



Szkolenie dla Pracowników i Pracodawców : Cyberbezpieczeństwo - ochrona informacji, rozpoznawanie zagrożeń i reagowanie na incydent

Numer usługi 2026/06/05/192372/3609322

8 118,00 PLN brutto
6 600,00 PLN netto
202,95 PLN brutto/h
165,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

ERNABO
SOFTWARE SPÓŁKA
Z OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,6 / 5

27 ocen

- 📄 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 📄 Zajęcia grupowe
- 🕒 40:00 h
- 📅 19.10.2026 do 24.11.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Grupa docelowa:

Szkolenie skierowane jest do pracowników oraz pracodawców wszystkich branż i sektorów, w szczególności osób korzystających w pracy z systemów informatycznych, poczty elektronicznej i danych firmowych. Adresatami są zarówno pracownicy biurowi i administracyjni, jak i kadra zarządzająca, którzy w ramach swoich obowiązków odpowiadają za bezpieczeństwo informacji, właściwe reagowanie na zagrożenia cyberbezpieczeństwa oraz przestrzeganie procedur ochrony danych w organizacji.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

16

Data zakończenia rekrutacji

14-10-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

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

Usługa potwierdza przygotowanie uczestników do rozpoznawania zagrożeń cyberbezpieczeństwa w pracy oraz stosowania podstawowych zasad ochrony informacji. Uczestnicy uczą się identyfikować i klasyfikować aktywa, analizować ryzyko, rozróżniać techniki Zero Trust i MFA, interpretować podatności oraz alerty bezpieczeństwa, a także stosować procedury reagowania na incydenty i współpracować z działem IT w zakresie bezpieczeństwa informacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia techniki zero trust oraz zasady uwierzytelniania wieloskładnikowego w organizacji	Wymienia co najmniej trzy elementy modelu zero trust	Test teoretyczny
	Wyjaśnia znaczenie wieloskładnikowego uwierzytelniania w bezpieczeństwie systemów	Test teoretyczny
Charakteryzuje zagrożenia bezpieczeństwa w łańcuchu dostaw oraz metody ich weryfikacji Wyjaśnia procesy zarządzania ryzykiem cyberbezpieczeństwa oraz etapy identyfikacji aktywów	Opisuje procesy ataku poprzez łańcuch dostaw oprogramowania	Test teoretyczny
	Wyjaśnia znaczenie weryfikacji integralności kodu i dostawców	Test teoretyczny
	Wymienia kluczowe kroki procesu zarządzania ryzykiem	Test teoretyczny
	Opisuje metodę klasyfikacji aktywów w organizacji	Test teoretyczny
Klasyfikuje typy zaawansowanych zagrożeń i metody ich wykrywania w systemach IT	Definiuje cztery typy zagrożeń APT i insider threat	Test teoretyczny
	Wyjaśnia różnicę między tradycyjnym antywirus a analizą behawioralną	Test teoretyczny
Przeprowadza identyfikację oraz priorytetyzację podatności w systemach organizacyjnych	Prawidłowo skanuje sieci pod kątem podatności systemów	Analiza dowodów i deklaracji
	Kategoryzuje znalezione podatności według poziomu zagrożenia	Test teoretyczny
Wdraża procedury reagowania na incydenty typu DDoS z użyciem filtrowania ruchu	Implementuje systemy anti-DDoS filtrujące ruch sieciowy	Analiza dowodów i deklaracji
	Weryfikuje skuteczność wdrożonych procedur reagowania na ataki	Analiza dowodów i deklaracji
Konfiguruje systemy SIEM do monitorowania zdarzeń bezpieczeństwa w organizacji	Określa krytyczne przypadki użycia dla systemu SIEM	Test teoretyczny
	Konfiguruje korelacje zdarzeń i alerty w oparciu o analizę ryzyka	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Organizuje stanowisko pracy zgodnie z zasadami bezpieczeństwa informacji oraz ergonomii Komunikuje zalecenia bezpieczeństwa pracownikom organizacji w zrozumiałym sposobie	Dostosowuje środowisko pracy do wymogów bezpieczeństwa danych	Analiza dowodów i deklaracji
	Wdraża procedury kontroli dostępu do systemów informatycznych	Analiza dowodów i deklaracji
	Wyjaśnia znaczenie szkoleń bezpieczeństwa dla wszystkich pracowników	Test teoretyczny
	Dostosowuje komunikację do poziomu wiedzy technicznej odbiorcy	Test teoretyczny
Współpracuje z zespołami IT w celu wdrażania strategii cyberbezpieczeństwa	Planuje spotkania zespołowe dotyczące incydentów bezpieczeństwa	Analiza dowodów i deklaracji
	Koordynuje działania między różnymi departamentami organizacji	Analiza dowodów i deklaracji
Wykazuje odpowiedzialność zawodową w podejmowaniu decyzji dotyczących bezpieczeństwa Zarządza czasem pracy przy realizacji złożonych zadań bezpieczeństwa systemów	Dokumentuje wszystkie decyzje związane z incydentami bezpieczeństwa	Analiza dowodów i deklaracji
	Stosuje etyczne zasady przy dostępie do danych wrażliwych	Analiza dowodów i deklaracji
	Planuje i realizuje projekty bezpieczeństwa według harmonogramu	Analiza dowodów i deklaracji
	Priorytetyzuje zadania w zależności od poziomu zagrożenia bezpieczeństwa	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://icvc.eu/kwalifikacje-icvc/#rejestr>

Strona internetowa Instytucji Walidującej: <https://standardgccs.com/>

Informacje

Program

Program szkolenia jest dostosowany do potrzeb uczestników usługi oraz głównego celu usługi i jej charakteru oraz obejmuje zakres tematyczny usługi. Uczestnik nie musi spełniać dodatkowych wymagań dot. poziomu zaawansowania.

Informacje organizacyjne:

Usługa prowadzona jest w **godzinach zegarowych**. Przerwy są **wliczone** w ogólny czas usługi rozwojowej.

Widelki przerw, uzależnione od długości zajęć:

- dzień szkoleniowy od 2 godzin do poniżej 4 godzin 30 minut – przerwa od 15 do 30 minut,
- dla dnia szkoleniowego trwającego od 4 godzin 30 minut – przerwa od 60 do 75 minut.

Dostawca deklaruje, iż dzień szkoleniowy nie będzie dłuższy aniżeli 7 godzin zegarowych aby zapewnić Pracodawcom możliwość delegowania pracowników ze szczególnymi potrzebami.

Harmonogram usługi może ulec **nieznacznemu przesunięciu**, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Dostawca zapewnia **elastyczność w mikro-zarządzaniu czasem przerw w trakcie realizacji** ale jednocześnie **utrzymuje zadeklarowany czas zajęć i nie przekracza łącznej długości przerw**.

Usługa jest zgodna z definicją cyfrowych kompetencji i kwalifikacji, a program szkolenia ma charakter praktyczny i uniwersalny, dzięki czemu zdobyta wiedza może być wykorzystywana przez pracowników różnych działów i stanowisk – administracyjnych, biurowych, operacyjnych, usługowych, logistycznych oraz menedżerskich. Uczestnicy rozwijają umiejętności bezpiecznego i świadomego korzystania z technologii cyfrowych w środowisku pracy, w tym systemów informatycznych, poczty elektronicznej oraz narzędzi do przetwarzania danych.

Szkolenie wspiera rozwój kompetencji cyfrowych w zakresie rozpoznawania zagrożeń cyberbezpieczeństwa, ochrony informacji, stosowania zasad bezpiecznej pracy w środowisku cyfrowym oraz właściwego reagowania na incydenty bezpieczeństwa. Uczestnicy poznają również podstawy działania nowoczesnych mechanizmów ochrony systemów informatycznych oraz zasady współpracy z działami IT w zakresie bezpieczeństwa cyfrowego.

Informacje o programie szkolenia:

Program szkolenia stanowi spójny i zintegrowany zakres treści objęty jednolitym procesem walidacji prowadzącym do uzyskania kwalifikacji. Efekty uczenia się oraz kryteria weryfikacji pochodzą bezpośrednio od instytucji walidującej i certyfikującej, co zapewnia maksymalną zgodność z wymaganiami kwalifikacji, wysoką jakość procesu kształcenia oraz jego przejrzystość i wiarygodność w odniesieniu do obowiązujących standardów.

MODUŁ 1. Podstawy cyberbezpieczeństwa

Czas: 6 godziny (3 godz. teoria, 1 godz. praktyka)

Moduł wprowadza uczestników w podstawowe zagadnienia cyberbezpieczeństwa występujące w codziennej pracy. Uczestnicy poznają najczęstsze zagrożenia dla organizacji oraz zasady bezpiecznego korzystania z komputerów, poczty elektronicznej i systemów firmowych. Omówione zostaną również podstawowe założenia modelu Zero Trust oraz znaczenie uwierzytelniania wieloskładnikowego.

Zakres tematyczny

- współczesne zagrożenia cyberbezpieczeństwa,
- zasady modelu Zero Trust w organizacji,
- bezpieczne korzystanie z kont użytkowników,
- uwierzytelnianie wieloskładnikowe (MFA),

- tworzenie i zarządzanie hasłami,
- ochrona danych służbowych,
- ćwiczenia z rozpoznawania bezpiecznych i niebezpiecznych zachowań.

MODUŁ 2. Bezpieczna współpraca z dostawcami i korzystanie z oprogramowania

Czas: 3 godziny (2 godz. teoria, 1 godz. praktyka)

Uczestnicy poznają zagrożenia związane z korzystaniem z zewnętrznych usług, aplikacji i dostawców. Moduł rozwija umiejętność oceny wiarygodności źródeł oprogramowania oraz rozpoznawania sytuacji mogących prowadzić do naruszenia bezpieczeństwa organizacji.

Zakres tematyczny

- czym jest łańcuch dostaw w cyberbezpieczeństwie,
- przykłady ataków wykorzystujących dostawców usług,
- bezpieczne pobieranie i aktualizowanie oprogramowania,
- weryfikacja nadawców wiadomości i dostawców usług,
- znaczenie aktualizacji bezpieczeństwa,
- studia przypadków incydentów bezpieczeństwa.

MODUŁ 3. Zarządzanie ryzykiem i ochrona zasobów organizacji

Czas: 3 godziny (2 godz. teoria, 1 godz. praktyka)

Moduł przedstawia podstawowe zasady identyfikacji i ochrony zasobów organizacji. Uczestnicy nauczą się rozpoznawać informacje wymagające szczególnej ochrony oraz właściwie reagować na sytuacje zwiększające ryzyko wystąpienia incydentu bezpieczeństwa.

Zakres tematyczny

- pojęcie aktywów informacyjnych,
- dane poufne i dane wrażliwe,
- klasyfikacja informacji w organizacji,
- identyfikacja ryzyka w codziennej pracy,
- odpowiedzialność pracownika za bezpieczeństwo informacji,
- ćwiczenia z oceny ryzyka w sytuacjach biurowych.

MODUŁ 4. Rozpoznawanie zaawansowanych zagrożeń

Czas: 4 godziny (2 godz. teoria, 2 godz. praktyka)

Moduł ma na celu rozwijanie umiejętności identyfikowania nietypowych zagrożeń występujących w środowisku pracy. Uczestnicy poznają metody działania cyberprzestępców oraz sygnały ostrzegawcze mogące świadczyć o próbie ataku.

Zakres tematyczny

- phishing i spear phishing,
- zagrożenia APT przedstawione w formie przykładów,
- insider threat – zagrożenia ze strony pracowników,
- socjotechnika i manipulacja,
- rozpoznawanie podejrzanych wiadomości,
- ćwiczenia na przykładach rzeczywistych incydentów.

MODUŁ 5. Identyfikacja podatności i bezpieczne użytkowanie systemów

Czas: 5 godzin (2 godz. teoria, 3 godz. praktyka)

Moduł pokazuje, w jaki sposób codzienne działania pracowników mogą wpływać na poziom bezpieczeństwa organizacji. Uczestnicy poznają podstawowe rodzaje podatności występujących w systemach informatycznych, nauczą się rozpoznawać sytuacje zwiększające ryzyko wystąpienia incydentów oraz właściwie reagować na wykryte nieprawidłowości. W części praktycznej uczestnicy będą pracować na przykładowych raportach bezpieczeństwa i analizować poziomy zagrożeń związanych z wykrytymi podatnościami.

Zakres tematyczny

- czym są podatności bezpieczeństwa i jak wpływają na funkcjonowanie organizacji,
- znaczenie aktualizacji systemów i aplikacji,

- bezpieczna konfiguracja stanowiska pracy,
- identyfikowanie nieprawidłowości i potencjalnych zagrożeń,
- procedury zgłaszania problemów bezpieczeństwa,
- prezentacja działania narzędzi do skanowania podatności,
- analiza przykładowych raportów ze skanowania bezpieczeństwa,
- klasyfikacja podatności według poziomu zagrożenia,
- określanie priorytetów działań naprawczych.

MODUŁ 6. Reagowanie na incydenty bezpieczeństwa

Czas: 3 godziny (1 godz. teoria, 3 godz. praktyka)

Moduł przygotowuje uczestników do właściwego reagowania na incydenty bezpieczeństwa występujące w organizacji. Uczestnicy poznają procedury postępowania w przypadku wykrycia zagrożenia, zasady współpracy z działem IT oraz podstawowe mechanizmy ochrony stosowane przez organizacje podczas ataków sieciowych, w tym ataków DDoS.

Zakres tematyczny

- rodzaje incydentów bezpieczeństwa,
- procedury zgłaszania incydentów,
- pierwsze działania po wykryciu zagrożenia,
- odpowiedzialność pracownika podczas incydentu,
- komunikacja kryzysowa,
- charakterystyka ataków DDoS,
- przykłady rozwiązań Anti-DDoS stosowanych w organizacjach,
- filtrowanie ruchu sieciowego i jego znaczenie dla ochrony usług,
- analiza skuteczności procedur reagowania na incydenty,
- ćwiczenia scenariuszowe związane z obsługą incydentów bezpieczeństwa.

MODUŁ 7. Monitorowanie bezpieczeństwa i współpraca z działem IT

Czas: 4 godziny (1 godz. teoria, 3 godz. praktyka)

Moduł wyjaśnia rolę monitorowania bezpieczeństwa w organizacji oraz znaczenie współpracy pracowników z zespołami IT i bezpieczeństwa. Uczestnicy poznają podstawowe funkcje systemów monitorowania zdarzeń, przykładowe alerty bezpieczeństwa oraz sposoby zgłaszania niepokojących zdarzeń. W części praktycznej zapoznają się z przykładowymi przypadkami użycia systemów SIEM oraz analizą alertów generowanych przez takie rozwiązania.

Zakres tematyczny

- znaczenie monitorowania bezpieczeństwa w organizacji,
- rola pracownika w procesie wykrywania zagrożeń,
- współpraca z działem IT i zespołami bezpieczeństwa,
- zgłaszanie nieprawidłowości i incydentów,
- podstawy działania systemów SIEM,
- źródła logów bezpieczeństwa,
- przykłady przypadków użycia (Use Cases) w systemach SIEM,
- korelacja zdarzeń bezpieczeństwa,
- analiza przykładowych alertów i poziomów ryzyka,
- ćwiczenia związane z interpretacją zdarzeń bezpieczeństwa.

MODUŁ 8. Bezpieczeństwo informacji i kultura cyberbezpieczeństwa

Czas: 5 godzin 30 minut (3 godz. teoria, 2 godz. 30 min praktyka)

Moduł rozwija kompetencje społeczne związane z bezpieczeństwem informacji. Uczestnicy uczą się skutecznej komunikacji, odpowiedzialnego postępowania z danymi oraz organizacji pracy zgodnej z politykami bezpieczeństwa organizacji.

Zakres tematyczny

- bezpieczeństwo informacji w codziennej pracy,
- ergonomia i bezpieczeństwo stanowiska pracy,
- ochrona danych osobowych i firmowych,
- komunikowanie zagrożeń i dobrych praktyk,
- etyka zawodowa,

- zarządzanie czasem i priorytetami,
- ćwiczenia warsztatowe i studia przypadków.

Walidacja- podmiot zewnętrzny (ICVC) (1 godzina)

Certyfikat: GCCS: SPECJALISTA DS. CYBERBEZPIECZEŃSTWA ICVC/CBB 207771.19

Metody walidacji: test teoretyczny - pisany synchronicznie,

Analiza dowodów i deklaracji.

Okres oczekiwania na wydanie wyniku przeprowadzonej walidacji: Czas oczekiwania na wydanie wyniku przeprowadzonej walidacji wynosi do 7 dni roboczych, licząc od kolejnego dnia roboczego po jej przeprowadzeniu.

Z uwagi na to, data zakończenia usługi została wydłużona.

Harmonogram

Liczba pozycji harmonogramu: 18

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 18 MODUŁ 1. Podstawy cyberbezpieczeństwa/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	19-10-2026	08:00	11:00	03:00
2 z 18 -	Przerwa	-	19-10-2026	11:00	12:00	01:00
3 z 18 kontynuacja MODUŁ 1. Podstawy cyberbezpieczeństwa/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	19-10-2026	12:00	15:00	03:00
4 z 18 MODUŁ 2. Bezpieczna współpraca z dostawcami i korzystanie z oprogramowania/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	22-10-2026	08:00	11:00	03:00
5 z 18 -	Przerwa	-	22-10-2026	11:00	12:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 18 MODUŁ 3. Zarządzanie ryzykiem i ochrona zasobów organizacji/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	22-10-2026	12:00	15:00	03:00
7 z 18 MODUŁ 4. Rozpoznawanie zaawansowanych zagrożeń/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	26-10-2026	08:00	12:00	04:00
8 z 18 -	Przerwa	-	26-10-2026	12:00	13:00	01:00
9 z 18 MODUŁ 5. Identyfikacja podatności i bezpieczne użytkowanie systemów/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	26-10-2026	13:00	15:00	02:00
10 z 18 MODUŁ 5. Identyfikacja podatności i bezpieczne użytkowanie systemów/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	28-10-2026	08:00	11:00	03:00
11 z 18 -	Przerwa	-	28-10-2026	11:00	12:00	01:00
12 z 18 MODUŁ 6. Reagowanie na incydenty bezpieczeństwa/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	28-10-2026	12:00	15:00	03:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 18 MODUŁ 7. Monitorowanie bezpieczeństwa i współpraca z działem IT/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	17-11-2026	08:00	12:00	04:00
14 z 18 -	Przerwa	-	17-11-2026	12:00	13:00	01:00
15 z 18 MODUŁ 8. Bezpieczeństwo informacji i kultura cyberbezpieczeństwa/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	17-11-2026	13:00	14:30	01:30
16 z 18 MODUŁ 8. Bezpieczeństwo informacji i kultura cyberbezpieczeństwa/ prezentacja, ćwiczenia	Zajęcia	Marcin Rał	18-11-2026	08:00	11:30	03:30
17 z 18 -	Przerwa	-	18-11-2026	11:30	12:30	01:00
18 z 18 -	Walidacja	-	18-11-2026	12:30	13:30	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	40:00
w tym suma godzin zajęć	33:00
w tym suma godzin walidacji	01:00
w tym suma przerw	06:00
Suma godzin dydaktycznych bez przerw	45:15

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 z zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 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	8 118,00 PLN
Koszt przypadający na 1 uczestnika netto	6 600,00 PLN
Koszt osobogodziny brutto	202,95 PLN
Koszt osobogodziny netto	165,00 PLN
W tym koszt walidacji brutto	180,00 PLN
W tym koszt walidacji netto	146,34 PLN
W tym koszt certyfikowania brutto	70,00 PLN
W tym koszt certyfikowania netto	56,91 PLN

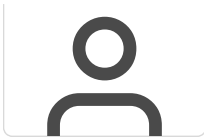
Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

Prowadzący

Liczba prowadzących: 1





Marcin Rał

Trener posiada praktyczną wiedzę w zakresie rozpoznawania zagrożeń cybernetycznych, ochrony danych, podstaw zarządzania ryzykiem oraz zasad bezpiecznego korzystania z systemów informatycznych w pracy biurowej i administracyjnej.

W latach 2024-2025 przeprowadził ponad 200 godzin praktyki szkoleniowej m.in dla pracowników Oświaty czy Instytucji publicznych, Urzędów czy prywatnych przedsiębiorstw.

W swojej praktyce szkoleniowej specjalizuje się w prowadzeniu zajęć dla pracowników różnych branż i poziomów stanowisk, w tym kadry zarządzającej oraz pracowników operacyjnych, dostosowując przekaz do poziomu wiedzy uczestników. Posiada doświadczenie w realizacji szkoleń z zakresu kompetencji cyfrowych, bezpieczeństwa IT oraz świadomości zagrożeń w środowisku pracy.

Trener łączy wiedzę teoretyczną z praktycznym podejściem do zagadnień cyberbezpieczeństwa, wykorzystując przykłady z rzeczywistych incydentów, studia przypadków oraz ćwiczenia warsztatowe. Dzięki temu uczestnicy zdobywają umiejętności możliwe do bezpośredniego zastosowania w codziennej pracy

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Prezentacja PDF

Warunki uczestnictwa

Warunkiem zdobycia certyfikatu potwierdzającego zdobyte kwalifikacje jest uzyskanie pozytywnego wyniku Egzaminu certyfikującego.

Na egzamin uczestnik nie musi dokonywać osobnego zapisu oraz jego koszt jest wliczony w koszt usługi.

Minimalny poziom frekwencji uczestnika na usłudze rozwojowej wynosi 80%.

Uczestnicy przyjmują do wiadomości, że usługa może być poddana monitoringowi z ramienia Operatora lub PARP i wyrażają na to zgodę.

Uczestnik ma obowiązek zapisania się na usługę przez BUR co najmniej w dniu zakończenia rekrutacji.

Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027”. W przypadku potrzeby zapewnienia specjalnych udogodnień prosimy o kontakt przed zapisem na usługę!

Informacje dodatkowe

Certyfikat: GCCS: SPECJALISTA DS. CYBERBEZPIECZEŃSTWA ICVC/CBB 207771.19

Podstawa zwolnienia z VAT:

§ 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 dofinansowania w co najmniej 70%

Warunki techniczne

1. Sprzęt uczestnika:

- **komputer lub laptop** z systemem operacyjnym Windows 10 / 11, macOS lub Linux,
- **wolną przestrzeń dyskową** ,
- **stabilne łącze internetowe (min. 10 Mbps)** – w przypadku zajęć zdalnych,
- **aktualna przeglądarka internetowa (Chrome, Edge, Firefox)**,

Obowiązkowe:

- **Kamera:** Uczestnik powinien posiadać działającą kamerę (wbudowaną w laptop/komputer lub zewnętrzną). Kamera umożliwia aktywny udział w sesjach, prezentację ćwiczeń grupowych oraz interakcję z prowadzącym.
- **Mikrofon:** Niezbędny jest sprawny mikrofon (wbudowany lub zewnętrzny, np. w zestawie słuchawkowym). Umożliwia zadawanie pytań, udział w dyskusjach i ćwiczeniach grupowych.
- Zalecane użycie słuchawek z mikrofonem, aby zredukować echo i poprawić jakość dźwięku.

2. Oprogramowanie:

Nie jest wymagane wcześniejsze przygotowanie środowiska. Wszystkie niezbędne programy, dane i narzędzia zostaną przekazane przez trenera w trakcie trwania szkolenia.

3. Łącze internetowe:

- Minimum 10 Mbps download / 5 Mbps upload
- Stabilne połączenie bez dużych przerw i opóźnień

4. Środowisko pracy:

- Ciche miejsce do pracy i nauki
- Dostęp do powierzchni roboczej umożliwiającej komfortowe używanie komputera
- Możliwość dzielenia ekranu w trakcie sesji praktycznych i konsultacji

5. Środowisko szkoleniowe

Szkolenie realizowane jest przez platformę umożliwiającą:

- udostępnianie ekranu,
- czat, komunikację audio-wideo,
- współdzielenie materiałów i plików,
- interaktywną prezentację kodu i analiz danych.

Kontakt



NIKOL WATOŁA

E-mail nikol.watola@ernabo.com

Telefon (+48) 530 642 270