Cortex XDR: Investigation and Response (EDU-262)

ID EDU-262 **Preis** CHF 1'980.– (exkl. MwSt.) **Dauer** 2 Tage

Zielgruppe

Cybersecurity-Analysten und -Ingenieure sowie Spezialisten für Sicherheitsoperationen

Empfohlenes Training für die Zertifizierung zum

Palo Alto Networks XDR Engineer (PXDRE)

Voraussetzungen

Die Teilnehmer müssen den Kurs Cortex XDR: Prevention and Deployment (EDU-260) besucht haben.

Kursziele

Nach erfolgreichem Abschluss dieses Kurses, der von einem Ausbilder geleitet wird und praktische Übungen beinhaltet, sollten die Teilnehmer in der Lage sein:

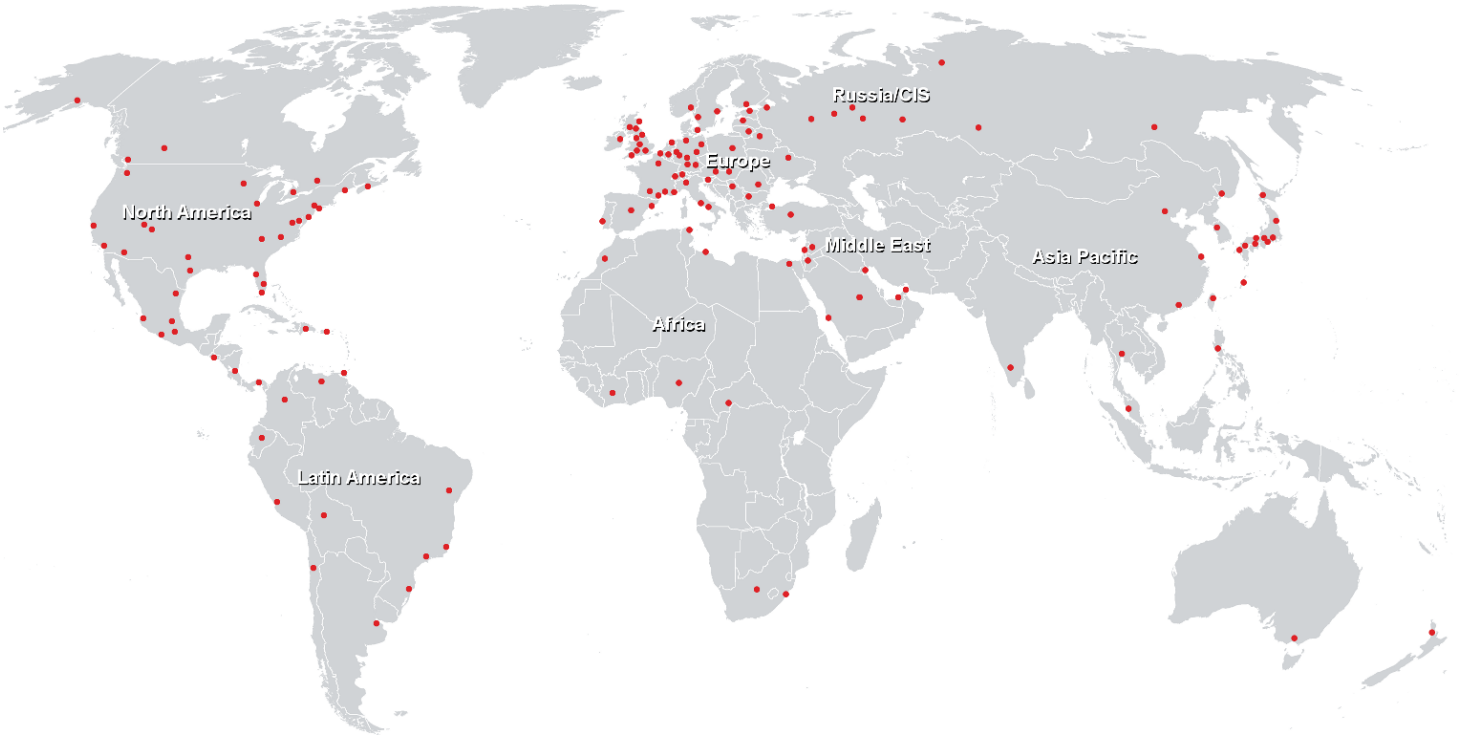
- Untersuchung und Verwaltung von Vorfällen
- Beschreiben Sie die Cortex XDR-Kausalitäts- und Analysekonzepte
- Analysieren Sie Alarme mit Hilfe der Kausalitäts- und Zeitachsenansicht
- Arbeit mit Cortex XDR Pro-Aktionen wie z. B. Remote-Skriptausführung
- Erstellen und Verwalten von On-Demand- und geplanten Suchanfragen im Query Center
- Erstellen und Verwalten der Cortex-XDR-Regeln BIOC und IOC
- Arbeiten mit Cortex XDR-Assets und -Beständen
- Schreiben von XQL-Abfragen zum Durchsuchen von Datensätzen und Visualisieren der Ergebnismengen
- Arbeit mit der externen Datensammlung des Cortex XDR

Kursinhalt

Kursmodule:

- 1 - Cortex XDR-Vorfälle
- 2 - Kausalität und Analysekonzepte
- 3 - Kausalitätsanalyse von Ausschreibungen
- 4 - Erweiterte Antwortaktionen
- 5 - Aufbau von Suchanfragen
- 6 - XDR-Regeln erstellen
- 7 - Cortex XDR-Vermögenswerte
- 8 - Einführung in XQL
- 9 - Externe Datenerhebung

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