Możliwość dofinansowania

Telemedika Polska
Katarzyna Warkocz

★★★★★

Zaawansowana konfiguracja i zarządzanie routingiem sieciowym oraz zasadami zabezpieczeń

Numer usługi 2024/09/29/19836/2333895

zdalna w czasie rzeczywistym
Usługa szkoleniowa
51 h
17.10.2024 do 31.10.2024

7 500,00 PLN brutto
7 500,00 PLN netto
147,06 PLN brutto/h
147,06 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	Pracownicy, współpracownicy, właściciele firm MMSP Osoby posiadające podstawową wiedzę i doświadczenie z zakresu budowy prostej sieci komputerowej opartej o urządzenia sieciowe (co najmniej niezarządzane z wiersza poleceń). Wszystkie osoby zainteresowane tematyką.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	16-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	51
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem jest samodzielne zarządzanie i zabezpieczanie sieci komputerowej z wykorzystaniem dedykowanych rozwiązań bezpieczeństwa (router NGFW). Przygotowuje do samodzielnego projektowania sieci komputerowej oraz konfigurowania jej zabezpieczeń przy użyciu wbudowanych rozwiązań.
Celem jest także umiejętność wyboru i stosowania zasad zabezpieczeń technicznych i organizacyjnych w celu przeciwdziałania atakom i/lub łagodzenia ich skutków.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się wiedzą w dziedzinie konfigurowanie i zarządzania sprzętem sieciowym (NGFW) oraz zasadami zabezpieczeń:	Charakteryzuje potencjalne źródła ataków cyfrowych w firmie (zagrożenia). Charakteryzuje podstawy zabezpieczania przesyłania danych w przedsiębiorstwie. Charakteryzuje działania dotyczące sprzętu sieciowego, jakie zapewniają odporność i bezpieczeństwo-m.in.zasady przydzielania dostępu, zbierania logów, zabezpieczania urządzeń.	Test teoretyczny
Stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji:	Konfiguruje sprzęt sieciowy (routery) w sposób zapewniający bezpieczeństwo. Przydziela dostęp do urządzenia. Konfiguruje reguły firewall. Stosuje zasady routingu statycznego i dynamicznego z wykorzystaniem protokołu OSFP (Open Shortest Path First) oraz konfiguruje koncentrację VPN z wykorzystaniem PPP (Point to Point Protocol) i IPIP. Konfiguruje interfejsy bezprzewodowe 2.4, 5 GHz. Przekierowuje logi urządzeń do pamięci masowych oraz zewnętrznych systemów do kolekcji logów. Odseparowuje sieci za pomocą VLAN. Tworzy strukturę sieci odporną na awarię L2/L3, wykorzystując bonding oraz VRRP (Virtual Router Redundancy Protocol)	Test teoretyczny
Stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji:	Zapewnia ciągłość działania organizacji Konfiguruje reguły firewall. Stosuje zasady routingu statycznego. Odseparowuje sieci za pomocą VLAN. Konfiguruje moduły bezpieczeństwa w celu ochrony ruchu. Konfiguruje Policy Routes Szacuje ryzyko w odniesieniu do poszczególnych aktywów informatycznych firmy i wpływ wystąpienia potencjalnych ryzyk na działanie firmy. Wdraża odpowiednie procedury bezpieczeństwa.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Stosuje nowo nabyte kompetencje społeczne:	Komunikuje się efektywnie ze specjalistami ds. cyberbezpieczeństwa oraz pracownikami. Przekonuje współpracowników i interesariuszy do własnego zdania.	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Zawiera, w rozbiciu na poszczególne kryteria (wiedza, edukacja, rozwój)

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

Proporcje godzin przeznaczonych na teorię/praktykę to 40/60 %

Moduł I - wprowadzenie do bezpieczeństwa systemów Informatycznych

Wprowadzenie do zagadnień z zakresu IT Security
Polityka haseł jako narzędzie wpływające na bezpieczeństwo
Metodyka zarządzania hasłami od strony formalnej
Narzędzia IT wspierające zarządzanie hasłami
Wprowadzenie do zagadnienia - Inżynieria społeczna
Warsztaty praktyczne

Moduł II - sieć Internet jako zagrożenie dla przedsiębiorstwa

Bezpieczeństwo związane z funkcjonowaniem systemów poczty elektronicznej
Prawo krajowe i międzynarodowe w odniesieniu do cyfryzacji komunikacji w przedsiębiorstwie
Uwarunkowania korzystania z usług hostingu stron www w odniesieniu do prawa krajowego i międzynarodowegoWprowadzenie do zagadnienia - Open Source Intelligence tzw. "biały wywiad"
Warsztaty praktyczne

Moduł III - ochrona informacji oraz środków pieniężnych

Urządzenia mobilne takie jak telefony, tablety, laptopy jako wektor ataku na przedsiębiorstwo
Case study: strona www przedsiębiorstwa jako wektor ataku
Cyfryzacja komunikacji w przedsiębiorstwie jako wektor ataku w odniesieniu do telefonów komórkowych oraz komunikatorówinternetowych
Warsztaty praktyczne

Moduł IV - ochrona środków pieniężnych

Case study: sieci WiFi jako wektor ataku na przedsiębiorstwo
Bezpieczeństwo danych w odniesieniu do zewnętrznych nośników danych takich jak pamięci pendrive oraz zewnętrzne dyski twarde
Metody ochrony środków pieniężnych w odniesieniu do bankowości internetowej oraz kart płatniczychCase study: poczta e-mail jako wektor ataku

Warsztaty praktyczne

Moduł V

1. Konfiguracja reguł firewalla, routing, sterowanie przepływem pakietów
2. Konfiguracja polityk bezpieczeństwa, sterowanie aplikacjami, zabezpieczanie ruchu sieciowego
3. Warsztaty praktyczne

Moduł VI

1. Konfiguracjja Security profiles- omówienie, konfiguracja
2. Konfiguracja i zabeczpieczanie połączeń VPN
3. Warsztaty praktyczne

Moduł VII

Konfiguracja pozostałych mechanizmów i modułów zabezpieczeń

Warsztaty praktyczne

Harmonogram

Liczba przedmiotów/zajęć: 26

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 **Walidacja (test)**	-	17-10-2024	08:00	09:30	01:30
2 z 26 **Moduł I - wykład (prezentacja, czat, rozmowa na żywo)**	Katarzyna Warkocz	17-10-2024	09:45	11:15	01:30
3 z 26 **Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)**	Katarzyna Warkocz	17-10-2024	11:30	13:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	17-10-2024	13:30	15:00	01:30
5 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	17-10-2024	15:15	16:45	01:30
6 z 26 Moduł II cz.1 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	18-10-2024	08:00	09:30	01:30
7 z 26 Moduł II cz.2 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	18-10-2024	09:45	11:15	01:30
8 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	18-10-2024	11:30	13:00	01:30
9 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	18-10-2024	13:30	15:00	01:30
10 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	18-10-2024	15:15	16:45	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 26 Moduł III cz.1 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	24-10-2024	08:00	09:30	01:30
12 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	24-10-2024	09:45	11:15	01:30
13 z 26 Moduł III cz.2 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	24-10-2024	11:30	13:00	01:30
14 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	24-10-2024	13:30	15:00	01:30
15 z 26 Moduł IV - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	24-10-2024	15:15	16:45	01:30
16 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	25-10-2024	08:00	09:30	01:30
17 z 26 Moduł V - wykład (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	25-10-2024	09:45	11:15	01:30
18 z 26 Moduł VI cz.1 - wykład	Katarzyna Warkocz	25-10-2024	11:30	13:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 26 Moduł VI cz.2 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	25-10-2024	13:30	15:00	01:30
20 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	25-10-2024	15:15	16:45	01:30
21 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	31-10-2024	08:00	09:30	01:30
22 z 26 Warsztaty praktyczne	Katarzyna Warkocz	31-10-2024	09:45	11:15	01:30
23 z 26 Moduł VII cz.1 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	31-10-2024	11:30	13:00	01:30
24 z 26 Moduł VII cz.2 - wykład (prezentacja, czat, rozmowa na żywo)	Katarzyna Warkocz	31-10-2024	13:30	15:00	01:30
25 z 26 Warsztaty praktyczne (rozmowa na żywo, współdzielenie ekranu, konsultacje)	Katarzyna Warkocz	31-10-2024	15:15	16:45	01:30
26 z 26 Walidacja (test)	-	31-10-2024	18:15	19:30	01:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 500,00 PLN
Koszt przypadający na 1 uczestnika netto	7 500,00 PLN
Koszt osobogodziny brutto	147,06 PLN
Koszt osobogodziny netto	147,06 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Katarzyna Warkocz

W ciągu ostatnich 2 lat przeprowadziła ponad 200 godzin szkoleniowych Specjalizuje się w szkoleniach dla właścicieli firm oraz dla handlowców. Posiada wieloletnie doświadczenie w zarządzaniu zespołem oraz prowadzeniu przedsiębiorstwa szkoleniowego. Ponad 5 letnia praca w obszarze IT, w tym w obszarze cybersecurity, w zakresie kompleksowej obsługi sieci komputerowych oraz wdrażania rozwiązań bezpieczeństwa. Posiada certyfikaty Network Security Proffessional (NSE4), Network Security Analyst (NSE5) oraz Network Security Architect (NSE7). Odpowiedzialna za wdrożenie systemu ISO 9001:2015, standardów przetwarzania danych osobowych, a także dokumentację akredytacyjną. Posiada zdolności analityczne, doświadczenie w sporządzeniu informacji prawnych, raportów, analiz, sprawozdań i procedur, przygotowywaniu prezentacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Organizator zapewnia wszelkie niezbędne materiały oraz wirtualne środowisko testowe.

Ćwiczenia oparte są o infrastrukturę Fortinet- Uczestnicy otrzymują niezbędne dostepy po rozpoczęciu ćwiczeń.

Ćwiczenia praktyczne polegają na otrzymaniu przez Uczestnika dostepu do środowiska wirtualnego zawierającego całą niebędną infrastrukturę. uczestnik samodzielnie wykonuje w nim zadania analogiczne do codziennej pracy w środowisku produkcyjnym.

Informacje dodatkowe

Usługa realizowana jest w godzinach dydaktycznych (1 godz.= 45 min.)

Usługa obejmuje 51 godzin dydaktycznych (po 45 min).

Podczas jej realizacji zapewniony jest dobrostan uczestników poprzez zaplanowane przerwy, natomiast czas przerw nie jest wliczany do czasu usługi.

Warunki techniczne

Usługa będzie realizowana przy użyciu Microsoft Teams.

Minimalne wymagania sprzętowe dla uczestników:
Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy)
2GB pamięci RAM (zalecane 4GB lub więcej)
System operacyjny taki jak Windows 10, Mac OS (zalecana najnowsza wersja), Linux,
Chrome OS.
Niezbędne oprogramowanie - przeglądarka internetowa. Polecamy szczególnie przeglądarki Chrome, Opera, Firefox.

Kontakt

Katarzyna Warkocz

E-mail k.warkocz@o2.pl
Telefon (+48) 793 338 397