# SC-200 zum Microsoft Certified: Security Operations Analyst Associate (Nebenberufliche Ausbildung)

## Überblick

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 die Security Operations Analysts die operative Ausgabe dieser Tools nutzt, sind sie auch wichtige Projektbeteiligte beim Konfigurieren und Bereitstellen dieser Technologien.

Nach dem Kurs können Sie die Prüfung SC-200 ablegen, um die Microsoft Certified: Security Operations Analyst Associate-Zertifizierung zu erhalten.

Dauer:
**4 Tage**

Preis:
**2.290,00 € (2.725,10 € inkl. MwSt.)**

## Kursinhalt

### SC-200 zum Microsoft Certified:  Security Operations Analyst Associate (Nebenberufliche Ausbildung)

Reduzieren von Bedrohungen mithilfe von Microsoft Defender for Endpoint

- Schutz gegen Bedrohungen mit Microsoft Defender for Endpoint
- Bereitstellen der Microsoft-Defender-for-Endpoint-Umgebung
- Implementieren von Windows-10-Sicherheitserweiterungen mit Microsoft Defender for Endpoint
- Verwalten von Alarmen und Vorfällen in Microsoft Defender for Endpoint
- Geräteuntersuchungen in Microsoft Defender for Endpoint
- Durchführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender for Endpoint
- Untersuchungen von Evidenz und Entitäten mithilfe von Microsoft Defender for Endpoint
- Konfigurieren und Verwalten der Automatisierung mithilfe von Microsoft Defender for Endpoint
- Konfigurieren von Alarmen und Entdeckungen in Microsoft Defender for Endpoint
- Bedrohungs- und Angreifbarkeitsverwaltung in Microsoft Defender for Endpoint

Reduzieren von Bedrohungen mithilfe von Microsoft 365 Defender

- Einführung in den Schutz vor Bedrohungen mit Microsoft 365
- Minimieren von Vorfällen mithilfe von Microsoft 365 Defender
- Schutz von Identitäten mit Azure AD Identity Protection
- Beseitigen von Risiken mit Microsoft Defender for Office 365
- Schutz der Umgebung mit Microsoft Defender for Identity

- Absichern von Cloudanwendungen und -diensten mit Microsoft Cloud App Security
- Antworten auf Alarme bezüglich Datenverlust mithilfe von Microsoft 365
- Verwalten von Insiderrisiken in Microsoft 365

Bedrohungen mithilfe von Azure Defender abwehren

- Planen des Schutzes von Cloudarbeitslasten mithilfe von Azure Defender
- Schutzmöglichkeiten für Cloudarbeitslasten in Azure Defender
- Verbinden von Azure-Medienobjekten mit Azure Defender
- Verbinden von Nicht-Azure-Ressourcen mit Azure Defender
- Beseitigen von Sicherheitsalarmen mithilfe von Azure Defender

Erstellen von Abfragen für Azure Sentinel mithilfe von Kusto Query Language (KQL)

- Konstruieren von KQL-Anweisungen für Azure Sentinel
- Analysieren von Abfrageergebnissen mithilfe von KQL
- Erstellen von Mehrtabellenanweisungen mithilfe von KQL
- Arbeiten mit Daten in Azure Sentinel mithilfe von Kusto Query Language

Konfiguration der Azure-Sentinel-Umgebung

- Einführung in Azure Sentinel
- Erstellen und Verwalten von Azure-Sentinel-Arbeitsräumen
- Abfragen von Logs in Azure Sentinel
- Verwenden von Watchlists in Azure Sentinel
- Verwenden von Threat Intelligence in Azure Sentinel

Verbinden von Logs mit Azure Sentinel

- Daten mithilfe von Datenkonnektoren mit Azure Sentinel verbinden
- Verbinden von Microsoft-Diensten mit Azure Sentinel
- Verbinden von Microsoft 365 Defender mit Azure Sentinel
- Verbinden von Windows-Hosts mit Azure Sentinel
- Verbinden von Common-Event-Format-Logs mit Azure Sentinel
- Verbinden von Syslogdatenquellen mit Azure Sentinel
- Verbinden von Bedrohungsindikatoren mit Azure Sentinel

Dedections erstellen und Untersuchungen mithilfe von Azure Sentinel durchführen

- Entdecken von Bedrohungen mit Azure-Sentinel-Analytik
- Antworten auf Bedrohungen mit Azure-Sentinel-Playbooks
- Verwalten von Sicherheitsvorfällen in Azure Sentinel
- Analyse des Entitätsverhaltens in Azure Sentinel
- Abfragen, Visualisieren und Überwachen von Daten in Azure Sentinel

Threat Hunting in Azure Sentinel

- Suche nach Bedrohungen mit Azure Sentinel
- Suche nach Bedrohungen mithilfe von Notebooks in Azure Sentina

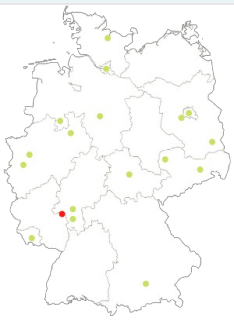
## Voraussetzungen

- Grundlegendes Verständnis von Microsoft 365
- Grundlegendes Verständnis der Sicherheits-, Compliance- und Identity Produkte von Microsoft
- Gutes Verständnis von Windows 10
- Vertrautheit mit Azure-Diensten, insbesondere Azure SQL Database und Azure Storage
- Vertrautheit mit virtuellen Maschinen und virtuellen Netzwerken in Azure
- Grundverständnis von Scripting-Konzepten

## Zielgruppe

Dieser Workshop richtet sich an Security Administratoren, System- und Netzwerkverwalter, IT- und Systemverantwortliche. Der Microsoft Security Operations Analyst arbeitet mit Stakeholdern des Unternehmens zusammen, um Informationstechnologiesysteme für das Unternehmen zu sichern.

## Ihr Weg zu uns



### Com training and services in Mainz / Wiesbaden AWMa GmbH & Co KG

Binger Straße 14 - 16
55122 Mainz
Phone: +49 6131 90705-0
Email: com@awma.de