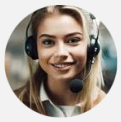
Defend against cyberthreats with Microsoft Defender XDR

Kurs ID: SC-5004 Dauer: 1 Tag ab: € 690,00 zzgl. MwSt.

Implementieren Sie die Microsoft Defender for Endpoint-Umgebung zum Verwalten von Geräten, führen Sie Untersuchungen zu Endpunkten durch, verwalten Sie Vorfälle in Defender XDR, und nutzen Sie die erweiterte Bedrohungssuche mit KQL (Kusto-Abfragesprache), um einzelne Bedrohungen zu erkennen.



Sie haben Fragen?

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

Kursdetails

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

Kursinhalte

Abmildern von Incidents mit Microsoft Defender

- 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

Bereitstellen der Microsoft Defender für Endpunkt-

Umgebung

- 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

Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt

- Konfigurieren erweiterter Features
- Konfigurieren von Warnungsbenachrichtigungen
- Verwalten der Warnungsunterdrückung
- Verwalten von Indikatoren

Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt

- Konfigurieren erweiterter Features
- Verwalten von Einstellungen für automatisierte Uploads und Ordner
- Konfigurieren der Funktionen für die automatisierte Untersuchung und Wartung
- Blockieren auf Risikogeräten

Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt

- Verwenden der Geräteinventarliste
- Untersuchen des Geräts
- Verwenden des verhaltensbasierten Blockierens
- Erkennen von Geräten mit Geräteermittlung

Labübungen zum Schutz vor Cyberbedrohungen mit Microsoft Defender XDR

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

Endpoint

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

Abschluß

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.