Microsoft Security Operations Analyst (MOC SC-200)

Überblick

Dieser Kurs vermittelt den Teilnehmern, wie man mit Microsoft Sentinel, Microsoft Defender for Cloud und Microsoft 365 Defender Bedrohungen untersuchen, auf sie reagieren und sie aufspüren kann.
Zudem erfahren die Teilnehmer, wie Cyberbedrohungen mithilfe dieser Technologien abgewehrt werden können.
Insbesondere konfigurieren und verwenden die Teilnehmer Microsoft Sentinel und nutzen Kusto Query Language (KQL) zur Erkennung, Analyse und Berichterstellung.

Dauer:
4 Tage

Preis:
2.150,00 € (2.558,50 € inkl. MwSt.)

Kursinhalt

Mitigate threats using Microsoft 365 Defender

- Introduction to threat protection with Microsoft 365
- Mitigate incidents using Microsoft 365 Defender
- Remediate risks with Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Protect your identities with Azure AD Identity Protection
- Microsoft Defender for Cloud Apps
- Respond to data loss prevention alerts using Microsoft 365
- Manage insider risk in Microsoft 365

Mitigate threats using Microsoft Defender for Endpoint

- Protect against threats with Microsoft Defender for Endpoint
- Deploy the Microsoft Defender for Endpoint environment
- Implement Windows security enhancements
- Perform device investigations
- Perform actions on a device
- Perform evidence and entities investigations
- Configure and manage automation
- Configure for alerts and detections
- Utilize Threat and Vulnerability Management

Mitigate threats using Microsoft Defender for Cloud

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Workload protections in Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure resources to Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

- Construct KQL statements for Microsoft Sentinel
- Analyze query results using KQL
- Build multi-table statements using KQL
- Work with string data using KQL statements

Configure your Microsoft Sentinel environment

- Introduction to Microsoft Sentinel
- Create and manage Microsoft Sentinel workspaces
- Query logs in Microsoft Sentinel
- Use watchlists in Microsoft Sentinel
- Utilize threat intelligence in Microsoft Sentinel

Connect logs to Microsoft Sentinel

- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft 365 Defender to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

Create detections and perform investigations using Microsoft Sentinel

- Threat detection with Microsoft Sentinel analytics
- Security incident management in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks
- User and entity behavior analytics in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel

Perform threat hunting in Microsoft Sentinel

- Threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel

Voraussetzungen

- Grundlegendes Verständnis von Microsoft 365
- Grundlegendes Verständnis der Sicherheits-, Compliance- und Identity Produkte von Microsoft
- Fortgeschrittene Kenntnisse über Windows 10
- Vertrautheit mit Azure-Diensten, insbesondere Azure SQL Database und Azure Storage
- Kenntnisse im Umgang mit virtuellen Azure-Computern und virtuellen Netzwerken
- Grundverständnis von Scripting-Konzepten

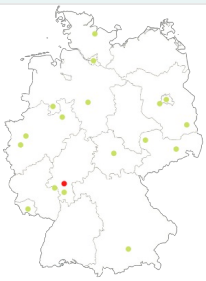
Zielgruppe

Dieser Kurs richtet sich an Security Analaysten und Security Spezialisten, die Informationstechnologiesysteme im Unternehmen sichern möchten.

Termine

Microsoft Security Operations Analyst (MOC SC-200)

Ihr Weg zu uns



Ihr Kooperationspartner in Frankfurt am Main.

Für weitere Informationen sprechen Sie uns an.

Phone: 0361 64433-95

Email: steve.liebing@com-training.com