Cortex XDR: Investigation and Analysis (PCXDR-IA)

ID PCXDR-IA **Preis** auf Anfrage **Dauer** 2 Tage

Zielgruppe

Dieser Kurs richtet sich an ein breites Spektrum von Sicherheitsexperten, darunter SOC-, CERT-, CSIRT- und XDR-Analysten, Manager, Incident Responder und Threat Hunters. Er eignet sich auch gut für Berater, Vertriebsingenieure und Servicepartner, die professionelle Dienstleistungen anbieten.

Voraussetzungen

Die Teilnehmer sollten über ein grundlegendes Verständnis der Cybersicherheitsprinzipien verfügen und Erfahrung mit der Analyse von Vorfällen und der Verwendung von Sicherheitstools für die Untersuchung haben.

Kursziele

Dieser Kurs soll Sie dazu befähigen:

- Untersuchen Sie die Fälle, analysieren Sie die wichtigsten Assets und Artefakte und interpretieren Sie die Kausalkette.
- Abfrage und Analyse von Protokollen mit XQL, um aussagekräftige Erkenntnisse zu gewinnen.
- Nutzen Sie fortschrittliche Tools und Ressourcen für eine umfassende Fallanalyse.

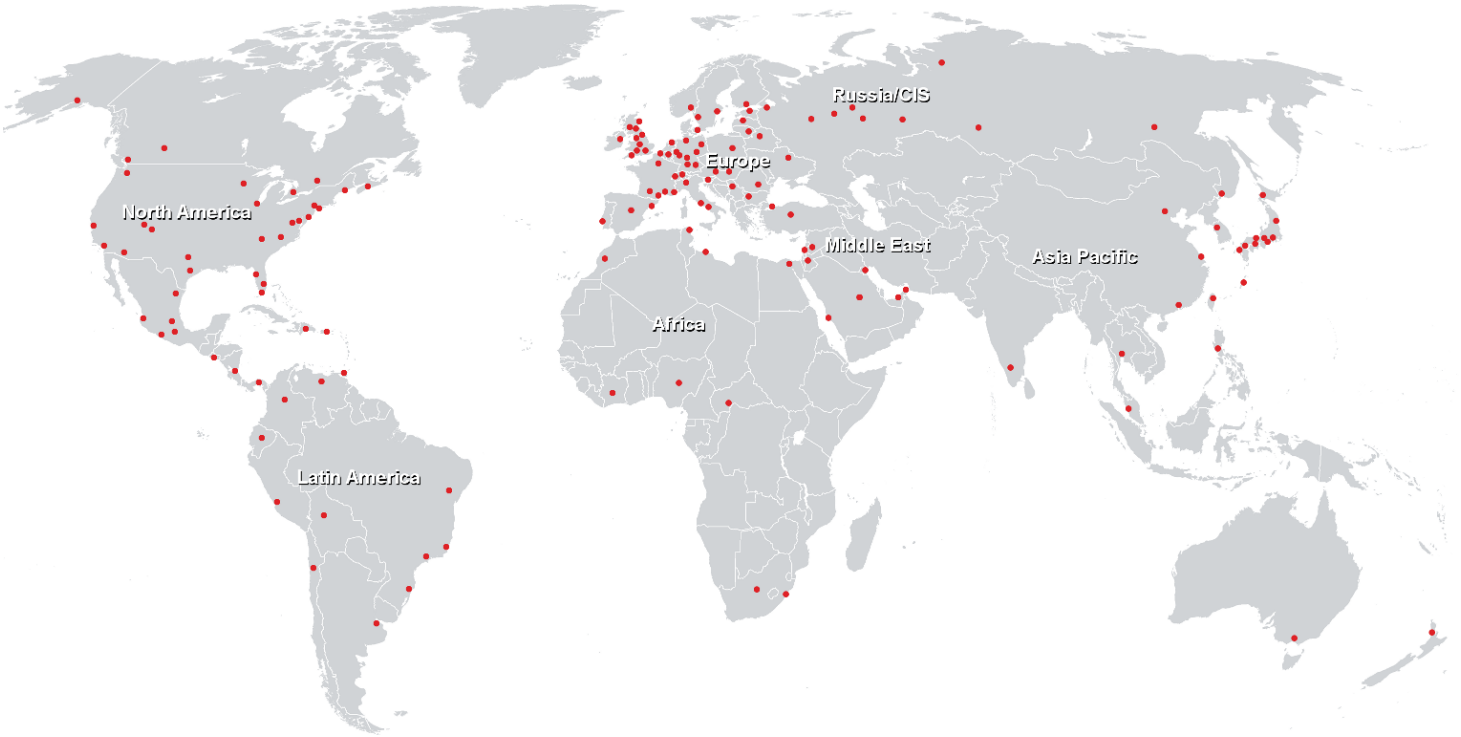
Kursinhalt

Kurs-Module

- 1 - Einführung in Cortex XDR
- 2 - Endpunkte
- 3 - XQL
- 4 - Alarmierung und Erkennung
- 5 - Anfälligkeit und Forensik
- 6 - Plattform-Automatisierung
- 7 - Case Management
- 8 - Dashboards und Berichte

Cortex XDR: Investigation and Analysis (PCXDR-IA)

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