

Szkolenie: CompTIA CompTIA Network+ Prep Course



DOSTĘPNE TERMINY

2026-06-29	5 dni	Warszawa / Virtual Classroom
2026-07-06	5 dni	Warszawa / Wirtualna sala
2026-08-03	5 dni	Kraków / Wirtualna sala
2026-08-03	5 dni	Virtual Classroom
2026-09-07	5 dni	Warszawa / Wirtualna sala
2026-09-28	5 dni	Virtual Classroom
2026-10-05	5 dni	Kraków / Wirtualna sala
2026-10-05	5 dni	Virtual Classroom
2026-11-02	5 dni	Warszawa / Wirtualna sala
2026-11-30	5 dni	Virtual Classroom
2026-12-07	5 dni	Kraków / Wirtualna sala
2026-12-07	5 dni	Virtual Classroom

Cel szkolenia:

Szkolenie przygotowuje do egzaminu certyfikacyjnego CompTIA Network+ (N10-009) oraz kształtuje kluczowe kompetencje administratora sieci. Program opiera się na modelu progresji, pozwalającym na systematyczne przyswajanie wiedzy teoretycznej i rozwijanie umiejętności praktycznych wymaganych w codziennej pracy zawodowej. Proces nauki obejmuje osadzenie materiału w kontekście biznesowym, pogłębioną analizę zaawansowanych zagadnień oraz utrwalenie wiedzy poprzez ćwiczenia w laboratoriach (labach) i quizy z ukierunkowaną informacją zwrotną.

Po ukończeniu szkolenia będziesz potrafić:

- Wdrażać i diagnozować sieci Ethernet oraz rozwiązywać występujące w nich problemy.
- Utrzymywać stabilną łączność w standardach IPv4 oraz IPv6.
- Konfigurować infrastrukturę routingu oraz skutecznie usuwać usterki konfiguracyjne.
- Wspierać kluczowe usługi i aplikacje sieciowe.
- Zapewniać bezpieczeństwo oraz wysoką dostępność (High Availability) zasobów sieciowych.
- Wdrażać i optymalizować sieci bezprzewodowe.
- Konfigurować łącza WAN oraz mechanizmy bezpiecznego dostępu zdalnego.
- Stosować procedury organizacyjne i kontrole bezpieczeństwa fizycznego (site security).
- Projektować i interpretować architekturę rozwiązań chmurowych oraz centrów danych.

Umiejętności, które zdobędziesz

- Implementacja urządzeń przewodowych i bezprzewodowych z uwzględnieniem adresacji IP, portów, protokołów i topologii sieci.
- Zarządzanie dokumentacją techniczną oraz procesami cyklu życia, zmian i konfiguracji.
- Wykorzystanie wirtualizacji i usług chmurowych w praktyce, w oparciu o koncepcje elastyczności i skalowalności.
- Monitorowanie wydajności sieci pod kątem utrzymania ciągłości usług i szybkiego rozwiązywania problemów z łącznością.
- Budowa bezpiecznych infrastruktur poprzez aktywne ograniczanie podatności i wzmacnianie mechanizmów obronnych.
- Zaawansowana diagnostyka sieciowa z wykorzystaniem profesjonalnych narzędzi analitycznych.

Role zawodowe, dla których przydatne są umiejętności Network+

- Administrator sieci (Network Administrator)
- Inżynier sieci (Network Engineer)
- Administrator systemów (System Administrator)
- Specjalista wsparcia IT (IT Support Specialist)
- Technik serwisu terenowego (Field Service Technician)
- Analityk sieci (Network Analyst)
- Technik NOC / Centrum Operacji Sieciowych (NOC Technician)
- Młodszy analityk cyberbezpieczeństwa (Junior Cybersecurity Analyst)

Każdy uczestnik autoryzowanego szkolenia CompTIA Network+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA Network+ N10-009.

Plan szkolenia:

- Omówienie topologii sieci
 - Wprowadzenie do sieci komputerowych
 - Podstawowe pojęcia sieciowe
 - Rodzaje sieci

- Topologie sieci
- Topologia gwiazdy
- Topologia siatki
- Topologie historyczne
- Podstawy modelu OSI
 - Model OSI
 - Enkapsulacja i dekapulacja danych
 - Warstwa 1 - fizyczna
 - Warstwa 2 - łącza danych
 - Warstwa 3 - sieciowa
 - Warstwa 4 - transportowa
 - Warstwy wyższe
 - Podsumowanie modelu OSI
- Sieci SOHO
 - Routery SOHO
 - Funkcje warstwy fizycznej
 - Funkcje warstwy łącza danych
 - Funkcje warstwy sieciowej
 - Funkcje warstwy transportowej i aplikacji oraz zagadnienia bezpieczeństwa
 - Internet
 - Systemy binarny i szesnastkowy
- Metodyka rozwiązywania problemów
 - Metodyka rozwiązywania problemów sieciowych
 - Identyfikacja problemu
 - Identyfikacja objawów
 - Sformułowanie hipotezy o prawdopodobnej przyczynie
 - Weryfikacja hipotezy i ustalenie przyczyny
 - Ustalenie planu działania
 - Wdrożenie rozwiązania
 - Weryfikacja rozwiązania
 - Dokumentowanie ustaleń, działań i rezultatów
- Materiały dodatkowe
 - Terminologia i typy sieci
 - Model OSI
 - Metodyka rozwiązywania problemów
- Okablowanie i instalacje fizyczne

- Ethernet
 - Transmisja danych w sieci
 - Standardy Ethernet
 - Adres MAC oraz domeny kolizyjne w sieciach
 - Standard Fast Ethernet 100BASE-TX
 - Standardy Gigabit Ethernet
 - Standardy Ethernet światłowodowego
- Kable i złącza miedziane
 - Kabel UTP (Unshielded Twisted Pair)
 - Kabel STP/ScTP (skrętka ekranowana)
 - Kategorie kabli
 - Rodzaje złączy do skrętki
 - Kable w klasie plenum
 - Kable koncentryczne
- Wdrażanie okablowania
 - System okablowania strukturalnego
 - Standardy zakończeń T568A i T568B
 - Panele krosowe jako punkty konsolidacji infrastruktury pasywnej
 - Instalacja okablowania strukturalnego
 - Narzędzia i techniki terminacji okablowania
- Kable i złącza światłowodowe
 - Dobór i ograniczenia kabli światłowodowych
 - Światłowód jednomodowy i wielomodowy
 - Rodzaje złączy światłowodowych
 - Instalacja okablowania światłowodowego
 - Panele dystrybucyjne światłowódów
 - Złącza MPO/MTP (Multi-Fiber Push On)
 - WDM - multipleksacja z podziałem długości fali
- Czynniki instalacji fizycznej
 - Systemy szaf i stelaży
 - Wilgotność i temperatura
 - Zarządzanie zasilaniem
 - Systemy gaszenia pożaru
- Diagnostyka okablowania
 - Specyfikacje i ograniczenia
 - Typowe problemy z kablami

- Problemy związane z kategorią kabla
- Testery kabli
- Testery mapy przewodów i generatory tonu
- Tłumienie i problemy z interferencją
- Przesłuchy w sieciach
- Narzędzia do testowania światłowodów
- Strategie rozwiązywania problemów z okablowaniem
- Materiały dodatkowe
 - Standardy Ethernet
 - Kable i złącza
 - Instalacja okablowania strukturalnego
 - Instalacja i diagnostyka okablowania strukturalnego
- Konfigurowanie interfejsów i przełączników
 - Interfejsy sieciowe
 - Karty sieciowe (NIC)
 - Wkładki modułowe do światłowodów
 - Problemy z niezgodnością transceiverów
 - Format ramki Ethernet
 - Format adresu MAC
 - Urządzenia w sieci Ethernet
 - Koncentratory
 - Mosty
 - Przełączniki
 - Rodzaje przełączników Ethernet
 - Konfiguracja interfejsów przełącznika
 - Podstawy Cisco IOS
 - Konfiguracja portów przełącznika
 - Agregacja łączy i teaming kart NIC
 - MTU - maksymalna jednostka transmisji
 - STP - protokół Spanning Tree
 - Konfiguracja STP
 - Technologia PoE: przesyłanie zasilania przez okablowanie strukturalne
 - Rozwiązywanie problemów z przełącznikami
 - Usterki sprzętowe
 - Wskaźniki stanu portów
 - Liczniki błędów interfejsu

- Tablica adresów MAC
- Pętle w warstwie 2 i zjawisko burzy rozgłoszeniowej
- Problemy z PoE
- Materiały dodatkowe
 - Karty NIC i adresy MAC
 - Przełączniki Ethernet
- Konfigurowanie adresacji sieciowej
 - Podstawy protokołu IP
 - Nagłówek datagramu IPv4
 - Adresowanie i przekazywanie: warstwa 2 vs warstwa 3
 - ARP - Address Resolution Protocol
 - Adresowanie unicast i broadcast
 - Adresowanie multicast i anycast
 - Adresacja IPv4
 - Format adresu IPv4
 - Maski sieci
 - Maski podsieci
 - Zakresy adresów hostów
 - Brama domyślna
 - Adresy rozgłoszeniowe
 - Konfiguracja interfejsu IP w systemie Windows
 - Konfiguracja interfejsu IP w systemie Linux
 - Podsielowanie IPv4: projektowanie i optymalizacja adresacji)
 - Adresowanie klasowe
 - Adresy publiczne i prywatne
 - Pozostałe zarezerwowane zakresy adresów
 - Projektowanie schematu adresacji IPv4
 - CIDR - Classless Inter-Domain Routing
 - VLSM - zmienna długość maski podsieci
 - Narzędzia do diagnostyki IP
 - ipconfig
 - ifconfig
 - arp
 - ping
 - IPv6
 - IPv4 vs IPv6

- Format adresu IPv6
- Prefiksy sieci IPv6
- Adresowanie unicast w IPv6
- Adresy link-local w IPv6
- Adresowanie multicast i anycast w IPv6
- Mechanizmy przejścia (transition) IPv4/IPv6
- Typowe prefiksy IPv6
- Rozwiązywanie problemów IP
 - Problemy z konfiguracją IP
 - Zduplikowane adresy IP i MAC
 - Problemy z przekazywaniem pakietów
- Materiały dodatkowe
 - Adresy sieciowe i typy komunikatów
 - Adresacja IPv4 i diagnostyka
 - Terminologia podsieciowania
 - Demonstracja podsieciowania
 - Adresacja IPv6 i diagnostyka
 - Narzędzia wiersza poleceń w sieciach
- Konfigurowanie routingu i zaawansowanego przełączania
 - Technologie routingu
 - Tablice routingu i wybór ścieżki
 - Trasy statyczne i domyślne
 - Przykład tablicy routingu
 - Przekazywanie pakietów
 - Fragmentacja
 - Konfiguracja routera
 - Narzędzia do analizy tablic routingu
 - tracert i traceroute
 - Dynamiczny routing
 - Protokoły routingu dynamicznego
 - RIP - Routing Information Protocol
 - EIGRP - Enhanced Interior Gateway Routing Protocol
 - OSPF - Open Shortest Path First
 - BGP - Border Gateway Protocol
 - Metody wyboru trasy
 - NAT - translacja adresów sieciowych

- Routery brzegowe
- Rodzaje NAT
- PAT - Port Address Translation
- Zapory sieciowe (firewalle)
 - Zastosowania i rodzaje firewalli
 - Dobór i umiejscowienie firewalli
- Topologie sieci w przedsiębiorstwie
 - Topologia hybrydowa
 - Trójwarstwowa hierarchia sieci
- VLAN - wirtualne sieci LAN
 - VLAN-y i podsieci
 - Identyfikatory VLAN i członkostwo
 - Trunking oraz IEEE 802.1Q
 - Porty tagowane i nietagowane
 - Voice VLAN
 - VLAN domyślny i VLAN natywny (native)
 - Routing między VLAN-ami
- Diagnostyka routingu i VLAN
 - Problemy z tablicą routingu
 - Problemy z trasą domyślną i pętlami routingu
 - Problemy z przypisaniem do VLAN
- Materiały dodatkowe
 - Podstawy routingu
 - NAT
 - Firewalle sprzętowe
 - Projektowanie sieci w przedsiębiorstwie
- Implementacja usług sieciowych
 - Protokoły warstwy transportowej i aplikacji
 - Porty i połączenia w warstwie transportowej
 - TCP - Transmission Control Protocol
 - Ustanawianie i kończenie połączenia TCP
 - UDP - User Datagram Protocol
 - netstat
 - Najczęściej używane porty TCP i UDP
 - DHCP - Dynamic Host Configuration Protocol
 - Proces DHCP

- Konfiguracja serwera DHCP
- Opcje DHCP
- Rezerwacje i wykluczenia DHCP
- Konfiguracja adresacji po stronie klienta
- APIPA i SLAAC
 - APIPA - automatyczna prywatna adresacja IP
 - Autokonfiguracja i testowanie interfejsu IPv6
 - Konfiguracja serwera DHCPv6
 - Konfiguracja adresacji alternatywnej
- Relay DHCP i diagnostyka
 - Relay DHCP i IP Helper
 - Typowe problemy z DHCP
 - Rozwiązywanie problemu wyczerpania puli DHCP
- DNS - Domain Name System
 - Nazwy hostów i domen
 - Hierarchia DNS
 - Rozwiązywanie nazw przy użyciu DNS
 - Typy rekordów zasobów w DNS
 - Rekordy A/AAAA (host address) oraz CNAME (canonical name)
 - Rekordy MX, SRV oraz TXT
 - Rekordy PTR
 - Konfiguracja serwera DNS
 - DNS wewnętrzny i zewnętrzny
 - Bezpieczeństwo DNS
 - Konfiguracja cache DNS w systemie Linux
- Diagnostyka DNS
 - Problemy DNS po stronie klienta
 - Problemy z rozwiązywaniem nazw
 - nslookup
 - dig
- Materiały dodatkowe
 - Protokoły warstwy transportowej i aplikacji
 - DHCP
 - DNS i diagnostyka DNS
- Omówienie usług aplikacyjnych
 - Bezpieczeństwo aplikacji i synchronizacja czasu

- TLS - Transport Layer Security
- NTP - Network Time Protocol
- PTP - Precision Time Protocol
- Usługi WWW, plików, wydruku i baz danych
 - HTTP - Hypertext Transfer Protocol
 - HTTPS - HTTP Secure
 - FTP - File Transfer Protocol
 - SFTP - Secure File Transfer Protocol
 - SMB - Server Message Block
 - NAS - Network Attached Storage
 - Usługi bazodanowe
- Usługi pocztowe i głosowe
 - SMTP - Simple Mail Transfer Protocol
 - IMAP - Internet Message Access Protocol
 - Usługi głosowe i wideo
 - Protokoły VoIP
 - Telefony VoIP
- Odzyskiwanie po awarii i wysoka dostępność
 - Strategie ciągłości działania i metryki odzyskiwania
 - Strategie wyboru lokalizacji alternatywnej w planowaniu DR
 - Odporność na błędy i redundancja
 - Zarządzanie ruchem i wysoką dostępnością za pomocą Load Balancerów
 - Klastry wysokiej dostępności
 - Pierwszy przeskok z redundancją
- Materiały dodatkowe
 - NTP
 - Usługi plików i WWW
 - Usługi e-mail, wideo i głosu
 - Ciągłość operacyjna: wysoka dostępność (HA) i odzyskiwanie po awarii (DR)
- Wsparcie zarządzania siecią
 - Polityki organizacyjne i dokumentacja
 - Zarządzanie konfiguracją
 - Zarządzanie kopiami zapasowymi urządzeń sieciowych
 - Zarządzanie zmianą
 - Dokumentacja inwentaryzacji zasobów
 - Zarządzanie cyklem życia

- Wycofywanie z eksploatacji
- Fizyczne diagramy sieci
- Logiczne diagramy sieci
- Zarządzanie adresacją IP (IPAM)
- Ramy kontraktowe i ustalenia operacyjne w administracji sieciami
- Wykrywanie hostów i monitoring
 - Wykrywanie zasobów w sieci (network discovery)
 - Nmap
 - Skanowanie portów Nmap
 - Monitorowanie wydajności
 - Monitorowanie dostępności
 - Monitorowanie konfiguracji
- SNMP - Simple Network Management Protocol
 - Agent i menedżer SNMP
 - Bezpieczeństwo SNMP
 - Konfiguracja SNMP na routerze
 - Monitorowanie przełącznika przez SNMP
 - Konfiguracja pułapek SNMP (SNMP trap)
- Zarządzanie zdarzeniami
 - Logi urządzeń sieciowych
 - Kolektory logów i syslog
 - Zarządzanie incydentami: priorytetyzacja zdarzeń i systemy alertowania
 - SIEM - Security Information and Event Management
 - Przeglądy logów
- Przechwytywanie i analiza pakietów
 - Przechwytywanie pakietów
 - tcpdump
 - Analityzatory protokołów
 - Wykorzystanie Wireshark do diagnozowania problemów sieciowych
- Monitorowanie ruchu
 - Typowe problemy wydajnościowe
 - Statystyki interfejsów
 - Dane z przepływów w sieci
 - Narzędzia do testowania ruchu
 - Zarządzanie pasmem
 - Kształtowanie ruchu

- Monitorowanie statystyk interfejsu
- Materiały dodatkowe
 - Diagramy sieci
 - Wykrywanie hostów i monitoring
 - Analiza sieci
- Podstawowe koncepcje bezpieczeństwa sieci
 - Koncepcje bezpieczeństwa
 - Najważniejsza terminologia bezpieczeństwa
 - Audyty i oceny bezpieczeństwa
 - Zgodność regulacyjna
 - Szyfrowanie
 - Klasyfikacja podatności i metod ich eksploatacji
 - Wykorzystanie systemów typu Honey-X w detekcji zagrożeń
 - Zagrożenia i ataki sieciowe
 - Typy zagrożeń i ich ocena
 - Rodzaje ataków
 - Ataki na dostępność: DoS, DDoS oraz infrastruktura botnetów
 - Ataki malware
 - Analiza mechanizmów spoofingu i metody obrony
 - Ataki on-path (MITM w ścieżce)
 - Przeprowadzenie ataku on-path na DHCP
 - Zatrucie ARP
 - Zalewanie tablicy CAM fałszywymi adresami MAC
 - Użycie SMAC do podszywania się pod adres MAC
 - Techniki omijania segmentacji VLAN w architekturze przełączanej
 - Ataki z wykorzystaniem nieautoryzowanych systemów
 - Nieautoryzowane urządzenia i usługi w sieci
 - Zagrożenia ze strony nieautoryzowanych serwerów DHCP
 - Konfiguracja funkcjonalności DHCP snooping
 - Ataki na DNS
 - Zatrucie DNS
 - Inżynieria społeczna
 - Ataki socjotechniczne
 - Ataki na hasła
 - Materiały dodatkowe
 - Koncepcje bezpieczeństwa

- Zagrozenia i ataki
- Inzynieria spoleczna
- Stosowanie mechanizmow bezpieczenstwa sieci
 - Uwierzytelnianie
 - Kontrola dostepu
 - Metody uwierzytelniania
 - Uwierzytelnianie lokalne
 - SSO i Kerberos
 - Certyfikaty cyfrowe i PKI
 - Zarzadzanie kluczami
 - Tozsamosc federacyjna i SAML
 - Uwierzytelnianie zdalne
 - Autoryzacja i zarzadzanie kontami
 - Autoryzacja i RBAC - kontrola dostepu oparta na rolach
 - PAM - Privileged Access Management
 - LDAP - Lightweight Directory Access Protocol
 - LDAPS - LDAP Secure
 - Wzmacnianie bezpieczenstwa sieci (hardening)
 - Zintegrowane mechanizmy kontrolne: podejscie Defense in Depth
 - Hardening urzadzen i uslug
 - Skanowanie pod katem niezabezpieczonych protokolow
 - Bezpieczenstwo przełączników
 - NAC i port security
 - EAP oraz IEEE 802.1X
 - Zabezpieczenia portow
 - Port mirroring
 - Reguly bezpieczenstwa sieci
 - Reguly bezpieczenstwa i konfiguracja ACL
 - Serwery proxy
 - Filtrowanie tresci
 - Bledy konfiguracji firewalli i ACL
 - Tworzenie list ACL na firewallu
 - Materiały dodatkowe
 - Uwierzytelnianie
 - Infrastruktura klucza publicznego (PKI)
 - Autoryzacja i zarzadzanie kontami

- Bezpieczeństwo portów przełącznika
- Wsparcie projektowania bezpieczeństwa sieci
 - Bezpieczeństwo strefowe
 - Strefy bezpieczeństwa sieci
 - Konfiguracja DMZ
 - Sieci perymetryczne
 - Podsieci ekranowane
 - IDS/IPS - systemy wykrywania i zapobiegania włamaniom
 - Wdrażanie IDS/IPS
 - Internet Rzeczy (IoT)
 - Urządzenia IoT
 - Przemysłowe systemy wbudowane
 - Sieci IoT
 - Bezpieczeństwo sieci IoT
 - Bezpieczeństwo fizyczne
 - Zamki
 - Kamery
 - Geofencing i geo-tagging
 - Materiały dodatkowe
 - Strefy i sieci perymetryczne
 - Systemy wbudowane i architektura Zero Trust
- Konfigurowanie sieci bezprzewodowych
 - Konceptcje i standardy sieci bezprzewodowych
 - Standardy bezprzewodowe IEEE 802.11
 - IEEE 802.11a i szerokość kanału w paśmie 5 GHz
 - IEEE 802.11b/g i szerokość kanału w paśmie 2,4 GHz
 - IEEE 802.11n, MIMO i łączenie kanałów
 - Wi-Fi 5 i Wi-Fi 6
 - MU-MIMO i sterowanie pasmem
 - Technologie komórkowe
 - Technologie satelitarne
 - Projektowanie sieci bezprzewodowej w przedsiębiorstwie
 - Sieć infrastrukturalna
 - Zasięg i siła sygnału
 - Audyt radiowy i modelowanie propagacji sygnału
 - Roaming bezprzewodowy

- Kontrolery sieci bezprzewodowych
- Rodzaje anten
- Inne typy sieci bezprzewodowych
- Bezpieczeństwo sieci bezprzewodowych
 - Standardy szyfrowania Wi-Fi
 - Uwierzytelnianie osobiste
 - Uwierzytelnianie w trybie enterprise
 - Sieci gościnne i captive portals
 - Analiza ryzyka w modelu BYOD
 - Ataki na sieci bezprzewodowe
- Rozwiązywanie problemów w sieciach bezprzewodowych
 - Ocena wydajności sieci bezprzewodowej
 - Niewystarczające pokrycie
 - Nakładanie się kanałów
 - Zakłócenia w sieciach bezprzewodowych
 - Roaming i rozłączanie klientów
 - Przeciążenie WLAN
- Materiały dodatkowe
 - Projektowanie sieci bezprzewodowej w przedsiębiorstwie
 - Standardy i bezpieczeństwo sieci bezprzewodowych
 - Diagnostyka sieci bezprzewodowych
- Porównanie metod dostępu zdalnego
 - WAN i łączność z Internetem
 - Sieci rozległe (WAN) i model OSI
 - Rodzaje dostępu do Internetu
 - FTTC i FTTP - światłowód do krawężnika i do budynku
 - VPN - wirtualne sieci prywatne
 - Kwestie dostępu zdalnego
 - Protokoły tunelowania
 - IPSec - Internet Protocol Security
 - IKE - Internet Key Exchange
 - VPN typu client-to-site
 - Dostęp zdalny typu Clientless VPN
 - VPN typu site-to-site
- Zdalne zarządzanie
 - Zdalny dostęp do hosta

- SSH - Secure Shell
- Telnet
- Połączenia terminalowe i RDP - Remote Desktop Protocol
- Połączenia konsolowe i zarządzanie poza pasmem (out-of-band)
- Stacje przesiadkowe
- Metody połączeń API
- Materiały dodatkowe
 - Typy sieci: LAN, WLAN i WAN
 - Typy połączeń internetowych
 - VPN
 - Dostęp zdalny
- Podsumowanie koncepcji chmury
 - Centrum danych i sieci pamięci masowej
 - Projektowanie sieci w centrum danych
 - Topologia spine-leaf
 - SAN - Storage Area Networks
 - Fiber Channel
 - Koncepcje chmury
 - Skalowalność i elastyczność chmury
 - Modele wdrożenia chmury
 - Modele usług chmurowych
 - CDN - Content Delivery Networks
 - Sieci w chmurze
 - Instancje w chmurze
 - VPC - Virtual Private Cloud
 - Bramy chmurowe
 - Opcje łączności z chmurą
 - Bezpieczeństwo firewalli w chmurze
 - Kontrola ruchu w chmurze: Security Groups vs. Security Lists
 - Nowoczesne środowiska sieciowe
 - IaC - Infrastructure as Code
 - Zastosowania Infrastructure as Code
 - Kontrola wersji
 - SDN - Software-Defined Networking
 - SD-WAN - Software-Defined WAN
 - Sieci nakładkowe (overlay networks)

- Architektura Zero Trust
- SASE - Secure Access Service Edge
- Materiały dodatkowe
 - Centrum danych i sieci pamięci masowej
 - Konceptcje i sieci w chmurze
 - Nowoczesne środowiska sieciowe

Wymagania:

Rekomendowane doświadczenie: certyfikacja CompTIA A+ oraz 9-12 miesięcy praktyki na stanowisku młodszego administratora sieci lub technika wsparcia sieci.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę CompTIA. Kurs pomaga przygotować się do egzaminu certyfikacyjnego CompTIA Network+, który jest dostępny w centrach egzaminacyjnych Pearson VUE.

Każdy uczestnik autoryzowanego szkolenia CompTIA Network+ Prep Course realizowanego w Compendium CE otrzyma bezpłatny voucher na egzamin certyfikacyjny CompTIA Network+ N10-009.

Prowadzący:

Autoryzowany trener CompTIA.