NEXIO Online Akademie GmbH

Cybersecurity und MS-Security Administration

IT-Sicherheit / Cybersecurity · Anbieter: NEXIO Online Akademie GmbH

FÖRDERUNG & KOSTEN

Kurspreis: 11.660 €

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

Kursdaten auf einen Blick

Durchführung	Online
Lernformat	Zeitgebunden
Dauer	16 Wochen in Vollzeit
Unterrichtssprache	Deutsch
Kursstart	Startet jede Woche
Vorkenntnisse	Grundlegende Kenntnisse
Abschluss	International anerkanntes CompTIA®-Zertifikat (nach bestandener Prüfung) & International anerkanntes Microsoft®-Zertifikat (nach bestandener Prüfung) & trägerinternes Zertifikat bzw. Teilnahmebescheinigung

Kurzbeschreibung

Direkt nach der Ausbildung den nächsten Karriereschritt gehen und Future Skills aufbauen: Diese Weiterbildung richtet sich an Nachwuchstalente, die hybride Serverstrukturen verstehen, sicher betreiben und mit international anerkannten Zertifizierungen Ihre Employability sichtbar steigern wollen. Wer …

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

Direkt nach der Ausbildung den nächsten Karriereschritt gehen und Future Skills aufbauen: Diese Weiterbildung richtet sich an Nachwuchstalente, die hybride Serverstrukturen verstehen, sicher betreiben und mit international anerkannten Zertifizierungen Ihre Employability sichtbar steigern wollen. Wer etwa als Fachinformatiker:in für Systemintegration startet, gewinnt damit schnell Verantwortung im Betrieb und in Projekten - mit einem Kompetenzprofil, das Praxisnähe und strategische Weitsicht vereint. Mit CompTIA Security legst Du ein herstellerneutrales Fundament für ganzheitliche IT-Sicherheit über Netzwerk, Endpoint, Cloud und Zero-Trust-Ansätze hinweg. Du wendest aktuelle Konzepte wie Firewall as a Service (FWaaS) und Security Automation an, um Risiken früher zu erkennen, Angriffsflächen zu reduzieren und Sicherheitsmaßnahmen messbar zu verankern. Microsofts Security, Compliance and Identity Fundamentals stärkt Dein Verständnis für Sicherheits-, Compliance- und Identitätsgrundlagen in Microsoft-Umgebungen und verbindet Geschäftsanforderungen mit technischer Umsetzung. Du ordnest Dienste und Konzepte wie Identity- and Access-Management-Systeme - IAMS, Datenklassifizierung, Bedrohungsschutz und Cloud-Modelle einschließlich Serverless Computing richtig ein und sprichst dadurch die Sprache von IT und Fachbereichen. Als Identity and Access Administrator vertiefst Du das Design und den Betrieb skalierbarer Identitätslösungen mit Single Sign-on, Bedingtem Zugriff und durchgängigen Berechtigungsprozessen über den gesamten User-Lifecycle. Du sicherst Identitäten in IAMS konsistent ab, etablierst Governance und gestaltest Rechtevergabe über Self-Service in Service-Portale und Apps nutzerfreundlich sowie revisionssicher. Im Zertifizierungspfad zum Security Operations Analyst analysierst und bearbeitest Du Sicherheitsvorfälle über SIEM und SOAR, nutzt Security Automation in Playbooks und arbeitest mit User and Entity Behavior Analytics zur Erkennung anomaler Aktivitäten. KI-gestütztes Wissensmanagement unterstützt Dich bei der Priorisierung, Anreicherung und Dokumentation von Alerts, sodass Entscheidungen schneller, fundierter und auditierbar werden. So verbindest Du direkt nach der Ausbildung praxisnahe Hands-on-Kompetenz mit gefragten Future Skills und positionierst Dich als gesuchte Nachwuchskraft für IT-Betrieb, Security und Cloud - mit Zertifikaten, die international anerkannt sind und Deine Entwicklung dauerhaft beschleunigen.

02 Lehrplan & Module

1. Cybersecurity- & Cloud-Security-Fundamentals

Du lernst die Grundprinzipien der Informationssicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit kennen. Zudem beschäftigst Du Dich mit dem Modell der geteilten Verantwortung und typischen Bedrohungen in Cloud-Umgebungen.

2. Identity and Governance

Du lernst Konzepte der Identitätsverwaltung und Governance in Microsoft-Umgebungen kennen, etwa Rollen, Richtlinien und Zugriffskontrollen. Außerdem erfährst Du, wie Compliance-Anforderungen technisch umgesetzt werden.

3. Verschlüsselungstechnologien

Du lernst symmetrische und asymmetrische Verschlüsselung, Hashverfahren und Zertifikate kennen. Dabei setzt Du Verschlüsselung für Daten im Ruhezustand und bei der Übertragung ein.

4. Networksecurity

Du sicherst Netzwerke durch Segmentierung, Zugriffslisten und sichere Protokolle ab. Außerdem lernst Du, Angriffe auf Netzwerkebene zu erkennen und abzuwehren.

5. System and Cloud Monitoring

Du richtest Monitoring für Systeme und Cloud-Ressourcen ein und wertest Protokolle und Metriken aus. So erkennst Du Auffälligkeiten und Sicherheitsvorfälle frühzeitig.

6. Business Continuity & Security-Audits

Du lernst, wie Notfall- und Wiederanlaufpläne den Geschäftsbetrieb bei Störungen sichern. Außerdem erfährst Du, wie Sicherheitsaudits geplant, durchgeführt und dokumentiert werden.

7. Firewallsysteme und FWaaS-Implementierungen

Du lernst Funktionsweise und Typen von Firewalls kennen, von Paketfiltern bis zu Next-Generation-Firewalls. Zusätzlich implementierst und konfigurierst Du Firewall-as-a-Service in Cloud-Umgebungen.

8. Security Automation

Du automatisierst wiederkehrende Sicherheitsaufgaben mit Skripten, Playbooks und Workflows. So reagierst Du schneller und einheitlicher auf Sicherheitsereignisse.

9. Identity- and Access-Management-Systems IAMS

Du lernst den Aufbau von Identity- und Access-Management-Systemen kennen. Mehrfaktor-Authentifizierung, Single Sign-on, bedingter Zugriff und das Prinzip der minimalen Rechte stehen dabei im Mittelpunkt.

10. User and Entity Behaviour Analytics

Du erfährst, wie User and Entity Behaviour Analytics ungewöhnliches Verhalten von Benutzern und Geräten erkennt. Dabei lernst Du, Warnmeldungen zu bewerten und echte Bedrohungen von Fehlalarmen zu unterscheiden.

11. Microsoft Purview & Sentinel

Du arbeitest mit Microsoft Purview für Datenklassifizierung, Informationsschutz und Compliance. Mit Microsoft Sentinel sammelst und analysierst Du Sicherheitsereignisse als SIEM- und SOAR-Lösung.

12. Azure Defender for Cloud and Endpoin

Du nutzt Microsoft Defender for Cloud, um den Sicherheitsstatus von Cloud-Ressourcen zu bewerten und zu verbessern. Mit Defender for Endpoint schützt Du Endgeräte und reagierst auf erkannte Angriffe.

13. Hybrid-Cloud Security

Du lernst, Sicherheitsrichtlinien über lokale Rechenzentren und Cloud-Umgebungen hinweg einheitlich umzusetzen. Dazu gehören hybride Identitäten, Netzwerkanbindung und zentrales Sicherheitsmanagement.

14. Remote-Access Security

Du sicherst den Fernzugriff auf Unternehmensressourcen ab, etwa mit VPN, Zero-Trust-Ansätzen und bedingtem Zugriff. Außerdem bewertest Du Risiken mobiler und privater Endgeräte.

15. Security posture management

Du lernst, die Sicherheitslage einer IT-Umgebung kontinuierlich zu bewerten und zu verbessern. Mit Sicherheitsbewertungen, Empfehlungen und Priorisierung von Maßnahmen reduzierst Du Schwachstellen systematisch.

03 Enthaltene Zertifikate

Trägerzertifikat: International anerkanntes CompTIA®-Zertifikat (nach bestandener Prüfung) & International anerkanntes Microsoft®-Zertifikat (nach bestandener Prüfung) & trägerinternes Zertifikat

bzw. Teilnahmebescheinigung

04 Voraussetzungen

Vorkenntnisse

Niveau: Grundlegende Kenntnisse

Vorausgesetzt werden gute Deutschkenntnisse auf dem Mindestniveau von A2. Aufgrund der Lerncenterumgebung empfehlen wir vielmehr B2, da die Lernenden dem Unterricht nicht nur aktiv folgen, sondern aktiv partizipieren können müssen. Englischkenntnisse auf dem Niveau B2 müssen vorhanden sein, da die Dokumentationen, die Übungsumgebungen, sowie die Prüfungen in Englisch gehalten sind. Fundierte Expertenkenntnisse im Umgang mit PC-Systemen generell, sowie im Bereich der Netzwerktechnik, sind zwingend erforderlich. Eine Ausbildung in diesem Bereich (z. B. Fachinformatiker - Systemintegration o. ä.), bzw. ein Studium sind nicht zwingend notwendig, jedoch von Vorteil.

05 Zielgruppen & Berufsperspektiven

- Arbeitssuchende

Mögliche Berufsbilder: IT-Sicherheitsadministrator, Cloud Security Engineer, IT-Security Engineer

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