

SC-200T00

Microsoft Security Operations Analyst

Erfahren Sie, wie Sie mit Microsoft Sentinel, Microsoft Defender for Cloud und Microsoft 365 Defender Bedrohungen untersuchen, auf sie reagieren und sie aufspüren können. In diesem Kurs lernen Sie, wie Sie Cyberbedrohungen mithilfe dieser Technologien abwehren können. Insbesondere konfigurieren und verwenden Sie Microsoft Sentinel und nutzen Kusto Query Language (KQL) zur Erkennung, Analyse und Berichterstellung. Der Kurs richtet sich an Personen, die im Bereich Security Operations tätig sind, und hilft Teilnehmern bei der Vorbereitung auf die Prüfung SC-200: Microsoft Security Operations Analyst.

Kursinhalt

- Einführung in den Bedrohungsschutz von Microsoft 365
- Abmildern von Incidents mithilfe von Microsoft 365 Defender
- Schützen Ihrer Identitäten mit Microsoft Entra ID Protection
- Remediate risks with Microsoft Defender for Office 365
- Schützen Sie Ihre Umgebung mit Microsoft Defender for Identity
- Sichern Ihrer Cloud-Apps und -Dienste mit Microsoft Defender for Cloud Apps
- Reagieren auf Warnungen zur Verhinderung von Datenverlust mithilfe von Microsoft 365
- Manage insider risk in Microsoft Purview
- Untersuchen von Bedrohungen mithilfe von Überwachungsfeatures in Microsoft 365 Defender und Microsoft Purview Standard
- Untersuchen von Bedrohungen mithilfe der Überwachung in Microsoft 365 Defender und Microsoft Purview (Premium)
- Untersuchen von Bedrohungen mit der Inhaltssuche in Microsoft Purview
- Protect against threats with Microsoft Defender for Endpoint
- Bereitstellen der Microsoft Defender für Endpunkt-Umgebung
- Implementieren von Windows-Sicherheitsverbesserungen mit Microsoft Defender für Endpunkt
- Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt
- Ausführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender für Endpunkt
- Untersuchen von Beweisen und Entitäten mithilfe von Microsoft Defender für Endpunkt
- Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt
- Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt
- Verwenden des Sicherheitsrisikomanagements in Microsoft Defender für Endpunkt
- Planen von Workloadschutz in der Cloud mit Microsoft Defender für Cloud
- Verbinden von Azure-Ressourcen mit Microsoft Defender für Cloud
- Verbinden Azure-fremder Ressourcen mit Microsoft Defender für Cloud
- Verwalten Ihrer Cloud Security Posture Management-Instanz
- Workloadschutz in der Cloud mit Microsoft Defender für Cloud
- Beheben von Sicherheitswarnungen mit Microsoft Defender für Cloud
- Erstellen von KQL-Anweisungen für Microsoft Sentinel
- Analysieren von Abfrageergebnissen mithilfe von KQL
- Erstellen von Anweisungen mit mehreren Tabellen mithilfe von KQL
- Arbeiten mit Daten in Microsoft Sentinel mithilfe der Kusto-Abfragesprache
- Einführung in Microsoft Sentinel
- Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen
- Abfragen von Protokollen in Microsoft Sentinel
- Verwenden von Watchlists in Microsoft Sentinel
- Verwenden der Threat Intelligence in Microsoft Sentinel
- Verbinden von Daten mit Microsoft Sentinel mithilfe von Datenconnectors
- Herstellen einer Verbindung von Microsoft-Diensten mit Microsoft Sentinel
- Verbinden von Microsoft 365 Defender mit Microsoft Sentinel
- Verbinden von Windows-Hosts mit Microsoft Sentinel
- Verbinden von Common Event Format-Protokollen mit Microsoft Sentinel
- Verbinden von Syslog-Datenquellen mit Microsoft Sentinel
- Verbinden von Bedrohungsindikatoren mit Microsoft Sentinel
- Bedrohungserkennung mit Microsoft Sentinel-Analysen
- Automatisierung in Microsoft Sentinel
- Verwaltung von Sicherheitsvorfällen in Microsoft Sentinel
- Identifizieren von Bedrohungen mithilfe der Verhaltensanalyse
- Datennormalisierung in Microsoft Sentinel
- Abfragen, Visualisieren und Überwachen von Daten in Microsoft Sentinel
- Verwalten von Inhalten in Microsoft Sentinel
- Erläutern der Bedrohungssuchkonzepte in Microsoft Sentinel
- Bedrohungssuche mit Microsoft Sentinel
- Verwenden von Suchaufträgen in Microsoft Sentinel
- Suchen von Bedrohungen mithilfe von Notebooks in Microsoft Sentinel

E-Book Die originalen Microsoft-Kursunterlagen werden Ihnen online zur Verfügung gestellt.

Zielgruppe

Der Microsoft Security Operations Analyst arbeitet mit Projektbeteiligten im Unternehmen zusammen, um IT-Systeme des Unternehmens zu schützen. Ihr Ziel ist es, Risiken für das Unternehmen zu verringern, indem sie aktive Angriffe in der Umgebung schnell abwehren, Empfehlungen zur Verbesserung der Bedrohungsschutzmethoden aussprechen und Verstöße gegen die Unternehmensrichtlinien an die zuständigen Stellen weiterleiten. Zu den Zuständigkeiten gehören das Verwalten und Überwachen von sowie das Reagieren auf Bedrohungen durch den Einsatz einer Vielzahl von Sicherheitslösungen in ihrer Umgebung. Zu den Aufgaben dieser Rolle gehört in erster Linie das Untersuchen, Reagieren und Suchen nach Bedrohungen mithilfe von Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender und Sicherheitsprodukten von Drittanbietern. Da der*die Security Operations Analyst die operative Ausgabe dieser Tools nutzt, ist er*sie auch ein*e wichtige*r Stakeholder*in beim Konfigurieren und Bereitstellen dieser Technologien.

Voraussetzungen

- Grundkenntnisse über Microsoft 365
- Grundlegendes Verständnis über Microsoft-Produkte zu Sicherheit, Compliance und Identität
- Fortgeschrittene Kenntnisse über Microsoft Windows
- Vertrautheit mit Azure-Diensten, insbesondere Azure SQL-Datenbank und Azure Storage
- Kenntnisse im Umgang mit virtuellen Azure-Computern und virtuellen Netzwerken
- Grundlegendes Verständnis der Konzepte zur Skripterstellung

Kursziel

Dieser Kurs unterstützt die Teilnehmer auf die Vorbereitung zum Examen SC-200, welches für die Zertifizierungen "Microsoft Certified: Security Operations Analyst Associate" vorausgesetzt wird.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/MC20

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.
Termine in Deutschland		4 Tage CHF 2.855,-
Online Training		4 Tage CHF 2.855,-
Termin/Kursort		Kurssprache Deutsch
23.06.-26.06.25 Hamburg	29.09.-02.10.25 Online	
23.06.-26.06.25 Online	03.11.-06.11.25 Düsseldorf	
04.08.-07.08.25 München	03.11.-06.11.25 Online	
04.08.-07.08.25 Online	09.12.-12.12.25 Hamburg	
29.09.-02.10.25 Frankfurt	09.12.-12.12.25 Online	

Stand 15.04.2025



EXPERTeach



Inhaltsverzeichnis

SC-200T00 – Microsoft Security Operations Analyst

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 weaknesses by using Threat and Vulnerability Management in Microsoft Defender for Endpoint.

Lessons

- 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

Lab : Mitigate threats using Microsoft Defender for Endpoint

- Deploy Microsoft Defender for Endpoint
- Mitigate Attacks using Defender for Endpoint

After completing this module, students will be able to:

- Define the capabilities of Microsoft Defender for Endpoint
- Configure Microsoft Defender for Endpoint environment settings
- Configure Attack Surface Reduction rules on Windows 10 devices
- Investigate alerts in Microsoft Defender for Endpoint
- Describe device forensics information collected by Microsoft Defender for Endpoint
- Conduct forensics data collection using Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Manage automation settings in Microsoft Defender for Endpoint
- Manage indicators in Microsoft Defender for Endpoint
- Describe 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 organization's 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.

Lessons

- 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

Lab : Mitigate threats using Microsoft 365 Defender

- Mitigate Attacks with Microsoft 365 Defender

After completing this module, students will be able to:

- Explain how the threat landscape is evolving.
- Manage incidents in Microsoft 365 Defender
- Conduct advanced hunting in Microsoft 365 Defender
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.
- Define the capabilities of Microsoft Defender for Endpoint.
- Explain how Microsoft Defender for Endpoint can remediate risks in your environment.
- Define the Cloud App Security framework
- Explain how Cloud Discovery helps you see what's going on in your organization

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.

Lessons

- 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

Lab : Mitigate threats using Azure Defender

- Deploy Azure Defender

- Mitigate Attacks with Azure Defender

After completing this module, students will be able to:

- Describe Azure Defender features
- Explain Azure Security Center features
- Explain which workloads are protected by Azure Defender
- Explain how Azure Defender protections function
- Configure auto-provisioning in Azure Defender
- Describe manual provisioning in Azure Defender
- Connect non-Azure machines to Azure Defender
- Describe alerts in Azure Defender
- Remediate alerts in Azure Defender
- Automate responses in 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.

Lessons

- 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

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

- Construct Basic KQL Statements
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

After completing this module, students will be able to:

- Construct KQL statements
- Search log files for security events using KQL
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Summarize data using KQL statements
- Render visualizations using KQL statements
- Extract data from unstructured string fields using KQL
- Extract data from structured string data using KQL

- Create Functions using KQL

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.

Lessons

- 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

Lab : Configure your Azure Sentinel environment

- Create an Azure Sentinel Workspace
- Create a Watchlist
- Create a Threat Indicator

After completing this module, students will be able to:

- Identify the various components and functionality of Azure Sentinel.
- Identify use cases where Azure Sentinel would be a good solution.



ExpertTeach AG

Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch