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

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

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

Sie benötigen Zugriff auf einen Microsoft 365 E5-Mandanten mit einer P2-Lizenz für Microsoft Defender for Endpoint, um die Übungen durchzuführen.

Kursinhalt

Abmildern von Incidents mit Microsoft Defender

Erfahren Sie, wie das Microsoft Defender-Portal eine einheitliche Ansicht von Vorfällen in der Microsoft Defender-Produktfamilie bereitstellt.

- Einführung
- Verwenden des Microsoft Defender-Portals
- Verwalten von Incidents
- Untersuchen von Incidents
- Verwalten und Untersuchen von Warnungen
- Verwalten von automatisierten Untersuchungen
- Verwenden des Info-Centers
- Erkunden der erweiterten Bedrohungssuche
- Untersuchen von Microsoft Entra-Anmeldeprotokollen
- Grundlegendes zur Microsoft-Sicherheitsbewertung
- Analysieren der Bedrohungsanalyse
- Berichte analysieren
- Konfigurieren des Microsoft Defender-Portals
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Bereitstellen der Microsoft Defender für Endpunkt-Umgebung

Hier erfahren Sie, wie Sie die Microsoft Defender für Endpunkt-Umgebung bereitstellen, einschliesslich des Onboardings von Geräten und der Sicherheitskonfiguration.

- Einführung
- Erstellen der Umgebung
- Grundlegendes zu Kompatibilität und Features von Betriebssystemen
- Integrieren von Geräten
- Verwalten des Zugriffs
- Erstellen und Verwalten von Rollen für die rollenbasierte Zugriffssteuerung
- Konfigurieren von Gerätegruppen
- Konfigurieren erweiterter Umgebungsfeatures
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt

Erfahren Sie, wie Sie Einstellungen zur Verwaltung von Warnungen und Benachrichtigungen konfigurieren. Ausserdem erfahren Sie, wie Sie Indikatoren im Rahmen des Erkennungsprozesses aktivieren.

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

Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt

Erfahren Sie, wie Sie die Automatisierung in Microsoft Defender für Endpunkt durch Verwalten der Umgebungseinstellungen konfigurieren.

- Einführung
- Konfigurieren erweiterter Features
- Verwalten von Einstellungen für automatisierte Uploads und Ordner
- Konfigurieren der Funktionen für die automatisierte

Untersuchung und Wartung
- Blockieren auf Risikogeräten
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt

Microsoft Defender für Endpunkt bietet umfassende Geräteinformationen, einschliesslich forensischer Informationen. Hier erfahren Sie mehr über die Informationen, die Ihnen über Microsoft Defender für Endpunkt zur Verfügung stehen und bei Untersuchungen hilfreich sind.

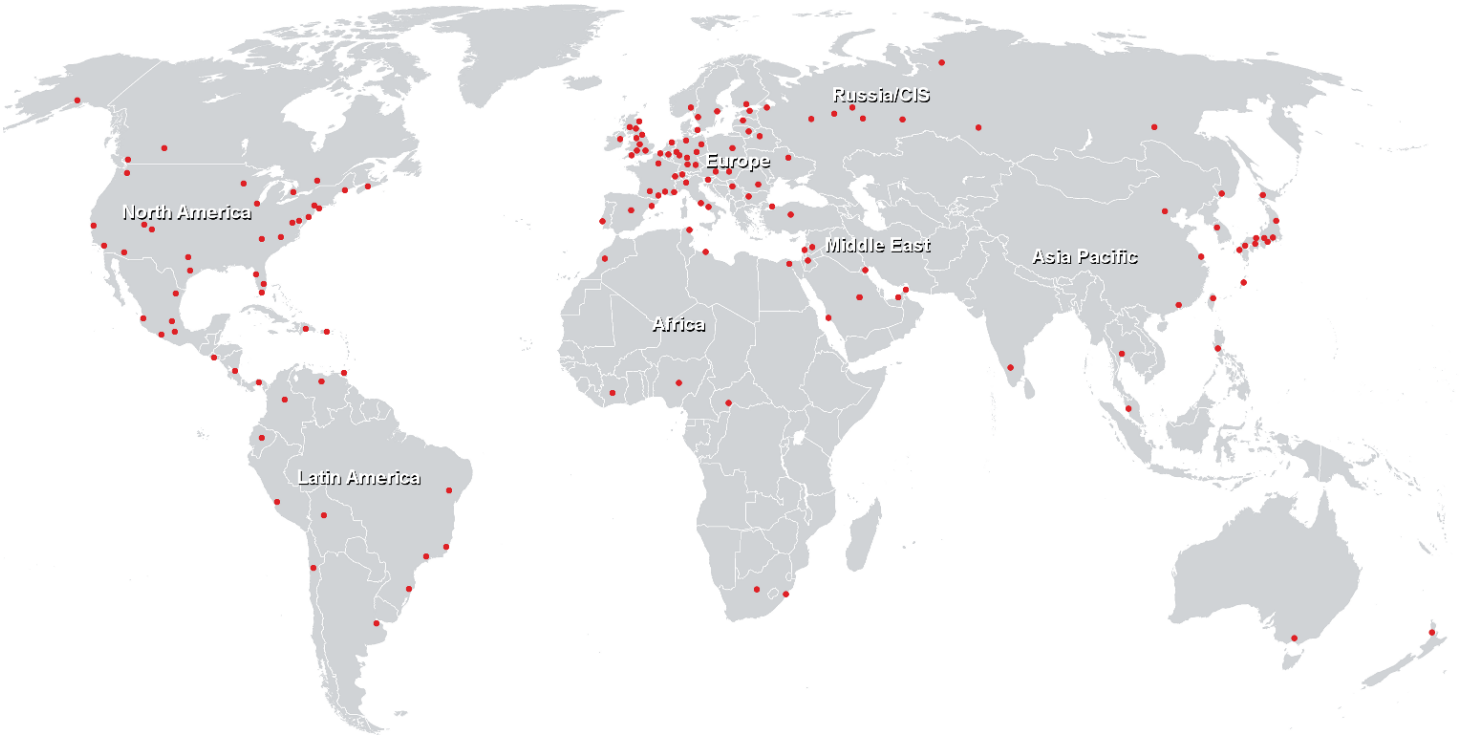
- Einführung
- Verwenden der Geräteinventarliste
- Untersuchen des Geräts
- Verwenden des verhaltensbasierten Blockierens
- Erkennen von Geräten mit Geräteermittlung
- Wissensbeurteilung
- Zusammenfassung und Ressourcen

Labübungen zum Schutz vor Cyberbedrohungen mit Microsoft Defender XDR

In diesem Modul haben Sie erfahren, wie Sie Microsoft Defender XDR konfigurieren, Microsoft Defender for Endpoint bereitstellen und Geräte onboarden. Sie haben auch Richtlinien konfiguriert, Bedrohungen entschärft und mit Defender XDR auf Vorfälle reagiert.

- 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