Defend against cyberthreats with Microsoft Defender XDR (SC-5004)

ID SC-5004 **Preis** CHF 690.– (exkl. MwSt.) **Dauer** 1 Tage

Voraussetzungen

- Erfahrung mit der Verwendung des Microsoft Defender-Portals
- Grundlegendes Verständnis von Microsoft Defender for Endpoint
- Grundlegende Microsoft Sentinel-Kenntnisse
- Erfahrung mit der Kusto-Abfragesprache (KQL) in Microsoft Sentinel

Kursinhalt

Abmildern von Incidents mit Microsoft Defender

- Einführung
- Verwenden des Microsoft Defender-Portals
- Verwalten von Incidents
- Untersuchen von Vorfällen
- Verwalten und Untersuchen von Warnungen
- Verwalten von automatisierten Untersuchungen
- Verwenden des Info-Centers
- Erkunden der erweiterten Bedrohungssuche
- Microsoft Entra-Anmeldeprotokolle untersuchen
- Grundlegendes zur Microsoft-Sicherheitsbewertung
- Untersuchen Sie Bedrohungsanalysen mit dem Security Copilot Threat Intelligence Briefing Agent
- Analysieren von Berichten
- Konfigurieren des Microsoft Defender-Portals
- Modulbewertung
- Zusammenfassung und Ressourcen

Bereitstellen der Microsoft Defender für Endpunkt-Umgebung

- Einführung
- Erstellen der Umgebung
- Grundlegendes zu Kompatibilität und Features von Betriebssystemen
- Integrieren von Geräten
- Zugriff verwalten
- Erstellen und Verwalten von Rollen für die rollenbasierte Zugriffssteuerung
- Konfigurieren von Gerätegruppen
- Konfigurieren von erweiterten Umgebungsfunktionen
- Modulbewertung
- Zusammenfassung und Ressourcen

Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt

- Einführung
- Konfigurieren erweiterter Features
- Konfigurieren von Warnungsbenachrichtigungen
- Verwalten der Warnungsunterdrückung
- Verwalten von Indikatoren
- Modulbewertung
- Zusammenfassung und Ressourcen

Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt

- Einführung
- Konfigurieren erweiterter Features
- Verwalten von Einstellungen für automatisierte Uploads und Ordner
- Konfigurieren der Funktionen für die automatisierte Untersuchung und Wartung
- Risikogeräte blockieren
- Modulbewertung
- Zusammenfassung und Ressourcen

Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt

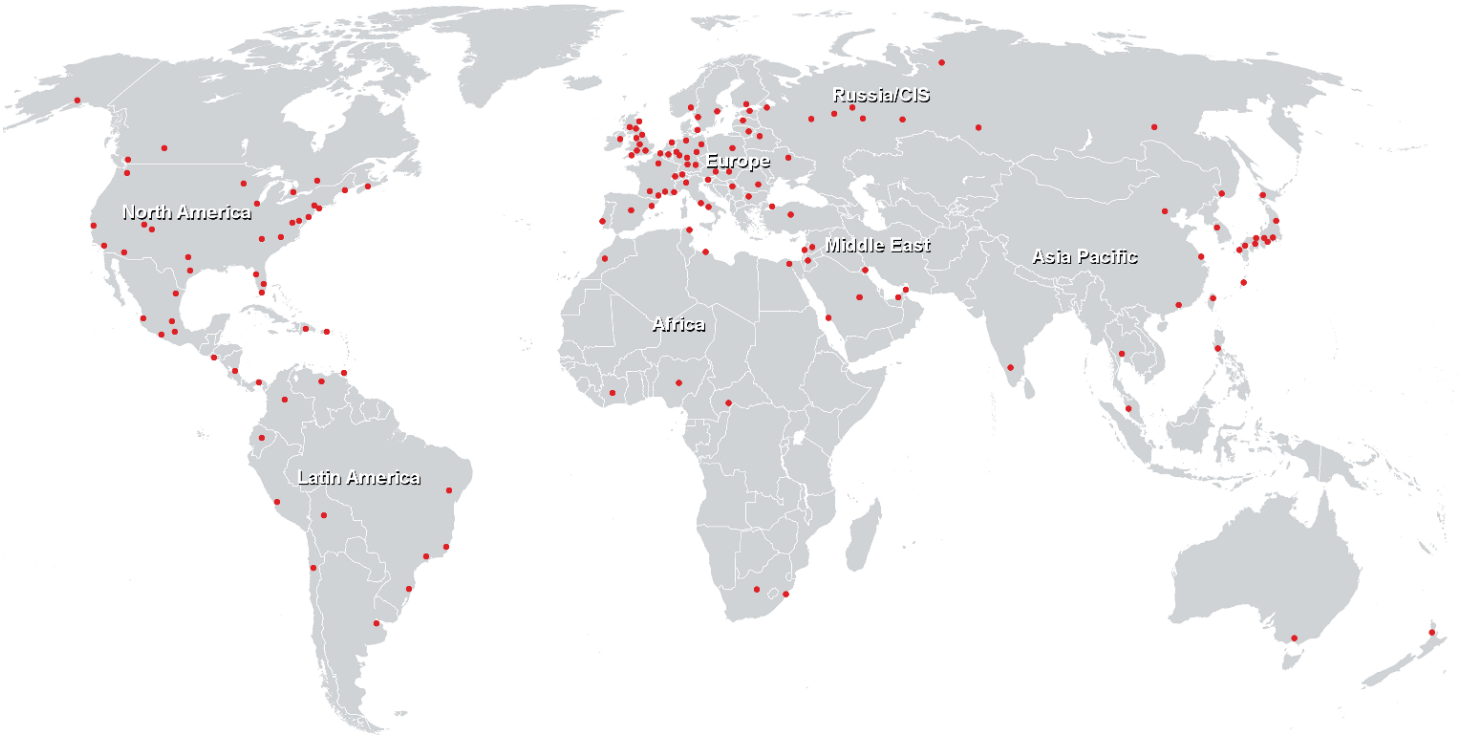
- Einführung
- Verwenden der Geräteinventarliste
- Untersuchen des Geräts
- Verwenden des verhaltensbasierten Blockierens
- Erkennen von Geräten mit Geräteermittlung
- Modulbewertung
- Zusammenfassung und Ressourcen

Labübungen zum Schutz vor Cyberbedrohungen mit Microsoft Defender XDR

- Einführung
- Konfigurieren der Microsoft Defender XDR-Umgebung
- Bereitstellen von Microsoft Defender für Endpunkt
- Entschärfung von Angriffen mit Microsoft Defender for Endpoint

- Zusammenfassung

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