

Kursstart alle 4 Wochen

Netzwerk-Expert:in (CompTIA Network+) und IT-Security-Administrator (CompTIA Security+)

Der Kurs behandelt das Konfigurieren von Netzwerken, unterschiedliche Netzwerkarchitekturen und gibt Einblicke in die Nutzung Künstlicher Intelligenz (KI) in deinem beruflichen Umfeld. Zusätzlich wird Fachwissen in den Grundsätzen der Netzwerksicherheit und im Risikomanagement vermittelt.

 **Abschlussart**
Zertifikat „CompTIA Network+“
Zertifikat „CompTIA Security+“

 **Abschlussprüfung**
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
CompTIA Network+ Zertifizierungsprüfung N10-008
CompTIA Security+ Zertifizierungsprüfung SY0-701 (in englischer Sprache)

 **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

Du verfügst über die wesentlichen Kenntnisse und Fähigkeiten für die kompetente Konzeption, Konfiguration, Verwaltung und Fehlerbehebung von beliebigen kabelgebundenen und drahtlosen Netzwerken.

Zudem verfügst du 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.

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 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.

VORAUSSETZUNGEN

Zwei Jahre Erfahrung in der IT-Administration mit einem Schwerpunkt auf Sicherheit werden empfohlen, gute Englisch-Kenntnisse für die

Zertifizierungsprüfung werden vorausgesetzt.

LEHRGANGSINHALTE

NETZWERK-EXPERT:IN MIT COMPTIA ZERTIFIZIERUNG NETWORK+

Netzwerkgrundlagen (ca. 4 Tage)

Open Systems Interconnection (OSI-Modell): Ebenen und Kapselungskonzepte
Netzwerktopologien und -typen
Kabellösungen und Anschlüsse
Subnetze und geeignete IP-Adressierungsschemata
Ports und Protokolle: Anwendungen und verschlüsselte Alternativen
Netzwerk-Services: DHCP, DNS und NTP
Grundlegende Netzwerkarchitektur und Rechenzentren von Unternehmen
Cloud-Konzepte und Konnektivitätsoptionen

Künstliche Intelligenz (KI) im Arbeitsprozess

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

Netzwerkimplementierungen (ca. 3 Tage)

Verschiedene Geräte, ihre Funktionen und geeignete Platzierung im Netzwerk
Routing-Technologien und Bandbreitenmanagementkonzepte
Ethernet-Switching-Funktionen
Wireless-Standards und -Technologien

Netzwerkbetrieb (ca. 3 Tage)

Statistiken und Sensoren zum Sicherstellen der Netzverfügbarkeit
Dokumente und Richtlinien
Hochverfügbarkeits- und Disaster-Recovery-Konzepte

Netzwerksicherheit (ca. 3 Tage)

Sicherheitskonzepte
Gängige Arten von Angriffen
Techniken zur Netzwerk-Härtung
Remote-Zugriffsmethoden und Auswirkungen auf die Sicherheit
Physische Sicherheit

Troubleshooting (ca. 4 Tage)

Methodik zur Fehlersuche im Netzwerk
Behebung häufig auftretender Kabelverbindungsprobleme
Netzwerk-Softwaretools und -befehle
Behebung häufiger Probleme bei drahtlosen Verbindungen
Fehlerbehebung bei allgemeinen Netzwerkproblemen

Projektarbeit/Fallstudie, Zertifizierungsvorbereitung und Zertifizierungsprüfung (ca. 3 Tage)

CompTIA Network+ N10-008

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)

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.

- ① Änderungen möglich. Die Lehrgangsinhalte werden regelmäßig aktualisiert. Die aktuellen Lehrgangsinhalte findest Du immer unter [smartbuilding.alfatraining.de](https://www.smartbuilding.alfatraining.de).