

Azure - SC-200 - Microsoft Security Operations Analyst (SC-200T00)

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 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 Security Operations Analyst die operative Ausgabe dieser Tools nutzt, ist er auch ein wichtiger Stakeholder beim Konfigurieren und Bereitstellen dieser Technologien.

Angesprochener Teilnehmerkreis:

Der Kurs richtet sich an Personen, die im Bereich Security Operations tätig sind.

Hinweis:

- Das Seminar kann auch zur Vorbereitung auf das Exam "Microsoft SC-200: Microsoft Security Operations Analyst" besucht werden. Das Bestehen dieser Prüfung ist Voraussetzung für die Zertifizierung als "Microsoft Certified: Security Operations Analyst Associate".
- Prüfungsgebühren sind nicht im Kurspreis inklusive.

Seminar- bzw. Schulungsinhalte

- Einführung in den Microsoft Defender XDR-Bedrohungsschutz
- 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 Defender XDR und Microsoft Purview Standard
- Untersuchen von Bedrohungen mithilfe der Überwachung in Microsoft Defender XDR 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 Defender XDR 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
- Reaktion auf Bedrohungen mit Microsoft Sentinel-Playbooks
- 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

Seminar- bzw. Schulungsvoraussetzungen

Dieser Kurs ist für Fortgeschrittene Anfänger konzipiert.

Seminarart

Dieses Seminar können Sie als **Präsenzseminar** oder als **Live-Online-Training** (virtuelles Präsenzseminar) buchen.

Dauer

4 Tage von 09:00 bis 16:00 Uhr

Preise

Teilnahmegebühr: ab 2.390,00 € (2.844,10 € inkl. 19% MwSt.) Preis abhängig vom Standort

Im Preis enthalten sind PC-COLLEGE - Zertifikat, Pausenverpflegung, Getränke und Kursmaterial.

Anmeldung

Bitte **online** anmelden oder per **Fax**.

Termine

Die aktuellen Termine und Standorte für Azure - SC-200 - Microsoft Security Operations Analyst (SC-200T00) finden Sie **online**.

Weitere Seminare

Alle Seminare finden Sie in unserer **Seminarübersicht**.

Gerne unterbreiten wir Ihnen auch ein individuelles Angebot entsprechend Ihrer Wünsche und Vorstellungen. Senden Sie hierfür Ihre Anfrage einfach an **training@pc-college.de**.

Erstellt am 17.05.2024

Viele Partner für ein Ziel: Beste Leistung und Rundum-Service

Live-Online-Training

Berlin
Bremen
Dortmund
Dresden
Düsseldorf
Erfurt
Essen
Frankfurt
Freiburg
Hamburg
Hannover
Jena
Karlsruhe
Kassel
Koblenz
Köln
Krefeld
Leipzig
Mannheim
München
Münster
Nürnberg
Paderborn
Regensburg
Saarbrücken
Siegen
Stuttgart
A-Wien
CH-Basel
CH-Bern
CH-Zürich



PC-COLLEGE Zentrale Berlin

Stresemannstraße 78 (Nähe Potsdamer Platz) | D-10963 Berlin
Telefon: 0800 5777 333 / +49 (0)30 235 0000 | Fax: +49 30 2142988 | E-Mail: training@pc-college.de
Ansprechpartner*in: Stefanie Wendt und Kollegen*innen

Alle Informationen und Aktionsangebote finden Sie unter www.pc-college.de