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

ID HYBSEC **Prix** CHF 4 780,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

Administrators with experience of at least 5 years in administering Windows Active Directory Domain Services, Azure Active Directory and Azure resources.

Contenu

Defender for Cloud

- Overview of Defender for Cloud
- Prerequisites and implementation
- Securing Azure workloads
- Securing on-premises workloads
- Cloud Security Posture Management overview
- Use automation to respond to alerts
- Mastering Azure Policy guest configuration

Defender for Identity

- Overview of MS Defender for Identity
- Planning MS Defender for Identity Deployment (Architecture, Prerequisites)+
- Implement Defender for Identity
- Investigate alerts/detections
    - Reconnaissance Alerts
    - Compromised Credential Alerts
    - Lateral Movement Alerts
    - and some more

KQL Primer

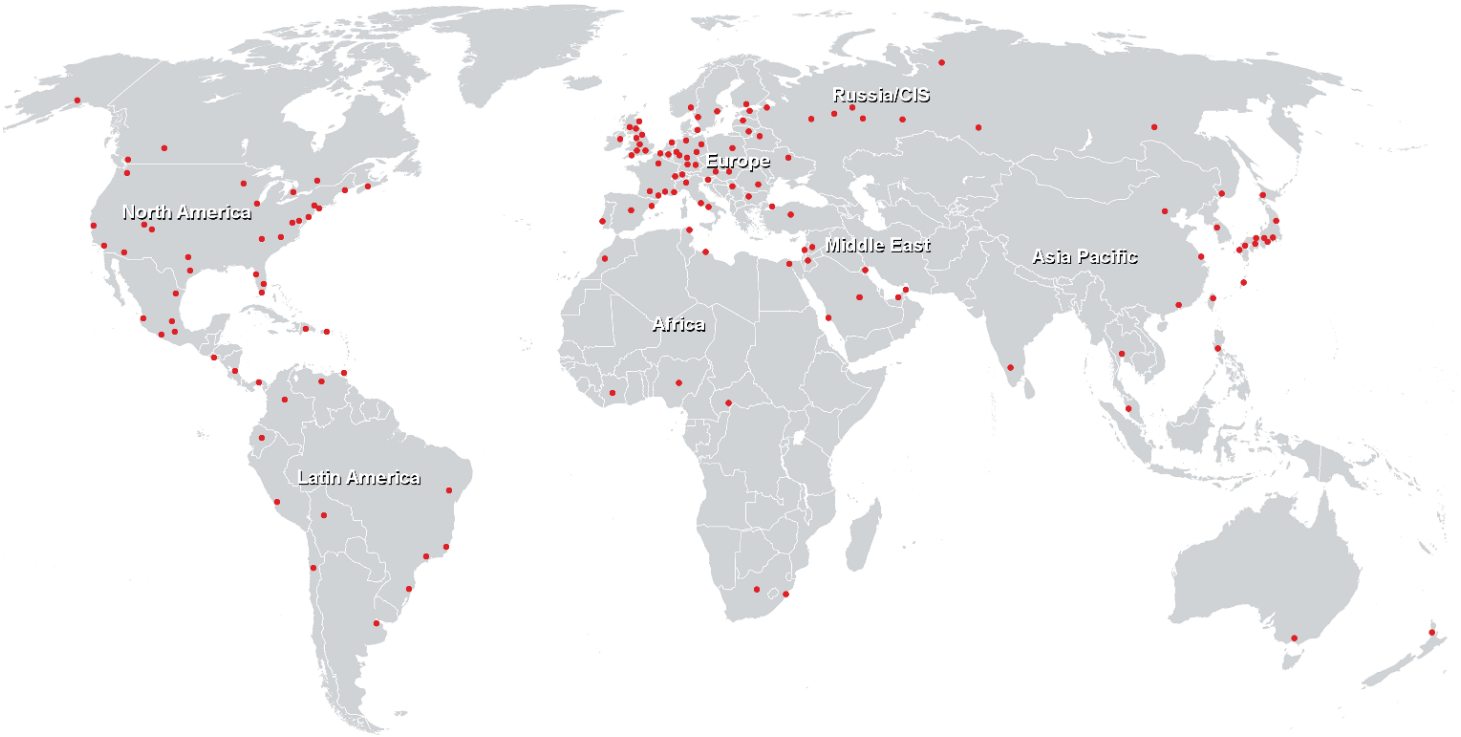
- Basic operators for querying tables and formatting output
- Working with variables
- Advance operators and functions
    - Extending tables
    - Querying and filtering property bags
    - Aggregate records and
    - Create custom functions
- working with multiple tables and external data

Microsoft Sentinel

- Data collectors Implementation
- Creating Analytic rules
- Use automation to respond to Incidents
- Automatically enrich incident information
- Investigate Incidents
- Perform threat hunting
- Create workbooks
- Investigate with UEBA

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

Centres de formation dans le monde entier



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