Możliwość dofinansowania

Notebook Master Sp. z o.o.

★★★★★

Cyber security / Etap I / Analiza ruchu sieciowego

Numer usługi 2024/04/08/158529/2116264

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

Usługa szkoleniowa

32 h

02.09.2024 do 05.09.2024

4 797,00 PLN brutto
3 900,00 PLN netto
149,91 PLN brutto/h
121,88 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 dot. cyberbezpieczeństwa i analizy ruchu sieciowego oraz wykorzystać je w ramach prowadzonej działalności gospodarczej i etatu.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną 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 do samodzielnego i prawidłowego wykonywania obowiązków w zakresie dot. cyberbezpieczeństwa z przeznaczeniem analizy ruchu sieciowego.

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
	Kategoryzuje podatności pod względem potencjalnego wpływu na bezpieczeństwo.	Test teoretyczny
Charakteryzuje rodzaje i cele ataków.	Wskazuje rodzaje ataków sieciowych.	Test teoretyczny
	Określa potencjalne cele ataków sieciowych.	Test teoretyczny
Skanuje środowisko sieciowe.	Dobiera narzędzia do rekonesansu infrastruktury sieciowe.	Test teoretyczny
	Ocenia zgromadzone dane pod kątem ich przydatności.	Test teoretyczny
Niweluje skutki ataków na infrastrukturę.	Opracowuje plan przywracania działania infrastruktury po ataku.	Test teoretyczny
	Stosuje przygotowane procedury po wystąpieniu incydentu.	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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
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 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.

Analiza ruchu sieciowego

I. Wprowadzenie do cyberbezpieczeństwa

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.

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.

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.

Szkolenie trwa 32 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).

Harmonogram

Liczba przedmiotów/zajęć: 29

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 29 Wprowadzenie do cyberbezpieczeństwa. Zagrożenia, środki przeciwdziałania, infrastruktura. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	02-09-2024	08:45	10:15	01:30	Tak
2 z 29 Przerwa.	Jacek Herold	02-09-2024	10:15	10:30	00:15	Tak
3 z 29 Fazy rozwoju ataku. Narzędzia dla poszczególnych faz. Omówienie poszczególnych faz. (Wykłady, dyskusja, ćwiczeni)	Jacek Herold	02-09-2024	10:30	12:00	01:30	Tak
4 z 29 Przerwa.	Jacek Herold	02-09-2024	12:00	12:45	00:45	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
5 z 29 Rodzaje ataków, cele ataków. Zbieranie informacji. Sposoby i techniki przeciwdziała nia. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	02-09-2024	12:45	14:15	01:30	Tak
6 z 29 Przerwa.	Jacek Herold	02-09-2024	14:15	14:30	00:15	Tak
7 z 29 Regeneracja padów oraz pól lutowniczych. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	02-09-2024	14:30	16:00	01:30	Tak
8 z 29 Czy jestem bezpieczny w sieci? – skanowanie i zbieranie informacji w sieci. Systemy monitoringu. Zarządzanie podatnością. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	03-09-2024	08:45	10:15	01:30	Tak
9 z 29 Przerwa.	Jacek Herold	03-09-2024	10:15	10:30	00:15	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
10 z 29 Audyt bezpieczeństwa. Cykl podnoszenia bezpieczeństwa. Normy i dobre praktyki. Cyberbezpieczeństwo (post factum) – podnoszenie infrastruktury po ataku sieciowym. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	03-09-2024	10:30	12:00	01:30	Tak
11 z 29 Przerwa.	Jacek Herold	03-09-2024	12:00	12:45	00:45	Tak
12 z 29 Rekonesans – wprowadzenie. Zbieranie informacji. Techniki i źródła zbierania informacji. Skanowanie. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	03-09-2024	12:45	14:15	01:30	Tak
13 z 29 Przerwa.	Jacek Herold	03-09-2024	14:15	14:30	00:15	Tak
14 z 29 Kiedy zakończyć zbieranie informacji. Jaka informacja jest przydatna a jaka zbędna. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	03-09-2024	14:30	16:00	01:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
15 z 29 Ryzyko wykrycia i anonimizacja. Namierzanie, wykrywanie intruza. Netflow, logi firewall-a, parsowanie logów. SIEM a skanowanie i rekonesans. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	04-09-2024	08:45	10:15	01:30	Tak
16 z 29 Przerwa.	Jacek Herold	04-09-2024	10:15	10:30	00:15	Tak
17 z 29 Analiza ruchu sieciowego i techniki skanowania. Wprowadzenie do analizatorów ruchu sieciowego – Wireshark. Nawiązanie połączenia oraz faza ARP. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	04-09-2024	10:30	12:00	01:30	Tak
18 z 29 Przerwa.	Jacek Herold	04-09-2024	12:00	12:45	00:45	Tak
19 z 29 Skanowanie pasywne i aktywne. NMAP – skanowanie L2, L3, L4 i skrypty nmap. Wykrywanie skanowania aktywnego/pasywnego. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	04-09-2024	12:45	14:15	01:30	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
20 z 29 Przerwa.	Jacek Herold	04-09-2024	14:15	14:30	00:15	Tak
21 z 29 Techniki skanowania (nmap). Blokowanie i detekcja technik skanowania przy pomocy firewall-a. Firewall L2. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	04-09-2024	14:30	16:00	01:30	Tak
22 z 29 Rozpoznawania topologii sieci - podsieci. Detekcja podstawowych parametrów systemu i sprzęty (LLDP). (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	05-09-2024	08:45	10:15	01:30	Tak
23 z 29 Przerwa.	Jacek Herold	05-09-2024	10:15	10:30	00:15	Tak
24 z 29 Analiza ruchu, zestawianie sesji szyfrowanej. Rozpoznawanie urządzeń na podstawie listy otwartych portów. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	05-09-2024	10:30	12:00	01:30	Tak
25 z 29 Przerwa.	Jacek Herold	05-09-2024	12:00	12:45	00:45	Tak

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
26 z 29 Analiza ruchu DHCP, Przechwytywanie sesji DHCP, detekcja liczby serwerów. (Wykłady, dyskusja, ćwiczenia.)	Jacek Herold	05-09-2024	12:45	14:15	01:30	Tak
27 z 29 Przerwa.	Jacek Herold	05-09-2024	14:15	14:30	00:15	Tak
28 z 29 Wykrywanie adresu IP bramy na podstawie fragmentu ruchu. Techniki detekcji adresacji w sieci lokalnej. (Wykłady, dyskusja, ćwiczenia, testy.)	Jacek Herold	05-09-2024	14:30	15:30	01:00	Tak
29 z 29 Walidacja.	-	05-09-2024	15:30	16:00	00:30	Tak

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	149,91 PLN
Koszt osobogodziny netto	121,88 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.

Informacje dodatkowe

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

Cena usługi jest ceną promocyjną obowiązującą od 19.04.2024 r. Cena nominalna kursu - 4 900 zł.

Szkolenie jest bardzo szczegółowe, ponieważ zależy nam na przekazaniu jak największej ilości informacji. Łącznie trwa 32 godziny dydaktyczne i prowadzone jest przez tydzień od poniedziałku do piątku, w godzinach od 8:45 do 16:00.

Harmonogram uwzględnia łączną liczbę godzin szkolenia, jako 29 godzin zegarowych, ponieważ uwzględnia również przerwy pomiędzy blokami zajęć (I przerwa - 15 min, II przerwa - 45 min, III przerwa 15 min / 1 dzień).

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.

Adres

ul. Krzeczowska 20
32-700 Bochnia
woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

Artur Kowalewski

E-mail szkolenia@notebookmaster.pl
Telefon (+48) 573 436 635