Master Class: Microsoft Defender and Microsoft Sentinel for Hybrid Cloud (HYBSEC)

ID HYBSEC **Preis** CHF 4'780.– (exkl. MwSt.) **Dauer** 5 Tage

Zielgruppe

Administratoren mit mindestens 5 Jahren Erfahrung in der Verwaltung von Windows Active Directory Domain Services, Azure Active Directory und Azure-Ressourcen.

Kursinhalt

Defender for Cloud

- Überblick über Defender for Cloud
- Voraussetzungen und Einrichtung
- Sichern von Azure Workloads
- Sichern von on-premises Workloads
- Cloud Security Posture Management Überblick
- Automatisch auf Alarme reagieren
- Implementieren von Azure Policy guest configuration

Defender for Identity

- Überblick über MS Defender for Identity
- Planen MS Defender for Identity Deployment (Architektur, Voraussetungen)
- Einrichten und konfigurieren von Defender for Identity
- Untersuchen von alerts/detections
    - Reconnaissance Alerts
    - Compromised Credential Alerts
    - Lateral Movement Alerts
    - und einige mehr

KQL Primer

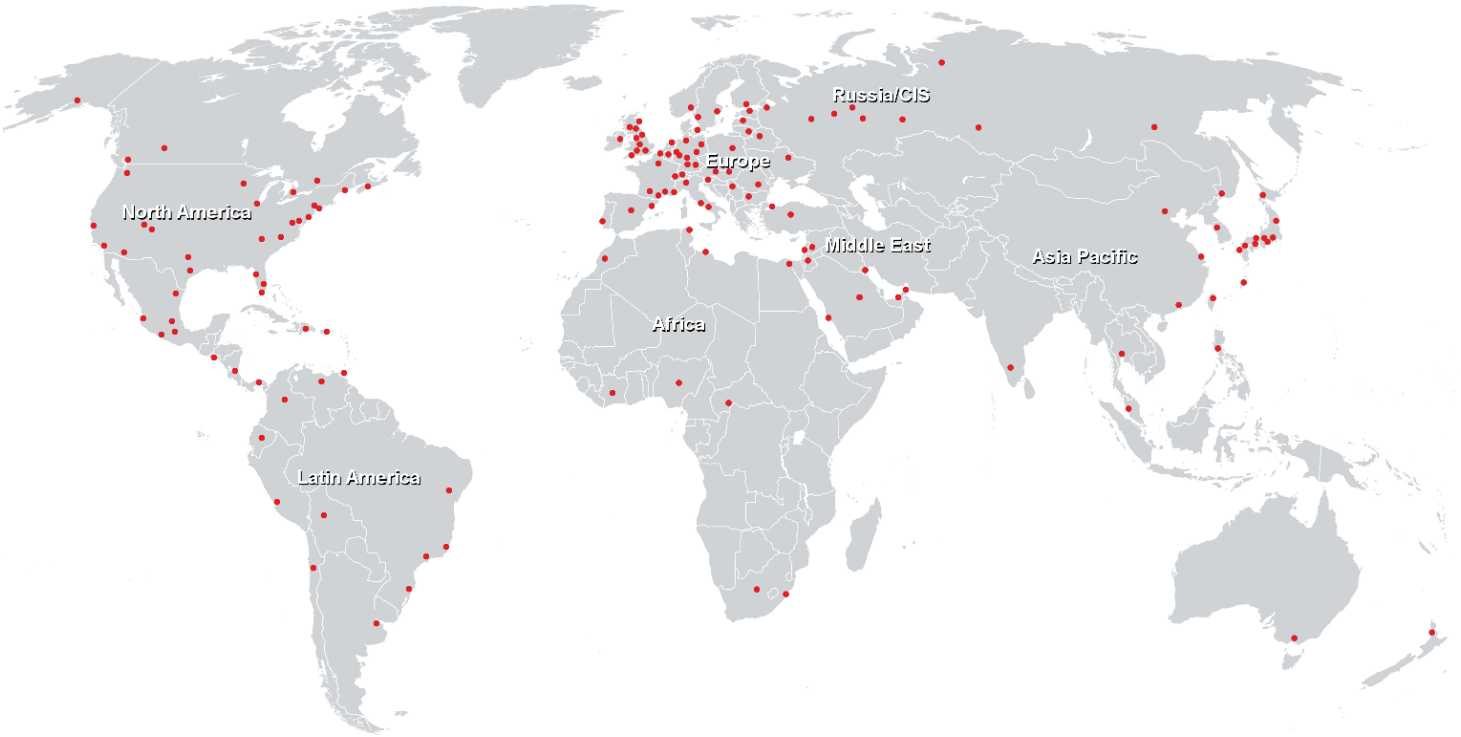
- Basic Operatoren um Tabellen abzufragen und Ausgaben zu formatieren
- Arbeiten mit Variablen
- Erweiterte Operatoren
    - Erweitern von Abfrageergebnissen
    - Abfragen und filtern von Property Bags
    - Aggregation
    - Erstellen von eigenen Funktionen
- Arbeiten mit mehreren Tabellen und externen Daten

Microsoft Sentinel

- Data collectors einrichten
- Erstellen von Analytic rules
- Automatisches Reagieren auf Incidents
- Automatisches erweitern der incident information
- Untersuchen von Incidents
- Threat hunting durchführen
- Workbooks erzeugen
- UEBA Einrichten und verwenden

Master Class: Microsoft Defender and Microsoft Sentinel for Hybrid Cloud (HYBSEC)

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