Możliwość dofinansowania

Fundacja ALTERnacja

Brak ocen dla tego dostawcy

# [Kierunek - Rozwój] Cisco Network Security - kurs zaawansowany (STACJONARNY)

**Numer usługi** 2024/09/13/165599/2307037

6 400,00 PLN brutto
6 400,00 PLN netto
91,43 PLN brutto/h
91,43 PLN netto/h

Bydgoszcz / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Usługa szkoleniowa
70 h
03.01.2025 do 31.03.2025

# Informacje podstawowe

| | |
|---|---|
| **Kategoria** | Informatyka i telekomunikacja / Administracja IT i systemy komputerowe |
| **Identyfikator projektu** | Kierunek - Rozwój |
| **Sposób dofinansowania** | wsparcie dla pracodawców i ich pracowników<br>wsparcie dla osób indywidualnych |
| **Grupa docelowa usługi** | Szkolenie przeznaczone jest dla osób fizycznych lub pracowników firm:<br>• pracujących w branży sieciowej, pragnących poszerzyć lub uzupełnić wiedzę za zakresu realizacji poufności informacji przesyłanych przez sieć Internet oraz przeciwdziałania cyberatakom,<br>• operatorskich (inżynierów sieci), który zamierzają pozyskać umiejętności związane z zabezpieczeniem infrastruktury IT firmy (CyberSEC),<br>• zainteresowanych wdrażaniem tuneli VPN oraz dostępu zdalnego do infrastruktury firmowej.<br>• chcących poszerzyć lub uporządkować wiedzę i umiejętności dotyczące zabezpieczenia sieci i urządzeń Cisco, tj. przełączników, routerów, firewalli,<br>• działów IT zarządzających infrastrukturę teleinformatyczną,<br>• pracujących na stanowiskach informatyka w MŚP, świadomych poziomu zagrożenia cyberprzestępczością,<br>• chcących uzupełnić wiedzę i kwalifikacje z zakresu bezpieczeństwa sieci korporacyjnych i kampusowy,<br>• planujących przebranżowienie wewnątrz firmy na stanowiska typu CyberSEC.<br><br>Dla uczestników proj. Kierunek - Rozwój |
| **Minimalna liczba uczestników** | 10 |
| **Maksymalna liczba uczestników** | 16 |

| | |
|---|---|
| **Data zakończenia rekrutacji** | 30-12-2024 |
| **Forma prowadzenia usługi** | mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym) |
| **Liczba godzin usługi** | 70 |
| **Podstawa uzyskania wpisu do BUR** | Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych |

# Cel

## Cel edukacyjny

Usługa „Cisco Network Security - kurs zaawansowany" przygotowuje do podjęcia pracy i samodzielnej realizacji zadań inżyniera bezpieczeństwa sieci (CyberSec / SIEM).

Usługa „Cisco Network Security - kurs zaawansowany” przygotowanie do samodzielnej konfiguracji i weryfikacji działania następujących rozwiązań i komponentów sieciowych: VPN, IPS, ACL, Firewalle, protokoły kryptograficzne, routery brzegowe.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| Charakteryzuje zagrożenia bezpieczeństwa, z którymi borykają się nowoczesne infrastruktury sieciowe. | Rozróżnia zagrożenia bezpieczeństwa | Test teoretyczny |
| Definiuje politykę zabezpieczeń dla routerów Cisco. | Rozróżnia zagrożenie i metody przeciwdziałania atakom | Test teoretyczny |
| Planuje wdrożenie AAA na routerach Cisco, wykorzystując lokalną bazę danych routera oraz zewnętrzny serwer. | Definiuje konfigurację AAA w urządzeniu sieciowym | Obserwacja w warunkach symulowanych |
| Rozróżnia zagrożenia dla routerów i sieci Cisco za pomocą list kontroli dostępu (ACL). | Projektuje listy kontroli dostępu. | Test teoretyczny |
| Zarządza sieciami w sposób zapewniający bezpieczeństwo. | Uzasadnia konieczność wdrożenie odpowiednich mechanizmów bezpieczeństwa. | Obserwacja w warunkach symulowanych |
| Konfiguruje urządzenia sieciowe w sposób chroniący sieć przed atakami na warstwę 2. | Zabezpiecza przełączniki sieciowe przed atakiem do strony sieci LAN. | Obserwacja w warunkach symulowanych |

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| Projektuje zestawy funkcji firewalla Cisco IOS. | Definiuje działania firewalla. | Obserwacja w warunkach rzeczywistych |
| Implementuje urządzenie Cisco ASA w celu świadczenia usług zapory sieciowej oraz translacji adresów sieciowych (NAT/PAT). | Wdraża i weryfikuje konfigurację firewalla sprzętowego ASA. | Obserwacja w warunkach rzeczywistych |
| Planuje i wdraża tunele VPN typu site-to-site z wykorzystaniem IPsec | Definiuje parametry protokołów kryptograficznych używanych do budowy tuneli VPN. | Obserwacja w warunkach symulowanych |
| Charakteryzuje rodzaje szyfrowania, poufności, integralności i uwierzytelniania. | Rozróżnia protokoły szyfrowania oraz algorytmy zapewnienia integralności. | Test teoretyczny |
| Uzasadnia potrzebę używania firewall'i Zone-Based Policy. | Definiuje ruch interesujący przechodzący przez firewall. | Test teoretyczny |

# Kwalifikacje

## Inne kwalifikacje

### Uznane kwalifikacje

**Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?**

Certyfikat ukończenia kurs Cisco Network Security jest certyfikatem globalnym dla którego wprowadzono jednolity system walidacji w każdej Akademii Cisco, które działają w 190 krajach. Walidacja efektów kształcenia odbywa się w trakcie egzaminu końcowego, ocienianego automatycznie.

### Informacje

| | |
|---|---|
| **Podstawa prawna dla Podmiotów / kategorii Podmiotów** | uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa |
| **Nazwa/Kategoria Podmiotu prowadzącego walidację** | Fundacja ALTERnacja - Lokalna Akademia Cisco ID 20043915 |
| **Podmiot prowadzący walidację jest zarejestrowany w BUR** | Tak |
| **Nazwa/Kategoria Podmiotu certyfikującego** | Fundacja ALTERnacja - Lokalna Akademia Cisco ID 20043915 |
| **Podmiot certyfikujący jest zarejestrowany w BUR** | Nie |

# Program

Kurs Cisco Network Security jest rozpoznawalnym na świecie kursem związanym z bezpieczeństwem sieci i infrastruktury sieciowym, w skrócie CyberSEC. Zawartość merytoryczna kolejnych modułów została tak dobrana, aby uczestnik szkolenia zapoznawał się kolejno i stopniowo z protokołami oraz mechanizmami sieciowymi niwelującymi próby cyberataku z wnętrze organizacji oraz od stronym Internetu.

**Kurs Cisco Network Security składa się z  22 modułów:**

1. Zabezpieczanie sieci
2. Zagrożenia sieciowe
3. Ograniczanie zagrożeń sieciowych
4. Bezpieczny dostęp do urządzeń
5. Role administracyjne
6. Zarządzanie i monitowanie urządzeń
7. AAA – autoryzacja, uwierzytelnienie i rejestracja
8. ACL – listy kontroli dostępu
9. Technologie Firewall'i
10. Zone-Based Policy Firewall
11. Technologia IPS
12. Implementacja i działanie IPS
13. Zabezpieczanie urządzeń końcowych
14. Bezpieczeństwo warstwy L2 sieci
15. Usługi i protokoły kryptograficzne
16. Postawy uwierzytelnienia i integralności
17. Infrastruktura klucza publicznego
18. VPN – wirtualne sieci prywatne
19. Implementacja Site-to-Siete VPN
20. Podstawowa konfiguracja ASA
21. Konfiguracja firewall'a w ASA
22. Testowanie zabezpieczeń sieci

**Oficjalne materiały szkoleniowe Cisco składają się z:**

- 22 modułów tematycznych
- 23 ćwiczeń wykonywanych na sprzęcie,
- 22 zadań symulacyjnych do realizacji w środowisku Packet Tracer
- 87 ćwiczeń interaktywnych w tym materiały video i quizy,
- 8 egzaminów modułowych
- 1 egzaminy końcowego uprawniającego do otrzymania certyfikatu ukończenia szklenia wraz ze zdobytemu kompetencjami.

**Sposób prowadzenia szkolenia:**

- Kurs prowadzony jest przez certyfikowanego trenera Cisco w języku polskim,  wykłady prowadzone są po polsku.
- Student otrzymuje dostęp do certyfikowanych materiałów szkoleniowych oraz egzaminów i ćwiczeń laboratoryjnych w języku angielskim.
- Ćwiczenia rozszerzające oficjale treści, przygotowane zostały w języku polskim.
- zajęcia praktyczne realizowane są w zespołach 2-3 osobowych. Każdy student Akademii Cisco ma dostęp do indywidualnego komputera PC, przełącznika Cisco 2960, routera Cisco 4021, routera Cisco 2801 oraz firewalla ASA.

**Forma kurs:**

Szkolenie trwać będzie 83 godziny lekcyjne z czego 47 godzin STACJONARNIE (w loaboratorium sieciowym) oraz 36 godzin ZDALNIE W CZASIE RZECZYWISTYM.

- Zajęcia ze sprzętem sieciowym będą realizowane w laboratorium sieciowym Wydziału Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. W trakcie zajęć każdy uczestnik będzie miała dostęp do fizycznego sprzętu Cisco i indywidualnego komputera, co pozwoli realizować zadania przewidziane w kursie Cisco oraz zadania dodatkowe przygotowane przez trenerów. Uczestnicy będą mieli dostęp do 30 routerów Cisco, 18 przełączników Catalyst i 10 firewalli ASA.
- Zajęcia zdalne będą realizowane z wykorzystaniem:
  - system pracy grupowej Cisco WebEx,
  - narzędzia symulacyjnego Cisco Packet Tracer, które każdy z uczestników będzie używał lokalnie i będzie mógł udostępniać trenerowi oraz pozostałym uczestnikom,
  - narzędzi edukacyjnych dostępnych na platformie Cisco Netacad,

- quizów i egzaminów oraz symulacji, pozwalających weryfikować wiedzę i umiejętności

Charakterysytka kurs: https://alternacja.pl/cisco/wp-content/uploads/2023/11/Network-Security-v1.0-Product-Overview.pdf

Oficjalna strona kursu: https://www.netacad.com/courses/networking/ccna-introduction-networks

wskazać warunki organizacyjne dla przeprowadzenia szkolenia

**Warunki organizacyjne dla przeprowadzenia szkolenia:**

- w trakcie zajęć parktyczych uczestniczy szkolenia będąreliazowali konfiguracyjne zadania praktyczne w zespołach 2 lub 3 osobowych, zależnie od konkretnego zadania. Każy zespół będzie konfigurował taką zamą sieć laboarotryjną złożoną z 2-3 routerów Cisco 4221, 2-3 przełączników Cisco Catalyst 2960 oraz 2 firewalli ASA 55xx 2 lub 3 komputerów PC wara z wymaganym oprogramowanie.
- Jako godzinę szkolenia przyjmije się 45 minut.
- Walidacja będzie relizowana na na ostatnich zajęciach w postaci:
  - egzamniu teoretycznego według miezynarodowych standardów szkolenia Cisco Network Security,
  - egzaminu praktyczengo polegającego na projektowaniu, konfiguracji, testowania sieci wskazanej przez egzaminatora z uprawniwniami Cisco, także według ogólnoświatowje metodyki Network Academy.
- Opłata za usługę pokrywa wszkoszt koszty, w tym: walidację, egzaminy podstawowy i poprawkowy oraz wydanie certyfikatów.

**Szkolenie adresowane jest dla osób fizycznych lub  pracowników firm:**

- pracujących w branży sieciowej, pragnących poszerzyć lub uzupełnić wiedzę za zakresu realizacji poufności informacji przesyłanych przez sieć Internet oraz przeciwdziałania cyberatakom,
- operatorskich (inżynierów sieci), który zamierzają pozyskać umiejętności związane z zabezpieczeniem infrastruktury IT firmy (CyberSEC),
- zainteresowanych wdrażaniem tuneli VPN oraz bezpiecznego dostępu zdalnego do infrastruktury firmowej.
- chcących poszerzyć lub uporządkować wiedzę i umiejętności dotyczące zabezpieczenia sieci i urządzeń Cisco, tj. przełączników, routerów,  firewalli,
- działów IT zarządzających infrastrukturę teleinformatyczną,
- pracujących na stanowiskach informatyka w MŚP, świadomych poziomu zagrożenia cyberprzestępczością,
- chcących uzupełnić wiedzę i kwalifikacje z zakresu szeroko pojętego bezpieczeństwa sieci  korporacyjnych i kampusowy,
- planujących przebranżowienie wewnątrz firmy na stanowiska typu CyberSEC.

# Harmonogram

Liczba przedmiotów/zajęć: 42

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin | Forma stacjonarna |
|---|---|---|---|---|---|---|
| 1 z 42 Securing Networks | Piotr Żmudziński | 05-01-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 2 z 42 przerwa | Piotr Żmudziński | 05-01-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 3 z 42 Network Threats | Piotr Żmudziński | 05-01-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 4 z 42 Mitigating Threats | Piotr Żmudziński | 13-01-2025 | 16:30 | 18:00 | 01:30 | Tak |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin | Forma stacjonarna |
|---|---|---|---|---|---|---|
| 5 z 42 przerwa kawowa | Piotr Żmudziński | 13-01-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 6 z 42 Secure Device Access | Piotr Żmudziński | 13-01-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 7 z 42 Assign Administrative Roles | Piotr Żmudziński | 20-01-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 8 z 42 przerwa | Piotr Żmudziński | 20-01-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 9 z 42 Device Monitoring and Management | Piotr Żmudziński | 20-01-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 10 z 42 Authentication, Authorization, and Accounting (AAA) | Piotr Żmudziński | 27-01-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 11 z 42 przerwa kawowa | Piotr Żmudziński | 27-01-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 12 z 42 Access Control Lists | Piotr Żmudziński | 27-01-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 13 z 42 Firewall Technologies | Piotr Żmudziński | 03-02-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 14 z 42 przerwa kawowa | Piotr Żmudziński | 03-02-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 15 z 42 Zone-Based Policy Firewalls | Piotr Żmudziński | 03-02-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 16 z 42 IPS Technologies | Piotr Żmudziński | 04-02-2025 | 16:30 | 18:00 | 01:30 | Tak |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin | Forma stacjonarna |
|---|---|---|---|---|---|---|
| 17 z 42 przerwa | Piotr Żmudziński | 04-02-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 18 z 42 IPS Operation and Implementation | Piotr Żmudziński | 04-02-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 19 z 42 Endpoint Security | Piotr Żmudziński | 10-02-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 20 z 42 przerwa | Piotr Żmudziński | 10-02-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 21 z 42 Layer 2 Security Considerations | Piotr Żmudziński | 10-02-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 22 z 42 Cryptographic Services cz.1 | Piotr Żmudziński | 17-02-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 23 z 42 przerwa | Piotr Żmudziński | 17-02-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 24 z 42 Basic Integrity and Authenticity | Piotr Żmudziński | 17-02-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 25 z 42 Public Key Cryptography | Piotr Żmudziński | 24-02-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 26 z 42 przerwa | Piotr Żmudziński | 24-02-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 27 z 42 VPNs | Piotr Żmudziński | 24-02-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 28 z 42 Implement Site-to-Site IPsec VPNs with CLI cz.1 | Piotr Żmudziński | 03-03-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 29 z 42 przerwa kawowa | Piotr Żmudziński | 03-03-2025 | 18:00 | 18:15 | 00:15 | Tak |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin | Forma stacjonarna |
|---|---|---|---|---|---|---|
| 30 z 42 Implement Site-to-Site IPsec VPNs with CLI cz.2 | Piotr Żmudziński | 03-03-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 31 z 42 Introduction to the ASA cz.1 | Piotr Żmudziński | 10-03-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 32 z 42 przerwa kawowa | Piotr Żmudziński | 10-03-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 33 z 42 Introduction to the ASA cz.2 | Piotr Żmudziński | 10-03-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 34 z 42 ASA Firewall Configuration cz.1 | Piotr Żmudziński | 17-03-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 35 z 42 przerwa kawowa | Piotr Żmudziński | 17-03-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 36 z 42 ASA Firewall Configuration cz.2 | Piotr Żmudziński | 17-03-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 37 z 42 Network Security Testing cz.1 | Piotr Żmudziński | 24-03-2025 | 16:30 | 18:00 | 01:30 | Tak |
| 38 z 42 przerwa kawowa | Piotr Żmudziński | 24-03-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 39 z 42 Network Security Testing cz.2 | Piotr Żmudziński | 24-03-2025 | 18:15 | 21:30 | 03:15 | Tak |
| 40 z 42 Egzamin TEORETYCZNY | - | 31-03-2025 | 16:30 | 18:00 | 01:30 | Tak |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin | Forma stacjonarna |
|---|---|---|---|---|---|---|
| 41 z 42 przerwa kawowa | - | 31-03-2025 | 18:00 | 18:15 | 00:15 | Tak |
| 42 z 42 Egzamin PRAKTYCZNY | - | 31-03-2025 | 18:15 | 21:30 | 03:15 | Tak |

# Cennik

## Cennik

| Rodzaj ceny | Cena |
|---|---|
| **Koszt usługi brutto** | 6 400,00 PLN |
| **Koszt usługi netto** | 6 400,00 PLN |
| **Koszt godziny brutto** | 91,43 PLN |
| **Koszt godziny netto** | 91,43 PLN |
| **W tym koszt walidacji brutto** | 0,00 PLN |
| **W tym koszt walidacji netto** | 0,00 PLN |
| **W tym koszt certyfikowania brutto** | 0,00 PLN |
| **W tym koszt certyfikowania netto** | 0,00 PLN |

# Prowadzący

Liczba prowadzących: 1

1 z 1

### Piotr Żmudziński

Wykładowca akademicki od 22 lat na Wydziale Informatyki Uniwersytetu Kazimierza Wielkiego. Trener i egzaminator kursów Cisco: CCNA, CCNP, Network Security, Linux NDG od 11 lat. Pracownik dydaktyczny z doświadczeniem ponad 10.000 godzin.

# Informacje dodatkowe

## Informacje o materiałach dla uczestników usługi

**Każdy z uczestnik szkolenia otrzyma:**

- dostęp do platformy elearningowej netacad.com, także po zakończeniu szkolenia. W netacad.com dostępne są kompletne materiały e-learningowe do kursu,
- dostęp do własnej platformy Fundacji ALTERnacja celem pobierania zadań symulacyjnych,
- imienną licencję na oprogramowanie symulacyjne Packet Tracer, wykorzystywaną do symulacji sieci,
- dodatkowe, autorskie materiały edukacyjne, wykraczające poza ramy szkolenia Cisco Network Security.

## Warunki uczestnictwa

Przystępując do kursu Cisco Network Security, uczetnik powinien posiadać postawową wiedzę związaną z działaniem i protokołami sieci komputerowych na poziomie odpowiadającym sem.1 i sem.2 kursu Cisco CCNA.

Nie jest wymagane posiadanie certyfiaktu ukończenia szkolenia CCNA.

Szkolenie przeznaczone dla uczestników projektu WUP 'Kierunek - Rozwój'.

# Warunki techniczne

Aby uczestniczyć w zajęiach zdalnych kursu Cisco CCNA, uczestnik powinien dysponować typowym komputerem stacjonarnym lublaptopem o minimalnych parametrach:

- łącze do Internetu w dowolnej technologii (także LTE) o przepustowości przynajmniej 2Mbit/s,
- procesor Intel Core2 Duo lub lepszy,
- pamięć RAM: 4GB lub więcej,
- wolne miejsce na dysku: przynajmniej 500 MB,
- kamera i mikrofon.

Laboratorium sprzętowe jest całkowicie wyposażone, nie ma konieczności dysponowanie własnym laptopem.

# Adres

ul. Mikołaja Kopernika 1/108

85-074 Bydgoszcz

woj. kujawsko-pomorskie

Szkolenie będzie realizowane w sposób - mieszany. Część zajęć w laboratorium część zdalnie.

Zajęcia ze sprzętem sieciowym będą realizowane w laboratorium sieciowym Wydziału Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Zajęcia zdalne będą realizowane z wykorzystaniem system pracy grupowej Cisco WebEx oraz narzędzia symulacyjnego Cisco Packet Tracer.

## Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

# Kontakt


## Piotr Żmudziński

**E-mail** piotr@alternacja.pl

**Telefon** (+48) 695 616 100