NEXIO Online Akademie GmbH

Cybersicherheit für IT-Profis: Vom Risiko zur Resilienz mit der CompTIA Security+ Zertifizierung

Sonstiges · Anbieter: NEXIO Online Akademie GmbH

FÖRDERUNG & KOSTEN

Kurspreis: 5.932 €

Förderfähig über: Bildungsgutschein

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

Kursdaten auf einen Blick

Durchführung	Online
Lernformat	Zeitgebunden
Dauer	8 Wochen in Vollzeit
Unterrichtssprache	Deutsch
Kursstart	Startet jede Woche
Vorkenntnisse	Grundlegende Kenntnisse
Abschluss	International anerkanntes CompTIA®-Zertifikat (nach bestandener Prüfung) & trägerinternes Zertifikat bzw. Teilnahmebescheinigung

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

Erweitere deinen beruflichen Horizont und steige mit der Zertifizierung CompTIA Security+ in die Welt der Cybersicherheit ein! Diese Zertifizierung vermittelt dir umfassende Kenntnisse über Sicherheitsprotokolle, Bedrohungsanalysen und Schutzmaßnahmen und ist ideal für IT-Profis, die ihre Fähigkeiten in der Cybersicherheit ausbauen möchten. Mit CompTIA Security+ wirst du zum Experten in der Identifizierung und Bekämpfung von Sicherheitsbedrohungen und kannst deine strategischen Fähigkeiten unter Beweis stellen. Diese Zertifizierung ist perfekt für IT-Experten, die sich als führende Spezialisten in der IT-Sicherheit positionieren möchten. Werde Teil der Zukunft der IT-Administration mit der Zertifizierung CompTIA Security+!

02 Lehrplan & Module

1. Grundlagen der Cybersicherheit

Du lernst die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sowie grundlegende Sicherheitskonzepte wie Defense in Depth und Least Privilege kennen. Außerdem verstehst du, wie Bedrohungen, Schwachstellen und Risiken zusammenhängen.

2. Rechtliche Grundlagen

Du erhältst einen Überblick über rechtliche Rahmenbedingungen wie DSGVO, BDSG und das IT-Sicherheitsgesetz. Dazu gehören Pflichten bei Sicherheitsvorfällen sowie die Bedeutung von Compliance und Richtlinien im Unternehmen.

3. Verschlüsselungstechnologien

Du lernst symmetrische und asymmetrische Verschlüsselung, Hashfunktionen und digitale Signaturen kennen. Ebenso verstehst du, wie Zertifikate und Public-Key-Infrastrukturen sichere Kommunikation ermöglichen.

4. Identitäten und Governance

Du beschäftigst dich mit Identitäts- und Zugriffsmanagement, Authentifizierungsverfahren wie Multi-Faktor-Authentifizierung und Rollenmodellen. Zudem lernst du, wie Governance-Prozesse Berechtigungen nachvollziehbar steuern.

5. Physische Sicherheit und Angriffsvektoren

Du lernst Maßnahmen der physischen Sicherheit wie Zutrittskontrolle und Überwachung kennen. Darüber hinaus analysierst du Angriffsvektoren wie Social Engineering, Phishing und manipulierte Hardware.

6. Systemsicherheitskonfigurationen

Du härtest Betriebssysteme und Anwendungen durch sichere Grundkonfigurationen, Patch-Management und das Abschalten unnötiger Dienste. Endpoint-Schutz und Konfigurationsrichtlinien gehören ebenfalls dazu.

7. Sicherheit für mobile Systeme

Du lernst Risiken mobiler Endgeräte kennen und setzt Schutzmaßnahmen wie Mobile Device Management, Verschlüsselung und App-Kontrolle um. Auch Betriebsmodelle wie BYOD werden aus Sicherheitssicht betrachtet.

8. Informationssicherheit und Datensicherheit

Du klassifizierst Informationen nach Schutzbedarf und setzt passende Maßnahmen wie Zugriffskontrolle, Verschlüsselung und Data Loss Prevention ein. Dabei lernst du, Daten über ihren gesamten Lebenszyklus zu schützen.

9. Sicherheit für Netzwerke

Du sicherst Netzwerke durch Segmentierung, sichere Protokolle und Zugangskontrollen ab. Dazu gehören auch Komponenten wie Proxy, IDS und IPS sowie Konzepte wie Zero Trust.

10. Schwachstellen und Angriffsarten

Du lernst gängige Angriffsarten wie Malware, Denial of Service, Injection-Angriffe und Man-in-the-Middle kennen. Außerdem führst du Schwachstellenanalysen durch und bewertest Ergebnisse nach ihrer Kritikalität.

11. Der sichere Remote-Zugriff

Du richtest sichere Fernzugriffe über VPN, verschlüsselte Protokolle wie SSH und abgesicherte Remote-Desktop-Verbindungen ein. Dabei berücksichtigst du Authentifizierung, Protokollierung und Zugriffsbeschränkungen.

12. Drahtlose Netzwerke sicher gestalten

Du lernst WLAN-Sicherheitsstandards wie WPA2 und WPA3 sowie Authentifizierung über 802.1X kennen. Typische Angriffe auf Funknetze wie Rogue Access Points erkennst du und leitest Gegenmaßnahmen ab.

13. System- und Netzwerküberwachung

Du überwachst Systeme und Netzwerke mit Protokollen, Logauswertung und SIEM-Lösungen. So erkennst du Auffälligkeiten frühzeitig und leitest Maßnahmen im Rahmen des Incident Response ein.

14. Firewallsysteme und Netzwerkanalysen

Du lernst Firewall-Typen und Regelwerke kennen und konfigurierst Paketfilter sowie zustandsbehaftete Firewalls. Mit Werkzeugen zur Netzwerkanalyse untersuchst du Datenverkehr und deckst Sicherheitsprobleme auf.

15. Business Continuity und Security-Audits

Du entwickelst Notfall- und Wiederanlaufpläne, um den Geschäftsbetrieb bei Störungen aufrechtzuerhalten. Außerdem lernst du, wie Sicherheitsaudits geplant, durchgeführt und dokumentiert werden.

03 Enthaltene Zertifikate

Trägerzertifikat: International anerkanntes CompTIA®-Zertifikat (nach bestandener Prüfung) & trägerinternes Zertifikat bzw. Teilnahmebescheinigung

04 Voraussetzungen

Vorkenntnisse

Niveau: Grundlegende Kenntnisse

Vorausgesetzt werden gute Deutschkenntnisse auf dem Mindestniveau von B2. Englischkenntnisse auf dem Niveau B2 sind notwendig, da die Zertifizierungsprüfung in Englisch stattfindet. Zwingend erforderlich sind fundierte Kenntnisse im Umgang mit PC-Systemen generell sowie im Bereich der Netzwerktechnik. Eine Ausbildung in diesem Bereich (z. B. als Fachinformatiker:in - Systemintegration o. ä.) bzw. ein Studium sind nicht zwingend notwendig, jedoch von Vorteil.

05 Zielgruppen & Berufsperspektiven

- Arbeitssuchende

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

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