Możliwość dofinansowania

Cyber security / Etap II / Ocena bezpieczeństwa sieci firmowej - szkolenie

Numer usługi 2025/10/10/158529/3071210

6 027,00 PLN brutto
4 900,00 PLN netto
150,68 PLN brutto/h
122,50 PLN netto/h

Notebook Master Sp. z o.o.

4,7 / 5

290 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
02.03.2026 do 06.03.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe, Regionalny Fundusz Szkoleniowy II, FELB.06.03-IZ.00-0003/24 ZIPH
Grupa docelowa usługi	Szkolenie skierowane jest zarówno do osób fizycznych, jak i do przedsiębiorców i ich pracowników, którzy chcą poszerzyć swoje umiejętności i zdobyć nowe kompetencje w obszarze oceny bezpieczeństwa sieci. Usługa rozwojowa adresowa również dla Uczestników projektów, m.in.: • Małopolski pociąg do kariery • Zachodniopomorskie Bony Szkoleniowe • Kierunek – Rozwój • Regionalny Fundusz Szkoleniowy II • Lubuskie Bony Rozwojowe • Usługi rozwojowe dla mieszkańców województwa lubuskiego • Kompleksowe wsparcie firm w okresowych trudnościach
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	6
Data zakończenia rekrutacji	01-03-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40

Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Usługa "Cyber security / Etap II / Ocena bezpieczeństwa sieci firmowej", prowadzi do nabycia specjalistycznych kompetencji w obszarze tematycznym szkolenia oraz przygotowuje do samodzielnego i prawidłowego wykonywania obowiązków w zakresie dot. cyberbezpieczeństwa z przeznaczeniem oceny bezpieczeństwa sieci firmowej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Określa ryzyka związane z zagrożeniami sieciowymi.	Identyfikuje różnorodne rodzaje zagrożeń sieciowych	Test teoretyczny
	Skutecznie korzysta ze skanerów sieci.	Test teoretyczny
Charakteryzuje zaawansowane techniki skanowania środowiska sieciowego.	Prawidłowo identyfikuje przydatność i zależności między Host Discovery, Port Discovery a Version Detection	Test teoretyczny
	Analizuje korzyści wykorzystania mechanizmu NSE	Test teoretyczny
Rozpoznaje wszelkie skanery podatności, dobierając je względem potrzeb.	Omawia działanie skanerów podatności sieciowych	Test teoretyczny
	Rekomenduje właściwe skanery, kierując się potrzebami konkretnej infrastruktury	Test teoretyczny
Charakteryzuje i ocenia podatności w kontekście konkretnych infrastruktur sieciowych.	Ocenia poziom ryzyka wynikający z konkretnych zagrożeń.	Test teoretyczny
	Eliminuje czynniki wpływające na zwiększenie poziomu ryzyka.	Test teoretyczny
		Test teoretyczny
Określa priorytety działań naprawczych.	Klasyfikuje zagrożenia według ich potencjalnego wpływu na bezpieczeństwo	Test teoretyczny
	Efektywnie ustala kolejność działań naprawczych	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje i reaguje na wybrane techniki skanowania.	Identyfikuje modele skanowania środowiska sieciowego	Test teoretyczny
	Określa sposoby blokowania technik skanowania i rozpoznawania usług	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, chcących zwiększyć zakres własnych umiejętności. Udział w usłudze umożliwi uczestnikowi uzupełnienie i uporządkowanie dotychczasowej wiedzy z obszaru cyber security.

RAMOWY PLAN KSZTAŁCENIA:

I. Pre-test. Ryzyka związane z zagrożeniami sieciowymi. (teoria + praktyka)

II. Skanery sieciowe. (teoria + praktyka)

III. Techniki skanowania. (teoria + praktyka)

1. Host discovery.
2. Port discovery.
3. Version detection.
4. NSE.

IV. Skanery podatności. (teoria + praktyka)

1. Podstawy działania.
2. Konfiguracja .
3. Dopasowanie profilu skanowania.

V. Rozpoznawanie i ocena podatności, ocena zagrożeń we kontekście infrastruktury. (teoria + praktyka)

VI. Wstęp do analizy ryzyka. (teoria + praktyka)

VII. Określanie priorytetów działań naprawczych. (teoria + praktyka)

VIII. Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego. (teoria + praktyka)

IX. Blokowanie wybranych technik skanowania i rozpoznawania usług. (teoria + praktyka)

X. Walidacja.

Szkolenie wraz z walidacją trwa 40 godzin dydaktycznych (1 godz. dydaktyczna = 45 min; przerwy nie są wliczane do czasu trwania usługi), z czego 8 godz. to teoria, a 32 godz. to praktyka i realizowane jest w kameralnych grupach, maksymalnie 6-osobowych. Walidacja twa 30 min i jest uwzględniona w czasie 8 godzin teoretycznych.

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 rozpoczyna się pre-testem weryfikującym początkową wiedzę uczestnika usługi rozwojowej i zakończone jest walidacją, tj. wewnętrznym egzaminem (post-test) weryfikującym pozyskaną wiedzę i nabyte efekty kształcenia, pozytywne jego zaliczenie honorowane jest certyfikatem potwierdzającym jego ukończenie i uzyskane efekty kształcenia. Walidacja przeprowadzana jest z wykorzystaniem testu wyboru zawierającego pytania zamknięte w tym pytań typu case study (analiza konkretnego przypadku), umożliwiające sprawdzenie osiągnięcia efektów kształcenia na podstawie określonych kryteriów weryfikacji.

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

Przerwy nie są wliczane do czasu trwania usługi.

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

Zaakceptowano Regulamin "Małopolskiego Pociągu do Kariery" dla instytucji szkoleniowych.

Harmonogram

Liczba przedmiotów/zajęć: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 **Pre-test. Ryzyka związane z zagrożeniami sieciowymi cz. I. (Wykłady, dyskusja, ćwiczenia, testy; teoria 45 min + praktyka 45 min)**	Jacek Herold	02-03-2026	08:45	10:15	01:30
2 z 36 **Przerwa.**	Jacek Herold	02-03-2026	10:15	10:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 36 Ryzyka związane z zagrożeniami sieciowymi cz. II. (Wykłady, dyskusja, ćwiczeni; teoria 30 min + praktyka 60 min)	Jacek Herold	02-03-2026	10:30	12:00	01:30
4 z 36 Przerwa.	Jacek Herold	02-03-2026	12:00	12:45	00:45
5 z 36 Skanery sieciowe cz. I. (Wykłady, dyskusja, ćwiczenia; teoria 20 min + praktyka 70 min)	Jacek Herold	02-03-2026	12:45	14:15	01:30
6 z 36 Przerwa.	Jacek Herold	02-03-2026	14:15	14:30	00:15
7 z 36 Skanery sieciowe cz. II. (Wykłady, dyskusja, ćwiczenia; teoria 20 min + 70 min praktyka)	Jacek Herold	02-03-2026	14:30	16:00	01:30
8 z 36 Techniki skanowania. Host discovery. (Wykłady, dyskusja, ćwiczenia; teoria 20 min + praktyka 70 min)	Jacek Herold	03-03-2026	08:45	10:15	01:30
9 z 36 Przerwa.	Jacek Herold	03-03-2026	10:15	10:30	00:15
10 z 36 Techniki skanowania. Port discovery. (Wykłady, dyskusja, ćwiczenia; teoria 20 min + praktyka 70 min)	Jacek Herold	03-03-2026	10:30	12:00	01:30
11 z 36 Przerwa.	Jacek Herold	03-03-2026	12:00	12:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 36 Techniki skanowania. Version detection. (Wykłady, dyskusja, ćwiczenia; teoria 20 min + praktyk 70 min)	Jacek Herold	03-03-2026	12:45	14:15	01:30
13 z 36 Przerwa.	Jacek Herold	03-03-2026	14:15	14:30	00:15
14 z 36 Techniki skanowania. NSE. (Wykłady, dyskusja, ćwiczenia; teoria 15 min + praktyka 75 min)	Jacek Herold	03-03-2026	14:30	16:00	01:30
15 z 36 Skanery podatności. Podstawy działania. (Wykłady, dyskusja, ćwiczenia; teoria 15 min + praktyka 75 min)	Jacek Herold	04-03-2026	08:45	10:15	01:30
16 z 36 Przerwa.	Jacek Herold	04-03-2026	10:15	10:30	00:15
17 z 36 Skanery podatności. Konfiguracja. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	04-03-2026	10:30	12:00	01:30
18 z 36 Przerwa.	Jacek Herold	04-03-2026	12:00	12:45	00:45
19 z 36 Skanery podatności. Dopasowanie profilu skanowania. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	04-03-2026	12:45	14:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 36 Przerwa.	Jacek Herold	04-03-2026	14:15	14:30	00:15
21 z 36 Rozpoznawanie i ocena podatności, ocena zagrożeń we kontekście infrastruktury. (Wykłady, dyskusja, ćwiczenia; teoria 15 min + praktyka 75 min)	Jacek Herold	04-03-2026	14:30	16:00	01:30
22 z 36 Wstęp do analizy ryzyka. (Wykłady, dyskusja, ćwiczenia; teoria 15 min + praktyka 75 min)	Jacek Herold	05-03-2026	08:45	10:15	01:30
23 z 36 Przerwa.	Jacek Herold	05-03-2026	10:15	10:30	00:15
24 z 36 Określanie priorytetów działań naprawczych cz. I. (Wykłady, dyskusja, ćwiczenia; teoria 15 min + praktyka 75 min)	Jacek Herold	05-03-2026	10:30	12:00	01:30
25 z 36 Przerwa.	Jacek Herold	05-03-2026	12:00	12:45	00:45
26 z 36 Określanie priorytetów działań naprawczych cz. II. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	05-03-2026	12:45	14:15	01:30
27 z 36 Przerwa.	Jacek Herold	05-03-2026	14:15	14:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 36 Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego cz. I. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	05-03-2026	14:30	16:00	01:30
29 z 36 Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego cz. II. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	06-03-2026	08:45	10:15	01:30
30 z 36 Przerwa.	Jacek Herold	06-03-2026	10:15	10:30	00:15
31 z 36 Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego cz. III. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	06-03-2026	10:30	12:00	01:30
32 z 36 Przerwa.	Jacek Herold	06-03-2026	12:00	12:45	00:45
33 z 36 Blokowanie wybranych technik skanowania i rozpoznawania usług cz. I. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 80 min)	Jacek Herold	06-03-2026	12:45	14:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
34 z 36 Przerwa.	Jacek Herold	06-03-2026	14:15	14:30	00:15
35 z 36 Blokowanie wybranych technik skanowania i rozpoznawania usług cz. II. (Wykłady, dyskusja, ćwiczenia; teoria 10 min + praktyka 50 min)	Jacek Herold	06-03-2026	14:30	15:30	01:00
36 z 36 Walidacja.	-	06-03-2026	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 027,00 PLN
Koszt przypadający na 1 uczestnika netto	4 900,00 PLN
Koszt osobogodziny brutto	150,68 PLN
Koszt osobogodziny netto	122,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jacek Herold

Doświadczenie zawodowe z zakresu tematycznego szkolenia (bezpieczeństwo sieci) zdobywane poprzez aktywnie prowadzoną własna działalność w zakresie systemów sieciowo serwerowych, cyberbezpieczeństwa, audytów bezpieczeństwa (od 2011 do obecnie) i świadczenie usług w tym zakresie. Prowadzenie wykładów i zajęć za zakresie cyber security w Politechnice Wrocławskiej na Wydziale Informatyki i Telekomunikacji, na profilu cyberbezpieczeństwa zarówno w 2025 r., jak i w latach poprzednich.
Ponad 20 lat doświadczenia zawodowego.

Wykształcenie wyższe (mgr inż. elektroniki). Politechnika Wrocławska.
Ponad 3 500 godzin przeprowadzonych zajęć. Ponad 10 lat doświadczenia szkoleniowego.

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.

Informacje dodatkowe

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.)).

Szkolenie łącznie trwa 40 godzin dydaktycznych (przerwy nie są wliczone do czasu trwania usługi) i prowadzone jest przez 5 dni od poniedziałku do piątku, w godzinach od 8:45 do 16:00.

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.

Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe.

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, min. 2 GB RAM.
- 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