>> Microsoft Sentinel

Configure SIEM Security Operations

Das Einrichten und Konfigurieren herkömmlicher SIEM-Systeme (Security Information & Event Management) erfordert in der Regel viel Zeit. Außerdem sind diese Systeme nicht unbedingt für Cloudworkloads konzipiert. Microsoft Sentinel ermöglicht es Ihnen, sich anhand Ihrer Cloud- und lokalen Daten schnell wertvolle sicherheitsrelevante Erkenntnisse zu verschaffen. Dieses Modul unterstützt Sie beim Einstieg.

Ihr Nutzen

Sie lernen das Identifizieren der verschiedenen Komponenten und Funktionen von Microsoft Sentinel sowie das Identifizieren von Anwendungsfällen.

Voraussetzungen

Kenntnisse über die Sicherheitsvorgänge in einer Organisation.
Grundlegende Kenntnisse über Azure-Dienste.

Preis pro Teilnehmer

EUR 850,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

SC-5001,

Version: N/A

Seminarinhalte

* Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen
- Einführung
- Planen des Microsoft Sentinel-Arbeitsbereichs
- Erstellen eines Microsoft Sentinel-Arbeitsbereichs
- Verwalten von mandantenübergreifenden Arbeitsbereichen mit Azure Lighthouse
- Verstehen der Microsoft Sentinel-Berechtigungen und -Rollen
- Verwalten von Microsoft Sentinel-Einstellungen
- Protokolle konfigurieren

* Verbinden von Microsoft-Diensten mit Microsoft Sentinel
- Einführung
- Planen Sie Konnektoren für Microsoft-Dienste
- Verbinden des Microsoft Office 365-Konnektors
- Verbinden Sie den Microsoft Entra-Konnektor
- Verbinden Sie den Microsoft Entra ID Protection-Konnektor
- Verbinden Sie den Azure Activity-Konnektor

* Verbinden von Windows-Hosts mit Microsoft Sentinel
- Einführung
- Planen Sie für den Windows-Hosts-Sicherheitsereignisse-Connector
- Verbinden mit dem Windows Security Events via AMA Connector
- Verbinden mit dem Security Events via Legacy Agent Connector
- Sysmon-Ereignisprotokolle sammeln

* Erkennung von Bedrohungen mit Microsoft Sentinel-Analysen
- Einführung
- Übung - Erkennen von Bedrohungen mit Microsoft Sentinel Analytics
- Was ist Microsoft Sentinel Analytics?
- Arten von Analyseregeln
- Erstellen einer Analyseregel aus Vorlagen
- Erstellen einer Analyseregel mit dem Assistenten
- Verwalten von Analyseregeln
- Übung - Erkennen von Bedrohungen mit Microsoft Sentinel Analytics

* Automatisierung in Microsoft Sentinel
- Einführung
- Automatisierungsoptionen verstehen
- Automatisierungsregeln erstellen

* Konfigurieren von SIEM-Sicherheitsoperationen mit Microsoft Sentinel
- Einführung
Übung - Konfigurieren von SIEM-Vorgängen mit Microsoft Sentinel -
Übung - Konfigurieren von SIEM-Vorgängen mit Microsoft Sentinel
- Übung - Installieren von Microsoft Sentinel Content Hub-Lösungen und Datenkonnektoren
- Übung - Konfigurieren Sie einen Datenkonnektor und eine Datensammelregel.
- Übung - Einen simulierten Angriff durchführen, um die Analyse- und Automatisierungsregeln zu validieren