Możliwość dofinansowania

Cisco Network Security - kurs zaawansowany (ZDALNY)

Numer usługi 2025/11/07/165599/3134375

6 400,00 PLN brutto
6 400,00 PLN netto
82,05 PLN brutto/h
82,05 PLN netto/h

Fundacja ALTERnacja

4,6 / 5

78 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
78 h
03.03.2026 do 26.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób fizycznych lub pracowników firm: • chcących uzupełnić wiedzę i kwalifikacje z zakresu bezpieczeństwa sieci korporacyjnych i kampusowych, • planujących przebranżowienie lub zmianę roli wewnątrz firmy na stanowiska typu CyberSEC. • studiują kierunki techniczne, • pracujących w branży sieciowej, pragnących poszerzyć lub uzupełnić wiedzę z zakresu realizacji poufności informacji przesyłanych przez sieć Internet oraz przeciwdziałania cyberatakom, • operatorskich (inżynierów sieci), którzy zamierzają pozyskać umiejętności związane z zabezpieczaniem sieci, • 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, • zarządzających infrastrukturę teleinformatyczną, • pracujących na stanowiskach informatyka w MŚP, świadomych poziomu zagrożenia ataków w cyberprzestrzeni.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	02-03-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	78
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 (ZDALNY)" przygotowuje do podjęcia pracy i samodzielnej realizacji zadań inżyniera bezpieczeństwa sieci (CyberSec / SIEM).

Usługa „Cisco Network Security - kurs zaawansowany (ZDALNY)” przygotowuje do samodzielnej konfiguracji i weryfikacji działania następujących rozwiązań i komponentów sieciowych: VPN, IPS, ACL, firewalle (polityki i reguły), algorytmy kryptograficzne, wzmacniania routerów brzegowych.

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 z wynikiem generowanym automatycznie
Definiuje politykę zabezpieczeń dla routerów Cisco.	Rozróżnia zagrożenie i metody przeciwdziałania atakom	Test teoretyczny z wynikiem generowanym automatycznie
Planuje wdrożenia AAA na routerach Cisco, wykorzystując lokalną bazę danych routera oraz zewnętrzny serwer.	Definiuje konfigurację AAA w urządzeniu sieciowym	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia zagrożenia dla routerów i sieci Cisco za pomocą list kontroli dostępu (ACL).	Projektuje listy kontroli dostępu.	Test teoretyczny z wynikiem generowanym automatycznie
Zarządza sieciami w sposób zapewniający bezpieczeństwo.	Uzasadnia konieczność wdrożenia odpowiednich mechanizmów bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Konfiguruje urządzenia sieciowe w sposób chroniący sieć przed atakami na warstwę 2.	Zabezpiecza przełączniki sieciowe przed atakiem od strony sieci LAN.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje zestawy funkcji firewalla Cisco IOS.	Definiuje działania firewalla.	Test teoretyczny z wynikiem generowanym automatycznie
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 z wynikiem generowanym automatycznie

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 z wynikiem generowanym automatycznie
Uzasadnia potrzebę używania firewall'i Zone-Based Policy.	Definiuje ruch interesujący przechodzący przez firewall.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kwalifikacje niewłączone do ZSK

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	Cisco Networking Academy, której członkiem jest Fundacja ALTERnacja (Lokalna Akademia Cisco ID 20043915) - zarejestrowana w BUR

Program

Kurs Cisco Network Security jest rozpoznawalnym na świecie kursem związanym z bezpieczeństwem sieci i infrastruktury sieciowej, 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. Nazewnictwo zgodne z oficjalnymi modułami Cisco NetAcad.

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. 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 firewalla 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 egzaminu końcowego uprawniającego do otrzymania certyfikatu ukończenia szkolenia wraz ze zdobytymi kompetencjami.

Sposób prowadzenia szkolenia:

- Kurs prowadzony jest za pomocą platformy Cisco Webex 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 indywidualnie przez każdego uczestnika w aplikacji Packet Tracer, którą uczestnicy otrzymują wraz z prawami do wykorzystania także po zakończeniu kursu. W środowisku symulacyjnym dostępne są routery, przełączniki oraz firewalle ASA.

Forma kurs:

- Szkolenie trwać będzie 78 godzin lekcyjnych, zajęcia realizowane będą w sposób zdalny w czasie rzeczywistym. Dydaktyka prowadzona będzie przez certyfikowanego (uprawnionego) trenera Cisco.

Charakterystyka kurs:

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

Zielone kompetencje oraz transformacja cyfrowa:

Szkolenie Cisco Network Security wpisuje się w koncepcję zielonych kompetencji ponieważ nowoczesne technologie komunikacyjne są rdzeniem transformacji cyfrowej, niezbędnej do faktycznej realizacji czystych oraz niskoemisyjnych technologii. Technologie zabezpieczeń sieci oraz informacje jakie sieciami są przesyłane zawarte w kursie Cisco Network Security umożliwiają firmom bezpieczną TRANSFORMACJĘ CYFROWA, która wprost pozwoli:

- skrócić czas realizacji procesów,
- na bezpieczne zarządzanie informacjami (w trakcie tranzytu),
- wprowadzać nowe produkty i usługi szybciej i bezpieczniej,
- zautomatyzować i przyspieszyć procesy w firmie, bez narażenia na utratę poufności danych,
- uzyskać przewagę konkurencyjną w stosunku do innych firm,
- na bezpieczną współpracę z dostawcami, klientami, partnerami,
- podnieść bezpieczeństwo obsługi klientów,
- zajmować mniej powierzchni magazynowej, szaf i dokumentów,
- lepiej chronić firmowe dane (CyberSecurity),
- obniżyć energochłonność komunikacji (GreenEthernet / Energy-Efficient Ethernet, IEEE 802.3az)

Nabyte przez uczestników szkolenia kompetencje cyfrowe wpisują się w Europejską Ramą Kompetencji Cyfrowych dla Obywateli (DigComp 2.2), w szczególności:

Obszar 2: Komunikacja i współpraca (2.1, 2.6)

Obszar 4: Bezpieczeństwo (4.1 / 4.4)

Obszar 5: Rozwiązywanie problemów (5.1 / 5.3)

Cisco Networking Academy, której członkiem jest Fundacja ALTERnacja (Lokalna Akademia Cisco ID 20043915) - zarejestrowana w BUR.

Uznawanie kwalifikacje

Kurs Cisco Network Securtiy jest rozpoznawalnym i cenionym kursem sieciowym na świecie. Kurs Network Security jest realizowany w strukturze edukacyjnej Cisco Networking Academy, która działa na świecie od ponad 20 lat i zrzesza ponad **11 700** akademii lokalnych w **190** krajach. Proces dydaktyczny jest identyczny na całym świecie, ponieważ Cisco Networking Academy ustandaryzowało szczegółowo proces dydaktyczny, dostarczając jednolite w skali świata: (1) wykłady, (2) instrukcje laboratoryjne, (3) środowisko realizacji kursu – netacad.com, (4) narzędzie symulacyjne Packet Tracer, (5) pliki symulacyjne z wbudowanym mechanizmem weryfikacyjnym. Na końcu procesu realizowana jest ujednolicona walidacja osiągniętych efektów kształcenia, która jest procesem zautomatyzowanym, przez co nie podlega ewentualnym wpływom ludzkim. Walidację nadzoruje egzaminator, który nie prowadził zajęć z daną grupą uczestników.

Fundacja ALTERnacja została pozytywnie zweryfikowana merytorycznie i na podstawie umowy z Cisco Networking Academy, będącą częścią Cisco Systems, Inc. z siedzibą w San Jose, otrzymała uprawnienia walidatora i wystawcy certyfikatów uzyskania wymaganych przez system kompetencji z zakresu kursów: CCNA, Network Security, CCNP etc. System walidacyjny efektów uczenia realizowany jest globalnie, na poziomie międzynarodowym. Wyniki walidacji są automatycznie generowane przez dedykowany system i dostarczane uczestnikowi jako ocena wiedzy i umiejętności. Pozytywna walidacja kwalifikacji i wydanie certyfikatu następuje dla uczestników, którzy otrzymali wymaganą sumę punktów z egzaminu. Na mocy umowy z Cisco Fundacja ALTERnacja posiada uprawnienia do umieszczania własnego logo obok logo Cisco Networking Academy jako instytucji certyfikującej. [Dot. 3.1.2.1 karty usługi 4) i 5)]

Warunki organizacyjne dla przeprowadzenia szkolenia:

- W trakcie zajęć symulacyjnych uczestnicy szkolenia realizują konfigurację urządzeń sieciowych w dedykowanym do kursu środowisku symulacyjnym Packet Tracer, umożliwiającym budowę sieci złożonych z routerów Cisco serii 4000, przełączników Catalyst oraz firewalli ASA 5506X.
- Jako godzinę szkolenia przyjmuje się 45 minut.
- Walidacja będzie realizowana na na ostatnich zajęciach w postaci egzaminu teoretycznego według międzynarodowych standardów szkolenia Cisco Network Security. Proces walidacji i prowadzenia szkolenia będą realizowały inne osoby, aby zyskać obiektywną ocenę uczestnika.
- Opłata za usługę pokrywa wszystkie koszty, w tym: walidację, egzaminy podstawowy i poprawkowy oraz wydanie i przesłanie pocztą uzyskanych 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.

Charakterystyka zajęć:

W - wykład na żywo

R - rozmowa z uczestnikami / interakcja

L - realizacja ćwiczenia laboratoryjne pod nadzorem wykładowcy, np. poprzez współdzielenie ekranu.

E - egzamin, realizowany indywidualnie przez uczestnika na platformie www.netacad.com pod nadzorem egzaminatora.

Harmonogram

Liczba przedmiotów/zajęć: 39

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 39 Securing Networks (W/R)	Piotr Żmudziński	03-03-2026	16:30	18:00	01:30
2 z 39 Network Threats (W/R)	Piotr Żmudziński	03-03-2026	18:15	19:45	01:30
3 z 39 Network Threats (L)	Piotr Żmudziński	03-03-2026	20:00	21:30	01:30
4 z 39 Mitigating Threats (W/R)	Piotr Żmudziński	10-03-2026	16:30	18:00	01:30
5 z 39 Secure Device Access (W)	Piotr Żmudziński	10-03-2026	18:15	19:45	01:30
6 z 39 Secure Device Access (W)	Piotr Żmudziński	10-03-2026	20:00	21:30	01:30
7 z 39 Assign Administrative Roles (W)	Piotr Żmudziński	17-03-2026	16:30	18:00	01:30
8 z 39 Device Monitoring and Management (L)	Piotr Żmudziński	17-03-2026	18:15	19:45	01:30
9 z 39 Authentication, Authorization, and Accounting (W)	Piotr Żmudziński	17-03-2026	20:00	21:30	01:30
10 z 39 Authentication, Authorization, and Accounting (L)	Piotr Żmudziński	24-03-2026	16:30	18:00	01:30
11 z 39 Access Control Lists (L)	Piotr Żmudziński	24-03-2026	18:15	19:45	01:30
12 z 39 Firewall Technologies (W)	Piotr Żmudziński	24-03-2026	20:00	21:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 39 Zone-Based Policy Firewalls cz.1 (L)	Piotr Żmudziński	31-03-2026	16:30	18:00	01:30
14 z 39 Zone-Based Policy Firewalls cz.2 (L)	Piotr Żmudziński	31-03-2026	18:15	19:45	01:30
15 z 39 Zone-Based Policy Firewalls cz.3 (L)	Piotr Żmudziński	31-03-2026	20:00	21:30	01:30
16 z 39 IPS Technologies (W)	Piotr Żmudziński	07-04-2026	16:30	18:00	01:30
17 z 39 IPS Operation and Implementation (W)	Piotr Żmudziński	07-04-2026	18:15	19:45	01:30
18 z 39 Endpoint Security (W)	Piotr Żmudziński	07-04-2026	20:00	21:30	01:30
19 z 39 Layer 2 Security Considerations (L)	Piotr Żmudziński	14-04-2026	16:30	18:00	01:30
20 z 39 Layer 2 Security Considerations (L)	Piotr Żmudziński	14-04-2026	18:15	19:45	01:30
21 z 39 Cryptographic Services (W)	Piotr Żmudziński	14-04-2026	20:00	21:30	01:30
22 z 39 Basic Integrity and Authenticity (W)	Piotr Żmudziński	21-04-2026	16:30	18:00	01:30
23 z 39 Public Key Cryptography (W)	Piotr Żmudziński	21-04-2026	18:15	19:45	01:30
24 z 39 VPNs (W)	Piotr Żmudziński	21-04-2026	20:00	21:30	01:30
25 z 39 Implement Site-to-Site IPsec VPNs with CLI (L)	Piotr Żmudziński	28-04-2026	16:30	18:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 39 Implement Site-to-Site IPsec VPNs with CLI (L)	Piotr Żmudziński	28-04-2026	18:15	19:45	01:30
27 z 39 Introduction to the ASA (W)	Piotr Żmudziński	28-04-2026	20:00	21:30	01:30
28 z 39 Introduction to the ASA (L)	Piotr Żmudziński	05-05-2026	16:30	18:00	01:30
29 z 39 Introduction to the ASA (L)	Piotr Żmudziński	05-05-2026	18:15	19:45	01:30
30 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	05-05-2026	20:00	21:30	01:30
31 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	12-05-2026	16:30	18:00	01:30
32 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	12-05-2026	18:15	19:45	01:30
33 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	12-05-2026	20:00	21:30	01:30
34 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	19-05-2026	16:30	18:00	01:30
35 z 39 ASA Firewall Configuration (L)	Piotr Żmudziński	19-05-2026	18:15	19:45	01:30
36 z 39 Network Security Testing (L)	Piotr Żmudziński	19-05-2026	20:00	21:30	01:30
37 z 39 Ćwiczenie podsumowujące (L)	Piotr Żmudziński	26-05-2026	16:30	18:00	01:30
38 z 39 Egzamin (E)	-	26-05-2026	18:15	19:45	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
39 z 39 Egzamin (E)	-	26-05-2026	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 najnowszych wersji kursów Cisco: CCNA, CCNP, Network Security, zrealizował 12 szkoleń Cisco:

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik szkolenia otrzyma:

- dostęp do platformy netacad.com, także po zakończeniu szkolenia. W netacad.com dostępne są kompletne materiały szkoleniowe kursu,
- dostęp do własnej platformy Cisco, celem pobierania zadań symulacyjnych,
- 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 elementarną wiedzę związaną z działaniem sieci komputerowych.

Nie jest wymagane posiadanie certyfikatu ukończenia szkolenia CCNA.

Szkolenie przeznaczone dla uczestników posiadających dowolne dofinansowanie z programów wsparcia RP.

Informacje dodatkowe

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. Zawiera 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.

Warunki techniczne

Aby uczestniczyć w certyfikowanym szkoleniu Cisco Network Security uczestnik powinien dysponować typowym komputerem stacjonarnym lub laptopem o minimalnych parametrach:

1. Łącze do Internetu w dowolnej technologii (także LTE) przepustowości przynajmniej 2 Mbit/s,
2. Procesor Intel Core2 Duo lepszy lub równoważny,
3. Pamięć RAM: 8GB lub więcej,
4. Wolne miejsce na dysku: przynajmniej 500 MB,
5. Kamerę oraz mikrofon.

Kontakt

Piotr Żmudziński

E-mail piotr@alternacja.pl
Telefon (+48) 695 616 100