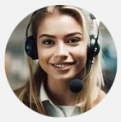
Microsoft Security Operations Analyst

Kurs ID: SC-200T00 Dauer: 1 Tag ab: € 2.490,00 zzgl. MwSt.

In diesem Seminar lernen Sie, Cyberbedrohungen mithilfe von Microsoft Azure Sentinel, Azure Defender und Microsoft 365 Defender zu minimieren. Insbesondere werden Sie Azure Sentinel und Kusto Query Language (KQL) für Entdeckung, Analyse und Berichterstellung konfigurieren und verwenden.



Sie haben Fragen?

+43 50 4510-0
Mo-Do 8-17 Uhr, Fr. 8-14 Uhr

Kursdetails

Kursinhalte

Minimieren von Bedrohungen mithilfe von Microsoft Defender for Endpoint

- Schutz gegen Bedrohungen mit Microsoft Defender for Endpoint
- Bereitstellen der Microsoft-Defender-for-Endpoint-Umgebung
- Implementieren von Windows-10-Sicherheitserweiterungen mit Microsoft Defender for Endpoint
- Verwalten von Alarmen und Vorfällen in Microsoft Defender for Endpoint
- Geräteuntersuchungen in Microsoft Defender for Endpoint
- Durchführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender for Endpoint
- Untersuchungen von Evidenz und Entitäten mithilfe von Microsoft Defender for Endpoint
- Konfigurieren und Verwalten der Automatisierung mithilfe von Microsoft Defender for Endpoint
- Konfigurieren von Alarmen und Entdeckungen in Microsoft Defender for Endpoint

ÖCERT

tecTrain ist ein zertifiziertes Schulungsinstitut nach Ö-Cert, dem Qualitätsrahmen für die Erwachsenenbildung in Österreich

- Bedrohungs- und Angreifbarkeitsverwaltung in Microsoft Defender for Endpoint

Minimieren von Bedrohungen mithilfe von Microsoft 365 Defender

- Einführung in den Schutz vor Bedrohungen mit Microsoft 365
- Minimieren von Vorfällen mithilfe von Microsoft 365 Defender
- Schutz von Identitäten mit Azure AD Identity Protection
- Beseitigen von Risiken mit Microsoft Defender for Office 365
- Schutz der Umgebung mit Microsoft Defender for Identity
- Absichern von Cloudanwendungen und -diensten mit Microsoft Cloud App Security
- Antworten auf Alarme bezüglich Datenverlustes mithilfe von Microsoft 365
- Verwalten von Insiderrisiken in Microsoft 365

Minimieren von Bedrohungen mithilfe von Azure Defender

- Planen des Schutzes von Cloudarbeitslasten mithilfe von Azure Defender
- Schutzmöglichkeiten für Cloudarbeitslasten in Azure Defender
- Verbinden von Azure-Medienobjekten mit Azure Defender
- Verbinden von Nicht-Azure-Ressourcen mit Azure Defender
- Beseitigen von Sicherheitsalarmen mithilfe von Azure Defender

Erstellen von Abfragen für Azure Sentinel mithilfe von Kusto Query Language (KQL)

- Konstruieren von KQL-Anweisungen für Azure Sentinel
- Analysieren von Abfrageergebnissen mithilfe von KQL
- Erstellen von Mehrtabellenanweisungen mithilfe von KQL
- Arbeiten mit Daten in Azure Sentinel mithilfe von Kusto Query Language

Konfiguration der Azure-Sentinel-Umgebung

- Einführung in Azure Sentinel
- Erstellen und Verwalten von Azure-Sentinel-Arbeitsräumen
- Abfragen von Logs in Azure Sentinel

- Verwenden von Watchlists in Azure Sentinel
- Verwenden von Threat Intelligence in Azure Sentinel

Verbinden von Logs mit Azure Sentinel

- Daten mithilfe von Datenkonnektoren mit Azure Sentinel verbinden
- Verbinden von Microsoft-Diensten mit Azure Sentinel
- Verbinden von Microsoft 365 Defender mit Azure Sentinel
- Verbinden von Windows-Hosts mit Azure Sentinel
- Verbinden von Common-Event-Format-Logs mit Azure Sentinel
- Verbinden von Syslogdatenquellen mit Azure Sentinel
- Verbinden von Bedrohungsindikatoren mit Azure Sentinel

Erstellen von Entdeckungen und Durchführen von Untersuchungen mithilfe von Azure Sentinel

- Entdecken von Bedrohungen mit Azure-Sentinel-Analytik
- Antworten auf Bedrohungen mit Azure-Sentinel-Playbooks
- Verwalten von Sicherheitsvorfällen in Azure Sentinel
- Analyse des Entitätsverhaltens in Azure Sentinel
- Abfragen, Visualisieren und Überwachen von Daten in Azure Sentinel

Threat Hunting in Azure Sentinel

- Suche nach Bedrohungen mit Azure Sentinel
- Suche nach Bedrohungen mithilfe von Notebooks in Azure Sentinel

Voraussetzungen

Grundverständnis für Microsoft 365 und Windows 10,Grundverständnis für Microsoft Sicherheits-, Compliance- und Identitätsprodukte, Vertrautheit mit Azure-Diensten, insbesondere Azure SQL Database und Azure Storage, Vertrautheit mit virtuellen Azure-Maschinen und virtuellem Networking , Grundverständnis für Scripting-Konzepte

Zielgruppe

Personen mit Verantwortung und Tätigkeiten im IT-Security-Umfeld.

Abschluß

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.