Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com
Phone: +49 (0)89 930 99 168

SC-200T00: Microsoft Security Operations Analyst

CODE:	LÄNGE:	PREIS:
MCS_SC-200T00	4 Tage	€2,290.00

Description

Lernen Sie, wie Sie mit Microsoft Azure Sentinel, Azure Defender und Microsoft 365 Defender Bedrohungen untersuchen, auf sie reagieren und sie aufspüren können. In diesem Kurs lernen Sie, wie Sie Cyber-Bedrohungen mit diesen Technologien abwehren können. Insbesondere werden Sie Azure Sentinel konfigurieren und verwenden sowie die Kusto Query Language (KQL) nutzen, um Erkennung, Analyse und Berichterstattung durchzuführen. Der Kurs wurde für Personen konzipiert, die in einer Security Operations Job-Rolle arbeiten und hilft den Lernenden bei der Vorbereitung auf die Prüfung SC-200: Microsoft Security Operations Analyst.

Lernziel

- Erklären, wie Microsoft Defender für Endpoint Risiken in Ihrer Umgebung beheben kann
- Eine Microsoft Defender for Endpoint-Umgebung erstellen
- Regeln zur Reduzierung der Angriffsfläche auf Windows 10-Geräten konfigurieren
- Aktionen auf einem Gerät mit Microsoft Defender for Endpoint durchführen
- Untersuchen von Domänen und IP-Adressen in Microsoft Defender for Endpoint
- Untersuchen von Benutzerkonten in Microsoft Defender für Endpoint
- Konfigurieren von Warneinstellungen in Microsoft Defender für Endpoint
- Erklären, wie sich die Bedrohungslandschaft weiterentwickelt
- Erweiterte Suche in Microsoft 365 Defender durchführen
- Verwalten von Vorfällen in Microsoft 365 Defender
- Erläutern, wie Microsoft Defender for Identity Risiken in Ihrer Umgebung beheben kann.
- Untersuchen Sie DLP-Warnungen in Microsoft Cloud App Security
- Erläutern Sie die Arten von Aktionen, die Sie bei einem Insider-Risikomanagementfall durchführen können.
- Konfigurieren Sie die automatische Bereitstellung in Azure Defender
- Beseitigen von Alarmen in Azure Defender
- KQL-Anweisungen konstruieren
- Filtern von Suchvorgängen 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
- Verwenden Sie KQL für den Zugriff auf die Überwachungsliste in Azure Sentinel
- Verwalten von Bedrohungsindikatoren in Azure Sentinel
- Erklären Sie die Unterschiede zwischen Common Event Format und Syslog-Connector in Azure Sentinel
- Verbinden von Azure Windows Virtual Machines mit Azure Sentinel
- Konfigurieren des Log Analytics-Agenten zum Sammeln von Sysmon-Ereignissen
- Neue Analyseregeln und Abfragen mithilfe des Assistenten für Analyseregeln erstellen
- Erstellen Sie ein Playbook, um eine Vorfallsreaktion zu automatisieren
- Verwenden Sie Abfragen, um nach Bedrohungen zu suchen
- Beobachten von Bedrohungen im Zeitverlauf mit Livestream

Zielgruppe

Der Microsoft Security Operations Analyst arbeitet mit den Stakeholdern des Unternehmens zusammen, um die Informationstechnologie-Systeme des Unternehmens zu sichern. Sein Ziel ist es, das Unternehmensrisiko zu reduzieren, indem er aktive Angriffe in der Umgebung schnell behebt, über Verbesserungen der Praktiken zum Schutz vor Bedrohungen berät und Verstöße gegen die Unternehmensrichtlinien an die entsprechenden Beteiligten weiterleitet. Zu den Aufgaben gehören das Bedrohungsmanagement, die Überwachung und die Reaktion auf Bedrohungen durch den Einsatz einer Vielzahl von Sicherheitslösungen in der gesamten Umgebung. Die Aufgabe besteht in erster Linie darin, Bedrohungen unter Verwendung von Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender und Sicherheitsprodukten von Drittanbietern zu untersuchen, auf

sie zu reagieren und nach ihnen zu fahnden. Da der Security Operations Analyst den operativen Output dieser Tools nutzt, ist er auch ein wichtiger Akteur bei der Konfiguration und Bereitstellung dieser Technologien.

Voraussetzungen

- Grundlegendes Verständnis von Microsoft 365
- Grundlegendes Verständnis der Sicherheits-, Compliance- und Identitätsprodukte von Microsoft
- Mittleres Verständnis von 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.

Inhalt

- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Create queries for Azure Sentinel using Kusto Query Language (KQL)
- Configure your Azure Sentinel environment
- Connect logs to Azure Sentinel
- Create detections and perform investigations using Azure Sentinel
- Perform threat hunting in Azure Sentinel

Test und Zertifizierung

Dieser Kurs hilft bei der Vorbereitung auf die Prüfung SC-200: Microsoft Security Operations Analyst.

Weitere Informationen

- E-BOOK - Die Original-Herstellerunterlage zu diesem Kurs erhalten Sie als digitale Kursunterlage.
- **Kostenfreie Labs für 180 Tage**
  Wow ! Das gibt's nur bei Arrow ECS Education. Nach Besuch Ihrer Schulung erhalten Sie von uns für weitere 180 Tage kostenfreien Zugang auf Ihre Lab-Umgebung!

Kurstermine

Datum	Lokation	Time Zone	Sprache	Type	Durchführungsgarantie	PREIS
13 Sep 2022	München	CEDT	German	Classroom		€2,290.00
15 Nov 2022	München	CET	German	Classroom		€2,290.00
13 Sep 2022	Virtual Classroom	CEDT	German	Instructor Led Online		€2,290.00
15 Nov 2022	Virtual Classroom	CET	German	Instructor Led Online		€2,290.00

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.