NEXIO Online Akademie GmbH

Microsoft Security Operations Analyst (SC-200)

Sonstiges · Anbieter: NEXIO Online Akademie GmbH

FÖRDERUNG & KOSTEN

Kurspreis: 2.966 €

Förderfähig über: Bildungsgutschein

AZAV-zertifizierter Bildungsträger — Förderung durch die Agentur für Arbeit möglich

Kursdaten auf einen Blick

Durchführung	Online
Lernformat	Zeitgebunden
Dauer	4 Wochen in Vollzeit
Unterrichtssprache	Deutsch
Kursstart	Startet jede Woche
Vorkenntnisse	Keine Vorerfahrung
Abschluss	International anerkannte Microsoft®-Zertifikate (nach bestandenen Prüfungen) & trägerinterne Zertifikate bzw. Teilnahmebescheinigungen

Kurzbeschreibung

Zu deinen Aufgaben als Microsoft Security Operations Analyst gehören das Bedrohungsmanagement, die Überwachung und die Reaktion mit Hilfe einer Vielzahl von Sicherheitslösungen in der gesamten Umgebung. In dieser Rolle untersuchst, reagierst und suchst du in erster Linie nach Bedrohungen beim …

Bildungsträger & Kontakt

NEXIO Online Akademie GmbH

Am Herrschaftsweiher 11, 67071 Ludwigshafen am Rhein

Telefon: 0800 100 87 34

E-Mail: beratung@nexio-akademie.de

Web: https://nexio-akademie.de

Kurs online ansehen

01 Kursbeschreibung

Zu deinen Aufgaben als Microsoft Security Operations Analyst gehören das Bedrohungsmanagement, die Überwachung und die Reaktion mit Hilfe einer Vielzahl von Sicherheitslösungen in der gesamten Umgebung. In dieser Rolle untersuchst, reagierst und suchst du in erster Linie nach Bedrohungen beim Umgang mit Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender und Sicherheitsprodukten von Drittanbietern. Da du als Analyst für Sicherheitsoperationen die Betriebsleistung dieser Tools nutzt, bist du auch ein wichtiger Interessenvertreter bei der Konfiguration und Bereitstellung dieser Technologien.

02 Lehrplan & Module

1. Mitigate threats using Microsoft 365 Defender

Du nutzt Microsoft 365 Defender, um Bedrohungen über E-Mail, Identitäten, Endgeräte und Cloud-Apps hinweg zu erkennen. Dabei untersuchst du Vorfälle in der zentralen Konsole und setzt automatisierte Reaktionen ein.

2. Mitigate threats using Microsoft Defender for Endpoint

Mit Microsoft Defender for Endpoint schützt du Arbeitsstationen und Server. Du konfigurierst die Umgebung, analysierst Gerätezeitachsen und führst Reaktionsmaßnahmen wie Isolierung oder Untersuchungspakete durch.

3. Wissen zu den Funktionen von Microsoft-Sicherheitslösungen

Du ordnest die Sicherheitslösungen von Microsoft in ein Gesamtbild ein und verstehst ihr Zusammenspiel im Security Operations Center. So erkennst du, welche Datenquellen welche Bedrohungen sichtbar machen.

4. Mitigate threats using Azure Defender

Behandelt wird der Schutz von Cloud- und Hybrid-Workloads mit Azure Defender, heute Microsoft Defender for Cloud. Du verbindest Ressourcen, bewertest Empfehlungen und reagierst auf Warnungen.

5. Create queries for Azure Sentinel using Kusto Query Language

Du schreibst Abfragen in der Kusto Query Language, um Protokolldaten in Azure Sentinel zu filtern, zusammenzufassen und zu verknüpfen. Diese Abfragen nutzt du für Analysen, Analyseregeln und Threat Hunting.

6. Configure your Azure Sentinel environment

Du richtest einen Azure Sentinel Arbeitsbereich ein, bindest Datenquellen über Connectoren an und erstellst Analyseregeln. Mit Playbooks automatisierst du die Reaktion auf erkannte Vorfälle.

7. Vorbereitung auf die externe Prüfung

Du wiederholst die Prüfungsinhalte der SC-200 und bearbeitest praxisnahe Testfragen. Außerdem lernst du den Ablauf der Zertifizierungsprüfung kennen.

03 Enthaltene Zertifikate

Trägerzertifikat: International anerkannte Microsoft®-Zertifikate (nach bestandenen Prüfungen) & trägerinterne Zertifikate bzw. Teilnahmebescheinigungen

04 Voraussetzungen

Vorkenntnisse

Niveau: Keine Vorerfahrung

Teilnehmende müssen über gute Deutschkenntnisse verfügen und im Umgang mit Windows geübt sein. Da die Maßnahme mit englischer Doku durchgeführt wird, sind außerdem gute Englischkenntnisse wichtig.

05 Zielgruppen & Berufsperspektiven

- Arbeitssuchende

Mögliche Berufsbilder: SOC Analyst, Security Operations Engineer, Incident Response Analyst

NÄCHSTER SCHRITT

Kursdetails online ansehen und Anbieter kontaktieren

NEXIO Online Akademie GmbH · Am Herrschaftsweiher 11, 67071 Ludwigshafen am Rhein
0800 100 87 34 · beratung@nexio-akademie.de · https://nexio-akademie.de

Online ansehen