Możliwość dofinansowania

CS Edu Idet Tadeusz Ruchlewicz

4,9 / 5

87 ocen

Technik wsparcia Cyberbezpieczeństwa CISCO (Cisco CCST Cybersecurity) Cisco Certified Support Technician Cybersecurity (oficjalny egzamin certyfikacyjny Cisco 100-160 CCST Cybersecurity) Małopolski pociąg do kariery – sezon I (TERMIN REALIZACJI DO USTALENIA) indywidualnie

Numer usługi 2026/05/16/153943/3564029

1 500,00 PLN brutto
1 500,00 PLN netto
1 500,00 PLN brutto/h
1 500,00 PLN netto/h

Egzamin
zdalna w czasie rzeczywistym
Zajęcia grupowe
01:00 h
01.09.2026 do 01.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	Obecni oraz przyszli administratorzy sieci komputerowych oraz pracownicy, których zakres obowiązków obejmuje zadania związane z administrowaniem sieciami komputerowymi. Osoby które chcą potwierdzić swoją wiedzę certyfikatem. Certyfikat Cisco Certified Support Technician (CCST) Networking jest skierowany do profesjonalistów sieciowych, którzy chcą zbudować kompleksową wiedzę o nowoczesnych technologiach i praktykach sieciowych. Certyfikat ten potwierdza Twoje umiejętności i wiedzę techniczną w zakresie podstawowych koncepcji i tematów sieciowych, w tym operacji sieciowych, adresowania IP, łączenia urządzeń sieciowych, mediów, rozwiązywania problemów z siecią oraz innych podstawowych protokołów umożliwiających komunikację sieciową. Certyfikat CCST Networking, idealny dla początkujących profesjonalistów IT, jest także pierwszym krokiem do uzyskania oficjalnego certyfikatu Cisco Certified Network Associate (CCNA).
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	10
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Usługa egzaminacyjna potwierdza przygotowanie do samodzielnej budowy infrastruktury teleinformatycznej opartej o sprzęt sieciowy Cisco w małej firmie. Potwierdza umiejętność samodzielnego zbudowania sieci lokalnej opartej o urządzenia firmy Cisco oraz podłączenia sieci lokalnej do Internetu.
Certyfik gwarantuje, że wybrani kandydaci posiadają podstawową wiedzę i umiejętności niezbędne do zademonstrowania działania sieci, w tym urządzeń, nośników i protokołów umożliwiających komunikację sieciową.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Projektuje, buduje i rozbudowuje sieci komputerowe.	Wykonuje projekt sieci i na jego podstawie prawidłowo buduje bądź rozbudowuje sieć komputerową.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje adresy IPv4 oraz IPv6 w zależności od zapotrzebowania sieci komputerowej.	Przyporządkowuje odpowiednie maski podsieci dla adresacji IPv4 i IPv6 na podstawie kryterium zapotrzebowania (planowanej ilości urządzeń w sieci komputerowej)	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera protokoły routingu.	Dobiera właściwy protokół routingu dla zadanej topologii sieciowej.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje protokoły routingu (RIP, EIGRP, OSPF).	Rozróżnia protokoły routingu, używa właściwego protokołu routingu dla zadanej topologii.	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje routing statyczny i dynamiczny na sprzęcie Cisco.	Konfiguruje routing statyczny i dynamiczny dla zadanej topologii sieciowej (ćwiczenie wykonywane w symulatorze sieci komputerowych)	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje switch Cisco.	Łączy się do urządzenia i je konfiguruje (samodzielne wykonanie ćwiczenia w symulatorze sieci komputerowych)	Test teoretyczny z wynikiem generowanym automatycznie
Zarządza sieciami LAN	Rozpoznaje topologię istniejącej sieci komputerowej i konfiguruje jej parametry. Bazuje na istniejącym projekcie sieci w symulatorze sieci komputerowej i dokonuje wymaganych zmian, wyświetla bieżące parametry (np. adresy MAC komputerów podpiętych do urządzenia sieciowego)	Test teoretyczny z wynikiem generowanym automatycznie
Tworzy i zarządza sieciami VLAN.	Sprawdza do jakich wirtualnych sieci podpięte są komputery, tworzy wirtualną sieć i podłącza do niej komputery. (Wykonanie ćwiczenia w symulatorze sieci komputerowej).	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: https://www.cisco.com/

Strona internetowa Instytucji Walidującej: https://www.cisco.com/

Informacje

Nazwa Podmiotu certyfikującego	Cisco Systems, Inc.

Program

Zamknięta usługa egzaminu z kwalifikacji Cisco 100-160 CCST Cybersecurity w zawodzie Technik wsparcia Cyberbezpieczeństwa CISCO.

Egzamin obejmuje następujące zagadnienia, których przyswojenie będzie zweryfikowane podczas zdawania części teoretycznej i praktycznej:

1.0 Essential Security Principles

1.1. Define essential security principles

- Vulnerabilities, threats, exploits, and risks; attack vectors; hardening; defense-in-depth; confidentiality, integrity, and availability (CIA); types of attackers; reasons for attacks; code of ethics

1.2. Explain common threats and vulnerabilities

- Malware, ransomware, denial of service, botnets, social engineering attacks (tailgating, spear phishing, phishing, vishing, smishing, etc.), physical attacks, man in the middle, IoT vulnerabilities, insider threats, Advanced Persistent Threat (APT)

1.3. Explain access management principles

- Authentication, authorization, and accounting (AAA); RADIUS; multifactor authentication (MFA); password policies

1.4. Explain encryption methods and applications

- Types of encryption, hashing, certificates, public key infrastructure (PKI); strong vs. weak encryption algorithms; states of data and appropriate encryption (data in transit, data at rest, data in use); protocols that use encryption

2.0 Basic Network Security Concepts

2.1. Describe TCP/IP protocol vulnerabilities

- TCP, UDP, HTTP, ARP, ICMP, DHCP, DNS

2.2. Explain how network addresses impact network security

- IPv4 and IPv6 addresses, MAC addresses, network segmentation, CIDR notation, NAT, public vs. private networks

2.3. Describe network infrastructure and technologies

- Network security architecture, DMZ, virtualization, cloud, honeypot, proxy server, IDS, IPS

2.4. Set up a secure wireless SoHo network

- MAC address filtering, encryption standards and protocols, SSID

2.5. Implement secure access technologies

- ACL, firewall, VPN, NAC

3.0 Endpoints Security Concepts

3.1. Describe operating system security concepts

- Windows, macOS, and Linux; security features, including Windows Defender and host-based firewalls; CLI and PowerShell; file and directory permissions; privilege escalation

3.2. Demonstrate familiarity with appropriate endpoint tools that gather security assessment information

- netstat, nslookup, tcpdump

3.3. Verify that endpoint systems meet security policies and standards

- Hardware inventory (asset management), software inventory, program deployment, data backups, regulatory compliance (PCI DSS, HIPAA, GDPR), BYOD (device management, data encryption, app distribution, configuration management)

3.4. Implement software and hardware updates

- Windows Update, application updates, device drivers, firmware, patching

3.5. Interpret system logs

- Event Viewer, audit logs, system and application logs, syslog, identification of anomalies

3.6. Demonstrate familiarity with malware removal

- Scanning systems, reviewing scan logs, malware remediation

4.0 Vulnerability Assesment and Risk Management

4.1. Explain vulnerability management

- Vulnerability identification, management, and mitigation; active and passive reconnaissance; testing (port scanning, automation)

4.2. Use threat intelligence techniques to identify potential network vulnerabilities

- Uses and limitations of vulnerability databases; industry-standard tools used to assess vulnerabilities and make recommendations, policies, and reports; Common Vulnerabilities and Exposures (CVEs), cybersecurity reports, cybersecurity news, subscription services, and collective intelligence; ad hoc and automated threat intelligence; the importance of updating documentation and other forms of communication proactively before, during, and after cybersecurity incidents; how to secure, share and update documentation

4.3. Explain risk management

- Vulnerability vs. risk, ranking risks, approaches to risk management, risk mitigation strategies, levels of risk (low, medium, high, extremely high), risks associated with specific types of data and data classifications, security assessments of IT systems (information security, change management, computer operations, information assurance)

4.4. Explain the importance of disaster recovery and business continuity planning

- Natural and human-caused disasters, features of disaster recovery plans (DRP) and business continuity plans (BCP), backup, disaster recovery controls (detective, preventive, and corrective)

5.0 Incident Handling

5.1. Monitor security events and know when escalation is required

- Role of SIEM and SOAR, monitoring network data to identify security incidents (packet captures, various log file entries, etc.), identifying suspicious events as they occur

5.2. Explain digital forensics and attack attribution processes

- Cyber Kill Chain, MITRE ATT&CK Matrix, and Diamond Model; Tactics, Techniques, and Procedures (TTP); sources of evidence (artifacts); evidence handling (preserving digital evidence, chain of custody)

5.3. Explain the impact of compliance frameworks on incident handling

- Compliance frameworks (GDPR, HIPAA, PCI-DSS, FERPA, FISMA), reporting and notification requirements

5.4. Describe the elements of cybersecurity incident response

- Policy, plan, and procedure elements; incident response lifecycle stages (NIST Special Publication 800-61 sections 2.3, 3.1-3.4

Usługa obejmuję:

1) pozyskanie i skonfigurowanie na czas egzaminu sprzętu zapewniającego dostęp do środowiska laboratoryjnego niezbędnego do przeprowadzenia egzaminu.

2) zapewnienie obsługi technicznej niezbędnej do zabezpieczenia bezawaryjnej pracy środowiska podczas egzaminu.

3) zapewnienie egzaminatora o odpowiednich kwalifikacjach niezbędnych do sprawdzenia egzaminu.

4) zapewnienie partnerstwa na potrzeby egzaminowania podczas procesu egzaminacyjnego na podstawie stosownych umów partnerstwa.

5) dostęp do platformy egzaminacyjnej na potrzeby przeprowadzenia egzaminu.

6) zapewnienie operatora systemu egzaminacyjnego jako personelu niezbędnego podczas procesu egzaminacyjnego dbającego o prawidłowy przebieg egzaminu.

Jednostką rozliczeniową jest godzina lekcyjna dydaktyczna (45 min).

Usługa z założenia prowadzona jest bez przerw.

Jeśli przerwy wystąpią nie będą wliczane w czas trwania usługi.

Jeśli przerwa wystąpi z przyczyn losowych godzina zakończenia danego bloku szkoleniowego zostanie przesunięta o czas trwania przerwy.

Jeśli jednak w danym dniu usługi przerwa zostałaby zaplanowana (np. na prośbę uczestnika) nie będzie ona wpisywana bezpośrednio jako pozycja w harmonogramie tylko blok szkoleniowy zostanie rozbity godzinowo na dwie pozycje uwzględniające rzeczywiste godziny odbywającej się usługi. Czas między tymi blokami będzie traktowany jako przerwa, która nie będzie wliczana w czas usługi.

Ilość zadań oraz czas trwania egzaminu różnią się w zależności od wylosowanego wariantu egzaminu Cisco Certified Support Technician Networking – 35-50 pytań

Czas trwania egzaminu: 50 minut.

Egzamin w formie testu jedno i wielokrotnego wyboru (test teoretyczny z wynikiem generowanym automatycznie)

Egzamin prowadzony jest w języku angielskim.

Harmonogram

Liczba pozycji harmonogramu: 1

Przedmiot / temat	Typ aktywności	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 1 -	Walidacja	01-09-2026	12:00	13:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	01:00

Rodzaj godzin	Liczba godzin
w tym suma godzin zajęć	00:00
w tym suma godzin walidacji	01:00
Suma godzin dydaktycznych bez przerw	01:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 500,00 PLN Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży
Koszt przypadający na 1 uczestnika netto	1 500,00 PLN
Koszt osobogodziny brutto	1 500,00 PLN
Koszt osobogodziny netto	1 500,00 PLN
W tym koszt certyfikowania brutto	713,40 PLN
W tym koszt certyfikowania netto	713,40 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	01:00

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Usługa egzaminacyjna (nie dotyczy) materiały udostępniono podczas usługi szkoleniowej.

Warunki uczestnictwa

Ukończona usługa administrator sieci Cisco lub posiadana wiedza przekazywana podczas usługi.

Dla uczestników projektu Kierunek Kariera Zawodowa warunkiem uczestnictwa jest zapisanie się również na usługę egzaminacyjną „Technik wsparcia Cyberbezpieczeństwa CISCO”.

W ramach usługi zapewniono jedno podejście do powyższego egzaminu certyfikującego.

Wymagana jest podstawowa wiedza na temat administrowania urządzeniami sieciowymi nie zarządzanymi z wiersza poleceń.

Informacje dodatkowe

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Kierunek Kariera Zawodowa".

EGZAMIN WYMAGANY: „Technik wsparcia Cyberbezpieczeństwa CISCO”.

Jedno podejście do wymaganego egzaminu dla uczestnika zapewniono w ramach tej usługi.

Certyfikat w Klasyfikacji Zawodów i Specjalności:

Szczegółowa nazwa kwalifikacji zawodowej: **Pozostali specjaliści do spraw sieci komputerowych (252390)**

Nazwa jednostki certyfikującej (egzaminującej): Cisco Systems, Inc.

Nazwa certyfikatu: **Cisco 100-160 CCST Cybersecurity (Cisco Certified Support Technician Cybersecurity)**

Warunki techniczne

Uczestnik powinien posiadać najnowszą wersję przeglądarki Google Chrome, najnowszą wersję programu Cisco Packet Tracer oraz łącze internetowe o przepustowości co najmniej 2 Mbps /1 Mbps z odblokowanymi portami 22, 23, 69, 3800, 5901-5908, 6101-6108, 6151-6158 na ruch wychodzący.

Linki z zaproszeniami do wideokonferencji będą wysyłane na adresy e-mail uczestników 15 minut przed rozpoczęciem spotkania.

Kontakt

TADEUSZ RUCHLEWICZ

E-mail tadeusz.ruchlewicz@gmail.com
Telefon (+48) 604 922 386