Możliwość dofinansowania

Telemedika Polska
Katarzyna Warkocz

★★★★★

Cyberbezpieczna firma

Numer usługi 2024/09/27/19836/2332508

5 400,00 PLN brutto
5 400,00 PLN netto
128,57 PLN brutto/h
128,57 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
42 h
19.10.2024 do 27.10.2024

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Właściciele i pracownicy przedsiębiorstw pragnący wzmacniać bezpieczeństwo firmy poprzez podniesienie kompetencji personelu. Wszystkie osoby zainteresowane tematyką.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	18-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	42
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

Po ukończeniu usługi uczestnik przygotowany będzie do podejmowania działań zmierzających do zidentyfikowania i zrozumienia zróżnicowanych źródeł zagrożeń ataków cyfrowych oraz 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
Posługuje się wiedzą z dziedziny cyberseurity:	Charakteryzuje potencjalne źródła ataków cyfrowych w firmie (zagrożenia). Charakteryzuje podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości. Charakteryzuje normy: ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania; ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa -Wymagania; oraz ISO/IEC 27005, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem bezpieczeństwa informacji.	Test teoretyczny
Posługuje się wiedzą z dziedziny cybersecurity:	Charakteryzowania podstawowych różnic pomiędzy modelem zabezpieczeń oprogramowania typu open-source i closedsource. Charakteryzowania podstaw zagadnień dotyczące zagrożeń cyberbezpieczeństwa wynikających ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych.	Test teoretyczny
Umiejętności: stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji.	Zapewnia ciągłość działania organizacji w procesie transformacji cyfrowej. II. Szacuje ryzyko w odniesieniu do poszczególnych aktywów informatycznych firmy i wpływ wystąpienia potencjalnych ryzyk na działanie firmy. III. Współpracuje ze specjalistami ds. cyberbezpieczeństwa danych i systemów w zakresie projektów realizowanych w transformacji cyfrowej firmy.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Umiejętności: stosuje best practices w dziedzinie bezpieczeństwa technologicznego w organizacji.	Weryfikacja zdobytej wiedzy pWdraża odpowiednie procedury bezpieczeństwa. V. Identyfikuje niezbędne akty prawne, dokumenty i zapisy w nich zawarte, określające podstawy bezpieczeństwa cyfrowego w firmie. VI. Zachęca pracowników do przestrzegania zasad cyberbezpieczeństwa.	Test teoretyczny
Stosuje nowo nabyte kompetencje społeczne:	Komunikuje się efektywnie ze specjalistami ds. cyberbezpieczeństwa. 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?

Tak, zawiera szczegółową listę efektów uczenia się z podziałem na wiedzę, umiejętności oraz kompetencji społeczne.

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, zawiera adnotację o rozdzieleniu tych procesów.

Program

Moduł I - wprowadzenie do bezpieczeństwa systemów Informatycznych - dotyczy następujących punktów z efektów uczenia się: 1-9

- 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
- Wprowadzenie do zagadnienia - Open Source Intelligence tzw. "biały wywiad"

- Warsztaty praktyczne

Moduł II - sieć Internet jako zagrożenie dla przedsiębiorstwa - dotyczy następujących punktów z efektów uczenia się: I - VI

- 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 międzynarodowego
- Case study: poczta e-mail jako wektor ataku
- Case study: strona www przedsiębiorstwa jako wektor ataku
- Cyfryzacja komunikacji w przedsiębiorstwie jako wektor ataku w odniesieniu do telefonów komórkowych oraz komunikatorów internetowych
- Warsztaty praktyczne

Moduł III - oprogramowanie wykorzystywane w firmie jako wektor ataku - dotyczy następujących punktów z efektów uczenia się: 1, 2, III, IV, a, b

- Kopie zapasowe danych jako podstawowy mechanizm bezpieczeństwa Informatycznego przedsiębiorstwa
- Case study: najczęściej popełniane błędy w odniesieniu do logiki funkcjonowania systemu kopii bezpieczeństwa
- Niewykonanie aktualizacji oprogramowania jako wektor ataku na przedsiębiorstwo
- Bezpieczeństwo IT w odniesieniu do oprogramowania Microsoft Office 2021
- Bezpieczeństwo IT w odniesieniu do oprogramowania Mozilla Thunderbird
- Bezpieczeństwo IT w odniesieniu do przeglądarek internetowych
- Warsztaty praktyczne

Moduł IV - ochrona informacji oraz środków pieniężnych - dotyczy następujących punktów z efektów uczenia się: 1-9, I-VI, a, b

- Urządzenia mobilne takie jak telefony, tablety, laptopy jako wektor ataku na przedsiębiorstwo
- 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 płatniczych

Warsztaty praktyczne

Efekty uczenia się:

Wiedza:

1. Charakteryzuje potencjalne źródła ataków cyfrowych w firmie (zagrożenia).
2. Charakteryzuje podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości.
3. Ma wiedzę na temat zaleceń ENISA do osiągniecia wysokiego poziomu bezpieczeństwa cybernetycznego2.
4. Charakteryzuje normy: ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania; ISO/IEC 27001, Technika informatyczna - Techniki bezpieczeństwa -Wymagania; oraz ISO/IEC 27005, Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem bezpieczeństwa informacji.
5. Charakteryzuje podstawowe regulacje prawne z zakresu ochrony i przetwarzania danych.
6. Charakteryzuje przykłady podstawowej dokumentacji opisującej zasady bezpieczeństwa w firmie (np. przykład metodologii szacowania ryzyka, dokumenty dotyczące zarządzania zidentyfikowanym ryzykiem, czy przykład analizy zabezpieczeń systemów teleinformatycznych).
7. Charakteryzuje różnice pomiędzy różnymi systemami IT i OT oraz podstawy sposobów ich zabezpieczania.
8. Charakteryzuje podstawowe różnice pomiędzy modelem zabezpieczeń oprogramowania typu open-source i closedsource.
9. Charakteryzuje podstawy zagadnień dotyczące zagrożeń cyberbezpieczeństwa wynikających ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych.

Umiejętności:

I. Zapewnia ciągłość działania organizacji w procesie transformacji cyfrowej.

II. Szacuje ryzyko w odniesieniu do poszczególnych aktywów informatycznych firmy i wpływ wystąpienia potencjalnych ryzyk na działanie firmy.

III. Współpracuje ze specjalistami ds. cyberbezpieczeństwa danych i systemów w zakresie projektów realizowanych w transformacji cyfrowej firmy.

IV. Wdraża odpowiednie procedury bezpieczeństwa.

V. Identyfikuje niezbędne akty prawne, dokumenty i zapisy w nich zawarte, określające podstawy bezpieczeństwa cyfrowego w firmie.

VI. Zachęca pracowników do przestrzegania zasad cyberbezpieczeństwa

Kompetencje społeczne:

a) Komunikuje się efektywnie ze specjalistami ds. cyberbezpieczeństwa.

b) Przekonuje współpracowników i interesariuszy do własnego zdania

Harmonogram

Liczba przedmiotów/zajęć: 37

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 37 Wprowadzenie, walidacja usługi: pre- test	-	19-10-2024	08:00	09:30	01:30
2 z 37 Przerwa	Katarzyna Warkocz	19-10-2024	09:30	09:45	00:15
3 z 37 Moduł I- wykład	Katarzyna Warkocz	19-10-2024	09:45	11:15	01:30
4 z 37 Przerwa	Katarzyna Warkocz	19-10-2024	11:15	11:30	00:15
5 z 37 Moduł I- wykład, ćwiczenia	Katarzyna Warkocz	19-10-2024	11:30	13:00	01:30
6 z 37 Przerwa obiadowa	Katarzyna Warkocz	19-10-2024	13:00	13:30	00:30
7 z 37 Moduł I- wykład, ćwiczenia	Katarzyna Warkocz	19-10-2024	13:30	15:00	01:30
8 z 37 Przerwa	Katarzyna Warkocz	19-10-2024	15:00	15:15	00:15
9 z 37 Moduł I- wykład, ćwiczenia	Katarzyna Warkocz	19-10-2024	15:15	16:45	01:30
10 z 37 Moduł II- wykład, ćwiczenia	Katarzyna Warkocz	20-10-2024	08:00	09:30	01:30
11 z 37 Przerwa	Katarzyna Warkocz	20-10-2024	09:30	09:45	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 37 Moduł II - wykład, ćwiczenia	Katarzyna Warkocz	20-10-2024	09:45	11:15	01:30
13 z 37 Przerwa	Katarzyna Warkocz	20-10-2024	11:15	11:30	00:15
14 z 37 Moduł II - wykład, ćwiczenia	Katarzyna Warkocz	20-10-2024	11:30	13:00	01:30
15 z 37 Przerwa obiadowa	Katarzyna Warkocz	20-10-2024	13:00	13:30	00:30
16 z 37 Moduł II - wykład, ćwiczenia	Katarzyna Warkocz	20-10-2024	13:30	15:00	01:30
17 z 37 Przerwa	Katarzyna Warkocz	20-10-2024	15:00	15:15	00:15
18 z 37 Moduł II - wykład, ćwiczenia	Katarzyna Warkocz	20-10-2024	15:15	16:45	01:30
19 z 37 Moduł III - wykład, ćwiczenia	Katarzyna Warkocz	26-10-2024	08:00	09:30	01:30
20 z 37 Przerwa	Katarzyna Warkocz	26-10-2024	09:30	09:45	00:15
21 z 37 Moduł III - wykład, ćwiczenia	Katarzyna Warkocz	26-10-2024	09:45	11:15	01:30
22 z 37 Przerwa	Katarzyna Warkocz	26-10-2024	11:15	11:30	00:15
23 z 37 Moduł III - wykład, ćwiczenia	Katarzyna Warkocz	26-10-2024	11:30	13:00	01:30
24 z 37 Przerwa obiadowa	Katarzyna Warkocz	26-10-2024	13:00	13:30	00:30
25 z 37 Moduł III - wykład, ćwiczenia	Katarzyna Warkocz	26-10-2024	13:30	15:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 37 Przerwa	Katarzyna Warkocz	26-10-2024	15:00	15:15	00:15
27 z 37 Moduł III - wykład, ćwiczenia	Katarzyna Warkocz	26-10-2024	15:15	16:45	01:30
28 z 37 Moduł IV - wykład, ćwiczenia	Katarzyna Warkocz	27-10-2024	08:00	09:30	01:30
29 z 37 Przerwa	Katarzyna Warkocz	27-10-2024	09:30	09:45	00:15
30 z 37 Moduł IV - wykład, ćwiczenia	Katarzyna Warkocz	27-10-2024	09:45	11:15	01:30
31 z 37 Przerwa	Katarzyna Warkocz	27-10-2024	11:15	11:30	00:15
32 z 37 Moduł IV - wykład, ćwiczenia	Katarzyna Warkocz	27-10-2024	11:30	13:00	01:30
33 z 37 Przerwa obiadowa	Katarzyna Warkocz	27-10-2024	13:00	13:30	00:30
34 z 37 Moduł IV - wykład, ćwiczenia	Katarzyna Warkocz	27-10-2024	13:30	15:00	01:30
35 z 37 Przerwa	Katarzyna Warkocz	27-10-2024	15:00	15:15	00:15
36 z 37 Walidacja usługi- post test	-	27-10-2024	15:15	16:45	01:30
37 z 37 Podsumowanie	Katarzyna Warkocz	27-10-2024	16:45	18:15	01:30

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	5 400,00 PLN
Koszt przypadający na 1 uczestnika netto	5 400,00 PLN
Koszt osobogodziny brutto	128,57 PLN
Koszt osobogodziny netto	128,57 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. Pracuje w obszarze IT od 2020, 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.

Prowadzone w ramach szkolenia zajęcia są realizowane metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

Informacje dodatkowe

Usługa realizowana jest w godzinach dydaktycznych (1 godz.= 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