alfatraining Beratung
beratung@alfatraining.de
0800 3456-500
Mo. - Fr. von 8 bis 17 Uhr kostenfrei aus allen Netzen.

Kursstart alle 4 Wochen

IT-Security-Administrator (CompTIA Security+) und und IT-Cybersecurity-Analyst (CompTIA CySA+)

Dieser Lehrgang vermittelt CompTIA-Fachwissen in den Grundsätzen der Netzwerksicherheit, im Risikomanagement und im Einsatz von Künstlicher Intelligenz (KI) in deinem Beruf. Du lernst Tools zur Erkennung von Bedrohungen zu konfigurieren und zu verwenden sowie Datenanalysen durchzuführen.

Abschlussart
Zertifikat „CompTIA Security+“
Zertifikat „CompTIA CySA+“

Abschlussprüfung
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
CompTIA Security+ Zertifizierungsprüfung SY0-701 (in englischer Sprache)
CompTIA CySA+ Zertifizierungsprüfung CS0-003 (in englischer Sprache)

Dauer
8 Wochen

Unterrichtszeiten
Montag bis Freitag von 08:30 bis 15:35 Uhr
(in Wochen mit Feiertagen von 8:30 bis 17:10 Uhr)

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.

Zudem bist du nach dem Lehrgang 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.

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+ und CySA+ erlangen Sie herstellerunabhängige, weltweit anerkannte Zertifizierungen, mit denen du deine beruflichen Perspektiven in der IT-Branche verbessern und dein Fachwissen aussagekräftig nachweist. Fachkräfte der IT-Security sowie IT-Sicherheitsanalytiker:innen, die Cybersicherheitsressourcen analysieren, überwachen und schützen können kommen sowohl direkt bei IT-Sicherheitsdienstleistern, aber auch Inhouse bei Unternehmen aller Branchen zum Einsatz.

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)

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.

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