Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Freistädterstraße 236, A-4040 Linz

Email: education.ecs.at@arrow.com
Phone: +43 1 370 94 40 - 34

Microsoft Security Operations Analyst

CODE:	LÄNGE:	PREIS:
MCS_SC-200T00	32 Hours (4 Tage)	€2,300.00

Description

Erfahren Sie, wie Sie Bedrohungen mithilfe von Microsoft Azure Sentinel, Azure Defender und Microsoft 365 Defender untersuchen, darauf reagieren und nach diesen suchen.
In diesem Kurs erfahren Sie, wie Sie Cyberbedrohungen mithilfe dieser Technologien abmildern können. Insbesondere konfigurieren und verwenden Sie Azure Sentinel sowie Kusto Query Language (KQL) für Erkennung, Analyse und Berichterstellung.
Der Microsoft Security Operations Analyst arbeitet mit Unternehmensbeteiligten zusammen, um IT-Systeme für die Organisation zu sichern. Ihr Ziel ist es, das Organisationsrisiko zu verringern, indem aktive Angriffe in der Umgebung schnell behoben, Verbesserungen von Bedrohungsschutzpraktiken beraten und Verstöße gegen Organisationsrichtlinien an geeignete Stakeholder verwiesen werden.

Zielgruppe

Dieses Training richtet sich an:
Personen, die mithilfe von Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender und Sicherheitsprodukten von Drittanbietern untersuchen, reagieren und Bedrohungen jagen
Personen, die diese Tools konfigurieren, bereitstellen möchten.

Voraussetzungen

Für dieses Training werden folgende Vorkenntnisse empfohlen:
Grundlegendes Verständnis von Microsoft 365
Grundlegendes Verständnis von Microsoft-Sicherheits-, Compliance- und Identitätsprodukten
Zwischenverständnis von Windows 10
Vertrautheit mit Azure-Diensten, insbesondere Azure SQL-Datenbank und Azure Storage
Vertrautheit mit virtuellen Azure-Computern und virtuellen Netzwerken
Grundlegendes Verständnis von Skriptkonzepten.

Inhalt

Module 1: Mitigate threats using Microsoft Defender for Endpoint
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 Defen
der for Endpoint
Configure for alerts and detections in Microsoft Defender for Endpoint
Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint
Module 2: Mitigate threats using Microsoft 365 Defender
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
Module 3: Mitigate threats using Azure Defender
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
Module 4: Create queries for Azure Sentinel using Kusto Query Language (KQL)
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
Module 5: Configure your Azure Sentinel environment
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
Module 6: Connect logs to Azure Sentinel
Connect data to Azure Sentinel using data connectors
Connect Microsoft services to Azure Sentinel
Connect Microsoft 365 Defender to Azure Sentinel
Connect Windows hosts to Azure Sentinel
Connect Common Event Format logs to Azure Sentinel
Connect syslog data sources to Azure Sentinel
Connect threat indicators to Azure Sentinel
Module 7: Create detections and perform investigations using Azure Sentinel
Threat detection with Azure Sentinel analytics
Threat response with Azure Sentinel playbooks
Security incident management in Azure Sentinel
Use entity behavior analytics in Azure Sentinel
Query, visualize, and monitor data in Azure Sentinel
Module 8: Perform threat hunting in Azure Sentinel
Threat hunting with Azure Sentinel
Hunt for threats using notebooks in Azure Sentinel

Test und Zertifizierung

Wichtige Information
Dieses Training behandelt prüfungsrelevante Themen zum Examen SC-200 Microsoft Security Operations Analyst

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

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