Możliwość dofinansowania

Szkolenie Cyberzagrożenia i metody obrony

Numer usługi 2025/07/24/51849/2899669

600,00 PLN brutto
600,00 PLN netto
150,00 PLN brutto/h
150,00 PLN netto/h

EFFECTIVE IT TRAININGS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,5 / 5

109 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
4 h
17.09.2025 do 17.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Akademia HR
Grupa docelowa usługi	Szkolenie adresowane jest do szerokiego grona odbiorców, w tym:• Pracowników wszystkich szczebli, którzy korzystają z technologii informatycznych w codziennej pracy • Specjalistów IT i administratorów systemów, chcących poszerzyć swoją wiedzę z zakresu cyberbezpieczeństwa • Managerów i kierowników odpowiedzialnych za bezpieczeństwo informacji w organizacji • Pracowników działów bezpieczeństwa informacji i ochrony danych osobowych • Osób zainteresowanych pogłębieniem wiedzy o cyberbezpieczeństwieSzkolenie jest odpowiednie zarówno dla osób z podstawową wiedzą techniczną, jak i dla zaawansowanych użytkowników, którzy chcą zaktualizować swoją wiedzę o najnowsze trendy w cyberbezpieczeństwie.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	16-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Liczba godzin usługi	4
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 uczestnika do świadomego i samodzielnego stosowania praktyk cyberbezpieczeństwa w zakresie ochrony danych, urządzeń i komunikacji elektronicznej, zarówno w pracy stacjonarnej, jak i zdalnej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia rodzaje złośliwego oprogramowania i ich potencjalne skutki.	przyporządkowuje konkretne przykłady zagrożeń (np. ransomware, spyware) do odpowiednich kategorii i opisuje możliwe konsekwencje ich działania.	Test teoretyczny z wynikiem generowanym automatycznie
Diagnozuje próby ataków opartych na socjotechnikach w różnych kanałach komunikacji.	analizuje przykładowe wiadomości e-mail, komunikaty i sytuacje pod kątem cech charakterystycznych manipulacji i oszustw.	Test teoretyczny z wynikiem generowanym automatycznie
Opisuje zasady bezpiecznego korzystania z sieci w różnych środowiskach (praca, dom, miejsca publiczne).	wskazuje odpowiednie działania ochronne w scenariuszach korzystania z Wi-Fi, stron internetowych i usług online w różnych lokalizacjach.	Test teoretyczny z wynikiem generowanym automatycznie
Przygotowuje zestaw dobrych praktyk dotyczących bezpiecznego korzystania z komunikatorów i mediów społecznościowych.	opracowuje listę zasad dotyczących bezpiecznego udostępniania informacji online oraz reagowania na podejrzane treści lub kontakty.	Test teoretyczny z wynikiem generowanym automatycznie
Opracowuje plan bezpiecznej pracy zdalnej uwzględniający ochronę urządzeń, danych i połączeń sieciowych.	tworzy uproszczony schemat zawierający elementy takie jak aktualizacje, korzystanie z VPN, hasła oraz zabezpieczenia sprzętu służbowego.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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

zajęcia będą realizowane metodami interaktywnymi i aktywizującymi …) i dopisać jakiego rodzaju metody będą użyte podczas realizacji zajęć (np. ćwiczenia, burza mózgów, obserwacja, dyskusja panelowa, metoda problemowa, studium przypadku itp.)

Przerwy są wliczane do czasu trwania usługi

ilość godzin 16 godziny zegarowych. Usługa jest realizowana w godzinach zegarowych.

Zaświadczenie otrzymuje uczestnik, który będzie miał co najmniej 80% obecności podczas szkolenia oraz uzyska pozytywną ocenę z walidacji.

Walidacja : Walidacja odbędzie się w formie testu online. Uczestnik powinien posiadać dostęp do Internetu. Test zostanie przesłany w formie linku na indywidualnego maila uczestnika szkolenia. Testy zostaną sprawdzone bez udziału człowieka (automatycznie przez system informatyczny) Uczestnicy otrzymają mailowo powiadomienie o % poprawnych odpowiedzi. Dostawca Usługi przeprowadzi rejestr wyników + rejestr wydanych zaświadczeń w ramach projektu/ szkolenia. Rozdzielność funkcji jest zachowana.

Po zakończeniu usługi uczestnik otrzymuje odpowiednie zaświadczenie/certyfikat, a warunkiem jego uzyskania jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz zaliczenie zajęć w formie testu

PROGRAM SZKOLENIA:

1. Zagrożenia związane ze złośliwym oprogramowaniem oraz praktyki obronne
2. • Przegląd różnych rodzajów złośliwego oprogramowania
3. • Praktyki obronne w zakresie wykrywania i zwalczania zagrożeń
4. Socjotechniki i zagrożenia
5. • Socjotechniki – jak działają?
6. • Rozpoznawanie pułapek
7. • Praktyczne wskazówki na rozpoznawanie zagrożeń
8. Bezpieczne korzystanie z sieci
9. • Sprawdzanie bezpieczeństwa stron internetowych
10. • Bezpieczne Wi-Fi: w pracy, domowe
11. • Korzystanie z publicznych miejsc z dostępem do sieci
12. Bezpieczne korzystanie z komunikacji elektronicznej
13. • Sposoby identyfikacji podejrzanych e-maili i załączników oraz unikania pułapek
14. • Komunikatory i media społecznościowe
15. • Ostrzeżenia dotyczące bezpiecznego korzystania z komunikatorów oraz zasad bezpiecznego dzielenia informacji online
16. Bezpieczeństwo transakcji online
17. • Zasady bezpiecznych transakcji
18. • Porady dotyczące bezpiecznych zakupów online i korzystania z usług bankowości internetowej
19. • Jak chronić dane finansowe i unikać oszustw związanych z transakcjami online
20. Bezpieczeństwo Pracy Zdalnej
21. • Zasady bezpiecznej pracy na odległość
22. • Wskazówki dotyczące bezpiecznego korzystania z urządzeń w pracy zdalnej
23. • Proste instrukcje dotyczące korzystania z VPN
24. Podsumowanie i Wnioski
25. Walidacja

Informacje dodatkowe

Usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub partnera w Regionalnym Programie lub FERS.

Usługa rozwojowa nie jest świadczona przez podmiot będący jednocześnie podmiotem korzystającym z usług rozwojowych o zbliżonej tematyce w ramach danego projektu. Usługa rozwojowa nie dotyczy kosztów usługi rozwojowej, której obowiązek przeprowadzenia nazajmowanym stanowisku pracy wynika z odrębnych przepisów prawa (np. wstępne i okresowe szkolenia z zakresu bezpieczeństwa i higieny pracy, szkolenia okresowe potwierdzające kwalifikacje na zajmowanym stanowisku pracy).

Usługa rozwojowa nie obejmuje wzajemnego świadczenia usług w Projekcie o zbliżonej tematyce przez Dostawców usług, którzy delegują na usługi siebie oraz swoich pracowników i korzystają z dofinansowania, a następnie świadczą usługi w zakresie tej samej tematyki dla Przedsiębiorcy, który wcześniej występował w roli Dostawcy tych usług.

Zgodnie ze stanowiskiem Ministerstwa Funduszy i Polityki Regionalnej dotyczącym procesu walidacji nabycia kompetencji w ramach Podmiotowych Systemów Finansowania zostanie zachowana rozdzielność funkcji nauczania od walidacji poprzez przekazanie przez osobę prowadzącą zajęcia testów uczestnikom do rozwiązania, a następnie przekazanie ich osobie walidującej efekty uczenia się do sprawdzenia.

Dostawca usługi potwierdza brak powiązań kapitałowych i osobowych pomiędzy dostawcą usługi a pracodawcą lub osobą dorosłą korzystająca ze wsparcia.

Dostawca usługi potwierdza, że usługa rozwojowa nie jest świadczona przez podmiot pełniący funkcję Operatora lub partnera w Projekcie albo przez podmiot powiązany kapitałowo lub osobowo z Operatorem lub partnerem

minimalny poziom odpowiedzi w teście wiedzy wynosi 80 %

walidacja obejmuje całość procesu, aż do momentu uzyskania efektów uczenia się.

usługa rozwojowa nie dotyczy umiejętności lub kompetencji podstawowych tj. (z ang. basic skills: literacy, numeracy, ICT skills)”

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	600,00 PLN
Koszt przypadający na 1 uczestnika netto	600,00 PLN
Koszt osobogodziny brutto	150,00 PLN

Koszt osobogodziny netto	150,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

DAWID KOZIOROWSKI

Wykształcenie:

University of Entrepreneurship and Administration in Lublin (WSPA) - Master of Science in Engineering (MSc Eng.), Computer Science – Specialization: Cybersecurity

Doświadczenie zawodowe: Doświadczony specjalista cyberbezpieczeństwa z 16-letnim stażem w prowadzeniu szkoleń. Cyber Security Instructor w Akademia PORTAL (2009-2024), równocześnie CEO firmy PORTAL Kompleksowe Rozwiązania Informatyczne (2009-2024). Obecnie Penetration Tester & Lecturer w DAGMA Bezpieczeństwo IT (od 2023) oraz wykładowca akademicki. Wcześniej Cyber Security Lecturer w HackerU Polska (2022-2024). Certyfikowany Ethical Hacker (CEH), Red Team Operator oraz ekspert sądowy w dziedzinie cyberbezpieczeństwa. Specjalizuje się w penetration testing, social engineering, physical security oraz bezpieczeństwie fizycznym.

Szkolenia 2024-2025: Przeprowadził około 850 godzin szkoleń z zakresu cyberbezpieczeństwa, penetration testing, ethical hacking oraz bezpieczeństwa fizycznego dla specjalistów IT, zespołów bezpieczeństwa oraz studentów akademickich.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają dostęp do materiałów szkoleniowych w formie elektronicznej- skrypt z zakresu programu szkolenia, ćwiczenia.

Cena usługi nie obejmuje kosztów niezwiązanych bezpośrednio z usługą rozwojową, w szczególności kosztów środków trwałych przekazywanych Przedsiębiorcom lub Pracownikom przedsiębiorcy, kosztów dojazdu i zakwaterowania

Warunki uczestnictwa

Uczestnicy nie muszą wykazywać się minimalnym doświadczeniem / stażem aby uczestniczyć w usłudze rozwojowej

Fakt uczestnictwa w każdym dniu usługi rozwojowej będzie potwierdzony przez uczestnika na udostępnionej przez organizatora szkolenia liście

Dostawca usługi zapewnia realizację usługi rozwojowej uwzględniając potrzeby osób z niepełnosprawnościami (w tym również dla osób ze szczególnymi potrzebami) zgodnie ze Standardami dostępności dla polityki spójności 2021-2027.

Informacje dodatkowe

Dostawca usługi oświadcza, że:

cena usługi nie odbiega od cen rynkowych oraz, że cena jest adekwatna do jej zakresu,

że karta usługi przygotowana została zgodnie z obowiązującym Regulaminem BUR m.in. w zakresie powierzenia usług

że usługa rozwojowa będzie realizowana zgodne z obowiązującymi przepisami prawa w tym przepisami prawa o VAT

Kontakt w sprawie szkolenia, dotyczące kwestii organizacyjnych :

justyna.kalbarczyk@eitt.pl

Kontakt w sprawie dofinansowania do szkolenia, karty BUR :

Patrycja Foremniak patrycja.foremniak@eitt.pl

W przypadku dofinansowania mniejszego niż 70% wartości netto szkolenia, Dostawca Usługi naliczy VAT do kwoty netto. Usługa szkoleniowa zwolniona z VAT tylko w przypadku gdy dofinansowanie ze środków publicznych wynosi co najmniej 70%.

Ocena efektów uczenia się prowadzona jest za pośrednictwem testu dostępnego online, a wynik jest generowany automatycznie bez udziału człowieka -> warunek rozdzielności procesów szkolenia i walidacji jest zachowa

Warunki techniczne

Podstawą do rozliczenia usługi, jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników, oraz zastosowanego narzędzia.

Link umożliwiający uczestnictwo w usłudze zdalnej jest dostępny przez cały okres jej trwania.

usługa rozwojowa zostanie przeprowadzona za pośrednictwem platformy/komunikatora wskazanego przez Organizatora Usługi : Microsoft Teams

uczestnik dysponuje urządzeniem spełniającym następujące wymagania sprzętowe: urządzenie przenośne/mobilne lub stacjonarne (komputer/laptop/tablet) z kamerą, mikrofonem i głośnikami; procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy) lub Core i5 Kaby Lake; min. 2GB pamięci RAM (zalecane 4GB lub więcej);

system operacyjny taki jak min. Windows 8 (zalecany Windows 11), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS;

aktualne wersje przeglądarki np.- Google Chrome, Mozilla Firefox, Microsoft Edge, Opera, Internet Explorer, Brave, Safari, Microsoft Edge, Opera, Internet Explorer, Yandex

uczestnik dysponuje łączem sieciowym spełniającym następujące parametry: dostęp do internetu o zalecanej szybkości - minimalna prędkość pobierania 2 Mb/s, prędkość wysyłania 512 kb/s;-

uczestnik dysponuje niezbędnym oprogramowaniem umożliwiającym dostęp do prezentowanych treści i materiałów;

liczba uczestników umożliwia wszystkim uczestnikom interaktywną swobodę udziału we wszystkich przewidzianych elementach zajęć (ćwiczenia, rozmowa na żywo, chat, testy, ankiety, współdzielenie ekranu itp.)

Kontakt

JUSTYNA KALBARCZYK

E-mail justyna.kalbarczyk@eitt.pl
Telefon (+48) 516 098 221