Możliwość dofinansowania

codebrainers

CODEBRAINERS SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,5 / 5

2 015 ocen

Cyberbezpieczeństwo w praktyce - Małopolski Pociąg do Kariery / Kierunek Rozwój / Graj po Zielone

Numer usługi 2026/05/04/118259/3536926

2 400,00 PLN brutto
2 400,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
261,33 PLN cena rynkowa

Usługa szkoleniowa
zdalna w czasie rzeczywistym
24:00 h
06.10.2026 do 22.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Małopolski Pociąg do kariery
Grupa docelowa usługi	Kurs skierowany jest dla osób, które chcą poszerzyć swoją wiedzę na temat bezpiecznego korzystania z Internetu i urządzeń cyfrowych, a także nauczyć się rozpoznawania zagrożeń oraz właściwego reagowania na nie. Uczestnikami mogą być wszyscy, którzy na co dzień korzystają z komputera, poczty elektronicznej lub Internetu — niezależnie od poziomu umiejętności technicznych, w tym specjaliści sektora zielonej gospodarki, chcący wykorzystać zdobytą wiedzę podczas tworzenia ekologicznych rozwiązań. Usługa adresowana również do uczestników Projektów: Kierunek Rozwój, Małopolski Pociąg do Kariery, Zachodniopomorskie Bony Szkoleniowe, Graj po Zielone, uczestników programów dof. w ramach FESL 5.15, 6.6 oraz 10.17 z woj. śląskiego oraz uczestników innych programów dofinansowań.
Minimalna liczba uczestników	8
Maksymalna liczba uczestników	18
Data zakończenia rekrutacji	05-10-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	24

Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Kurs przygotowuje do samodzielnego i efektywnego wykorzystania wiedzy i umiejętności praktycznych w zakresie bezpieczeństwa cyfrowego – w celu ochrony danych i urządzeń, rozpoznawania zagrożeń cyfrowych, bezpiecznego korzystania z technologii oraz właściwego reagowania na incydenty z jednoczesnym uwzględnieniem zasad zrównoważonego rozwoju, odpowiedzialnego korzystania z zasobów cyfrowych oraz zwiększania świadomości wpływu TIK na środowisko.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Posługuje się wiedzą z zakresu cyberbezpieczeństwa	wskazuje najczęstsze typy zagrożeń (phishing, malware, ransomware itp.)	Test teoretyczny z wynikiem generowanym automatycznie
	wyjaśnia, czym jest poufność, integralność i dostępność informacji	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje zasady tworzenia i przechowywania silnych haseł	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje sposoby jak skonfigurować dwuskładnikowe uwierzytelnianie (2FA)	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje i ogranicza zagrożenia cyberbezpieczeństwa	Rozpoznaje podstawowe typy cyberataków oraz ocenia potencjalne ryzyko dla użytkownika i organizacji.	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje przykłady bezpiecznych i niebezpiecznych zachowań w sieci (np. analiza przykładowych e-maili lub stron)	Test teoretyczny z wynikiem generowanym automatycznie
	Analizuje przykłady incydentów bezpieczeństwa i identyfikuje błędy techniczne, procesowe oraz ludzkie	Test teoretyczny z wynikiem generowanym automatycznie
Posługuje się wiedzą z zakresu zrównoważonego rozwoju, niezbędną do pracy w sektorze zielonej gospodarki	charakteryzuje główne poglądy na temat zrównoważonego rozwoju	Test teoretyczny z wynikiem generowanym automatycznie
	charakteryzuje zasady środowiskowe 6R w kontekście TIK	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje zagrożenia związane z cyberbezpieczeństwem w sektorach zielonej gospodarki	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Współpracuje i komunikuje się z innymi członkami zespołu	wskazuje prawidłowe sposoby komunikacji i współpracy z zespołem	Test teoretyczny z wynikiem generowanym automatycznie

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

Szkolenie „Cyberbezpieczeństwo w praktyce" przeznaczone jest dla osób, które na co dzień korzystają z komputerów, poczty elektronicznej i Internetu, zarządzają infrastrukturą OZE – niezależnie od poziomu zaawansowania technicznego. Ma ono na celu podniesienie świadomości oraz umiejętności użytkowników w zakresie bezpiecznego korzystania z technologii informatycznych w codziennym życiu oraz przy rozwijaniu rozwiązań TIK w sektorach zielonej gospodarki.

Podczas zajęć uczestnicy poznają najczęstsze zagrożenia, takie jak phishing, ransomware czy ataki socjotechniczne, oraz uczą się, jak skutecznie im przeciwdziałać.

Szkolenie łączy teorię z praktyką – uczestnicy zdobywają wiedzę o zasadach bezpiecznego korzystania z Internetu, tworzenia silnych haseł, ochrony danych osobowych i firmowych oraz reagowania na incydenty bezpieczeństwa.

Uczestnicy dowiedzą się również, jak budować kulturę bezpieczeństwa w organizacji i jakie działania podejmować, aby minimalizować ryzyko cyberataków. Dzięki praktycznym ćwiczeniom i przykładom uczestnicy nauczą się chronić siebie, swoje dane, systemy i swoją firmę przed zagrożeniami cyfrowymi.

--

STRUKTURA KURSU

- **kurs obejmuje 24h lekcyjnych (45 min) = w przeliczeniu 18h zegarowych (60 min)) prowadzonych na żywo (on-line)**, na platformie webinarowej, w formie wirtualnej klasy, w formule live-coding - przez cały czas z trenerem
- dodatkowo planowana jest samodzielna praca własna kursantów w domu (ćwiczenia, projekty), z możliwością konsultacji na platformie Slack - praca ta pozwala utrwalić zdobyta podczas zajęć wiedzę i nie jest wliczana do czasu trwania usługi - nie jest to obowiązkowe;

- zajęcia odbywają się na żywo (online, w formie wirtualnej klasy) w formule wieczorowo-weekendowej - x w tygodniu (wieczorem) oraz w wybraną sobotę

Moduł 1. Wprowadzenie – cyberbezpieczeństwo, zagrożenia, wprowadzenie do zielonej gospodarki

1. Czym jest cyberbezpieczeństwo i dlaczego jest kluczowe
2. wprowadzenie do zielonej gospodarki, charakterystyka głównych poglądów dotyczących zrównoważonego rozwoju, zasady środowiskowe 6R
3. Kategorie cyberzagrożeń: cyberprzestępczość, ataki na dane finansowe i tożsamość, ransomware
4. Przegląd współczesnych incydentów (phishing, malware, DDoS)
5. Statystyki naruszeń i ich wpływ na działalność firm
6. Najczęstsze błędy użytkowników i ich konsekwencje
7. Wpływ cyberbezpieczeństwa na efektywność energetyczną i odpowiedzialne korzystanie z ICT
    1. bezpieczna i prawidłowa utylizacja nośników (kasowanie danych przed recyklingiem)
    2. wpływ ataków (np. kryptokoparki/botnety) na zużycie energii
    3. dłuższe życie sprzętu dzięki prawidłowej konfiguracji i aktualizacjom
    4. minimalizacja zbędnych kopii danych (mniej storage = mniej energii w DC)
8. Jak firmy bronią się przed cyberatakami
    1. jak działa Blue Team (zespół obrony w firmach) - monitorowanie systemów, wykrywanie ataków, reagowanie na incydenty
    2. Jak działa Red Team - testowanie zabezpieczeń tak, jak zrobiłby to realny atakujący
9. Ochrona zielonej infrastruktury (sieci energetycznych, farm wiatrowych etc) przed cyberatakami

Moduł 2. Cyberprzestępczość, Dark Web i realne incydenty

1. Cybercrime: motywacje, modele biznesowe przestępców
    1. cybercrime-as-a-service (gotowe pakiety ataków), ransomware gangi, handel danymi i dostępami (initial access brokers
    2. przykłady cyberataków na strukturę OZE
2. Dark Web: czym jest, do czego służy, zagrożenia
    1. jak trafiają do dark webu (oraz na fora cyberprzestępcze) dane użytkowników: wycieki, phishing, malware
    2. jak wycieki z dark webu są potem używane: przejęcia kont, ataki na firmy, szantaż
3. Studium przypadków naruszeń bezpieczeństwa (światowe i polskie firmy)
    1. Incydenty wpływające na:
        1. ciągłość działania organizacji
        2. reputację i zaufanie klientów
        3. środowisko naturalne – ataki na infrastrukturę energetyczną, wodociągową, IoT
4. Analiza błędów procesowych i ludzkich
5. Jak minimalizować ryzyko powtórzenia incydentu

Moduł 3.

Jak działa Internet i sieć firmowa

1. Jak w praktyce działa sieć w firmie i w domu
    1. adres IP, port, router, Wi-Fi, różnica LAN/Internet
    2. co to jest DNS
2. Co jest celem ataków w sieci
    1. podsłuch w sieci (sniffing, MITM, Wi-Fi)
    2. blokowanie usług (DDoS wytłumaczone jednym zdaniem)
    3. wyszukiwanie otwartych drzwi (skanowanie portów, podatne urządzenia IoT)
    4. skutki ataków na infrastrukturę (prąd, woda, transport, IoT)
3. Podstawowe zabezpieczenia sieciowe
    1. silne hasło do Wi-Fi, WPA2/WPA3, zmiana domyślnych haseł routera
    2. HTTPS, VPN, firewall, segmentacja biuro a IoT
4. Sieci a zielona gospodarka
    1. sieci i sensory w OZE, smart-metry, monitoring środowiska
    2. co się dzieje, gdy ktoś przejmie takie urządzenia (fałszywe dane, większe zużycie energii, awarie)
    3. Dlaczego urządzenia OZE i IoT są szczególnie wrażliwe (często słabe hasła, brak aktualizacji).

Moduł 4. Firewalle, ochrona systemów i operacje bezpieczeństwa

1. Jak chronić sieć: firewalle i segmentacja
    1. co robi firewall
    2. firewalle ochrona organizacji i lokalna warstwa ochrony

2. Jak chronić komputery i serwery
    1. antywirus / antymalware
    2. EDR - monitorowanie zachowania systemu
    3. systemy wykrywania i blokowania ataków w sieci (IDS/IPS)

3. Zarządzanie bezpieczeństwem na co dzień (Security Operations)
    1. monitoring systemów i usług
    2. analiza logów i wykrywanie anomalii
    3. reagowanie na incydenty i wyciąganie wniosków

4. Ekologiczne aspekty zarządzania infrastrukturą ICT
    1. mądre zarządzanie zasobami (konsolidacja usług, wyłączanie zbędnych systemów)
    2. optymalne przechowywanie logów i danych (retencja zamiast wiecznych danych)
    3. automatyzacja i dobra konfiguracja jako sposób na mniejsze marnotrawstwo energii

Moduł 5. Psychologia ataków i inżynieria społeczna

1. Mechanizmy manipulacji i psychologia oszustw
2. Inżynieria społeczna (social engineering)
    1. phishing i spear phishing
    2. vishing, smishing
    3. pretexting
    4. tailgating i shoulder surfing

3. Analiza prawdziwych kampanii socjotechnicznych
4. Ataki na tożsamość i kanały komunikacji
    1. SIM swap - podmiana karty SIM, przejęcie SMS-ów do banku / 2FA
    2. przejęcie maila i podmiana numeru konta na fakturach
    3. ataki na komunikatory (WhatsApp, Messenger, Telegram) – podszywanie się pod znajomych / współpracowników

5. Rozpoznawanie fałszywych stron i treści
6. Warsztaty: analiza e-maili i wiadomości
    1. analiza przykładowych maili / SMSów

| **Walidacja efektów kształcenia oraz egzamin**

Po zakończeniu kursu zostanie przeprowadzony egzamin potwierdzający nabycie kwalifikacji. Uczestnicy szkolenia otrzymują imienne certyfikaty potwierdzające nabycie kwalifikacji sygnowane przez Codebrainers.

--

- **całość zajęć prowadzona jest na żywo online**
- **aby osiągnąć zakładany cel** realizacji usługi, uczestnik powinien być obecny w trakcie zajęć zdalnych w czasie rzeczywistym
- usługa szkoleniowa realizowana jest w godzinach dydaktycznych (1 godzina dydaktyczna = 45 min.) - łącznie 18h dydaktycznych, w tym. ok. 9 h teoretycznych oraz 9 h praktycznych (w formie wirtualnej klasy)
- w ramach usługi przewidziane są przerwy podczas zajęć 6 godzinnych w soboty, które zostały uwzględnione w harmonogramie usługi, jednak nie wliczają się do ilości godzin samej usługi
- walidacja efektów kształcenia odbywa się w formie testu teoretycznego w formie cyfrowej, z wynikiem generowanym automatycznie. Test prowadzony jest na zewnętrznej platformie, w oparciu o indywidualne kody dostępu przypisane do każdego z uczestników, z zapewnieniem rozdzielności pomiędzy szkoleniem, a walidacją

--

Dodatkowe informacje odnośnie walidacji:

Na zakończenie kursu zostanie przeprowadzony egzamin potwierdzający nabycie kwalifikacji (test w formie cyfrowej). Egzamin nadzorowany jest przez prowadzącego zajęcia (osoba ta jedynie rozsyła test, sprawdza obecność, nie ingeruje w jego wypełnianie ani sprawdzanie wyników).

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	2 400,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Mateusz Augustyn

Doświadczony specjalista który realizuje projekty z zakresu cyberbezpieczeństwa, rozwoju oprogramowania oraz doradztwa IT. Prowadzi również działalność szkoleniową, przekazując praktyczną wiedzę z zakresu bezpieczeństwa cyfrowego.
2025 – obecnie - Właściciel firmy / Ekspert ds. cyberbezpieczeństwa - Synframe
2024 – 2025 - Software Developer / Server Administrator - ZETO-RZESZÓW Sp. z o.o.
2023 - Software Developer - Appgo Sp. z o. o.
2022 – 2024 - Badacz w dziedzinie bezpieczeństwa - HackerOne

Posiada dośw. w zakresie ziel.kompetencji, łącząc cyberbezpieczeństwo z: efektywnym wykorzystaniem zasobów IT, redukcją wpływu technologii na środowisko, promowaniem trwałych i odpowiedzialnych rozwiązań cyfrowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W ramach szkolenia uczestnik otrzymuje:

- dostęp do materiałów oraz ćwiczeń podsumowujących zdobytą wiedzę (materiały on-line w formie pdf)
- dostęp do materiałów z zakresu zielonej gospodarki (min. charakterystyka poglądów dotyczących zrównoważonego rozwoju, zasady środowiskowe 6R…
- dostęp do kanałów Slack dedykowanych szkoleniu
- dostęp do nagrań z odbytych zajęć

Warunki uczestnictwa

- szkolenie prowadzone jest od podstaw, więc może wziąć w nim udział każda osoba korzystająca z komputerów, poczty elektronicznej i Internetu – niezależnie od poziomu zaawansowania technicznego
- kurs jest odpowiedni dla uczestników zaangażowanych w działania związane ze zrównoważonym rozwojem, efektywnością energetyczną, raportowaniem środowiskowym lub transformacją cyfrową
- w przypadku korzystania z dofinansowania, warunkiem uczestnictwa jest zapisanie się przez BUR wraz z podaniem aktualnego ID wsparcia

Informacje dodatkowe

- zakres zg. z RSI Woj. Śl. 2030: Techn. Inf. i kom., (i) techn. szt. int. i uczenia masz., (ii) techn. data mining, (iii) techn. zaaw. baz danych i hurtowni danych oraz z RSI Woj. Mał.. Met. i urz. służące do poz. dan.
- zapisanie się w BUR nie jest jednoznaczne z zarezerwowaniem miejsca. W celu potwierdzenia miejsca prosimy o dodatkowy kontakt telefoniczny, mailowy, lub za pośrednictwem messengera albo www
- zawarto umowę z WUP w Krakowie w ramach projektu Małopolski Pociąg do Kariery
- zawarto umowę z WUP w Toruniu w ramach projektu Kierunek Rozwój
- zawarto umowę z WUP w Szczecinie w ramach projektu Zachodniopomorskie Bony Szkoleniowe
- usługi dedykowane również uczestnikom innych programów dofinansowań
- zdobyte kompetencje dotyczą cyfrowej transformacji
- podstawa zwolnienia z VAT: Dz.U.2013.1722, art. 3, ust. 1, pkt. 14 - usł. kszt. zaw. lub przekw. zaw., fin. w co najmniej 70% ze środków publ. - podstawa zwolnienia jest każdorazowo weryfikowana w stosunku do danego Uczestnika

Warunki techniczne

- zajęcia prowadzone są w czasie rzeczywistym na platformie Zoom, wraz z dostępem do kanałów grupowych na platformie Slack
- **Minimalne wymagania sprzętowe:** komputer / laptop / lub inne urządzenie ze stałym dostępem do internetu, wyposażone w kamerę internetową
- **Minimalne wymagania dotyczące parametrów łącza sieciowego:** szybkość pobierania / przesyłania: minimalna 2 Mb/s / 128 kb/s, zalecana: 4 Mb/s / 512 kb/s
- **Niezbędne oprogramowanie umożliwiające dostęp do zajęć oraz materiałów:** przeglądarka internetowa, Zoom w wersji bezpłatnej dla użytkownika
- Uczestnicy otrzymują linki do spotkań przed każdymi zajęciami. Link umożliwiający uczestnictwo w kursie jest aktywny w godzinach wskazanych na karcie usługi

Kontakt

Kacper Pajerski

E-mail k.pajerski@codebrainers.pl

Telefon (+48) 575 202 507