Configure SIEM security operations using Microsoft Sentinel (SC-5001)

ID SC-5001 **Preis** auf Anfrage **Dauer** 1 Tag

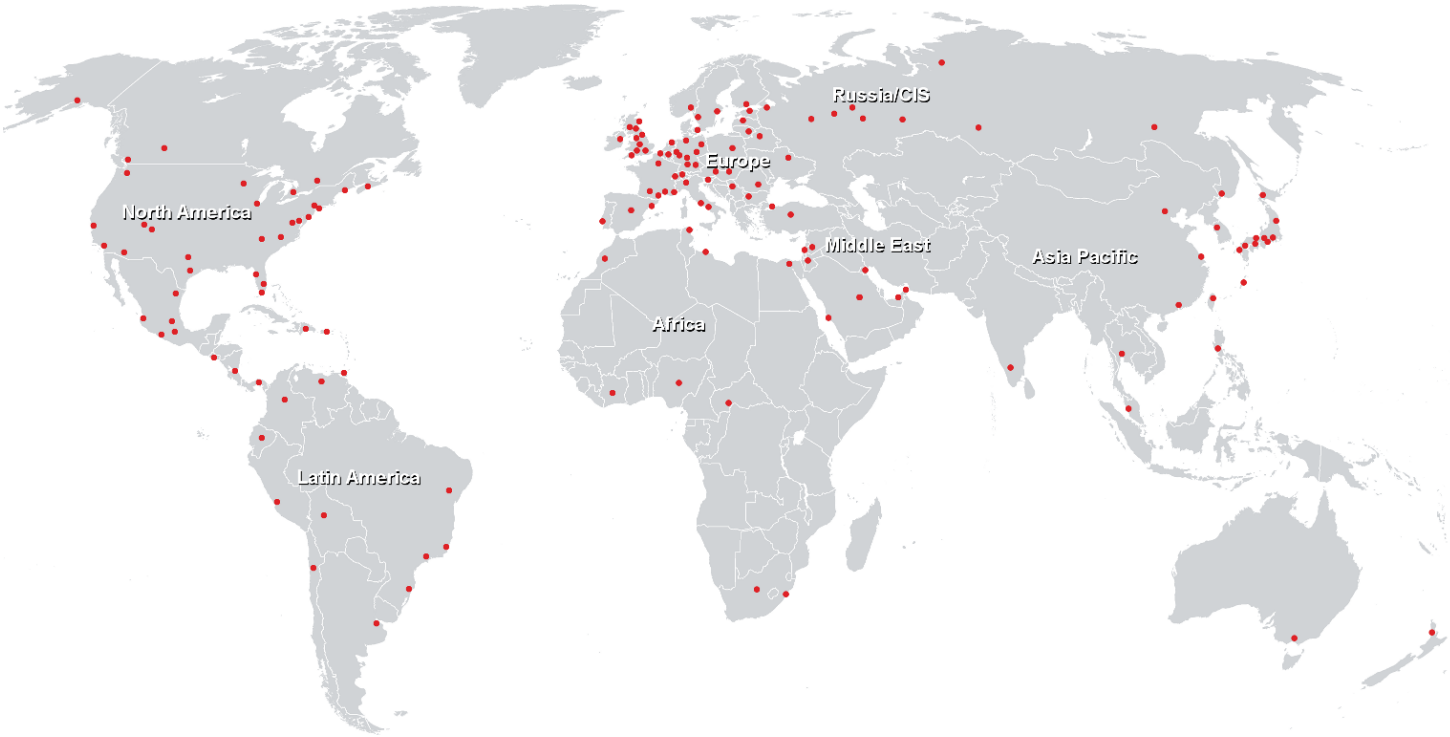
Voraussetzungen

- Grundlegendes Verständnis von Microsoft Azure
- Grundlegende Microsoft Sentinel-Kenntnisse
- Erfahrung mit der Kusto-Abfragesprache (KQL) in Microsoft Sentinel

Kursinhalt

- Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen
- Herstellen einer Verbindung von Microsoft-Diensten mit Microsoft Sentinel
- Verbinden von Windows-Hosts mit Microsoft Sentinel
- Bedrohungserkennung mit Microsoft Sentinel-Analysen
- Automatisierung in Microsoft Sentinel
- Konfigurieren von SIEM-Sicherheitsvorgängen mit Microsoft Sentinel

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