Możliwość dofinansowania

CS Edu Idet Tadeusz Ruchlewicz

4,9 / 5

89 ocen

Technik wsparcia Cyberbezpieczeństwa CISCO (szkolenie przygotowujące do oficjalnej certyfikacji Cisco 100-160 CCST Cybersecurity) Cisco Certified Support Technician Cybersecurity (Cisco CCST Cybersecurity). Małopolski pociąg do kariery – sezon I (TERMIN REALIZACJI DO USTALENIA).

Numer usługi 2026/05/16/153943/3564019

3 600,00 PLN brutto
3 600,00 PLN netto
120,00 PLN brutto/h
120,00 PLN netto/h
332,00 PLN cena rynkowa

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 30:00 h
- 01.08.2026 do 14.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikatory projektów	Małopolski Pociąg do kariery
Grupa docelowa usługi	Szkolenie jest adresowane do: • Osób chcących wejść do branży Cyberbezpieczeństwa. • Pracowników działów IT, którzy chcą rozszerzyć swoje kompetencje o ochronę danych. • Administratorów systemów operacyjnych odpowiedzialnych za hardening (utwardzanie) środowiska. • Osób odpowiedzialnych za zgodność z procedurami bezpieczeństwa w firmach. **Usługa również adresowana dla Uczestników Projektu "Małopolski pociąg do kariery - sezon 1" i/lub dla Uczestników Projektu "Nowy start w Małopolsce z EURESem".**
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

Celem jest przygotowanie uczestnika do pracy na stanowiskach typu Entry-level Cybersecurity Analyst lub Security Support. Szkolenie kładzie nacisk na praktyczne aspekty monitorowania bezpieczeństwa, reagowania na incydenty oraz przygotowanie do egzaminu certyfikacyjnego Cisco CCST Cybersecurity.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia techniki stosowane przez hakerów oraz metody obrony przed nimi; stosuje zasady kryptografii i kontroli dostępu.	Diagnozuje wektory ataków.	Test teoretyczny z wynikiem generowanym automatycznie
	Klasyfikuje rodzaje zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie
Zabezpiecza stację roboczą, przeprowadza audyt podstawowych ustawień sieciowych.	Stosuje model CIA w praktyce.	Test teoretyczny z wynikiem generowanym automatycznie
	Ocenia ryzyko dla zasobów IT.	Test teoretyczny z wynikiem generowanym automatycznie
	Konfiguruje bezpieczne konto użytkownika.	Test teoretyczny z wynikiem generowanym automatycznie
	Zarządza poprawkami systemu.	Test teoretyczny z wynikiem generowanym automatycznie
	Konfiguruje zaporę ogniową.	Test teoretyczny z wynikiem generowanym automatycznie
Diagnozuje naruszenie bezpieczeństwa	Wymienia zalety stosowania bezpiecznych tuneli VPN.	Test teoretyczny z wynikiem generowanym automatycznie
		Test teoretyczny z wynikiem generowanym automatycznie
	Identyfikuje podejrzaną aktywność w sieci.	Test teoretyczny z wynikiem generowanym automatycznie
	Samodzielnie rozwiązuje test egzaminacyjny na poziomie CCST Cybersecurity.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykazuje odpowiedzialność za dane wrażliwe.	Przygotowuje dokumentację zdarzenia.	Test teoretyczny z wynikiem generowanym automatycznie
	Przeszukuje logi systemowe.	Test teoretyczny z wynikiem generowanym automatycznie
	Postępuje zgodnie z instrukcją incydentu.	Test teoretyczny z wynikiem generowanym automatycznie
Współpracuje w zespole ds. bezpieczeństwa i komunikuje zagrożenia kierownictwu.	Identyfikuje incydenty i przydziela wagę do standardów cyberbezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	Stosuje procedury cyberbezpieczeństwa w przypadku potencjalnego ataku.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie to "bezpieczeństwo od podstaw" przygotowuje uczestników do rozumienia zagrożeń w świecie cyfrowym oraz wdrażania mechanizmów obronnych na poziomie systemów i sieci.

I Krajobraz zagrożeń (Threat Landscape) (Typy ataków: Malware, Phishing, Social Engineering, Ransomware)

II Zasady i ramki bezpieczeństwa (Triada CIA, standardy NIST, polityki bezpieczeństwa, zarządzanie ryzykiem)

III Bezpieczeństwo systemów końcowych (Uprawnienia, kontrola dostępu, aktualizacje, hardening Windows/Linux)

IV Ochrona sieci i komunikacji (Firewalle, systemy IDS/IPS, VPN, szyfrowanie danych, protokoły bezpieczne)

V Monitorowanie i analiza (SOC) (Analiza logów, użycie Wireshark, wykrywanie anomalii w ruchu sieciowym)

VI Reagowanie na incydenty i dokumentacja (Procedury Response, etyka zawodowa, tworzenie raportów technicznych)

VII Powtórzenie i Egzamin Próbny (Testy wiedzy, symulacje scenariuszy ataku, omówienie egzaminu)

Sposób organizacji zajęć i zastosowane metody dydaktyczne:

• Wirtualizacja: Maszyny wirtualne z systemami Kali Linux i Windows.

• Symulacje: Cisco Packet Tracer do budowy bezpiecznych topologii sieciowych.

• Analiza: Realne logi systemowe i próbki ruchu sieciowego.

Szczegółowy harmonogram i tematyka realizowana w konkretne dni ma charakter orientacyjny. Na które tematy poświęcone będzie więcej, a na które mniej czasu zależne będzie od wiedzy Uczestnika na temat omawianych zagadnień i zapotrzebowania na szczegółowe umówienie konkretnych zagadnień.

To na które zagadnienia poświęcone zostanie więcej, a na które mniej czasu jak również kolejność ich omawiania zależna będzie od potrzeb Uczestnika oraz stopnia zainteresowania i chęci zgłębienia konkretnego tematu.

W ramach szkolenia uczestnik pozna zaawansowane urządzenia sieciowe zarządzane z wiersza poleceń oraz zaawansowane mechanizmy stosowane w tego typu urządzeniach.

Zajęcia prowadzone są w formie warsztatowej gdzie każdy uczestnik uzyskuje indywidualne wsparcie w rozwiązywaniu problemów konfiguracyjnych podczas realizacji ćwiczeń laboratoryjnych na sprzęcie CISCO.

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.

Walidacja efektów uczenia przeprowadzona będzie w ostatnim dniu usługi. Odbędzie się będzie w formie testu wiedzy końcowej (z wynikiem generowanym automatycznie). Test oceniany będzie przez inną osobę niż prowadząca szkolenie (automatycznie przez system). Osoba prowadząca szkolenie nie ma wpływu na wynik uzyskany przez uczestnika.

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Krajobraz zagrożeń (Threat Landscape) (Typy ataków: Malware, Phishing, Social Engineering, Ransomware) (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	01-08-2026	17:30	22:00	04:30
2 z 11 -	Przerwa	-	01-08-2026	22:00	23:15	01:15
3 z 11 Zasady i ramki bezpieczeństwa (Triada CIA, standardy NIST, polityki bezpieczeństwa, zarządzanie ryzykiem) (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	02-08-2026	17:30	22:00	04:30
4 z 11 -	Przerwa	-	02-08-2026	22:00	23:15	01:15
5 z 11 Bezpieczeństwo syst końcowych, Uprawnienia, kontrola dostępu, aktualizacje, hardening Windows/Linux, Ochrona sieci i komunikacji, Firewalle, systemy IDS/IPS, VPN, szyfrowanie danych, prot bezpieczne	Zajęcia	TADEUSZ RUCHLEWICZ	03-08-2026	17:30	22:00	04:30
6 z 11 -	Przerwa	-	03-08-2026	22:00	23:15	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 11 Monitorowanie i analiza (SOC) (Analiza logów, użycie Wireshark, wykrywanie anomalii w ruchu sieciowym) (prezentacja + samodzielne ćwiczenia)	Zajęcia	TADEUSZ RUCHLEWICZ	05-08-2026	16:30	21:00	04:30
8 z 11 -	Przerwa	-	05-08-2026	22:30	23:45	01:15
9 z 11 Reagowanie na incydenty, dokumentacja, Procedury Response, etyka zawodowa, tworzenie raportów technicznych, Powtórzenie i Egzamin Próbny (Testy wiedzy, symulacje scenariuszy ataku, omówienie egzaminu)	Zajęcia	TADEUSZ RUCHLEWICZ	14-08-2026	16:15	21:00	04:45
10 z 11 -	Walidacja	TADEUSZ RUCHLEWICZ	14-08-2026	21:00	22:00	01:00
11 z 11 -	Przerwa	-	14-08-2026	22:00	23:15	01:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	30:00
w tym suma godzin zajęć	22:45
w tym suma godzin walidacji	01:00

Rodzaj godzin	Liczba godzin
w tym suma przerw	06:15
Suma godzin dydaktycznych bez przerw	31:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 600,00 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	3 600,00 PLN
Koszt osobogodziny brutto	120,00 PLN
Koszt osobogodziny netto	120,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	30:00

Prowadzący

Liczba prowadzących: 1

1 z 1

TADEUSZ RUCHLEWICZ

Specjalność w zakresie administrowania systemami i sieciami komputerowymi.

Uprawnienia;
instruktorskie z zakresu Cisco Certified Network Associate (CCNA) (Akademia Górniczo-Hutnicza), Cisco Certified Network Professional (CCNP) (Route, Switch, Troubleshoot) (WSiZ Rzeszów), certyfikat Cisco CCNAv7 200-301.
certyfikat trenera MikroTik (Łotwa); instruktor z zakresu: MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE, MTCSE, MTCSWE, certyfikat inżyniera MikroTik: MTCEWE.
Piętnastoletnie doświadczenie w pracy na stanowisku administratora sieci komputerowej Instytutu Informatyki Uniwersytetu Rzeszowskiego.

Pełnienie funkcji Koordynatora Lokalnej Akademii Cisco Uniwersytetu Rzeszowskiego.
Organizacja i prowadzenie autoryzowanych szkoleń Cisco Certified Network Associate Routing and Switching (CCNA R&S).
Organizacja i prowadzenie certyfikowanych szkoleń MikroTik Certified [Network Associate, (Routing, Wireless, Security, Traffic Control) Engineer].

Autor programu studiów podyplomowych: "Systemy i sieci komputerowe (Cisco Certified)" oraz szkolenia "Administrator sieci komputerowej (Cisco, MikroTik)" realizowanego na Uniwersytecie Rzeszowskim.

Absolwent Politechniki Rzeszowskiej: kierunek Informatyka; specjalność systemy i sieci komputerowe - uzyskany stopień mgr inż.
Absolwent Uniwersytetu Rzeszowskiego: kierunek fizyka komputerowa - uzyskany stopień mgr.
Absolwent kwalifikacyjnych studiów podyplomowych praktyczne nauczanie zawodu w grupie przedmiotów elektryczno - elektronicznych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W ramach szkolenia uczestnik otrzymuje dostęp do materiałów na platformie edukacyjnej z zakresu administrowania sieciami komputerowymi, interaktywnych ćwiczeń praktycznych, testów, quizów itd.

Uczestnik otrzymuje dostęp do symulatora sieci komputerowych oraz praktycznych ćwiczeń do wykonania przy jego użyciu.

Uczestnik otrzymuje również dostęp do autorskich ćwiczeń praktycznych z zakresu zarządzania siecią komputerową zbudowaną na bazie o urządzeń Cisco.

Warunki uczestnictwa

• Znajomość podstawowych pojęć infrastruktury IT.

• Podstawowa wiedza o sieciach komputerowych (mile widziane CCST Networking).

• Umiejętność poruszania się w systemach Windows/Linux na poziomie użytkownika.

Dla uczestników projektu Małopolski pociąg do kariery - sezon I warunkiem uczestnictwa jest zapisanie się również na usługę egzaminacyjną „Technik wsparcia Cyberbezpieczeństwa CISCO”.

Wymagany egzamin dostępny w formie osobnej usługi o numerze 2026/05/16/153943/3564029. (opublikowanej na BUR).

W ramach szkolenia uczestnik otrzymuje dostęp do materiałów na platformie edukacyjnej z zakresu administrowania sieciami komputerowymi (przygotowujących do certyfikacji CCST), interaktywnych ćwiczeń praktycznych, testów, quizów itd.

Informacje dodatkowe

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Małopolski pociąg na kariery - sezon I".

EGZAMIN WYMAGANY: „Technik wsparcia Cyberbezpieczeństwa CISCO”.

Egzamin dostępny pod nr usługi 2026/05/16/153943/3564029 na BUR.

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