



Fundacja
ALTERnacja

Brak ocen dla tego dostawcy

Cisco Network Security

Numer usługi 2024/04/30/165599/2139249

📍 Bydgoszcz / mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

🏠 Usługa szkoleniowa

🕒 72 h

📅 12.09.2024 do 27.12.2024

6 400,00 PLN brutto

6 400,00 PLN netto

88,89 PLN brutto/h

88,89 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Identyfikator projektu	Kierunek - Rozwój
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	<p>Szkolenie przeznaczone jest dla osób fizycznych lub pracowników firm:</p> <ul style="list-style-type: none">• 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 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.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	16
Data zakończenia rekrutacji	12-07-2024

Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	72
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Zasadniczym celem certyfikowanego kursu Cisco Network Security jest:

- dostarczenie kluczowej wiedzy i umiejętności z obszaru bezpieczeństwa sieci,
- wskazanie potencjalnych zagrożeń dla przechowywania i przesyłu danych przez infrastrukturę teleinformatyczną
- zwiększenie odporności infrastruktury sieciowej na cyberataki,
- uzupełnianie wcześniej nabytej wiedzy sieciowej o komponent SEC, w tym VPN, IPS, Firewallle,
- poszerzanie świadomości zagrożenia CyberSEC dla organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozumie zagrożenia bezpieczeństwa, z którymi borykają się nowoczesne infrastruktury sieciowe.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi bezpiecznie konfigurować routery Cisco.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi wdrażać AAA na routerach Cisco, wykorzystując lokalną bazę danych routera oraz zewnętrzny serwer.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi zwalczać zagrożenia dla routerów i sieci Cisco za pomocą list kontroli dostępu (ACL).	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi projektować, zarządzać sieciami w sposób zapewniający bezpieczeństwo.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi zabezpieczać przed powszechnymi atakami na warstwę 2.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi wdrażać zestaw funkcji firewalle Cisco IOS.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Potrafi implementować urządzenie Cisco ASA w celu świadczenia usług zapory sieciowej oraz translacji adresów sieciowych (NAT/PAT).	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi wdrażać tunele VPN typu site-to-site z wykorzystaniem IPsec	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Wie jak wyjaśniać rodzaje szyfrowania, poufności, integralności i uwierzytelniania.	Egzaminy według globalnych standardów Cisco.	Test teoretyczny
Potrafi wdrożyć firewall'a Zone-Based Policy.	Egzaminy według globalnych standardów Cisco.	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, ocenianego 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 wnętrza organizacji oraz od strony Internetu.

Kurs Cięci 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-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 końcowo 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.

Charakterystyka kursu: <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>

Harmonogram

Liczba przedmiotów/zajęć: 23

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 23 Securing Networks	Piotr Żmudziński	12-09-2024	16:30	18:30	02:00	Nie
2 z 23 Network Threats	Piotr Żmudziński	12-09-2024	18:30	21:30	03:00	Nie
3 z 23 Mitigating Threats	Piotr Żmudziński	19-09-2024	16:30	18:30	02:00	Nie
4 z 23 Secure Device Access	Piotr Żmudziński	19-09-2024	18:30	21:30	03:00	Nie
5 z 23 Introduction to the ASA	Piotr Żmudziński	20-09-2024	16:30	21:30	05:00	Tak
6 z 23 Device Monitoring and Management	Piotr Żmudziński	23-09-2024	18:30	21:30	03:00	Nie
7 z 23 Assign Administrative Roles	Piotr Żmudziński	26-09-2024	16:30	18:30	02:00	Nie
8 z 23 Authentication, Authorization, and Accounting (AAA)	Piotr Żmudziński	03-10-2024	16:30	18:30	02:00	Tak
9 z 23 Access Control Lists	Piotr Żmudziński	03-10-2024	18:30	21:30	03:00	Tak
10 z 23 Firewall Technologies	Piotr Żmudziński	10-10-2024	16:30	18:30	02:00	Tak
11 z 23 Zone-Based Policy Firewalls	Piotr Żmudziński	10-10-2024	18:30	21:30	03:00	Tak
12 z 23 IPS Technologies	Piotr Żmudziński	17-10-2024	16:30	18:30	02:00	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
13 z 23 IPS Operation and Implementation	Piotr Żmudziński	17-10-2024	18:30	21:30	03:00	Tak
14 z 23 Endpoint Security	Piotr Żmudziński	24-10-2024	16:30	18:30	02:00	Tak
15 z 23 Layer 2 Security Considerations	Piotr Żmudziński	24-10-2024	18:30	21:30	03:00	Tak
16 z 23 Cryptographic Services	Piotr Żmudziński	07-11-2024	16:30	21:30	05:00	Tak
17 z 23 Basic Integrity and Authenticity	Piotr Żmudziński	14-11-2024	16:30	21:30	05:00	Tak
18 z 23 Public Key Cryptography	Piotr Żmudziński	21-11-2024	16:30	18:30	02:00	Tak
19 z 23 VPNs	Piotr Żmudziński	21-11-2024	18:30	21:30	03:00	Tak
20 z 23 Implement Site-to-Site IPsec VPNs with CLI	Piotr Żmudziński	28-11-2024	18:30	21:30	03:00	Tak
21 z 23 ASA Firewall Configuration	Piotr Żmudziński	05-12-2024	16:30	21:30	05:00	Tak
22 z 23 Network Security Testing	Piotr Żmudziński	19-12-2024	16:30	21:30	05:00	Tak
23 z 23 Egzamin fianłowy - CERTYFIKATY	Piotr Żmudziński	27-12-2024	16:30	20:30	04:00	Nie

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	88,89 PLN
Koszt osobogodziny netto	88,89 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

Terner

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,
- dotatkowe, 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 i protokołami sieci komputerowych na poziomie odpowiadającym sem.1 i sem.2 kursu Cisco CCNA.

Nie jest wymagane posiadanie certyfiaktu ukończenia szkolenia CCNA.

Warunki techniczne

Aby uczestniczyć w zajęciach zdalnych kursu Cisco CCNA, uczestnik powinien dysponować typowym komputerem stacjonarnym lub laptopem 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. 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 udostępnić trenerowi oraz pozostałym uczestnikom,
- narzędzi edukacyjnych dostępnych na platformie Cisco Netacad,
- quizów i egzaminów oraz symulacji, pozwalających weryfikować wiedzę i umiejętności

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt



Piotr Żmudziński

E-mail piotr@alternacja.pl

Telefon (+48) 695 616 100