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 TageCHF 2.855,-**
Online Training	**4 TageCHF 2.855,-**

Termin/Kursort — Kurssprache Deutsch

23.06.-26.06.25	HYHamburg	29.09.-02.10.25	HYOnline
23.06.-26.06.25	HYOnline	03.11.-06.11.25	HYDüsseldorf
04.08.-07.08.25	HYMünchen	03.11.-06.11.25	HYOnline
04.08.-07.08.25	HYOnline	09.12.-12.12.25	HYHamburg
29.09.-02.10.25	HYFrankfurt	09.12.-12.12.25	HYOnline

Stand 15.04.2025

Inhaltsverzeichnis

SC-200T00 – Microsoft Security Operations Analyst

ExperTeach AG

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