Microsoft Security Operations Analyst (SC-200).

Microsoft Defender und Azure Sentinel als Security Lösung gegen Cyberattacken

Seminar | 16 Termine verfügbar | Teilnahmebescheinigung
Präsenz / Virtual Classroom | 32 Unterrichtseinheiten | Garantietermine vorhanden

Seminarnummer: 29529 | Herstellernummer: MOC-SC-200

Stand: 04.03.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/29529

Lernen Sie Cyber-Bedrohungen mithilfe von Azure Sentinel, Azure Defender und Microsoft 365 Defender zu identifizieren, zu untersuchen und abzuwehren. Insbesondere werden Sie Azure Sentinel konfigurieren und verwenden sowie die Kusto Query Language (KQL) nutzen, um Analyse und Reports durchzuführen.

Nutzen

Nach diesem Seminar verfügen Sie über folgende Kenntnisse

- Microsoft Defender für Endpoint Risiken in Ihrer Umgebung
- Regeln zur Reduzierung der Angriffsfläche auf Windows 10-Geräten
- Untersuchung von Domänen und IP-Adressen in Microsoft Defender for Endpoint
- Untersuchung von Benutzerkonten in Microsoft Defender für Endpoint
- Konfiguration von Warneinstellungen in Microsoft Defender für Endpoint
- Die erweiterte Suche in Microsoft 365 Defender
- Verwalten von Vorfällen in Microsoft 365 Defender
- Untersuchung der DLP-Warnungen in Microsoft Cloud App Security
- Umgang mit Insider-Risikomanagementfällen
- Beseitigen von Alarmen in Azure Defender
- Konfiguration von KQL-Anweisungen
- Filtern von Suchanfragen basierend auf Ereigniszeit, Schweregrad, Domäne und anderen relevanten Daten mit KQL
- Extrahieren von Daten aus unstrukturierten String-Feldern mithilfe von KQL
- Verwalten eines Azure Sentinel-Arbeitsbereichs
- Verwendung von KQL für den Zugriff auf die Überwachungsliste in Azure Sentinel
- Verwalten von Bedrohungsindikatoren in Azure Sentinel

- Verbinden von Azure Windows Virtual Machines mit Azure Sentinel
- Konfiguration des Log Analytics-Agenten zum Sammeln von Sysmon-Ereignissen
- Erstellen eines Playbooks, um eine Vorfallsreaktion zu automatisieren
- Einsatz von Abfragen für die Suche nach Bedrohungen
- Beobachtung von Bedrohungen im Zeitverlauf mit Livestream

Zielgruppe

Microsoft Security Operations Analyst:innen arbeiten mit den Stakeholdern des Unternehmens zusammen, um die Informationstechnologie-Systeme des Unternehmens zu sichern. Ihr Ziel ist es, das Unternehmensrisiko zu reduzieren, indem sie aktive Angriffe in der Umgebung schnell beheben, über Verbesserungen der Praktiken zum Schutz vor Bedrohungen beraten und Verstöße gegen die Unternehmensrichtlinien an die entsprechenden Verantwortlichen weiterleiten. Zu den Aufgaben gehören das Bedrohungsmanagement, die Überwachung und die Reaktion auf Bedrohungen durch den Einsatz einer Vielzahl von Sicherheitslösungen in der gesamten Umgebung.

Voraussetzungen

- Grundlegendes Verständnis von Microsoft 365
- Grundlegendes Verständnis der Sicherheits-, Compliance- und Identitätsprodukte von Microsoft
- Kenntnisse zu Windows 10
- Vertrautheit mit Azure-Diensten, insbesondere Azure SQL Database und Azure Storage
- Vertrautheit mit virtuellen Maschinen und virtuellen Netzwerken in Azure
- Grundlegendes Verständnis von Scripting-Konzepten.

Diese Vorkenntnisse können z.B. in unseren Azure AZ- und Microsoft 365 MS-Seminaren erworben werden.

Inhalte des Seminars

Module 1: Mitigate threats using Microsoft Defender for Endpoint

Implement the Microsoft Defender for Endpoint platform to detect, investigate, and respond to advanced threats. Learn how Microsoft Defender for Endpoint can help your organization stay secure. Learn how to deploy the Microsoft Defender for Endpoint environment, including onboarding devices and configuring security. Learn how to investigate incidents and alerts using Microsoft Defender for Endpoints. Perform advanced hunting and consult with threat experts. You will also learn how to configure automation in Microsoft Defender for Endpoint by managing environmental settings. Lastly, you will learn about your environment's weakness by using Threat and Vulnerability Management in Microsoft Defender for Endpoint.

- Protect against threats with Microsoft Defender for Endpoint

- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows 10 security enhancements with Microsoft Defender for Endpoint
- Manage alerts and incidents in Microsoft Defender for Endpoint
- Perform device investigations in Microsoft Defender for Endpoint
- Perform actions on a device using Microsoft Defender for Endpoint
- Perform evidence and entities investigations using Microsoft Defender for Endpoint
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint

Module 2: Mitigate threats using Microsoft 365 Defender

Analyze threat data across domains and rapidly remediate threats with built-in orchestration and automation in Microsoft 365 Defender. Learn about cybersecurity threats and how the new threat protection tools from Microsoft protect your organizations users, devices, and data. Use the advanced detection and remediation of identity-based threats to protect your Azure Active Directory identities and applications from compromise.

- Introduction to threat protection with Microsoft 365
- Mitigate incidents using Microsoft 365 Defender
- Protect your identities with Azure AD Identity Protection
- Remediate risks with Microsoft Defender for Office 365
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Cloud App Security
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365

Module 3: Mitigate threats using Azure Defender

Use Azure Defender integrated with Azure Security Center, for Azure, hybrid cloud, and on-premises workload protection and security. Learn the purpose of Azure Defender, Azure Defender's relationship to Azure Security Center, and how to enable Azure Defender. You will also learn about the protections and detections provided by Azure Defender for each cloud workload. Learn how you can add Azure Defender capabilities to your hybrid environment.

- Plan for cloud workload protections using Azure Defender
- Explain cloud workload protections in Azure Defender
- Connect Azure assets to Azure Defender
- Connect non-Azure resources to Azure Defender
- Remediate security alerts using Azure Defender

Module 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)

Write Kusto Query Language (KQL) statements to query log data to perform detections, analysis, and reporting in Azure Sentinel. This module will focus on the most used operators. The example KQL statements will showcase security related table queries. KQL is the query language used to perform analysis on data to create analytics, workbooks, and perform hunting in Azure Sentinel. Learn how basic KQL statement structure provides the foundation to build more complex statements. Learn how to summarize and visualize data with a KQL statement provides the foundation to build detections in Azure Sentinel. Learn how to use the Kusto Query Language (KQL) to manipulate string data ingested from log sources.

- Construct KQL statements for Azure Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with data in Azure Sentinel using Kusto Query Language

Module 5: Configure your Azure Sentinel environment

Get started with Azure Sentinel by properly configuring the Azure Sentinel workspace. Traditional security information and event management (SIEM) systems typically take a long time to set up and configure. They're also not necessarily designed with cloud workloads in mind. Azure Sentinel enables you to start getting valuable security insights from your cloud and on-premises data quickly.

This module helps you get started. Learn about the architecture of Azure Sentinel workspaces to ensure you configure your system to meet your organization's security operations requirements. As a Security Operations Analyst, you must understand the tables, fields, and data ingested in your workspace. Learn how to query the most used data tables in Azure Sentinel.

- Introduction to Azure Sentinel
- Create and manage Azure Sentinel workspaces
- Query logs in Azure Sentinel
- Use watchlists in Azure Sentinel
- Utilize threat intelligence in Azure Sentinel

Module 6: Connect logs to Azure Sentinel

Connect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds to Azure Sentinel. The primary approach to connect log data is using the Azure Sentinel provided data connectors. This module provides an overview of the available data connectors. You will get to learn about the configuration options and data provided by Azure Sentinel connectors for Microsoft 365 Defender.

- Connect data to Azure Sentinel using data connectors
- Connect Microsoft services to Azure Sentinel
- Connect Microsoft 365 Defender to Azure Sentinel
- Connect Windows hosts to Azure Sentinel
- Connect Common Event Format logs to Azure Sentinel
- Connect syslog data sources to Azure Sentinel
- Connect threat indicators to Azure Sentinel

Module 7: Create detections and perform investigations using Azure Sentinel

Detect previously uncovered threats and rapidly remediate threats with built-in orchestration and automation in Azure Sentinel. You will learn how to create Azure Sentinel playbooks to respond to security threats. You'll investigate Azure Sentinel incident management, learn about Azure Sentinel events and entities, and discover ways to resolve incidents. You will also learn how to query, visualize, and monitor data in Azure Sentinel.

- Threat detection with Azure Sentinel analytics
- Threat response with Azure Sentinel playbooks
- Security incident management in Azure Sentinel
- Use entity behavior analytics in Azure Sentinel
- Query, visualize, and monitor data in Azure Sentinel

Module 8: Perform threat hunting in Azure Sentinel

In this module, you'll learn to proactively identify threat behaviors by using Azure Sentinel queries. You'll also learn to use bookmarks and livestream to hunt threats. You will also learn how to use notebooks in Azure Sentinel for advanced hunting.

- Threat hunting with Azure Sentinel
- Hunt for threats using notebooks in Azure Sentinel

Wichtige Hinweise

Damit Sie von einer möglichst hohen Durchführungschance profitieren, behalten wir uns vor, bei Bedarf mit dem autorisierten Microsoft Partner ETC – Enterprise Training Center GmbH zusammenzuarbeiten.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/29529 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.