Team Bildungsberatung
beratung@smartbuilding.pro
0800 5770577
Mo. - Fr. von 8 bis 17 Uhr kostenfrei aus allen deutschen Netzen.

Kursstart alle 4 Wochen

IT-Cybersecurity-Analyst (CompTIA CySA+) mit IT-Security-Beauftragte:r

Nach dem Kurs kannst du Tools zur Erkennung von Bedrohungen konfigurieren und verwenden und Datenanalysen durchführen. Außerdem vermittelt der Lehrgang organisatorische und technische Sicherheitsmaßnahmen im Bereich IT-Security sowie den Einsatz von Künstlicher Intelligenz in deinem Beruf.

Abschlussart
Zertifikat „CompTIA CySA+“
Zertifikat „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation“

Abschlussprüfung
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
CompTIA CySA+ Zertifizierungsprüfung CS0-003 (in englischer Sprache)
IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation

Dauer
8 Wochen

Unterrichtszeiten
Montag bis Freitag von 8:30 bis 15:35 Uhr
(in Wochen mit Feiertagen von 8:30 bis 17:10 Uhr)

Nächste Kursstarts
14.10.2024
11.11.2024
09.12.2024

LEHRGANGSZIEL

Nach dem Lehrgang bist du in der Lage, Tools zur Erkennung von Bedrohungen und Schwachstellen, die Software- und Systemsicherheit gewährleisten, zu konfigurieren und zu verwenden sowie Anwendungen und Systeme innerhalb eines Unternehmens abzusichern und zu schützen.

Des Weiteren kennst du als IT-Sicherheitsbeauftragte:r die wesentlichen Aspekte und Anforderungen der IT-Sicherheit: Datensicherheit und -schutz, physische IT-Sicherheit, Kryptographie, Netzsicherheit, PKI, Computersicherheit und organisatorische Sicherheit. Du weißt, die relevanten Standards nach ISO/IEC 27001 und des IT-Grundschutzes nach BSI in der Praxis umzusetzen.

ZIELGRUPPE

IT-Fachleute, Datenbank- und Netzwerkfachleute, (Fach-)Informatiker:innen, Programmierer:innen und Personen mit praktischer Erfahrung im IT-Bereich (auch Quereinsteiger:innen).

BERUFSAUSSICHTEN

Mit den gestiegenen Anforderungen an die IT-Infrastruktur spielt die IT-Sicherheit eine zunehmende Schlüsselrolle in Unternehmen. Mit CompTIA CySA+ erlangst du eine herstellerübergreifende, weltweit anerkannte Zertifizierung, mit der du deine beruflichen Perspektiven in der IT-Branche verbessern und dein Fachwissen aussagekräftig nachweist. IT-Sicherheitsanalytiker:innen, die Cybersicherheitsressourcen analysieren, überwachen und schützen können sind stark gefragt und kommen sowohl direkt bei IT-Sicherheitsdienstleistern, aber auch Inhouse bei Unternehmen aller Branchen zum Einsatz.

Zudem werden IT-Security-Beauftragte werden in Unternehmen aller Branchen eingesetzt, um einen sicheren und zuverlässigen IT-Betrieb zu gewährleisten.

VORAUSSETZUNGEN

Die Prüfungen Network+, Security+ oder gleichwertige Kenntnisse und mindestens 4 Jahre praktische Erfahrung als Incident Response Analyst oder Security Operations Center (SOC) Analyst oder gleichwertige Erfahrung sowie gute Englisch-Kenntnisse für die CompTIA-Zertifizierungsprüfung werden vorausgesetzt.

LEHRGANGSINHALTE

IT-CYBERSECURITY-ANALYST MIT COMPTIA-ZERTIFIZIERUNG CYSA+

Sicherheitsoperationen (ca. 5 Tage)
System- und Sicherheitslösungen für die Infrastruktur
Netzwerk-, Host- und anwendungsbezogene Sicherheitsanalyse
Maßnahmen und Tools zur Risikominimierung
Threat-Intelligence, Threat-Hunting
Prozessverbesserung und Automatisierung

Künstliche Intelligenz (KI) im Arbeitsprozess
Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Vulnerability Management (ca. 4,5 Tage)
Schwachstellenbewertung
Analyse und Interpretation von Schwachstellenberichten
Priorisierung von Schwachstellen
Maßnahmen zur Behandlung von Angriffen und Schwachstellen

Incident Response Management (ca. 3 Tage)
Prozessmodell und Lebenszyklus
IoCs (Indicators of Compromise)
Exkurs: Forensische Analyse

Berichterstattung und Kommunikation (ca. 2,5 Tage)
Berichterstattung zum Schwachstellenmanagement und Compliance
Stakeholder-Kommunikation
Key Performance Indicators (KPIs)

Projektarbeit/Fallstudie, Zertifizierungsvorbereitung und Zertifizierungsprüfung (ca. 5 Tage)
CompTIA CySA+ CS0-003 (in englischer Sprache)

IT-SECURITY-BEAUFTRAGTE:R MIT TÜV RHEINLAND GEPRÜFTER QUALIFIKATION

Aufbau und Kernprozesse der IT-Sicherheit (ca. 2 Tage)
Struktur der IT-Security in Unternehmen und deren wirtschaftliche Bedeutung
Beteiligte Personen, Funktionen und Kommunikationswege innerhalb des IT-Netzwerks
Grundlegende Vorschriften, rechtliche Grundsätze, Normen

Physische Sicherheit im IT-Umfeld (ca. 2 Tage)
Klassifizierung der physikalischen Sicherheit
Einführung in die physischen Gefahrennormen
Sicherheitsmaßnahmen für die IT-Infrastruktur
Kontroll- und Alarmierungsmechanismen

Künstliche Intelligenz (KI) im Arbeitsprozess
Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Identity- und Access-Management (ca. 2 Tage)
Grundlagen des Access-Managements
Unterscheidung und Spezifizierung der Zutritts-, Zugangs- und Zugriffkontrollen in einem Unternehmen sowie deren Umsetzung
Konzeption und Kontrolle im Accessmanagement
Revisionssichere Archivierung
Identitätsprüfung und Rechtezuweisung
Schutzmechanismen für die IT-Infrastruktur

Bedrohungsszenarien und Konsequenzen für die Umsetzung im Unternehmen (ca. 3 Tage)
DLP – die Bedeutung von Data Loss Prevention und Data Leakage Prevention in der IT-Security
Maßnahmen der Data Loss Prevention und Data Leakage Prevention
Klassifizierung und Schutz vor Schadprogrammen
IOT (Internet Of Things) und Industrie 4.0 – mögliche Bedrohungsszenarien

Network-Security (ca. 2 Tage)
Besondere Maßnahmen für den Schutz des Netzwerkes
Datenschutzanforderungen an Mailserver
Verwaltung und Sicherheit bei Cloud-Nutzung
Prüfung der Systembestandteile und -anwendungen gegenüber unautorisierten Personen/Programmen/Fernzugriffen

Analyse und Realisierung eines IT-Sicherheitssystems für Unternehmen (ca. 2 Tage)

Grundlagen des Informationssicherheitsstandards nach ISO/IEC 27001:2022 sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) (ca. 2 Tage)

Struktur und Umsetzung des Notfallmanagements nach BSI-Standard 100-4 und 200-4 (BCM) (ca. 1 Tag)

IT-Sicherheit im Unternehmen – Trainings und Sensibilisierung für Mitarbeiter:innen (ca. 1 Tag)

Projektarbeit, Zertifizierungsvorbereitung und Zertifizierungsprüfung „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation" (ca. 3 Tage)

UNTERRICHTSKONZEPT

Didaktisches Konzept

Deine Dozierenden sind sowohl fachlich als auch didaktisch hoch qualifiziert und werden dich vom ersten bis zum letzten Tag unterrichten (kein Selbstlernsystem).
Du lernst in effektiven Kleingruppen. Die Kurse bestehen in der Regel aus 6 bis 25 Teilnehmenden. Der allgemeine Unterricht wird in allen Kursmodulen durch zahlreiche praxisbezogene Übungen ergänzt. Die Übungsphase ist ein wichtiger Bestandteil des Unterrichts, denn in dieser Zeit verarbeitest du das neu Erlernte und erlangst Sicherheit und Routine in der Anwendung. Im letzten Abschnitt des Lehrgangs findet eine Projektarbeit, eine Fallstudie oder eine Abschlussprüfung statt.

Virtueller Klassenraum alfaview®

Der Unterricht findet über die moderne Videotechnik alfaview® statt - entweder bequem von zu Hause oder bei uns im Bildungszentrum. Über alfaview® kann sich der gesamte Kurs face-to-face sehen, in lippensynchroner Sprachqualität miteinander kommunizieren und an gemeinsamen Projekten arbeiten. Du kannst selbstverständlich auch deine zugeschalteten Trainer:innen jederzeit live sehen, mit diesen sprechen und du wirst während der gesamten Kursdauer von deinen Dozierenden in Echtzeit unterrichtet. Der Unterricht ist kein E-Learning, sondern echter Live-Präsenzunterricht über Videotechnik.

FÖRDERMÖGLICHKEITEN

Alle Lehrgänge werden von der Agentur für Arbeit gefördert und sind nach der Zulassungsverordnung AZAV zertifiziert. Bei der Einreichung eines Bildungsgutscheines oder eines Aktivierungs- und Vermittlungsgutscheines werden in der Regel die gesamten Lehrgangskosten von Ihrer Förderstelle übernommen.
Eine Förderung ist auch über den Europäischen Sozialfonds (ESF), die Deutsche Rentenversicherung (DRV) oder über regionale Förderprogramme möglich. Als Zeitsoldat:in besteht die Möglichkeit, Weiterbildungen über den Berufsförderungsdienst (BFD) zu besuchen. Auch Firmen können ihre Mitarbeiter:innen über eine Förderung der Agentur für Arbeit (Qualifizierungschancengesetz) qualifizieren lassen.

ⓘ Änderungen möglich. Die Lehrgangsinhalte werden regelmäßig aktualisiert. Die aktuellen Lehrgangsinhalte findest Du immer unter smartbuilding.alfatraining.de.