



Fundacja
ALTERnacja

★★★★★ 4,6 / 5

78 ocen

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

Numer usługi 2025/12/07/165599/3197060

📍 Bydgoszcz / stacjonarna

🏠 Usługa szkoleniowa

🕒 78 h

📅 07.04.2026 do 29.06.2026

6 400,00 PLN brutto

6 400,00 PLN netto

82,05 PLN brutto/h

82,05 PLN netto/h

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Identyfikatory projektów

Kierunek - Rozwój

Grupa docelowa usługi

Szkolenie przeznaczone 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 cyberatakam,
- operatorskich (inżynierów sieci), którzy zamierzają pozyskać umiejętności związane z zabezpieczeniem infrastruktury IT firmy (CyberSEC),
- zainteresowanych wdrażaniem tuneli VPN oraz 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 bezpieczeństwa sieci korporacyjnych i kampusowy,
- planujących przebranżowienie wewnątrz firmy na stanowiska typu CyberSEC.

Dla uczestników proj. Kierunek - Rozwój

Minimalna liczba uczestników

8

Maksymalna liczba uczestników

17

Data zakończenia rekrutacji

03-04-2026

Forma prowadzenia usługi

stacjonarna

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	Test teoretyczny
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.	Test teoretyczny
Konfiguruje urządzenia sieciowe w sposób chroniący sieć przed atakami na warstwę 2.	Zabezpiecza przełączniki sieciowe przed atakiem do strony sieci LAN.	Test teoretyczny
Projektuje zestawy funkcji firewalla Cisco IOS.	Definiuje działania firewalla.	Test teoretyczny
Implementuje urządzenie Cisco ASA w celu świadczenia usług zapory sieciowej oraz translacji adresów sieciowych (NAT/PAT).	Wdraża i weryfikuje konfigurację firewalla sprzętowego ASA.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Planuje i wdraża tunele VPN typu site-to-site z wykorzystaniem IPsec	Definiuje parametry protokołów kryptograficznych używanych do budowy tuneli VPN.	Test teoretyczny
Definiuje parametry protokołów kryptograficznych używanych do budowy tuneli VPN.	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?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	Fundacja ALTERnacja - Lokalna Akademia Cisco ID 20043915, wpisana do BUR
Nazwa Podmiotu certyfikującego	Fundacja ALTERnacja - Lokalna Akademia Cisco ID 20043915, wpisana do BUR

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 wnętrza organizacji oraz od strony 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 monitorowanie 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. Podstawy uwierzytelnienia i integralności
17. Infrastruktura klucza publicznego
18. VPN – wirtualne sieci prywatne
19. Implementacja Site-to-Site 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 egzamin końcowy uprawniający do otrzymania certyfikatu ukończenia szkolenia wraz ze zdobytymi 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 oficjalne 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 kursu:

- Szkolenie trwać będzie 78, zajęcia stacjonarne tj. w laboratorium sieciowym. Zajęcia ze sprzętem sieciowym będą realizowane w laboratorium sieciowym Wydziału Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. W trakcie zajęć każdy uczestnik będzie miał 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.

Charakterystyka kursu:

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

Warunki organizacyjne dla przeprowadzenia szkolenia:

- w trakcie zajęć praktycznych uczestnicy szkolenia będą realizowali konfiguracyjne zadania praktyczne w zespołach 2 lub 3 osobowych, zależnie od konkretnego zadania. Każdy zespół będzie konfigurował taką samą sieć laboratoryjną złożoną z 2-3 routerów Cisco 4221, 2-3 przełączników Cisco Catalyst 2960 oraz 2 firewalli ASA 55xx 2 lub 3 komputerów PC wraz z wymaganym oprogramowaniem.
- Jako godzinę szkolenia przyjmuje się 45 minut.
- Walidacja będzie realizowana na ostatnich zajęciach w postaci:
 - egzaminu teoretycznego według międzynarodowych standardów szkolenia Cisco Network Security,
 - egzaminu praktycznego polegającego na projektowaniu, konfiguracji, testowaniu sieci wskazanej przez egzaminatora z uprawnieniami Cisco, także według ogólnoświatowej metodyki Network Academy.
- Opłata za usługę pokrywa wszystkie 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 z zakresu realizacji poufności informacji przesyłanych przez sieć Internet oraz przeciwdziałania cyberatakam,

- 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.

charakterystyka zajęć:

W - wykład

L - laboratorium

E - egzamin

Harmonogram

Liczba przedmiotów/zajęć: 39

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 39 Securing Networks (W)	Piotr Żmudziński	07-04-2026	16:30	18:00	01:30
2 z 39 Network Threats (W)	Piotr Żmudziński	07-04-2026	18:15	19:45	01:30
3 z 39 Network Threats (L)	Piotr Żmudziński	07-04-2026	20:00	21:30	01:30
4 z 39 Mitigating Threats (W)	Piotr Żmudziński	13-04-2026	16:30	18:00	01:30
5 z 39 Secure Device Access (W)	Piotr Żmudziński	13-04-2026	18:15	19:45	01:30
6 z 39 Secure Device Access (W)	Piotr Żmudziński	13-04-2026	20:00	21:30	01:30
7 z 39 Assign Administrative Roles (W)	Piotr Żmudziński	20-04-2026	16:30	18:00	01:30
8 z 39 Device Monitoring and Management (L)	Piotr Żmudziński	20-04-2026	18:15	19:45	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 39 Authentication, Authorization, and Accounting (W)	Piotr Żmudziński	20-04-2026	20:00	21:30	01:30
10 z 39 Authentication, Authorization, and Accounting (L)	Piotr Żmudziński	27-04-2026	16:30	18:00	01:30
11 z 39 Access Control Lists (L)	Piotr Żmudziński	27-04-2026	18:15	19:45	01:30
12 z 39 Firewall Technologies (W)	Piotr Żmudziński	27-04-2026	20:00	21:30	01:30
13 z 39 Zone-Based Policy Firewalls cz.1 (L)	Piotr Żmudziński	04-05-2026	16:30	18:00	01:30
14 z 39 Zone-Based Policy Firewalls cz.2 (L)	Piotr Żmudziński	04-05-2026	18:15	19:45	01:30
15 z 39 Zone-Based Policy Firewalls cz.3 (L)	Piotr Żmudziński	04-05-2026	20:00	21:30	01:30
16 z 39 IPS Technologies (W)	Piotr Żmudziński	11-05-2026	16:30	18:00	01:30
17 z 39 IPS Operation and Implementation (W)	Piotr Żmudziński	11-05-2026	18:15	19:45	01:30
18 z 39 Endpoint Security (W)	Piotr Żmudziński	11-05-2026	20:00	21:30	01:30
19 z 39 Layer 2 Security Considerations (L)	Piotr Żmudziński	18-05-2026	16:30	18:00	01:30
20 z 39 Layer 2 Security Considerations (L)	Piotr Żmudziński	18-05-2026	18:15	19:45	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 39 Cryptographic Services (W)	Piotr Żmudziński	18-05-2026	20:00	21:30	01:30
22 z 39 Basic Integrity and Authenticity (W)	Piotr Żmudziński	25-05-2026	16:30	18:00	01:30
23 z 39 Public Key Cryptography (W)	Piotr Żmudziński	25-05-2026	18:15	19:45	01:30
24 z 39 VPNs (W)	Piotr Żmudziński	25-05-2026	20:00	21:30	01:30
25 z 39 Implement Site-to-Site IPsec VPNs with CLI (L)	Piotr Żmudziński	01-06-2026	16:30	18:00	01:30
26 z 39 Implement Site-to-Site IPsec VPNs with CLI (L)	Piotr Żmudziński	01-06-2026	18:15	19:45	01:30
27 z 39 Introduction to the ASA (W)	Piotr Żmudziński	01-06-2026	20:00	21:30	01:30
28 z 39 Introduction to the ASA (L)	Piotr Żmudziński	08-06-2026	16:30	18:00	01:30
29 z 39 Introduction to the ASA (L)	Piotr Żmudziński	08-06-2026	18:15	19:45	01:30
30 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	08-06-2026	20:00	21:30	01:30
31 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	15-06-2026	16:30	18:00	01:30
32 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	15-06-2026	18:15	19:45	01:30
33 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	15-06-2026	20:00	21:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
34 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	22-06-2026	16:30	18:00	01:30
35 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	22-06-2026	18:15	19:45	01:30
36 z 39 Network Security Testing (L)	Piotr Żmudziński	22-06-2026	20:00	21:30	01:30
37 z 39 Ćwiczenie podsumowujące (L)	Piotr Żmudziński	29-06-2026	16:30	18:00	01:30
38 z 39 Egzamin (E)	-	29-06-2026	18:15	19:45	01:30
39 z 39 Egzamin (E)	-	29-06-2026	20:00	21:30	01:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 400,00 PLN
Koszt przypadający na 1 uczestnika netto	6 400,00 PLN
Koszt osobogodziny brutto	82,05 PLN
Koszt osobogodziny netto	82,05 PLN
W tym koszt walidacji brutto	100,00 PLN
W tym koszt walidacji netto	100,00 PLN
W tym koszt certyfikowania brutto	200,00 PLN
W tym koszt certyfikowania netto	200,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Piotr Żmudziński

Przez ostatnie 5 lat: (1) wykładowca akademicki na Wydziale Informatyki Uniwersytetu Kazimierza Wielkiego, (2) przeprowadził ponad 3.000 zajęć dydaktycznych. Przez ostatnie 5 lat trener i egzaminator njanowszych wersji kursów Cisco: CCNA, CCNP, Network Security, zrealizował 12 szkoleń Cisco:

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, uczestnik powinien posiadać podstawową wiedzę związaną z działaniem sieci oraz wiedzy związanej z protokołami sieci komputerowych na poziomie odpowiadającym sem.1 i sem.2 kursu Cisco CCNA.

Nie jest wymagane posiadanie certyfikatu ukończenia szkolenia CCNA.

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

Informacje dodatkowe

Zawarto umowę z WUP w Toruniu w ramach projektu Kierunek – Rozwój

Jako godzinę szkolenia przyjmuje się godzinę dydaktyczną tj. 45 minut. Przerwy między w zajęciach nie są wliczane do czasu szkolenia.

Kwalifikacja lub kompetencja związana z cyfrową transformacją. Zawierza także treści dot. zielonych technologii.

Podatnik zwolniony z podatku VAT na podstawie art. 43 ust. 1 pkt 29c ustawy o podatku od towarów i usług.

Adres

ul. Mikołaja Kopernika 1/108

85-074 Bydgoszcz

woj. kujawsko-pomorskie

Zajęcia ze sprzętem sieciowym będą realizowane w laboratorium sieciowym Wydziału Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy.

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt



Piotr Żmudziński

E-mail piotr@alternajca.pl

Telefon (+48) 695 616 100