursplan lassen wenig Zeit, um die Grundlagen zu erlernen.

Um erfolgreich zu sein, sollten die Studierenden über ein solides Verständnis der folgenden Punkte verfügen:

- Erfahrung mit Python-Programmierung
- Verwalten von Splunk SOAR
- Entwicklung von Splunk SOAR Playbooks
- Splunk-Datenverwaltung für Unternehmen
- Splunk-Systemverwaltung für Unternehmen
- Splunk Enterprise Security entweder verwenden oder administrieren

Kursziele

- Externe Splunk-Suche in SOAR verwenden
- Senden von Ereignissen von Splunk zu SOAR
- Aktualisieren von Splunk-Ereignissen aus SOAR
- SOAR-Berichte auf Splunk ausführen
- Ausführen von SOAR-Playbooks aus Splunk
- Splunk von SOAR-Playbooks aus durchsuchen
- Schreiben von benutzerdefiniertem Code zur Verwendung in SOAR Playbooks
- Verwendung der SOAR REST API in SOAR Playbooks

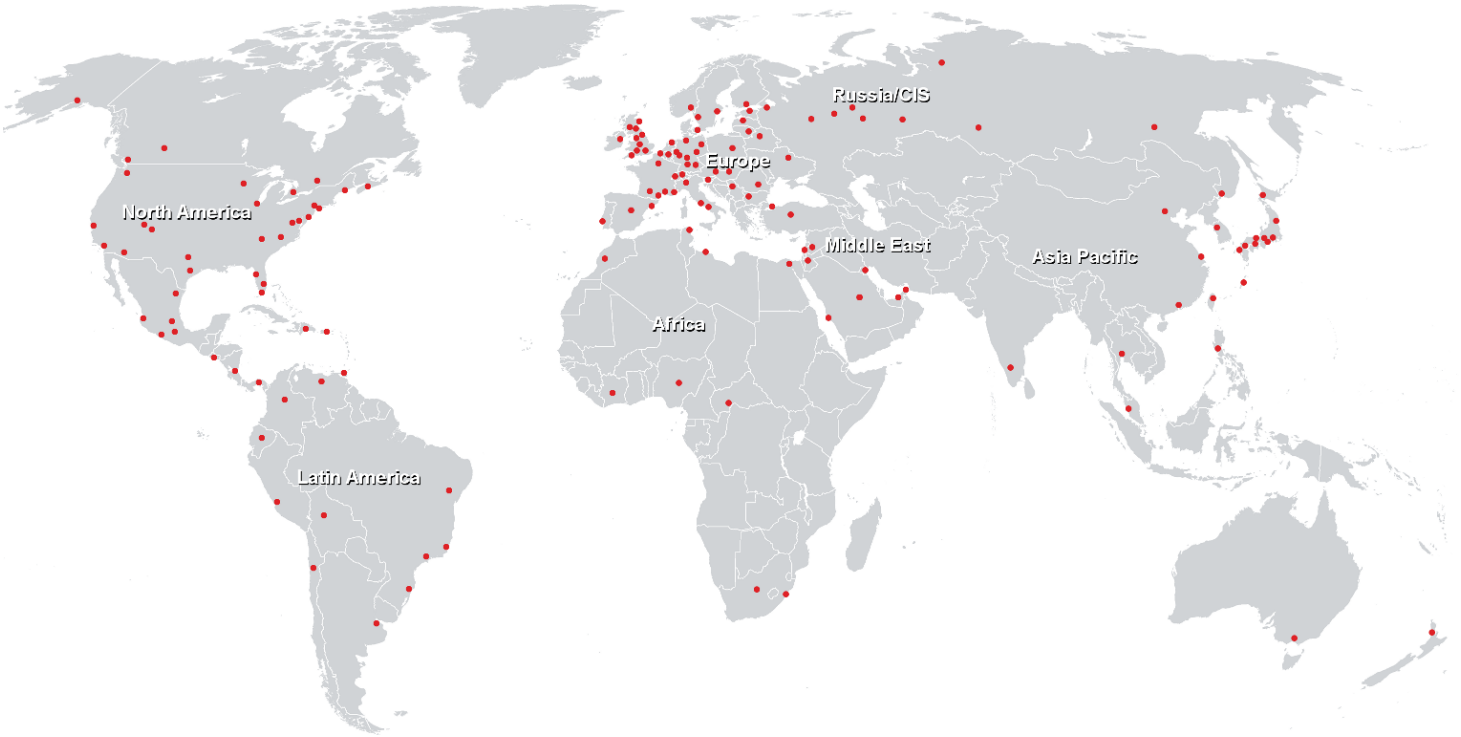
Kursinhalt

Dieser 13,5-stündige Kurs richtet sich an erfahrene SOAR-Berater, die für die Entwicklung komplexer SOAR-Lösungen verantwortlich sind. Er bereitet die Teilnehmer auf die Integration von SOAR mit Splunk sowie auf die Entwicklung von Playbooks vor, die benutzerdefinierte Kodierung und die Verwendung von REST APIs erfordern.

Potenzielle Teilnehmer haben alle vorausgesetzten Kurse bestanden und müssen sicherstellen, dass sie dem Kurs ihre ganze Aufmerksamkeit widmen können, da die Kursarbeit sehr anspruchsvoll ist. Die Teilnehmer entwickeln eine kundenspezifische Lösung mit SOAR, Splunk und kundenspezifischem Python-Code. In den Übungen werden die Anforderungen für die Lösung vorgegeben; die Studenten müssen die Entwicklung planen und durchführen. Dies erfordert überlegtes Handeln, Experimentieren und Problemlösungsfähigkeiten.

Advanced SOAR Implementation (ASOARI)

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