Możliwość dofinansowania

Cyberbezpieczeństwo i zagrożenia hybrydowe dla lokalnych struktur - warsztat praktyczny

Numer usługi 2026/09/03/212309/3787425

3 936,00 PLN brutto
3 200,00 PLN netto
281,14 PLN brutto/h
228,57 PLN netto/h
261,33 PLN cena rynkowa

Centrum Praw Migrantów i Integracji Europejskiej - Viktoriia Gubanova

Brak ocen dla tego dostawcy

- Wrocław
- Usługa szkoleniowa
- mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
- Zajęcia grupowe
- 14:00 h
- 12.09.2026 do 11.09.2027

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do osób dorosłych, które chcą rozwijać kompetencje w zakresie cyberbezpieczeństwa i reagowania na zagrożenia hybrydowe. W szczególności zapraszamy mieszkańców, pracowników jednostek gminnych, członków OSP, sołtysów, członków rad sołeckich, Kół Gospodyń Wiejskich, organizacji pozarządowych oraz lokalnych liderów. Usługa jest przeznaczona dla użytkowników urządzeń i informacji; nie wymaga przygotowania technicznego ani uprawnień administratora.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	11-09-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Uczestnik po zakończeniu usługi bezpiecznie konfiguruje podstawowe zabezpieczenia konta, rozpoznaje phishing i socjotechnikę, chroni dane, wykonuje pierwsze czynności po incydencie, weryfikuje informacje i realizuje prostą procedurę ciągłości działania podczas zdarzenia cyber-hybrydowego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje silne uwierzytelnianie i bezpieczne ustawienia konta.	Na koncie treningowym tworzy unikalne hasło lub frazę hasłową, uruchamia uwierzytelnianie wieloskładnikowe albo poprawnie opisuje procedurę jego uruchomienia, sprawdza aktywne sesje i urządzenia oraz wskazuje bezpieczny kanał odzyskiwania dostępu.	Obserwacja w warunkach symulowanych
Uczestnik identyfikuje phishing i socjotechnikę.	W zbiorze 10 wiadomości poprawnie klasyfikuje co najmniej 8, wskazuje minimum dwa sygnały ostrzegawcze w każdej podejrzanej wiadomości oraz nie uruchamia linku ani załącznika.	Test teoretyczny
Uczestnik bezpiecznie reaguje na podejrzaną wiadomość.	W symulacji przerywa interakcję z wiadomością, weryfikuje nadawcę niezależnym kanałem, zgłasza próbę właściwą ścieżką oraz zabezpiecza wiadomość jako dowód.	Obserwacja w warunkach symulowanych
Uczestnik dobiera zasady ochrony i udostępniania danych.	Dla 5 przypadków wybiera właściwego odbiorcę, kanał przekazania, zakres danych i poziom dostępu, stosuje zasadę minimalizacji danych oraz nie przesyła informacji chronionych kanałem niezatwierdzonym.	Test teoretyczny
Uczestnik wykonuje pierwsze czynności po podejrzeniu incydentu cyberbezpieczeństwa.	Nie usuwa dowodów, ogranicza dalsze ryzyko zgodnie ze scenariuszem, zapisuje czas i objawy zdarzenia, zgłasza incydent właściwym kanałem oraz nie podejmuje nieautoryzowanych działań technicznych.	Obserwacja w warunkach symulowanych
Uczestnik sporządza kompletne zgłoszenie incydentu.	Zgłoszenie zawiera informacje: kto, kiedy i co zauważył, jakiego urządzenia lub konta dotyczy zdarzenie, jakie wystąpiły objawy, jakie działania podjęto, jakie dowody zachowano, jaki jest możliwy wpływ zdarzenia oraz dane kontaktowe zgłaszającego. Zgłoszenie nie zawiera hasła ani tokenu.	Analiza dowodów i deklaracji
Uczestnik weryfikuje informację dotyczącą sytuacji kryzysowej.	Sprawdza autora, datę publikacji, źródło pierwotne i kontekst informacji oraz potwierdza ją w co najmniej dwóch niezależnych wiarygodnych źródłach albo oznacza ją jako niepotwierdzoną.	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik przygotowuje komunikat korygujący nieprawdziwą lub zmanipulowaną informację.	Komunikat jest rzeczowy, nie powiela szkodliwej treści ponad konieczny zakres, wskazuje potwierdzony fakt, zalecane bezpieczne działanie, oficjalne źródło informacji oraz termin kolejnej aktualizacji.	Prezentacja
Uczestnik realizuje prostą procedurę ciągłości działania podczas incydentu cyber-hybrydowego.	Dla scenariusza przerwy w dostępie do systemu wskazuje usługę priorytetową, bezpieczny tryb pracy offline, sposób komunikacji, sposób rejestrowania wykonanych działań oraz warunek powrotu do standardowego trybu pracy.	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Usługa realizowana jest stacjonarnie w formie praktycznego szkolenia warsztatowego. Łączny czas usługi wynosi 14 godzin zegarowych, w tym 11 godzin zajęć szkoleniowych, 1 godzina walidacji efektów uczenia się oraz 2 godziny przerw. Czas zajęć wraz z walidacją, bez przerw, wynosi 12 godzin zegarowych, co odpowiada 16 godzinom dydaktycznym. Przerwy nie są wliczane do czasu zajęć ani do godzin dydaktycznych.

Program obejmuje 4 godziny części teoretycznej, 7 godzin ćwiczeń praktycznych i symulacji oraz 1 godzinę walidacji efektów uczenia się.

Moduł 1. Krajobraz zagrożeń cyfrowych i hybrydowych w środowisku lokalnym - 1 godz. 30 min

Rodzaje zagrożeń dotyczących mieszkańców, pracowników jednostek gminnych i lokalnych organizacji. Mechanizmy cyberataków, socjotechniki i działań hybrydowych. Możliwe skutki incydentów dla funkcjonowania lokalnych struktur. Podstawowe role i zasady zgłaszania zagrożeń.

Moduł 2. Cyberhigiena i ochrona kont, urządzeń oraz danych - 2 godz. 15 min

Tworzenie bezpiecznych haseł i fraz hasłowych. Menedżery haseł. Uwierzytelnianie wieloskładnikowe. Kontrola aktywnych sesji i urządzeń. Aktualizacje, blokada ekranu, kopie zapasowe i bezpieczne ustawienia urządzeń. Zasada minimalnego dostępu. Bezpieczne korzystanie z publicznych sieci Wi-Fi. Ćwiczenia praktyczne dotyczące konfiguracji zabezpieczeń.

Moduł 3. Phishing, socjotechnika i bezpieczna reakcja na podejrzane wiadomości - 2 godz. 15 min

Rozpoznawanie fałszywych wiadomości, linków, stron logowania i załączników. Sygnały ostrzegawcze i techniki wywierania presji. Weryfikacja nadawcy niezależnym kanałem. Zabezpieczanie wiadomości jako dowodu i jej zgłaszanie. Analiza przykładów oraz symulacja reakcji na phishing.

Moduł 4. Reagowanie na incydent i ciągłość działania - 2 godz. 15 min

Pierwsze czynności po podejrzeniu incydentu. Ograniczanie ryzyka bez podejmowania nieautoryzowanych działań technicznych. Zachowanie dowodów. Dokumentowanie czasu, objawów i podjętych działań. Sporządzanie kompletnego zgłoszenia incydentu. Organizacja bezpiecznego trybu pracy zastępczej i komunikacji podczas niedostępności systemu.

Moduł 5. Dezinformacja i komunikacja w sytuacji kryzysowej - 2 godz. 15 min

Mechanizmy dezinformacji i manipulacji. Ocena autora, daty, źródła pierwotnego i kontekstu informacji. Weryfikacja informacji w niezależnych, wiarygodnych źródłach. Zasady przygotowania rzeczowego komunikatu korygującego. Ćwiczenia z weryfikacji informacji i przygotowania komunikatu dla lokalnej społeczności.

Moduł 6. Symulacja zdarzenia cyber-hybrydowego - 30 min

Zespołowa realizacja scenariusza łączącego podejrzaną wiadomość, próbę wyłudzenia danych, dezinformację i czasową niedostępność systemu. Podział ról, wybór sposobu zgłoszenia, przygotowanie komunikatu oraz uruchomienie prostego trybu ciągłości działania.

Walidacja efektów uczenia się - 1 godzina

Walidacja obejmuje test teoretyczny, obserwację uczestnika w warunkach symulowanych, analizę przygotowanego zgłoszenia incydentu oraz ocenę sposobu wykonania zadań praktycznych. Walidację przeprowadza osoba inna niż trener prowadzący zajęcia. Kryteria walidacji są zgodne z efektami uczenia się wskazanymi w Karcie Usługi.

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 10 Moduł 1. Krajobraz zagrożeń cyfrowych i hybrydowych – miniwykład, analiza przypadków i dyskusja	Zajęcia	Vitalii Suprun	12-09-2026	09:00	10:30	01:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
2 z 10 Moduł 2. Cyberhigiena i ochrona kont, urządzeń oraz danych – pokaz i ćwiczenia praktyczne	Zajęcia	Vitalii Suprun	12-09-2026	10:30	12:45	02:15	Tak
3 z 10 -	Przerwa	-	12-09-2026	12:45	13:45	01:00	Tak
4 z 10 Moduł 3. Phishing, socjotechnika i bezpieczna reakcja na podejrzane wiadomości – analiza przykładów i symulacja	Zajęcia	Vitalii Suprun	12-09-2026	13:45	16:00	02:15	Tak
5 z 10 Moduł 4. Reagowanie na incydent i ciągłość działania – ćwiczenia i analiza scenariuszy	Zajęcia	Vitalii Suprun	13-09-2026	09:00	11:15	02:15	Tak
6 z 10 Moduł 5. Dezinformacja i komunikacja kryzysowa, część I – analiza informacji i źródeł	Zajęcia	Vitalii Suprun	13-09-2026	11:15	12:45	01:30	Tak
7 z 10 -	Przerwa	-	13-09-2026	12:45	13:45	01:00	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
8 z 10 Moduł 5. Dezinformacja i komunikacja kryzysowa, część II – przygotowanie komunikatu korygującego	Zajęcia	Vitalii Suprun	13-09-2026	13:45	14:30	00:45	Tak
9 z 10 Moduł 6. Symulacja zdarzenia cyber-hybrydowego	Zajęcia	Vitalii Suprun	13-09-2026	14:30	15:00	00:30	Tak
10 z 10 -	Walidacja	-	13-09-2026	15:00	16:00	01:00	Tak

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:00
w tym suma godzin walidacji	01:00
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	16:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 936,00 PLN
Koszt przypadający na 1 uczestnika netto	3 200,00 PLN
Koszt osobogodziny brutto	281,14 PLN
Koszt osobogodziny netto	228,57 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Vitalii Suprun

Vitalii Suprun - specjalista IT i trener kompetencji cyfrowych posiadający wykształcenie wyższe oraz praktyczne doświadczenie w prowadzeniu zajęć szkoleniowych dla osób dorosłych. Prowadził 80-godzinne szkolenie w zakresie podnoszenia kompetencji cyfrowych, realizowane w ramach projektu współfinansowanego ze środków programu Fundusze Europejskie dla Dolnego Śląska 2021–2027. Zakres prowadzonych zajęć obejmował między innymi: cyberhigienę, rozpoznawanie phishingu, socjotechniki i złośliwego oprogramowania, bezpieczne korzystanie z poczty elektronicznej i urządzeń cyfrowych, tworzenie bezpiecznych haseł, uwierzytelnianie wieloskładnikowe, ochronę danych osobowych, prywatność w Internecie, bezpieczne korzystanie z sieci Wi-Fi, podstawy VPN, wykonywanie kopii zapasowych, ochronę przed wyłudzeniami, ocenę wiarygodności źródeł oraz rozpoznawanie fake newsów i dezinformacji.
Trener wykorzystuje metody praktyczne, w tym ćwiczenia wykonywane na urządzeniach, analizę przykładów, zadania problemowe oraz symulacje sytuacji związanych z zagrożeniami cyfrowymi. Posiada doświadczenie w pracy z osobami o zróżnicowanym poziomie kompetencji cyfrowych i potrafi przekazywać zagadnienia techniczne w sposób zrozumiały dla użytkowników nieposiadających specjalistycznego przygotowania informatycznego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma skrypt szkoleniowy dotyczący cyberhigieny i reagowania na incydenty, checklistę rozpoznawania phishingu i socjotechniki, instrukcję zabezpieczania kont i urządzeń, wzór zgłoszenia incydentu, zasady bezpiecznego udostępniania danych, checklistę weryfikacji informacji i dezinformacji, wzór komunikatu korygującego, uproszczony schemat ciągłości działania oraz karty ćwiczeń wykorzystywane podczas symulacji. Materiały zostaną przekazane w wersji drukowanej, a wybrane materiały również w wersji elektronicznej

Warunki techniczne

Uczestnik otrzyma skrypt szkoleniowy dotyczący cyberhigieny i reagowania na incydenty, checklistę rozpoznawania phishingu i socjotechniki, instrukcję zabezpieczania kont i urządzeń, wzór zgłoszenia incydentu, zasady bezpiecznego udostępniania danych, checklistę weryfikacji informacji i dezinformacji, wzór komunikatu korygującego, uproszczony schemat ciągłości działania oraz karty ćwiczeń wykorzystywane podczas symulacji. Materiały zostaną przekazane w wersji drukowanej, a wybrane materiały również w wersji elektronicznej

Adres

ul. Aleksandra Hercena 3-5/45

50-453 Wrocław

woj. dolnośląskie

Szkolenie odbędzie się w sali szkoleniowej przy ul. Aleksandra Hercena 3-5 we Wrocławiu. Dokładny numer sali oraz informacje organizacyjne dotyczące wejścia do budynku zostaną przekazane uczestnikom przed rozpoczęciem usługi.

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

Viktoriia Gubanova

E-mail centrumprawmigrantow@gmail.com

Telefon (+48) 730 637 903