

Kursstart alle 4 Wochen

IT-Security-Administrator (CompTIA Security+) mit Microsoft Endpoint und Information Protection Administration

In diesem Kurs erlernst du die Anforderungen in der Netzwerksicherheit und im Risikomanagement. Du verstehst, wie du als Microsoft Endpoint Administrator das Windows Betriebssystem bereitstellen und aktualisieren kannst. Auch kannst du Steuerelemente für die Complianceanforderungen planen und implementieren. Du erfährst, wie Künstliche Intelligenz (KI) in deinem Beruf eingesetzt wird.



Abschlussart

Zertifikat „CompTIA Security+“

Original Microsoft-Zertifikat „Microsoft 365 Certified: Endpoint Administrator Associate“

Original Microsoft-Zertifikat „Microsoft Certified: Information Protection and Compliance Administrator Associate“



Dauer

12 Wochen



Unterrichtszeiten

Montag bis Freitag von 08:30 bis 15:35 Uhr

(in Wochen mit Feiertagen von 8:30 bis 17:10 Uhr)



Abschlussprüfung

Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
CompTIA Security+ Zertifizierungsprüfung SY0-701 (in englischer Sprache)

Microsoft-Zertifizierungsprüfung MD-102: Endpoint Administrator

Microsoft-Zertifizierungsprüfung SC-400: Microsoft Information Protection and Compliance Administrator



Nächste Kursstarts

27.05.2024

24.06.2024

22.07.2024

LEHRGANGSZIEL

Du verfügst über Fachwissen in den wesentlichen Grundsätzen der Netzwerksicherheit und im Risikomanagement. Weiterhin kennst du mögliche Bedrohungen, Schwachstellen und Abhilfemaßnahmen gegen Hackerangriffe. Außerdem erhältst du einen Einblick in die Verwaltung und Überwachung von Sicherheitsprogrammen.

Zusätzlich kannst du als Endpoint Administrator die Bereitstellung, Konfiguration, Sicherung, Verwaltung und Überwachung von Microsoft 365 Netzwerken und Anwendungen in deinem Unternehmen übernehmen.

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

(Fach-)Informatiker:innen, IT- und Netzwerk-Fachkräfte, Personen mit praktischer Erfahrung und guten Kenntnissen 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 Security+ erlangen Sie eine herstellerunabhängige, weltweit anerkannte Zertifizierung, mit der du deine beruflichen Perspektiven in der IT-Branche verbesserst und dein Fachwissen aussagekräftig nachweisen. Fachkräfte der

IT-Security 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 Sie Ihre beruflichen Perspektiven auf dem Arbeitsmarkt branchenübergreifend verbessern. Fachkräfte mit entsprechenden Kenntnissen sind sowohl bei großen als auch mittelständischen Unternehmen nachgefragt.

VORAUSSETZUNGEN

Die Prüfung CompTIA Network+ und zwei Jahre Erfahrung in der IT-Administration mit einem Schwerpunkt auf Sicherheit werden empfohlen, gute Englisch-Kenntnisse für die Zertifizierungsprüfung werden 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 Datenbestandsverwaltung
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)

MICROSOFT ENDPOINT ADMINISTRATION

Windows Client Deployment (ca. 4 Tage)

Planung, Endpoint Analytics
Windows Autopilot
Microsoft Deployment Toolkit (MDT)
Remoteverwaltung, Konfiguration

Identity und Compliance Management (ca. 2,5 Tage)

Identität verwalten in Azure Active Directory
Compliancerichtlinien für Geräteplattformen

Künstliche Intelligenz (KI) im Arbeitsprozess

Vorstellung von konkreten KI-Technologien im beruflichen Umfeld
Anwendungsmöglichkeiten und Praxis-Übungen

Management, Wartung und Schutz von Geräten (ca. 7 Tage)

Lebenszyklus von Geräten
Gerätekonfiguration
Geräteüberwachung
Geräte-Updates
Endpoint Protection

Management von Apps (ca. 1,5 Tage)

Apps bereitstellen und aktualisieren
App-Schutz und Konfigurations-Richtlinien für iOS und Android

Projektarbeit (ca. 5 Tage)

Zur Vertiefung der gelernten Inhalte
Präsentation der Ergebnisse
Zertifizierungsprüfung MD-102: Endpoint Administrator

MICROSOFT INFORMATION PROTECTION ADMINISTRATION

Implementieren von Informationsschutz (ca. 4,5 Tage)

Vertrauliche Informationstypen (Benutzerdefinierte Typen, EDM-Klassifizieren)
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

Die Lehrgänge bei alfatraining 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 deiner 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.

- ① Änderungen möglich. Die Lehrgangsinhalte werden regelmäßig aktualisiert. Die aktuellen Lehrgangsinhalte findest Du immer unter www.alfatraining.de.