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

Kursstart alle 4 Wochen

CCNA und IT-Security-Beauftragte:r

Der Kurs vermittelt die Konfiguration von Cisco-Netzwerken, die Umsetzung von LAN-Konzepten und Routingtechnologien, Sicherheits- und Schutzmaßnahmen sowie psychologische Aspekte zur Sensibilisierung der Mitarbeitenden. Du erfährst, wie Künstliche Intelligenz (KI) im Beruf eingesetzt wird.

Abschlussart
Cisco Certified Network Associate-Zertifikat (CCNA)
Zertifikat „IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation"

Abschlussprüfung
Praxisbezogene Projektarbeiten mit Abschlusspräsentationen
Cisco-Zertifizierungsprüfung CCNA 200-301 (in englischer Sprache)
IT-Security-Beauftragte:r mit TÜV Rheinland geprüfter Qualifikation

Dauer
12 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 kannst du Cisco-Netzwerke in Unternehmen konfigurieren und verwalten. Du kennst die wichtigsten LAN-Konzepte, aber auch gängige Sicherheitslücken, bist mit Netzwerkinfrastrukturen und Automatisierungen in Netzwerken vertraut und beherrschst Routingtechnologien wie WAN, IPv4 und IPv6.

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

Personen mit praktischer Erfahrung und guten Kenntnissen im IT-Bereich und in der Netzwerktechnik (auch Quereinsteiger:innen und Studienabbrecher:innen) sowie IT-Fachkräfte.

Zusätzlich richtet sich dieser Kurs an verantwortliche Personen aus den Bereichen IT-Sicherheit, Netz- und Systemadministration, IT-Organisation, IT-Beratung, Revision und Risikomanagement.

BERUFSAUSSICHTEN

In allen Branchen wächst der Bedarf an qualifizierten Netzwerk-Fachkräften - die Zertifikate von Cisco gehören dabei zu den begehrtesten Qualifikationsnachweisen. Mit dem neuen CCNA-Zertifikat kannst du dich sich als Netzwerktechniker:in, im Help-Desk-Bereich oder im Bereich der IT-Security bewerben.

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

VORAUSSETZUNGEN

Dieser Lehrgang setzt Netzwerkgrundkenntnisse sowie gute Englisch-Kenntnisse für die Zertifizierungsprüfung voraus.

LEHRGANGSINHALTE

CCNA – CISCO CERTIFIED NETWORK ASSOCIATE

Network Fundamentals (ca. 8 Tage)
Rolle und Funktion von Netzwerkkomponenten
Router, Layer 2 und Layer 3 Switches, Next-Gen Firewalls und IPS
Access Points, Controller (Cisco DNA Center und WLC), Endpunkte, Server, PoE
Netzwerk-Topologie-Architekturen: Two-Tier, Three-Tier, Spine-Leaf, WAN, SOHO, On-Premise und Cloud
Physische Schnittstellen und Kabeltypen
Single-Mode-Faser, Multimode-Faser, Kupfer
Schnittstellen- und Kabelprobleme erkennen
Kollisionen, Fehler, Duplex- und Geschwindigkeitsfehler
Vergleich von TCP und UDP
Konfiguration und Überprüfung von IPv4-Adressen und Subnetting
Private IPv4-Adressen
Konfiguration und Überprüfung von IPv6-Adressen und Präfixen
IPv6-Adresstypen: Unicast, Anycast, Multicast, Modified EUI 64
IP-Parameter für Client-Betriebssysteme überprüfen
Drahtlos-Prinzipien
Nicht überlappende Wi-Fi-Kanäle, SSID, RF, Verschlüsselung
Virtualisierungsgrundlagen (Server-Virtualisierung, Container, VRFs)
Switching-Konzepte: MAC-Learning und -Aging, Frame-Switching, Frame-Flooding, MAC-Adress-Tabelle

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

Network Access (ca. 8 Tage)
Konfiguration und Überprüfung von VLANs: Access-Ports, Default VLAN, InterVLAN-Konnektivität
Interswitch-Konnektivität
Trunk-Ports, 802.1Q, Native VLAN
Layer 2 Discovery-Protokolle (CDP und LLDP)
Layer 2/Layer 3 EtherChannel (LACP)
Rapid PVST+ Spanning Tree Protocol
Root Port, Root Bridge, Port States, PortFast, Guard-Funktionen (Root,loop, BPDU)
Cisco Wireless-Architekturen und AP-Modi
Physische Infrastrukturverbindungen von WLAN-Komponenten
AP, WLC, Access-/Trunk-Ports, LAG
Netzwerkgeräte-Verwaltungszugriff (Telnet, SSH, HTTP, HTTPS, Konsole, TACACS+/RADIUS, Cloud-Management)
WLAN-GUI-Konfiguration für Client-Konnektivität

IP Connectivity (ca. 8,5 Tage)
Komponenten der Routing-Tabelle interpretieren
Routing-Protokollcode, Präfix, Netzmaske, Next Hop, Administrative Distance, Metrik, Gateway of Last Resort
Routing-Entscheidungen von Routern: Longest Prefix Match, Administrative Distance, Routing-Protokoll-Metrik
IPv4- und IPv6-Static Routing: Default Route, Network Route, Host Route, Floating Static
Single Area OSPFv2 konfigurieren und überprüfen
Neighbor Adjacencies, Point-to-Point, Broadcast (DR/BDR-Auswahl), Router ID
First Hop Redundancy Protocols (Zweck, Funktionen und Konzepte)

IP Services (3,5 Tage)
Inside Source NAT konfigurieren und überprüfen (Statische NAT und Pools)
NTP im Client- und Server-Modus
DHCP und DNS im Netzwerk
Funktion von SNMP
Syslog-Funktionen
DHCP-Client und Relay konfigurieren und überprüfen
Forwarding Per-Hop Behavior (PHB) für QoS

Security Fundamentals und Automation/Programmability (ca. 7 Tage)
Wichtige Sicherheitskonzepte
Bedrohungen, Schwachstellen, Exploits, und Gegenmaßnahmen
Sicherheitselemente und Programmbestandteile
Benutzerbewusstsein, Schulung, physische Zugangskontrolle
Gerätezugriffskontrolle mit lokalen Passwörtern
Sicherheits-Passwortrichtlinien:Verwaltung, Komplexität, Passwortalternativen
IPsec-VPNs
Access Control Lists konfigurieren und überprüfen
Layer 2-Sicherheitsfunktionen (DHCP-Snooping, Dynamic ARP Inspection, Port-Security)
Authentifizierung, Autorisierung, und Abrechnung
Drahtlose Sicherheitsprotokolle (WPA, WPA2, WPA3)
WLAN mit WPA2 PSK konfigurieren und überprüfen
Auswirkungen der Automatisierung auf das Netzwerkmanagement
Vergleich traditioneller Netzwerke und Controller-basiertes Networking
Controller-basierte, softwaredefinierte Architektur: Overlay, Underlay, Fabric, Trennung von Steuerungsebene und Datenebene, Northbound und Southbound APIs
KI und maschinelles Lernen im Netzwerkbetrieb
Merkmale von REST-basierten APIs (Authentifizierungstypen, CRUD, HTTP-Verben, Datenkodierung)
Konfigurationsmanagement-Mechanismen (Ansible, Terraform)
Komponenten von JSON-codierten Daten

Projektarbeit, Zertifizierungsvorbereitung und Zertifizierungsprüfung (ca. 5 Tage)
Cisco Certified Network Associate – 200-301 CCNA (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.