Możliwość dofinansowania

Sieci teleinformatyczne / Etap III / Bezpieczeństwo sieci - ćwiczenia praktyczne.

Numer usługi 2025/06/26/158529/2838672

4 797,00 PLN brutto
3 900,00 PLN netto
199,88 PLN brutto/h
162,50 PLN netto/h

Notebook Master Sp. z o.o.

4,7 / 5

179 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
24 h
17.11.2025 do 19.11.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest zarówno do osób fizycznych, jak i do przedsiębiorców i ich pracowników pracujących w branży IT, którzy chcą nabyć wiedzę i umiejętności z zakresu dot. sieci teleinformatycznych, i wykorzystać je w ramach prowadzonej działalności gospodarczej i etatu. Usługa również adresowana dla Uczestników Projektu "Małopolski pociąg do kariery - sezon 1".
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	16-11-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Usługa "Sieci teleinformatyczne / Etap III / Bezpieczeństwo sieci - ćwiczenia praktyczne.", prowadzi do nabycia specjalistycznych kompetencji w obszarze tematycznym szkolenia (w tym do rozwoju umiejętności w obszarze TIK (ITC)

oraz kompetencji cyfrowych) oraz przygotowuje do samodzielnego i prawidłowego wykonywania obowiązków w zakresie dot. administrowania i konfiguracji sieci, zgodnie z planem ramowym szkolenia.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Projektuje sieci wobec indywidualnych potrzeb klientów.	Prawidłowo czyta makiety szkieletowe.	Test teoretyczny
	Rozróżnia adresacje publiczną i niepubliczną zgodnie zasadami.	Test teoretyczny
Konfiguruje routing w rozbudowanych sieciach.	Rozróżnia mechanizmy translacji adresów.	Test teoretyczny
	Dobiera do sytuacji odpowiednie rodzaje routingu.	Test teoretyczny
Konfiguruje dostęp do żądanych usług w sposób bezpieczny.	Diagnozuje dostęp do konkretnych usług z poziomu konsoli.	Test teoretyczny
	Definiuje pojęcie DMZ.	Test teoretyczny
Konfiguruje firewalle dostosowane do potrzeb konkretnej sieci	Rozróżnia rodzaje firewalli.	Test teoretyczny
	Omawia budowę logiczną tabeli w firewallu.	Test teoretyczny
Zapewnia bezpieczeństwo sieciom udostępniającym usługi publicznie.	Ogranicza sfery wystąpienia ataku.	Test teoretyczny
	Monitoruje stan oprogramowania w obliczu nowych podatności.	Test teoretyczny
Zarządza ruchem w sieci.	Wymienia korzyści płynące z mądrego planowania podsieci VLAN.	Test teoretyczny
	Określa działanie VLAN.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie skierowane jest zarówno do osób fizycznych, jak i do przedsiębiorców i ich pracowników pracujących w branży IT, którzy chcą nabyć wiedzę i umiejętności z zakresu dot. sieci teleinformatycznych, i wykorzystać je w ramach prowadzonej działalności gospodarczej i etatu.

Ramowy plan kształcenia:

I. Projektowanie sieci z uwzględnieniem:

1. Standardów bezpieczeństwa.
2. Dobrych praktyk z zakresu podziału na podsieci.
3. Współpracy z sieciami obcymi.
4. Optymalizacji ruchu sieciowego.
5. Bezpiecznego udostępniania usług w sieciach publicznych.

II. Podstawy bezpieczeństwa konfiguracji sieciowych.

1. Projektowanie ograniczenia połączeń sieciowych.
2. Analiza scenariuszy typowych ataków na sieć komputerową – faza rekonesansu.
3. Projektowanie DLP (Data Leak Prevention).
4. Projektowanie całej infrastruktury sieci wraz z systemem zabezpieczeń.
5. Analiza projektu.

III. Zaawansowane konfiguracje firewalla:

1. Firewall stateful w praktyce.
2. Budowanie reguł w oparciu o dodatkowe informacje protokołów sieciowych.
3. Analiza jakości zabezpieczeń firewall.
4. Testowanie zabezpieczeń firewall.
5. Proste użycie skanera sieciowego w diagnostyce firewall.
6. Monitoring i logowanie ruchu przy pomocy firewall.
7. Zabezpieczanie podatnych usług.
8. Gromadzenie informacji dowodowej z wykonanych połączeń.

IV. Bezpieczeństwo współpracy z sieciami podmiotów partnerskich.

1. Zagadnienia bezpieczeństwa dostępu do usług.
2. Sposoby udostępnienia usług.
3. Projektowanie i wdrażanie bezpiecznego dostępu do usług.
4. Diagnostyka zabezpieczeń.

V. Ćwiczenia praktyczne z zakresu:

1. Praktycznych scenariuszy konfiguracji sieciowych.
2. Routingu w rozbudowanych sieciach firmowych.
3. Konfigurowania bezpiecznego dostępu do usług w sieciach firmowych.
4. Konfiguracji firewalli stateless i stateful.
5. Bezpieczeństwo udostępnienia usług w sieciach publicznych.
6. Ograniczania ruchu sieciowego.

Szkolenie trwa 24 godzin dydaktycznych (przerwy nie są wliczane do czasu trwania usługi) i realizowane jest w kameralnych grupach, maksymalnie 8-osobowych. Każdy uczestnik realizujący szkolenie w formie zdalnej w czasie rzeczywistym ma możliwość otrzymania od nas (za pośrednictwem kuriera) wyposażenie stanowiska szkoleniowego (po ukończeniu szkolenia sprzęt zostaje odebrany przez kuriera).

Na czas trwania usługi składa się 3 godziny zajęć teoretycznych i 21 godzin zajęć praktycznych.

Przerwy nie są wliczane do czasu trwania usługi.

Udział uczestników szkolenia realizujących je w formie zdalnej w czasie rzeczywistym potwierdza raport generowany z platformy Zoom.

Wymagana jest frekwencja na poziomie min. 80%.

Szkolenie prowadzone jest z wykorzystaniem metod nauczania aktywizujących uczestników: dyskusja w grupie, burza mózgów, ćwiczenia.

Faktura za usługę rozwojową podlega zwolnieniu z VAT dla osób korzystających z dofinansowania powyżej 70% (zgodnie z § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz. U. z 2023 r. poz. 955 z późn. zm.)).

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 22 Projektowanie sieci z uwzględnieniem: Standardów bezpieczeństwa; Dobrych praktyk z zakresu podziału na podsieci; Współpracy z sieciami obcymi. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	17-11-2025	08:45	10:15	01:30
2 z 22 Zaawansowane konfiguracje firewalla: Firewall stateful w praktyce; Budowanie reguł w oparciu o dodatkowe informacje protokołów sieciowych. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-11-2025	08:45	10:15	01:30
3 z 22 Przerwa.	Jacek Herold	17-11-2025	10:15	10:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 22 Projektowanie sieci z uwzględnieniem: Optymalizacji ruchu sieciowego; Bezpiecznego udostępniania usług w sieciach publicznych. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-11-2025	10:30	12:00	01:30
5 z 22 Przerwa.	Jacek Herold	17-11-2025	12:00	12:45	00:45
6 z 22 Podstawy bezpieczeństwa konfiguracji sieciowych:Projektowanie ograniczenia połączeń sieciowych; Analiza scenariuszy typowych ataków na sieć komputerową– faza rekonesansu. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-11-2025	12:45	14:15	01:30
7 z 22 Przerwa.	Jacek Herold	17-11-2025	14:15	14:30	00:15
8 z 22 Podstawy bezpieczeństwa konfiguracji sieciowych: Projektowanie DLP; Projektowanie całej infrastruktury sieci wraz z systemem zabezpieczeń; Analiza projektu. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-11-2025	14:30	16:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 22 Przerwa.	Jacek Herold	18-11-2025	10:15	10:30	00:15
10 z 22 Zaawansowane konfiguracje firewalla: Analiza jakości zabezpieczeń firewall; Testowanie zabezpieczeń firewall; Proste użycie skanera sieciowego w diagnostyce firewall. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-11-2025	10:30	12:00	01:30
11 z 22 Przerwa.	Jacek Herold	18-11-2025	12:00	12:45	00:45
12 z 22 Zaawansowane konfiguracje firewalla: Monitoring i logowanie ruchu przy pomocy firewall; Zabezpieczanie usług; Gromadzenie informacji dowodowej z wykonanych połączeń. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-11-2025	12:45	14:15	01:30
13 z 22 Przerwa.	Jacek Herold	18-11-2025	14:15	14:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 22 Bezpieczeństwo współpracy z sieciami podmiotów partnerskich: Zagadnienia bezpieczeństwa dostępu do usług; Sposoby udostępnienia usług. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-11-2025	14:30	16:00	01:30
15 z 22 Bezpieczeństwo współpracy z sieciami podmiotów partnerskich: Projektowanie i wdrażanie bezpiecznego dostępu do usług; Diagnostyka zabezpieczeń. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-11-2025	08:45	10:15	01:30
16 z 22 Przerwa.	Jacek Herold	19-11-2025	10:15	10:30	00:15
17 z 22 Ćwiczenia praktyczne z zakresu: Praktycznych scenariuszy konfiguracji sieciowych; Routingu w rozbudowanych sieciach. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-11-2025	10:30	12:00	01:30
18 z 22 Przerwa.	Jacek Herold	19-11-2025	12:00	12:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 22 Ćwiczenia praktyczne z zakresu: Konfigurowania bezpiecznego dostępu do usług w sieciach; Konfiguracji firewalli stateless i stateful. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-11-2025	12:45	14:15	01:30
20 z 22 Przerwa.	Jacek Herold	19-11-2025	14:15	14:30	00:15
21 z 22 Ćwiczenia praktyczne z zakresu: Bezpieczeństwo udostępnienia usług w sieciach publicznych; Ograniczania ruchu sieciowego. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	19-11-2025	14:30	15:30	01:00
22 z 22 Walidacja.	-	19-11-2025	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 797,00 PLN
Koszt przypadający na 1 uczestnika netto	3 900,00 PLN
Koszt osobogodziny brutto	199,88 PLN
Koszt osobogodziny netto	162,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jacek Herold

Sieci teleinformatyczne, audyty bezpieczeństwa, wsparcie techniczne.
Ponad 20 lat doświadczenia zawodowego. Bezpieczeństwa systemów operacyjnych i sieci. Audyty bezpieczeństwa w tym sektor bankowy - rekomendacja "D"KNF. 8 lat pracy w Wrocławskim Centrum Sieciowo Superkomputerowym WCSS.
Wykształcenie wyższe (mgr inż. elektroniki). Politechnika Wrocławska.
Ponad 3 500 godzin przeprowadzonych zajęć. Ponad 10 lat doświadczenia szkoleniowego.
Prowadzenie zajęć z zakresu bezpieczeństwa na Politechnice Wrocławskiej.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Całość opracowanych materiałów składa się z: opisów, wykresów, schematów, zdjęć i filmów. Po zakończeniu kształcenia wszyscy uczestnicy otrzymują materiały w formie skryptu dotyczące całości przekazywanej wiedzy.

Każdy uczestnik realizujący szkolenie w formie zdalnej w czasie rzeczywistym ma możliwość otrzymania od nas (za pośrednictwem kuriera) wyposażenia stanowiska szkoleniowego tj. jednostka sprzętowa wyposażona w dostęp do serwera z przygotowanym ekosystemem do wykonywania ćwiczeń oraz oprogramowanie tj. emulatory sieci i routerów oraz analizatory ruchu sieciowego Wireshark, Nmap i IPtables. Po zakończonym szkoleniu sprzęt zostaje odebrany przez kuriera.

Informacje dodatkowe

Faktura za usługę rozwojową podlega zwolnieniu z VAT dla osób korzystających z dofinansowania powyżej 70%.

Szkolenie łącznie trwa 24 godziny dydaktyczne (przerwy nie są wliczone do czasu trwania usługi), w tym 3 godziny zajęć teoretycznych i 21 godzin zajęć praktycznych.

Pierwsza przerwa zaczyna się 10:15 i kończy 10:30.

Druga przerwa zaczyna się 12:00 i kończy 12:45.

Trzecia przerwa zaczyna się 14:15 i kończy 14:30.

Szkolenie rozpoczyna się pre-testem weryfikującym początkową wiedzę uczestnika usługi rozwojowej i zakończone jest wewnętrznym egzaminem (post-test) weryfikującym i potwierdzającym pozyskaną wiedzę, pozytywne jego zaliczenie honorowane jest certyfikatem potwierdzającym jego ukończenie i uzyskane efekty kształcenia.

Warunki techniczne

Warunki techniczne niezbędne do udziału w usłudze:

- Do połączenia zdalnego w czasie rzeczywistym pomiędzy uczestnikami, a trenerem służy program “Zoom Client for Meetings” (do pobrania ze strony https://zoom.us/download).
- Komputer/laptop z kamerką internetową z zainstalowanym klientem Zoom, minimum dwurdzeniowy CPU o taktowaniu 2 GHz.
- Mikrofon i słuchawki (ewentualnie głośniki).
- System operacyjny MacOS 10.7 lub nowszy, Windows 7, 8, 10, Linux: Mint, Fedora, Ubuntu, RedHat.
- Przeglądarkę internetowa: Chrome 30 lub nowszy, Firefox 27 lub nowszy, Edge 12 lub nowszy, Safari 7 lub nowsze.

- Dostęp do internetu. Zalecane parametry przepustowości łącza: min. 5 Mbps - upload oraz min. 10 Mbps - download, zarezerwowane w danym momencie na pracę zdalną w czasie rzeczywistym. Umożliwi to komfortową komunikację pomiędzy uczestnikami, a trenerem.
- Link umożliwiający dostęp do szkolenia jest aktywny przez cały czas jego trwania, do końca zakończenia danego etapu szkolenia. Każdy uczestnik będzie mógł użyć go w dowolnym momencie trwania szkolenia.

Kontakt

Artur Kowalewski

E-mail szkolenia@notebookmaster.pl

Telefon (+48) 573 436 635