Możliwość dofinansowania

Szkolenia i Rozwój
Ewelina Zięcina

Brak ocen dla tego dostawcy

Świadomy i bezpieczny pracownik w mediach społecznościowych- bezpieczne korzystanie z narzędzi internetowych

Numer usługi 2024/05/11/158240/2146863

zdalna w czasie rzeczywistym
Usługa szkoleniowa
33 h
20.07.2024 do 28.07.2024

5 000,00 PLN brutto
5 000,00 PLN netto
151,52 PLN brutto/h
151,52 PLN netto/h

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych
Grupa docelowa usługi	Przedsiębiorcy i pracownicy przedsiębiorstw wykorzystujący lub zamierzający wykorzystywać narzędzia internetowe (szczególnie social media) w pracy i kreowaniu wizerunku firmy. Szkolenie w głównym stopniu kierowane jest do pracowników oraz przedsiębiorcow którzy posiadają mniejszą świadomość możliwości i zagrożeń płynących z publikowanych informacji, nie mają też wiedzy o zachodzących relacjach między profilami prywatnymi,a firmowymi. Wszystkie osoby zainteresowane poruszaną tematyką.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	19-07-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	33
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

Szkolenie przygotowuje do samodzielnego identyfikowania i zrozumienia zróżnicowanych źródeł zagrożeń ataków cyfrowych oraz do podniesienia świadomości pracowników w firmie, tym samym skutecznie podnosząc jej bezpieczeństwo w obszarze całej infrastruktury teleinformatycznej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik, który ukończył szkolenie: • Ma wiedzę na temat osiągniecia wysokiego poziomu bezpieczeństwa cybernetycznego, charakteryzuje źródła ataków, • Zapewnia ciągłość działania organizacji, szacyje ryzyko, współpracuje e specjalistami ds.bezpieczeństwa, wdraża procedury bezpieczeństwa • Komunikuje się efektywnie ze specjalistami ds. cyberbezpieczeństwa. • Przekonuje współpracowników i interesariuszy do własnego zdania.	Ćwiczenia praktyczne poddawane ocenie trenera.	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Dokument potwierdzający uzyskanie kompetencji 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?

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?

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

1. Wprowadzenie i omówienie ogólnych pojęć związanych z bezpieczeństwem w IT.
2. Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji. Algorytmy sztucznej inteligencji, chmura, rozwiązania mobilne.
3. Sposoby ochrony, metody rozpoznawania incydentów, monitoring, reagowanie.
4. Źródła ataków cyfrowych.
5. Zasada działania ransomware, sposoby ochrony - praktyczne przykłady w tym ćwiczenia.
6. Szyfrowanie poczty oraz danych wrażliwych, tworzenie szyfrowanych magazynów danych, metody bezpiecznej wymiany danych.
7. Jak poprawnie tworzyć bezpieczne hasła oraz jak korzystać z tzw. menadżerów haseł, mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F.
8. Czym jest phishing, w jaki sposób poprawnie rozpoznać próbę oszustwa, wyłudzenia danych w tym danych autoryzacyjnych.
9. Zasady dotyczące bezpieczeństwa wysyłanych danych oraz ich przechowywania.

Harmonogram

Liczba przedmiotów/zajęć: 28

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 28 Wprowadzenie i omówienie ogólnych pojęć związanych z bezpieczeństwem w IT cz.1 - wykład	Michał Cygan	20-07-2024	08:00	09:30	01:30
2 z 28 Przerwa	Michał Cygan	20-07-2024	09:30	09:45	00:15
3 z 28 Wprowadzenie i omówienie ogólnych pojęć związanych z bezpieczeństwem w IT cz.2 - wykład	Michał Cygan	20-07-2024	09:45	11:15	01:30
4 z 28 Przerwa	Michał Cygan	20-07-2024	11:15	11:30	00:15
5 z 28 Wprowadzenie i omówienie ogólnych pojęć związanych z bezpieczeństwem w IT - ćwiczenia	Michał Cygan	20-07-2024	11:30	13:00	01:30
6 z 28 Przerwa obiadowa	Michał Cygan	20-07-2024	13:00	13:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 28 Źródła ataków cyfrowych - wykład	Michał Cygan	20-07-2024	13:30	15:00	01:30
8 z 28 Przerwa	Michał Cygan	20-07-2024	15:00	15:15	00:15
9 z 28 Źródła ataków cyfrowych - ćwiczenia	Michał Cygan	20-07-2024	15:15	16:00	00:45
10 z 28 Tworzenie bezpiecznych haseł	Michał Cygan	21-07-2024	08:00	09:30	01:30
11 z 28 Przerwa	Michał Cygan	21-07-2024	09:30	09:45	00:15
12 z 28 Mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F - wykład	Michał Cygan	21-07-2024	09:45	11:15	01:30
13 z 28 Przerwa	Michał Cygan	21-07-2024	11:15	11:30	00:15
14 z 28 Jak poprawnie tworzyć bezpieczne hasła oraz jak korzystać z menadżerów haseł, mechanizmy podwójnej autoryzacji w tym omówienie i zastosowanie kluczy U2F - ćwiczenia	Michał Cygan	21-07-2024	11:30	13:00	01:30
15 z 28 Przerwa obiadowa	Michał Cygan	21-07-2024	13:00	13:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 28 Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji - wykład, ćwiczenia	Michał Cygan	21-07-2024	13:30	15:45	02:15
17 z 28 Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji - wykład	Michał Cygan	27-07-2024	08:00	09:30	01:30
18 z 28 Przerwa	Michał Cygan	27-07-2024	09:30	09:45	00:15
19 z 28 Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji - wykład cd	Michał Cygan	27-07-2024	09:45	11:15	01:30
20 z 28 Przerwa	Michał Cygan	27-07-2024	11:15	11:30	00:15
21 z 28 Zapoznanie z najczęściej spotykanymi atakami na infrastrukturę IT oraz pracowników organizacji - ćwiczenia	Michał Cygan	27-07-2024	11:30	13:30	02:00
22 z 28 Przerwa obiadowa	Michał Cygan	27-07-2024	13:30	14:00	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 28 Sposoby ochrony, metody rozpoznawania incydentów, monitoring, reagowanie - wykład, ćwiczenia	Michał Cygan	27-07-2024	14:00	15:45	01:45
24 z 28 Czym jest phishing, w jaki sposób poprawnie rozpoznać próbę oszustwa, wyłudzenia danych w tym danych autoryzacyjnych - wykład, ćwiczenia	Michał Cygan	28-07-2024	09:00	11:00	02:00
25 z 28 Przerwa	Michał Cygan	28-07-2024	11:00	11:15	00:15
26 z 28 Zasady dotyczące bezpieczeństwa wysyłanych danych oraz ich przechowywania - wykład i ćwiczenia	Michał Cygan	28-07-2024	11:15	13:15	02:00
27 z 28 Przerwa	Michał Cygan	28-07-2024	13:15	13:30	00:15
28 z 28 Walidacja	-	28-07-2024	13:30	14:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	151,52 PLN

Koszt osobogodziny netto	151,52 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Michał Cygan

Doświadczenie i wiedzę zdobyte w dużych korporacjach oraz przy prowadzeniu projektów jako Project Manager zwinnie wykorzystuje w codziennej pracy z biznesem.

Uczestniczył w wielu projektach unijnych wspierających rozwój informatyzacji, np. 8.3 e-Inclucion, oraz jako ekspert w wielu instytucjach państwowych oraz prywatnych jak i jednostkach samorządu terytorialnego doradzał w transformacji cyfrowej (m.in.projekt dotyczący 4 powiatów, o wartości 12mln zł).

Jako uczestnik zespołu projektowego odpowiadał za Zintegrowany System Bezpieczeństwa w Infrastrukturze Krytycznej.

Specjalizuje się w rozwiązaniach cybersecurity i chętnie dzieli się swoją wiedzą.

Posiada szereg certyfikatów technicznych potwierdzających wysokie kwalifikacje i szeroki zasób wiedzy.

W ciągu ostatnich 2 lat przeprowadził ponad 120h szkoleń z zarządzania transformacją cyfrową oraz ponad 200h doradztwa w tym zakresie

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Wszelkie niezbędne materiały zapewnia Organizator.

Informacje dodatkowe

Usługa realizowana jest w godzinach dydaktycznych.

1 godzina dydaktyczna to 45min.

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

EWELINA ZIĘCINA

E-mail ew.ziecina@o2.pl

Telefon (+48) 514 426 116