NEXIO Online Akademie GmbH

Cloud-Security-Expert:in

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

FÖRDERUNG & KOSTEN

Kurspreis: 0 €

Förderfähig über: Bildungsgutschein

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 jeden Monat
Vorkenntnisse	Grundlegende Kenntnisse
Abschluss	Internationales Zertifikat AWS (nach bestandener Prüfung) und trägerinternes Zertifikat bzw. Teilnahmebescheinigung

Kurzbeschreibung

In diesem viermonatigen Kurs bauen Sie eine fundierte Expertise im Bereich Cloud-Security auf und qualifizieren sich für anspruchsvolle Sicherheitsrollen in Cloud-Umgebungen. Sie lernen, sichere Cloud-Architekturen zu entwerfen, Bedrohungen frühzeitig zu erkennen und auf …

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

In diesem viermonatigen Kurs bauen Sie eine fundierte Expertise im Bereich Cloud-Security auf und qualifizieren sich für anspruchsvolle Sicherheitsrollen in Cloud-Umgebungen. Sie lernen, sichere Cloud-Architekturen zu entwerfen, Bedrohungen frühzeitig zu erkennen und auf Sicherheitsvorfälle strukturiert zu reagieren. Im Mittelpunkt stehen die zentralen Handlungsfelder der Cloud-Security: Threat Detection und Incident Response, Security Logging und Monitoring, Infrastruktur- und Netzwerk-Sicherheit, Identitäts- und Zugriffsverwaltung sowie Datenschutz und Verschlüsselung. Ergänzend erarbeiten Sie sich Kenntnisse in Compliance, Governance, Sicherheits-Automatisierung sowie Grundlagen der Generative-AI/ML-Security.

02 Lehrplan & Module

1. Sicherheitsbedrohungsmodelle und Risikomanagement

Du lernst, Bedrohungsmodelle wie STRIDE auf Cloud-Architekturen anzuwenden und Risiken systematisch zu bewerten. Darauf aufbauend leitest du Schutzmaßnahmen ab und priorisierst sie nach Eintrittswahrscheinlichkeit und Schadenshöhe.

2. Threat Detection und Incident Response

Im Fokus steht das Erkennen verdächtiger Aktivitäten in AWS-Umgebungen mit Diensten wie GuardDuty und Security Hub. Du übst außerdem, Sicherheitsvorfälle strukturiert einzudämmen, zu analysieren und nachzubereiten.

3. Security Logging und Monitoring

Du richtest zentrale Protokollierung mit CloudTrail, CloudWatch und VPC Flow Logs ein und wertest die Daten gezielt aus. Dabei geht es auch um Alarmierung, Aufbewahrungsfristen und die Integrität von Logdaten.

4. Infrastructure Security und Netzwerk-Sicherheit

Behandelt werden sichere Netzwerkarchitekturen mit VPCs, Subnetzen, Security Groups und Network ACLs. Du lernst zudem, Workloads mit Firewalls, WAF und DDoS-Schutz abzusichern.

5. Identity and Access Management (IAM)

Du konfigurierst Benutzer, Rollen und Richtlinien nach dem Prinzip der minimalen Rechtevergabe. Themen sind außerdem Föderation, Multi-Faktor-Authentifizierung und die Verwaltung von Berechtigungen über mehrere Konten hinweg.

6. Data Protection und Verschlüsselung

Hier lernst du, Daten im Ruhezustand und bei der Übertragung zu verschlüsseln und Schlüssel mit KMS sicher zu verwalten. Ebenso behandelt werden Zertifikatsverwaltung, Secrets Management und die Klassifizierung sensibler Daten.

7. Security Operations

Du lernst, den laufenden Sicherheitsbetrieb zu organisieren, etwa durch Schwachstellenmanagement, Patch-Prozesse und automatisierte Sicherheitsprüfungen. Auch die Zusammenarbeit von Betriebs- und Sicherheitsteams wird betrachtet.

8. Compliance- und Governance-Aspekte

Im Mittelpunkt stehen regulatorische Anforderungen, Sicherheitsrichtlinien und deren technische Durchsetzung in der Cloud. Du setzt Werkzeuge wie AWS Config und Organizations ein, um Compliance kontinuierlich zu überwachen.

9. Backup- und Disaster-Recovery-Kontrollen

Du planst Backup-Strategien und Wiederherstellungsverfahren für Cloud-Workloads und definierst Ziele wie RPO und RTO. Zudem prüfst du, wie Sicherungen gegen Manipulation und Verlust geschützt werden.

03 Enthaltene Zertifikate

Trägerzertifikat: Internationales Zertifikat AWS (nach bestandener Prüfung) und trägerinternes Zertifikat bzw. Teilnahmebescheinigung

04 Voraussetzungen

Vorkenntnisse

Niveau: Grundlegende Kenntnisse

Vorausgesetzt werden angemessene Deutschkenntnisse in Wort und Schrift (Niveau B1) sowie Englischkenntnisse in Wort und Schrift (Niveau B2). Außerdem sind Grundlagen und Vorkenntnisse in IT-Sicherheit und in der Nutzung von AWS-Cloud-Services erforderlich. Zusätzlich empfohlenes Wissen: ein vorhandenes AWS Associate- oder Professional-Zertifikat. Dieses Zertifikat richtet sich bewusst an ambitionierte Lernende mit umfassenden IT-Vorkenntnissen und Sicherheitserfahrung.

05 Zielgruppen & Berufsperspektiven

- Arbeitssuchende

Mögliche Berufsbilder: Cloud Security Engineer, Cloud Security Architect

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