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

Kursstart alle 4 Wochen

IT-Security-Spezialist:in mit Microsoft Information Protection Administration

Du verfügst über Fachwissen in den wesentlichen Informationssicherheitsstandards, der Netzwerksicherheit und dem Einsatz von Künstlicher Intelligenz (KI). Ebenso erwirbst du Fähigkeiten zum Sichern eines Netzwerks sowie zur Abwehr von Hackerangriffen und kennst mögliche Bedrohungen. Du verfügst zusätzlich über das original Microsoft-Zertifikat „Microsoft Certified: Information Protection and Compliance Administrator Associate".

Abschlussart
Zertifikat „IT-Security-Spezialist:in"
Original Microsoft-Zertifikat „Microsoft Certified: Information Protection and Compliance Administrator Associate"

Abschlussprüfung
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
CompTIA Security+ Zertifizierungsprüfung SY0-701 (in englischer Sprache)
CompTIA CySA+ Zertifizierungsprüfung CS0-003 (in englischer Sprache)
IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation
Microsoft-Zertifizierungsprüfung SC-400: Microsoft Information Protection and Compliance Administrator

Dauer
16 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

Du kennst die entscheidenden Aspekte und Anforderungen der IT-Sicherheit und verfügst über Fachwissen in den wesentlichen Grundsätzen der Netzwerksicherheit und im Risikomanagement, über die Fähigkeiten zum Sichern eines Netzwerks und zur Abwehr von Hackerangriffen. Zudem bist du in der Lage, mögliche Bedrohungen und Schwachstellen zu identifizieren, Anwendungs-, Daten- und Hostsicherheit zu erzielen sowie die relevanten Standards nach ISO/IEC 27001 und des IT-Grundschutzes nach BSI in die Praxis umzusetzen.

Du bist in der Lage, die technische Implementierung und Definition von Anforderungen und Kontrollen für den Informationsschutz vorzunehmen, und kannst IT-Prozesse und -Vorgänge entsprechend bewerten. Des Weiteren hast du ein Verständnis für die Bereiche Inhaltsklassifizierung, Datenverlust und Governance.

ZIELGRUPPE

IT-Sicherheitsverantwortliche, Mitarbeiter:innen in IT-Systemhäusern, IT-Unternehmen und Rechenzentren, aber auch Datenschutzfachkräfte, IT-Fachleute, Datenbank- und Netzwerkfachkräfte, (Fach-)Informatiker:innen, Programmierer:innen und Personen mit praktischer Erfahrung im IT-Bereich.

BERUFSAUSSICHTEN

Mit den gestiegenen Anforderungen an die IT-Infrastruktur spielt die IT-Sicherheit eine zunehmende Schlüsselrolle in Unternehmen. IT-Security-Spezialist:innen, die Sicherheitsressourcen analysieren, überwachen und schützen können sind stark gefragt und kommen sowohl direkt bei IT-Sicherheitsdienstleistern, aber auch Inhouse bei Unternehmen aller Branchen zum Einsatz.

Die weltweit einheitlichen und anerkannten Microsoft-Zertifizierungen zählen zu den wichtigsten Herstellerzertifizierungen, mit der du deine beruflichen Perspektiven auf dem Arbeitsmarkt branchenübergreifend verbesserst. Fachkräfte mit entsprechenden Kenntnissen sind sowohl bei großen als auch mittelständischen Unternehmen nachgefragt.

VORAUSSETZUNGEN

Die Prüfung CompTIA Network+ und mindestens zwei Jahre Erfahrung in der IT-Administration mit Schwerpunkt auf Sicherheit werden empfohlen, gute Englisch-Kenntnisse für die CompTIA-Zertifizierungsprüfungen vorausgesetzt.

LEHRGANGSINHALTE

IT-SECURITY-ADMINISTRATOR MIT COMPTIA-ZERTIFIZIERUNG SECURITY+

Allgemeine Sicherheitskonzepte (ca. 2 Tage)
Arten von Sicherheitskontrollen
Grundlegende Sicherheitskonzepte
Changemanagement-Prozesse
Verwendung von geeigneter Kryptografie

Bedrohungen, Schwachstellen und Abhilfemaßnahmen (ca. 3,5 Tage)
Verschiedene Arten von Social-Engineering-Techniken
Angriffsarten
Indikatoren bei Angriffen auf Applikationen
Bedrohungsakteure und -motivationen
Bedrohungsvektoren und Angriffsflächen
Arten von Schwachstellen
Indikatoren für böswillige Aktivitäten
Zweck von Risikominderungstechniken

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

Architektur und Design (ca. 4 Tage)
Sicherheitsauswirkungen von Architekturmodellen
Sicherheitsprinzipien
Konzepte und Strategien zum Schutz von Daten
Resilienz und Wiederherstellung in der Sicherheitsarchitektur

Sicherheitsoperationen (ca. 5 Tage)
Sicherheitstechniken auf Computerressourcen
Sicherheitsauswirkungen einer Hardware-, Software- und Datenbeständeverwaltung
Schwachstellenmanagement
Konzepte und Tools für Sicherheitswarnungen und -überwachung
Funktionen zur Erhöhung der Sicherheit im Unternehmen
Identitäts- und Zugriffsmanagement
Automatisierung und Orchestrierung
Maßnahmen zur Reaktion auf Vorfälle
Datenquellen zur Unterstützung einer Untersuchung

Verwalten und Überwachen von Sicherheitsprogrammen (ca. 3,5 Tage)
Security-Governance
Risikomanagementprozess
Prozesse der Risikobewertung
Security-Compliance
Audits und Bewertungen

Projektarbeit/Fallstudie, Zertifizierungsvorbereitung und Zertifizierungsprüfung (ca. 3 Tage)
CompTIA Security+ SY0-701 (in englischer Sprache)

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)

MICROSOFT INFORMATION PROTECTION ADMINISTRATION

Implementieren von Informationsschutz (ca. 4,5 Tage)
Vertrauliche Informationstypen (Benutzerdefinierte Typen, EDM-Klassifizierern)
Trainierbare Klassifizierer
Vertraulichkeitsbezeichnungen
Verschlüsselung von E-Mail-Nachrichten

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

Implementieren von DLP (ca. 3 Tage)
DLP-Richtlinien
DLP-Einstellungen für Endpunkte
DLP-Aktivitäten (Berichte, Aktivitäten, Warnungen)

Implementieren der Datenlebenszyklus- und Datensatzverwaltung (ca. 2 Tage)
Aufbewahren und Löschen von Daten mithilfe von Aufbewahrungsbezeichnungen
Datenaufbewahrung in Microsoft 365-Workloads
Microsoft Purview-Datensatzverwaltung

Überwachen und Untersuchen von Daten und Aktivitäten mithilfe von Microsoft Purview (ca. 2,5 Tage)
Gesetzliche Anforderungen mithilfe des Compliance Managers
eDiscovery und Inhaltssuche
Überwachungsprotokolle und Berichte

Verwalten von Insider- und Datenschutzrisiken in Microsoft 365 (ca. 3 Tage)
Microsoft Purview-Kommunikationscompliance
Insider-Risikomanagement (IRM)
Microsoft Purview-Informationsbarrieren (IBs)
Datenschutzanforderungen

Projektarbeit (ca. 5 Tage)
Zur Vertiefung der gelernten Inhalte
Präsentation der Ergebnisse
Zertifizierungsprüfung SC-400: Microsoft Information Protection and Compliance Administration

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.