Możliwość dofinansowania

Cyberbezpieczeństwo – zagrożenia w sieci

Numer usługi 2024/06/10/8117/2178229

900,00 PLN brutto
900,00 PLN netto
112,50 PLN brutto/h
112,50 PLN netto/h

ZETO Lublin SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★★

Lublin / stacjonarna
Usługa szkoleniowa
8 h
20.09.2024 do 20.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników wsparcie dla osób indywidualnych
Grupa docelowa usługi	• pracownicy i/lub właściciele pracujących z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	06-09-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	8
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 szkolenia jest dostarczenie specjalistycznej wiedzy i umiejętności z zakresu identyfikowania i zrozumienia zróżnicowanych źródeł zagrożeń ataków cyfrowych oraz do zwiększenia świadomości pracowników w firmie w obszarze

cyberbezpieczeństwa.
Uczestnik pozna procedury, które należy wdrożyć w celu zapewnienia bezpieczeństwa infrastruktury cyfrowej. Uczestnik uzyska wiedzę jak analizować i zgłaszać incydenty.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik pozna rodzaje ataków socjotechnicznych i na infrastrukturę	potrafi rozpoznać zagrożenie płynące z sieci i skutecznie je zneutralizować, zna zasady funkcjonowania metod socjotechnicznych w celu wyłudzenia danych (m.in. phishing)	Test teoretyczny
Uczestnik zna zasady bezpiecznego korzystania z Internetu, poczty e-mail oraz mediów społecznościowych i chmury	potrafi rozpoznać fałszywy adres e-mail, aplikację, link, zna metody wyłudzania danych i umie je zidentyfikować i opisać	Test teoretyczny
Uczestnik stosuje najlepsze praktyki bezpieczeństwa danych i skutecznie reaguje na incydenty cyberbezpieczeństwa.	Potrafi stosować techniki zapobiegania atakom.	Test teoretyczny
	Prawidłowo reaguje na incydenty związane z atakami. Promuje kulturę bezpieczeństwa cyfrowego w organizacji.	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 potwierdza 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 wal

Program

1. Pre test
2. Cyberbezpieczeństwo co to jest i czy nas dotyczy?
3. Ataki socjotechniczne
   - Czym są ataki socjotechniczne
   - Omówienie przykładów ataków socjotechnicznych
   - Wykrywanie ataków socjotechnicznych
   - Prawidłowa reakcja na ataki socjotechniczne
4. Ataki na infrastrukturę
   - Aplikacje i urządzenia mobilne
   - Niebezpieczeństwa związane z pocztą e-mail i załącznikami
   - Strony WWW
   - Ataki przez telefony
   - Ataki typu ransomware
   - Oszustwa phishingowe – rodzaje i charakter ataków
5. Zapewnienie bezpieczeństwa
   - Bezpieczeństwo poczty e-mail
   - Polityka zarządzania hasłami
   - Podpisywanie i szyfrowanie dokumentów
   - Bezpieczeństwo fizyczne – polityka czystego biurka oraz czystego ekranu.
6. Post test

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	900,00 PLN
Koszt przypadający na 1 uczestnika netto	900,00 PLN
Koszt osobogodziny brutto	112,50 PLN
Koszt osobogodziny netto	112,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Katarzyna Żółkiewska-Malicka

Dyrektor ds. bezpieczeństwa informacji w ZETO sp. z o.o. w Lublinie. Audytor wewnętrzny, specjalista ds. bezpieczeństwa informacji z 20 letnim stażem pracy, w zakresie przeprowadzania audytów cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych oraz audytów śledczych. Auditor Wiodący systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001. Posiada tytuł Executive Master of Bussines Administration.
Wykładowca w Wyższej Szkole Przedsiębiorczości i Administracji w Lublinie (zajęcia z zakresu ochrony danych osobowych oraz audytu na studiach podyplomowych na kierunku Inspektor Ochrony Danych). Trener prowadzący szkolenia z zakresu bezpieczeństwa informacji, ochrony danych osobowych oraz cyberbezpieczeństwa.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacja zawierająca główne tematy szkolenia.

Informacje dodatkowe

Szkolenie realizowane jest w godzinach dydaktycznych (45 min). Łącznie realizowanych jest 8 godzin dydaktycznych i 60 minut przerw każdego dnia (przerwy nie wliczane do czasu szkolenia).

Po zakończeniu udziału w szkoleniu uczestnik otrzymuje odpowiednie zaświadczenie o ukończeniu szkolenia oraz dokonuje oceny szkolenia w BUR.

Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz zaliczenie zajęć w formie testu wykonywanego na zakończenie szkolenia.

Adres

ul. Diamentowa 2
20-447 Lublin
woj. lubelskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe
- Udogodnienia dla osób ze szczególnymi potrzebami

Kontakt

Ewa Fronczyk - Kowalczyk

E-mail ewa.kowalczyk@zeto.lublin.pl

Telefon (+48) 81 7184 250