Konfigurieren von SIEM-Sicherheitsvorgängen mit Microsoft Sentinel (SC-5001)

Konfigurieren Sie den Microsoft Sentinel-Arbeitsbereich, stellen Sie eine Verbindung von Microsoft-Diensten und Windows-Sicherheitsereignissen mit Microsoft Sentinel her, konfigurieren Sie Microsoft Sentinel-Analyseregeln, und reagieren Sie mit automatisierten Antworten auf Bedrohungen.

INHALTE

Create and manage Microsoft Sentinel workspaces

- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs

Connect Microsoft services to Microsoft Sentinel

- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector

Connect Windows hosts to Microsoft Sentinel

- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs

Threat detection with Microsoft Sentinel analytics

- What is Microsoft Sentinel Analytics?
- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules

Automation in Microsoft Sentinel

PREIS P. P.

€ 450,- (zzgl. MwSt.)

DAUER

0.5 Tage (09:00 - 12:30 Uhr)

SIE HABEN FRAGEN?

+43 50 4510-0

E-Mail Anfrage: office@tectrain.at

https://www.tectrain.at/seminare/microsoft-technisch/microsoft-applied-skills/konfigurieren-von-siem-sicherheitsvorgaengen-mit-microsoft-sentinel

- Understand automation options
- Create automation rules

Configure SIEM security operations using Microsoft Sentinel

VORAUSSETZUNGEN

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

ABSCHLUSS

Nach Seminarabschluss erhalten Sie ein tecTrain-Teilnahmezertifikat.