Możliwość dofinansowania

Cyber security / Etap I / Analiza ruchu sieciowego - szkolenie

Numer usługi 2026/01/12/158529/3253039

5 412,00 PLN brutto
4 400,00 PLN netto
169,13 PLN brutto/h
137,50 PLN netto/h

Notebook Master Sp. z o.o.

4,7 / 5

353 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
32:00 h
11.08.2026 do 14.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, FELB.06.03-IZ.00-0003/24 ZIPH, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe, Regionalny Fundusz Szkoleniowy II
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 analizy ruchu sieciowego. 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	8
Data zakończenia rekrutacji	10-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32

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

Cel

Cel edukacyjny

Usługa "Cyber security / Etap I / Analiza ruchu sieciowego" przygotowuje uczestnika do analizy ruchu sieciowego poprzez monitorowanie ruchu w sieci, identyfikowanie zagrożeń oraz wykorzystanie technik skanowania sieci.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje zagrożenia w sieci.	Identyfikuje typowe źródła zagrożeń w sieci.	Test teoretyczny
	Klasyfikuje zachowania w sieci sugerujące obecność zagrożeń.	Test teoretyczny
Wykorzystuje techniki przeciwdziałania atakom sieciowym.	Opisuje różne metody przeciwdziałania atakom sieciowym.	Test teoretyczny
Monitoruje bezpieczeństwo infrastruktury sieciowej.	Definiuje kryteria monitorowania bezpieczeństwa infrastruktury sieciowej.	Test teoretyczny
	Ocenia poziom bezpieczeństwa infrastruktury sieciowej.	Test teoretyczny
Identyfikuje podatności softwarowe.	Wykrywa słabe punkty w oprogramowaniu.	Test teoretyczny
Charakteryzuje rodzaje i cele ataków.	Kategoryzuje podatności pod względem potencjalnego wpływu na bezpieczeństwo.	Test teoretyczny
		Test teoretyczny
	Wskazuje rodzaje ataków sieciowych.	Test teoretyczny
Skanuje środowisko sieciowe.	Określa potencjalne cele ataków sieciowych.	Test teoretyczny
	Dobiera narzędzia do rekonesansu infrastruktury sieciowe.	Test teoretyczny
	Ocenia zgromadzone dane pod kątem ich przydatności.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Niweluje skutki ataków na infrastrukturę.	Analizując ruch sieciowy, identyfikuje modele skanowania środowiska sieciowego	Test teoretyczny
	Skutecznie blokuje zidentyfikowane techniki skanowania i rozpoznawania usług	Test teoretyczny
Wykonuje rekonesans infrastruktury sieciowej pod kątem bezpieczeństwa.	Przeprowadza analizę środowiska sieciowego pod kątem identyfikacji potencjalnych zagrożeń.	Test teoretyczny
	Ocenia poziom zagrożenia atakiem na podstawie przeprowadzonego rekonesansu.	Test teoretyczny
Wykrywa i namierza intruza w sieci oraz zbiera o nim informacje.	Stosuje techniki wykrywania i lokalizacji intruza w sieci.	Test teoretyczny
	Analizuje informacje na temat działań intruza w celu neutralizacji incydentu.	Test teoretyczny
Analizuje ruch sieciowy i stosuje techniki skanowania sieci (z wykorzystaniem programów Wireshark, Snort, Tcpdump, Tshark).	Interpretuje dane dotyczące ruchu sieciowego.	Test teoretyczny
	Stosuje dedykowane rozwiązania w celu identyfikacji potencjalnych zagrożeń.	Test teoretyczny
	Obsługuje narzędzia do analizy ruchu sieciowego (Wireshark, Snort, Tcpdump, Tshark).	Test teoretyczny
Wykorzystuje techniki detekcji adresacji w sieciach lokalnych.	Stosuje zaawansowane techniki detekcji adresacji za NAT.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają 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, którzy chcą poszerzyć swoje umiejętności i zdobyć nowe kompetencje w obszarze analizy ruchu sieciowego.

Analiza ruchu sieciowego

I. Pre-test. Wprowadzenie do cyberbezpieczeństwa (teoria+praktyka)

1. Zagrożenia, środki przeciwdziałania, infrastruktura.
2. Wprowadzenie pojęcia podatności CVE i CVSS
3. Fazy rozwoju ataku.
4. Narzędzia dla poszczególnych faz.
5. Omówienie poszczególnych faz.
6. Rodzaje ataków, cele ataków.
7. Zbieranie informacji.
8. Sposoby i techniki przeciwdziałania.
9. Czy jestem bezpieczny w sieci? – skanowanie i zbieranie informacji w sieci.
10. Systemy monitoringu.
11. Zarządzanie podatnością.
12. Audyt bezpieczeństwa.
13. Cykl podnoszenia bezpieczeństwa – diagram / cykl Deminga.
14. Normy i dobre praktyki.
15. CIA i ciągłość działania.
16. Cyberbezpieczeństwo (post factum) – podnoszenie infrastruktury po ataku sieciowym.
17. Ścieżka szkoleniowa specjalisty ds. cyberbezpieczeństwa.
18. Ścieżka podnoszenia bezpieczeństwa.
19. Podatności, na które nie ma łatek bezpieczeństwa.
20. Reputacja IP.

II. Rekonesans – wprowadzenie. (teoria+praktyka)

1. Zbieranie informacji.
2. Cel zbieranie informacji.
3. Techniki i źródła zbierania informacji.
4. Skanowanie.
5. OSINT.
6. SE.
7. Kiedy zakończyć zbieranie informacji.
8. Jaka informacja jest przydatna a jaka zbędna.
9. Ryzyko wykrycia i anonimizacja.
10. Ukrywanie w szumie informacyjnym.
11. Namierzanie, wykrywanie intruza.
12. Zbieranie informacji o intruzie.
13. Honey pot.
14. Netflow, logi firewall-a, parsowanie logów.
15. IDS, IPS.
16. SIEM a skanowanie i rekonesans.

III. Analiza ruchu sieciowego i techniki skanowania. (teoria+praktyka)

1. Wprowadzenie do analizatorów ruchu sieciowego – Wireshark.
2. Nawiązanie połączenia oraz faza ARP.
3. Skanowanie pasywne i aktywne.
4. Wprowadzenie do NMAP-a.
5. NMAP – skanowanie L2, L3, L4 i skrypty nmap.
6. Wykrywanie skanowania aktywnego.
7. Wykrywanie skanowania pasywnego.
8. Wykrywanie skanowania
9. Analiza ruchu sieciowego
10. Techniki skanowania (nmap).
11. Blokowanie i detekcja technik skanowania przy pomocy firewall-a.
12. Firewall L2.
13. Rozpoznawania topologii sieci - podsieci.
14. Detekcja podstawowych parametrów systemu i sprzęty (LLDP)
15. Analiza ruchu, zestawianie sesji szyfrowanej.
16. Rozpoznawanie urządzeń na podstawie listy otwartych portów.
17. Analiza ruchu DHCP, Przechwytywanie sesji DHCP, detekcja liczby serwerów
18. Wykrywanie adresu IP bramy na podstawie fragmentu ruchu.
19. Techniki detekcji adresacji w sieci lokalnej.

IV. Walidacja.

Szkolenie wraz z walidacją trwa 32 godziny dydaktyczne (1 godz. dydaktyczna = 45 min; przerwy nie są wliczane do czasu trwania usługi), z czego 12 godz. to teoria, a 20 godz. to praktyka i realizowane jest w kameralnych grupach, maksymalnie 6-osobowych. Walidacja twa 30 min i jest uwzględniona w czasie 12 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 prowadzone jest z wykorzystaniem metod nauczania aktywizujących uczestników: dyskusja w grupie, burza mózgów, ćwiczenia.

Sposób organizacji walidacji: 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.

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 pozycji harmonogramu: 29

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 29 Wprowadzenie do cyberbezpieczeństwa, zarządzanie podatnością, zagrożenia, środki przeciwdziałania, infrastruktura. (Wykłady, dyskusja, ćwiczenia, testy; teoria 70 min + praktyka 20 min)	Jacek Herold	11-08-2026	08:45	10:15	01:30
2 z 29 Przerwa.	Jacek Herold	11-08-2026	10:15	10:30	00:15
3 z 29 Audyt bezpieczeństwa, CVE i CVSS, cykl podnoszenia bezpieczeństwa, diagram, cykl Deminga. (Wykłady, dyskusja, ćwiczenia; teoria 45 min + praktyka 45 min)	Jacek Herold	11-08-2026	10:30	12:00	01:30
4 z 29 Przerwa.	Jacek Herold	11-08-2026	12:00	12:45	00:45
5 z 29 Fazy rozwoju ataku, normy i dobre praktyki, narzędzia dla poszczególnych faz. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	11-08-2026	12:45	14:15	01:30
6 z 29 Przerwa.	Jacek Herold	11-08-2026	14:15	14:30	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 29 CIA, ciągłość działania, omówienie faz, cyberbezpieczeństwo post factum po ataku. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	11-08-2026	14:30	16:00	01:30
8 z 29 Rodzaje i cele ataków, ścieżka szkoleniowa specjalisty ds. cyberbezpieczeństwa. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	12-08-2026	08:45	10:15	01:30
9 z 29 Przerwa.	Jacek Herold	12-08-2026	10:15	10:30	00:15
10 z 29 Zbieranie informacji, ścieżka podnoszenia bezpieczeństwa, techniki przeciwdziałania. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	12-08-2026	10:30	12:00	01:30
11 z 29 Przerwa.	Jacek Herold	12-08-2026	12:00	12:45	00:45
12 z 29 Podatności bez łatek, bezpieczeństwo w sieci, skanowanie, reputacja IP, monitoring. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	12-08-2026	12:45	14:15	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 29 Przerwa.	Jacek Herold	12-08-2026	14:15	14:30	00:15
14 z 29 Rekonesans – wykrywanie intruza, zbieranie informacji, cele i źródła informacji. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	12-08-2026	14:30	16:00	01:30
15 z 29 Zbieranie informacji o intruzie, honeypot, OSINT, inżynieria społeczna (SE). (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	13-08-2026	08:45	10:15	01:30
16 z 29 Przerwa.	Jacek Herold	13-08-2026	10:15	10:30	00:15
17 z 29 Netflow, logi firewall-a, parsowanie logów, IDS, IPS, SIEM i rekonesans. (Wykłady, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	13-08-2026	10:30	12:00	01:30
18 z 29 Przerwa.	Jacek Herold	13-08-2026	12:00	12:45	00:45
19 z 29 Koniec zbierania informacji, przydatność danych, ryzyko wykrycia, anonimizacja. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	13-08-2026	12:45	14:15	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 29 Przerwa.	Jacek Herold	13-08-2026	14:15	14:30	00:15
21 z 29 Ukrywanie w szumie informacyjnym, analiza ruchu sieciowego – wprowadzenie. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	13-08-2026	14:30	16:00	01:30
22 z 29 Techniki skanowania NMAP, skanowanie aktywne i pasywne, rozpoznanie topologii. (Wykłady, dyskusja, ćwiczenia; teoria 30 min + praktyka 60 min)	Jacek Herold	14-08-2026	08:45	10:15	01:30
23 z 29 Przerwa.	Jacek Herold	14-08-2026	10:15	10:30	00:15
24 z 29 Wireshark, Snort, firewall L2, ARP, LLDP, blokowanie i detekcja skanowania. (Wykłady, dyskusja, ćwiczenia; teoria 25 min + praktyka 65 min)	Jacek Herold	14-08-2026	10:30	12:00	01:30
25 z 29 Przerwa.	Jacek Herold	14-08-2026	12:00	12:45	00:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 29 Skanowanie L2–L4, skrypty NMAP, identyfikacja urządzeń, sesje szyfrowane. (Wykłady, dyskusja, ćwiczenia; teoria 20 min + praktyka 70 min)	Jacek Herold	14-08-2026	12:45	14:15	01:30
27 z 29 Przerwa.	Jacek Herold	14-08-2026	14:15	14:30	00:15
28 z 29 DHCP, wykrywanie skanowania, adresacja lokalna, analiza i korelacja ruchu. (Wykłady, dyskusja, ćwiczenia, testy; teoria 20 min + praktyka 40 min)	Jacek Herold	14-08-2026	14:30	15:30	01:00
29 z 29 Walidacja.	-	14-08-2026	15:30	16:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 412,00 PLN
Koszt przypadający na 1 uczestnika netto	4 400,00 PLN
Koszt osobogodziny brutto	169,13 PLN
Koszt osobogodziny netto	137,50 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 4 900 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 32 godziny dydaktyczne (przerwy nie są wliczone do czasu trwania usługi) i prowadzone jest przez 4 dni od poniedziałku do czwartku, 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