Możliwość dofinansowania

Notebook Master Sp. z o.o.

★★★★★

Cyber security / Etap II / Ocena bezpieczeństwa sieci firmowej

Numer usługi 2024/08/23/158529/2276354

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
16.12.2024 do 20.12.2024

4 797,00 PLN brutto
3 900,00 PLN netto
119,93 PLN brutto/h
97,50 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane jest do przedsiębiorców i ich pracowników pracujących w branży IT, którzy chcą nabyć wiedzę i umiejętności z zakresu dotyczącego cyberbezpieczeństwa i oceny bezpieczeństwa sieci firmowej oraz 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
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 (w tym do rozwoju umiejętności w obszarze TIK (ITC) oraz kompetencji

cyfrowych) 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
Określa priorytety działań naprawczych.	Eliminuje czynniki wpływające na zwiększenie poziomu ryzyka.	Test teoretyczny
		Test teoretyczny
	Klasyfikuje zagrożenia według ich potencjalnego wpływu na bezpieczeństwo	Test teoretyczny
	Efektywnie ustala kolejność działań naprawczych	Test teoretyczny
Skutecznie analizuje zmiany w infrastrukturze sieciowej.	Umiejętnie wykorzystuje NdiFF i OpenVAS	Test teoretyczny
	Interpretuje wyniki w celu podniesienia bezpieczeństwa infrastruktury sieciowej	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje i reaguje na wybrane techniki skanowania.	Analizując ruch sieciowy, identyfikuje modele skanowania środowiska sieciowego	Test teoretyczny
	Skutecznie blokuje zidentyfikowane techniki 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, dokument zawiera opis efektów uczenia się.

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Szkolenie skierowane jest 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. Ryzyka związane z zagrożeniami sieciowymi

II. Skanery sieciowe

III. Techniki skanowania.

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

IV. Skanery podatności.

1. Podstawy działania.

2. Konfiguracja .
3. Dopasowanie profilu skanowania.

V. Rozpoznawanie i ocena podatności, ocena zagrożeń we kontekście infrastruktury.

VI. Wstęp do analizy ryzyka.

VII. Określanie priorytetów działań naprawczych.

VIII. Analiza zmian infrastruktury: Ndiff, OpenVAS Delta Report.

IX. Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego.

X. Blokowanie wybranych technik skanowania i rozpoznawania usług. .

Szkolenie trwa 40 godziny dydaktyczne i realizowane jest w kameralnych grupach, maksymalnie 8-osobowych. Każdy uczestnik stacjonarny ma do dyspozycji indywidualne stanowisko szkoleniowe. 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 składają się 8 godzin zajęć teoretycznych i 32 godziny zajęć praktycznych.

Przerwy nie są wliczane do czasu trwania usługi .

Harmonogram

Liczba przedmiotów/zajęć: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 Ryzyka związane z zagrożeniami sieciowymi. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	16-12-2024	08:45	10:15	01:30
2 z 36 Przerwa.	Jacek Herold	16-12-2024	10:15	10:30	00:15
3 z 36 Ryzyka związane z zagrożeniami sieciowymi. (Wykłady, dyskusja, ćwiczeni)	Jacek Herold	16-12-2024	10:30	12:00	01:30
4 z 36 Przerwa.	Jacek Herold	16-12-2024	12:00	12:45	00:45
5 z 36 Skanery sieciowe. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	16-12-2024	12:45	14:15	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 36 Przerwa.	Jacek Herold	16-12-2024	14:15	14:30	00:15
7 z 36 Skanery sieciowe. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	16-12-2024	14:30	16:00	01:30
8 z 36 Techniki skanowania. Host discovery. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-12-2024	08:45	10:15	01:30
9 z 36 Przerwa.	Jacek Herold	17-12-2024	10:15	10:30	00:15
10 z 36 Techniki skanowania. Port discovery. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-12-2024	10:30	12:00	01:30
11 z 36 Przerwa.	Jacek Herold	17-12-2024	12:00	12:45	00:45
12 z 36 Techniki skanowania. Version detection. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-12-2024	12:45	14:15	01:30
13 z 36 Przerwa.	Jacek Herold	17-12-2024	14:15	14:30	00:15
14 z 36 Techniki skanowania. NSE. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	17-12-2024	14:30	16:00	01:30
15 z 36 Skanery podatności. Podstawy działania. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-12-2024	08:45	10:15	01:30
16 z 36 Przerwa.	Jacek Herold	18-12-2024	10:15	10:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 36 Skanery podatności. Konfiguracja. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-12-2024	10:30	12:00	01:30
18 z 36 Przerwa.	Jacek Herold	18-12-2024	12:00	12:45	00:45
19 z 36 Skanery podatności. Dopasowanie profilu skanowania. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-12-2024	12:45	14:15	01:30
20 z 36 Przerwa.	Jacek Herold	18-12-2024	14:15	14:30	00:15
21 z 36 Rozpoznawanie i ocena podatności, ocena zagrożeń we kontekście infrastruktury. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	18-12-2024	14:30	16:00	01:30
22 z 36 Wstęp do analizy ryzyka. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-12-2024	08:45	10:15	01:30
23 z 36 Przerwa.	Jacek Herold	19-12-2024	10:15	10:30	00:15
24 z 36 Określanie priorytetów działań naprawczych. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-12-2024	10:30	12:00	01:30
25 z 36 Przerwa.	Jacek Herold	19-12-2024	12:00	12:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 36 Określanie priorytetów działań naprawczych. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-12-2024	12:45	14:15	01:30
27 z 36 Przerwa.	Jacek Herold	19-12-2024	14:15	14:30	00:15
28 z 36 Analiza zmian infrastruktury: Ndiff, OpenVAS Delta Report. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	19-12-2024	14:30	16:00	01:30
29 z 36 Analiza zmian infrastruktury: Ndiff, OpenVAS Delta Report. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	20-12-2024	08:45	10:15	01:30
30 z 36 Przerwa.	Jacek Herold	20-12-2024	10:15	10:30	00:15
31 z 36 Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	20-12-2024	10:30	12:00	01:30
32 z 36 Przerwa.	Jacek Herold	20-12-2024	12:00	12:45	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
33 z 36 Rozpoznawanie wybranych technik skanowania przy pomocy analizy ruchu sieciowego. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	20-12-2024	12:45	14:15	01:30
34 z 36 Przerwa.	Jacek Herold	20-12-2024	14:15	14:30	00:15
35 z 36 Blokowanie wybranych technik skanowania i rozpoznawania usług. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	20-12-2024	14:30	15:30	01:00
36 z 36 Walidacja.	-	20-12-2024	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	119,93 PLN
Koszt osobogodziny netto	97,50 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 z niezbędnym oprogramowaniem, peryferia. Po zakończonym szkoleniu sprzęt zostaje odebrany przez kuriera. Każdy uczestnik stacjonarny ma do dyspozycji indywidualne stanowisko szkoleniowe.

Informacje dodatkowe

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

Szkolenie jest bardzo szczegółowe, ponieważ zależy nam na przekazaniu jak największej ilości informacji. Łącznie trwa 40 godzin dydaktycznych i prowadzone jest przez tydzień od poniedziałku do piątku, w godzinach od 8:45 do 16:00.

Harmonogram uwzględnia łączną liczbę godzin szkolenia, jako 36:15 godzin zegarowych, ponieważ uwzględnia również przerwy pomiędzy blokami zajęć.

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