Cortex XDR: Investigation and Response (EDU-262)

ID EDU-262 **Preis** auf Anfrage **Dauer** 2 Tage

Zielgruppe

Cybersecurity-Analysten und -Ingenieure sowie Spezialisten für Sicherheitsoperationen

Voraussetzungen

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

Kursziele

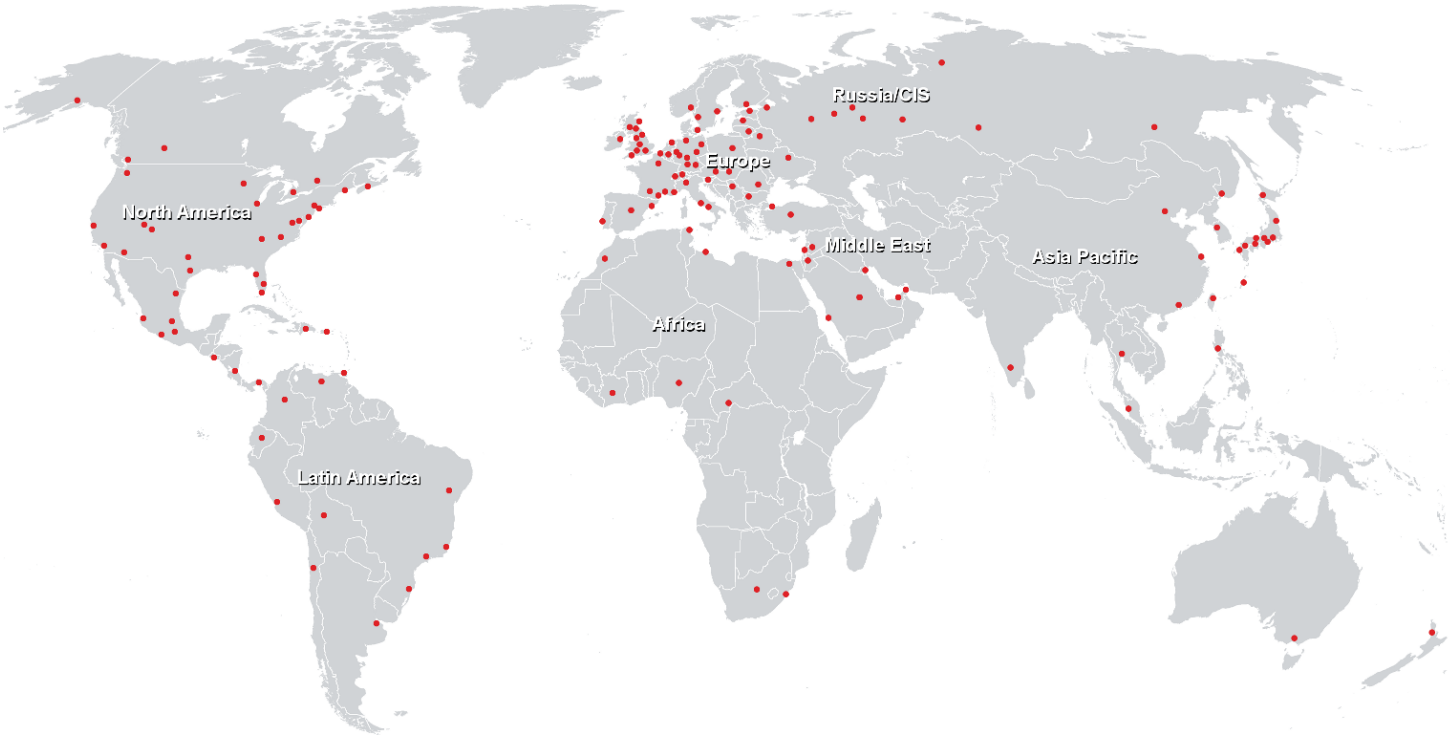
Nach erfolgreichem Abschluss dieses Kurses, der von einem Ausbilder geleitet wird und praktische Übungen beinhaltet, sollten die Teilnehmer in der Lage sein:

- Untersuchen Sie Angriffe auf der Seite mit den Vorfällen und bewerten, ordnen und schliessen Sie sie
- Untersuchen Sie Artefakte mit Hilfe der spezialisierten Ansichten wie IP View und Hash View
- Arbeit mit Cortex XDR Pro-Aktionen: die Remote-Skriptausführung und der EDL-Dienst
- Beschreiben Sie die Cortex XDR-Kausalitäts- und Analysekonzepte
- Analysieren Sie Alarme mit Hilfe der Kausalitäts- und Zeitachsenansicht
- Erstellen und Verwalten von On-Demand- und geplanten Suchanfragen im Query Center
- Erstellen und Verwalten der Cortex-XDR-Regeln BIOC und IOC
- Arbeit mit der Unterstützung der externen Dateneingabe des Cortex XDR
- Schreiben von XQL-Abfragen zum Durchsuchen von Datensätzen und Visualisieren der Ergebnismengen
- Einfache Korrelationsregeln und Parsing-Regeln mit XQL erstellen

Kursinhalt

- Cortex XDR-Vorfälle
- 2. Untersuchung Ansichten
- 3. Erweiterte Antwortaktionen
- 4. Kausalität und Analysekonzepte
- 5. Kausalitätsanalyse von Ausschreibungen
- 6. Erstellen von grundlegenden Suchanfragen
- 7. Erstellung grundlegender XDR-Regeln
- 8. Externe Datenerhebung
- 9. Einführung in XQL
- 10. Korrelations- und Parsingregeln

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer GmbH

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch