Configure SIEM security operations using Microsoft Sentinel (SC-5001)

ID SC-5001 **Preis** CHF 870.– (exkl. MwSt.) **Dauer** 1 Tage

Zielgruppe

Der Microsoft Security Operations Analyst arbeitet mit Organisationsbeteiligten zusammen, um Informationstechnologiesysteme für die Organisation zu sichern. Ihr Ziel ist es, das Organisationsrisiko zu reduzieren, indem aktive Angriffe in der Umgebung schnell behoben werden, Beratungen zu Verbesserungen der Bedrohungsschutzpraktiken angeboten und Verstösse gegen Organisationsrichtlinien an geeignete Interessengruppen weitergeleitet werden. Zu den Verantwortlichkeiten gehören Bedrohungsverwaltung, Überwachung und Reaktion mithilfe einer Vielzahl von Sicherheitslösungen in ihrer gesamten Umgebung. Die Rolle untersucht, reagiert auf und sucht nach Bedrohungen mithilfe von Microsoft Sentinel, Microsoft Defender für Cloud, Microsoft Defender XDR und Sicherheitsprodukten von Drittanbietern. Da der Security Operations Analyst die operative Ausgabe dieser Tools nutzt, sind sie auch ein wichtiger Stakeholder bei der Konfiguration und Bereitstellung dieser Technologien.

Voraussetzungen

- Grundlegendes Verständnis von Microsoft Azure
- Grundlegende Microsoft Sentinel-Kenntnisse
- Erfahrung mit der Kusto-Abfragesprache (KQL) in Microsoft Sentinel

Kursinhalt

Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen

- Einleitung
- Planen des Microsoft Sentinel-Arbeitsbereichs
- Erstellen eines Microsoft Sentinel-Arbeitsbereichs
- Mandantenübergreifende Verwaltung von Arbeitsbereichen mithilfe von Azure Lighthouse
- Grundlegendes zu Microsoft Sentinel-Berechtigungen und -Rollen
- Verwalten von Microsoft Sentinel-Einstellungen
- Konfigurieren von Protokollen
- Modulbewertung
- Zusammenfassung und Ressourcen

Herstellen einer Verbindung von Microsoft-Diensten mit Microsoft Sentinel

- Einführung
- Plan für Konnektoren für Microsoft-Dienste
- Verbinden des Microsoft 365-Connectors
- Herstellen einer Verbindung mit dem Microsoft Entra-Connector
- Herstellen einer Verbindung mit dem Microsoft Entra ID Protection-Connector
- Verbinden des Azure-Aktivitätsconnectors
- Modulbewertung
- Zusammenfassung und Ressourcen

Verbinden von Windows-Hosts mit Microsoft Sentinel

- Einleitung
- Plan für den Connector für sicherheitsrelevante Ereignisse für Windows-Hosts
- Herstellen einer Verbindung mit den Windows-Sicherheitsereignissen über AMA Connector
- Herstellen einer Verbindung mithilfe der Sicherheitsereignisse über den Connector des Agents einer Vorgängerversion
- Erfassen von Sysmon-Ereignisprotokollen
- Modulbewertung
- Zusammenfassung und Ressourcen

Bedrohungserkennung mit Microsoft Sentinel-Analysen

- Einführung
- Übung: Erkennen von Bedrohungen mit Microsoft Sentinel Analytics
- Was ist Microsoft Sentinel Analytics?
- Typen von Analyseregeln
- Erstellen einer Analyseregel anhand von Vorlagen
- Erstellen einer Analyseregel im Assistenten
- Verwalten von Analyseregeln
- Übung: Erkennen von Bedrohungen mit Microsoft Sentinel Analytics
- Zusammenfassung

Automatisierung in Microsoft Sentinel

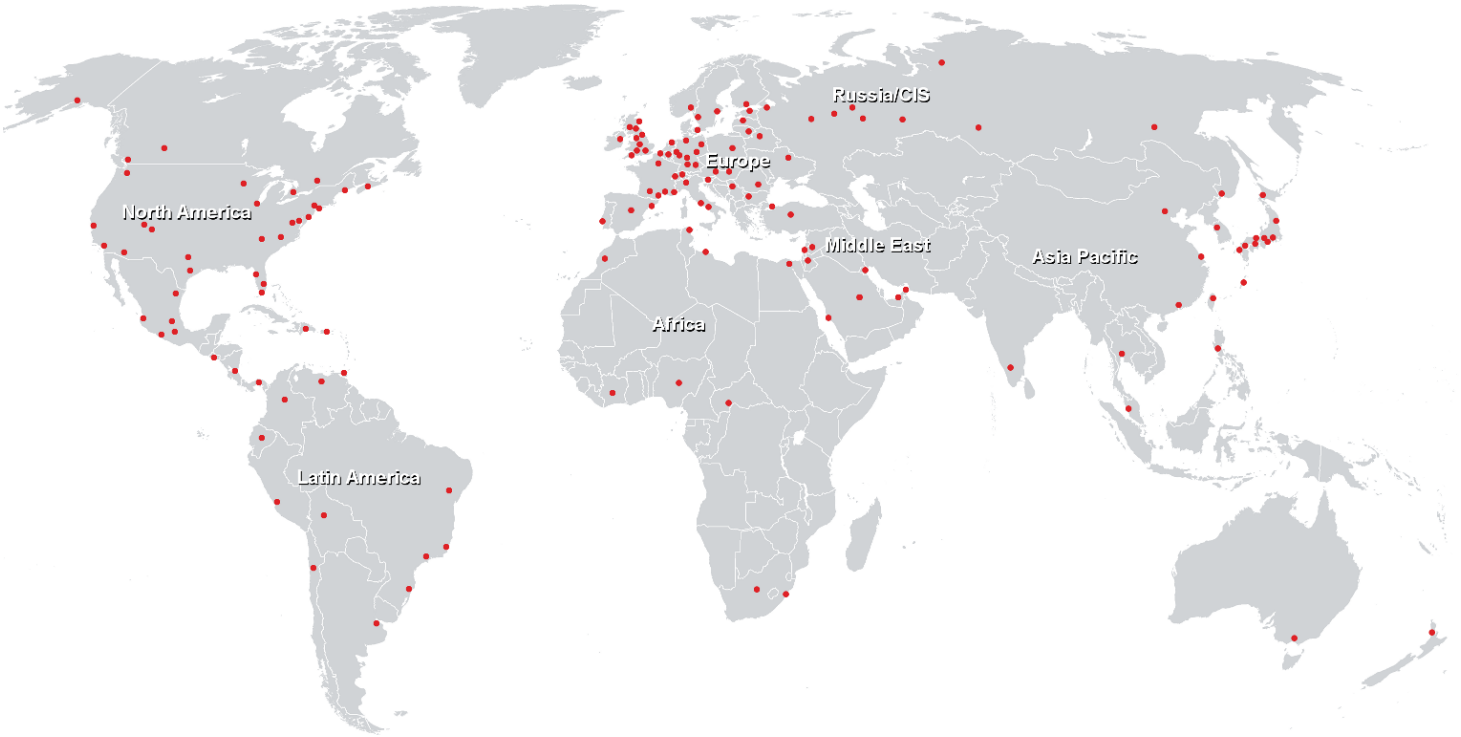
- Einleitung
- Verstehen von Automatisierungsoptionen
- Erstellen von Automatisierungsregeln
- Modulbewertung
- Zusammenfassung und Ressourcen

Konfigurieren von SIEM-Sicherheitsvorgängen mit Microsoft Sentinel

- Einleitung
- Übung: Konfigurieren von SIEM-Sicherheitsvorgängen mit Microsoft Sentinel
- Übung: Installieren von Microsoft Sentinel-Inhaltshublösungen und Datenconnectors
- Übung: Konfigurieren einer Datenconnector-Datensammlungsregel
- Übung: Durchführen eines simulierten Angriffs zum Überprüfen der Analyse- und Automatisierungsregeln
- Übung – Verbinden von Microsoft Sentinel mit Microsoft Defender XDR
- Zusammenfassung

Microsoft Solutions Partner
Microsoft Cloud Training Services

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