Master Class: Microsoft Defender for Endpoint (MDE)

ID MDE **Preis** auf Anfrage **Dauer** 4 Tage

Zielgruppe

SecOps-Teammitglieder, Geräteadministratoren und alle interessierten Verantwortlichen.

Kursinhalt

Microsoft Defender XDR

- Überblick über MS Defender XDR
- MDE-Übersicht und Lizenzierung
- MDE vs. Microsoft Intune
- Null Vertrauen und MDE

Microsoft Defender für Endpunkte

- MDE-Architektur
- MDE-Portal
- MDE-Aktivierung
- MDE-Rollen und -Berechtigungen

Onboarding/Offboarding

- Windows-Geräte über lokales Skript, MS Intune und Gruppenrichtlinien
- MacOS-Geräte über lokales Skript und MS Intune
- Linux und Windows Server über Azure Arc
- Behebung von Problemen beim Onboarding
- Offboard-Geräte

Endpunktschutz - Reduzierung der Angriffsfläche

- Dienst-zu-Dienst-Verbindung zu Microsoft Intune
- Regeln zur Reduzierung der Angriffsfläche
- Kontrollierter Ordnerzugriff
- Gerätesteuerung

Endpunktschutz - Schutz der nächsten Generation

- Schutz in der Cloud
- Überwachung von Verhaltensweisen
- Schutz in Echtzeit
- EDR im Blockmodus

Endpunkt-Erkennung und -Reaktion

- Verwaltung von Warnungen und Zwischenfällen
- Automatisierte Untersuchung und Reaktion (AIR)
- Abhilfemassnahmen
- Untersuchung des Geräts
- Antwortaktionen des Geräts

Zusätzliche Konfigurationen

- Erweiterte Funktionen
- Indikatoren
- Filterung von Webinhalten
- Schwachstellen-Management

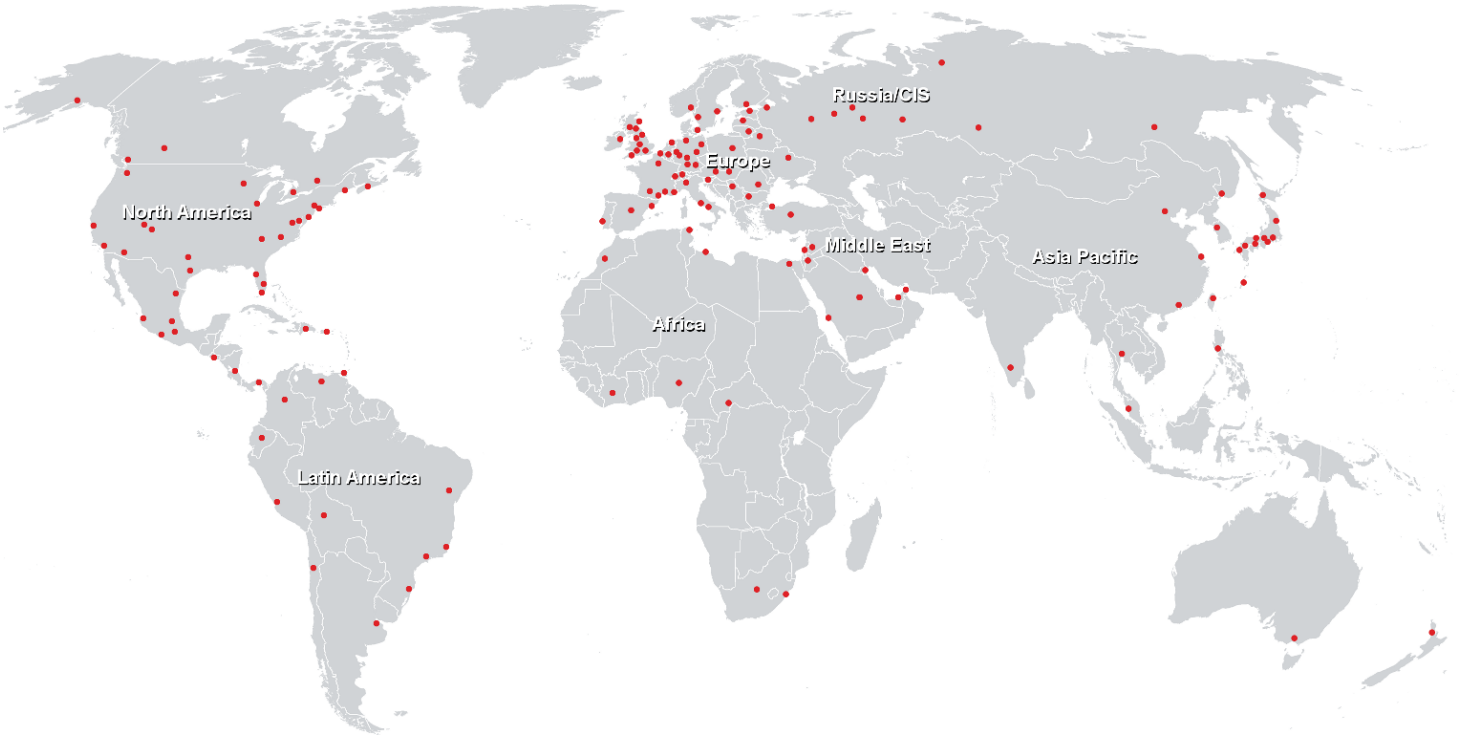
Fortgeschrittenes Jagen

- KQL-Beispiel
- Wichtige MDE-Queries

Endpunkt-DLP (wenn es die Zeit erlaubt)

Master Class: Microsoft Defender for Endpoint (MDE)

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