Możliwość dofinansowania

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

Numer usługi 2026/06/30/192372/3659512

4 477,20 PLN brutto
3 640,00 PLN netto
319,80 PLN brutto/h
260,00 PLN netto/h
261,33 PLN cena rynkowa

ERNABO SOFTWARE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,2 / 5

58 ocen

Myszków
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
14:00 h
08.12.2026 do 17.12.2026

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	6
Maksymalna liczba uczestników	9
Data zakończenia rekrutacji	04-12-2026
Forma prowadzenia usługi	stacjonarna
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	Opisuje procesy ataku poprzez łańcuch dostaw oprogramowania	Test teoretyczny
	Wyjaśnia znaczenie weryfikacji integralności kodu i dostawców	Test teoretyczny
Wyjaśnia procesy zarządzania ryzykiem cyberbezpieczeństwa oraz etapy identyfikacji aktywów	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	Dostosowuje środowisko pracy do wymogów bezpieczeństwa danych	Analiza dowodów i deklaracji
	Wdraża procedury kontroli dostępu do systemów informatycznych	Analiza dowodów i deklaracji
Komunikuje zalecenia bezpieczeństwa pracownikom organizacji w zrozumiały sposób	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	Dokumentuje wszystkie decyzje związane z incydentami bezpieczeństwa	Analiza dowodów i deklaracji
	Stosuje etyczne zasady przy dostępie do danych wrażliwych	Analiza dowodów i deklaracji
Zarządza czasem pracy przy realizacji złożonych zadań bezpieczeństwa systemów	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://standardgccs.com/

Strona internetowa Instytucji Walidującej: https://icvc.eu/kwalifikacje-icvc/#rejestr

Informacje

Nazwa Podmiotu prowadzącego walidację	ICVC Certyfikacja Sp. z o.o.

Nazwa Podmiotu certyfikującego	Talent Odyssey Ltd,

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 w formie zdalnej w czasie rzeczywistym na platformie ClickMeeting.** Przerwy oraz walidacja **są wliczone** w ogólny czas usługi rozwojowej.

Widełki 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 I. Zero Trust i zarządzanie tożsamością użytkowników

Liczba godzin: 3 godziny (1 godzina teorii / 2 godziny praktyki)

Celem modułu jest zdobycie wiedzy i praktycznych umiejętności w zakresie wdrażania modelu Zero Trust oraz skutecznego zarządzania dostępem do zasobów organizacji. Uczestnicy poznają nowoczesne metody uwierzytelniania użytkowników, mechanizmy kontroli dostępu oraz zasady ochrony tożsamości cyfrowej. W części praktycznej skonfigurują mechanizmy wieloskładnikowego uwierzytelniania oraz przeanalizują przykładowe scenariusze ograniczania ryzyka nieautoryzowanego dostępu.

Zakres

- aktualne zagrożenia cyberbezpieczeństwa,
- model Zero Trust i jego filary,
- zasada najmniejszych uprawnień (Least Privilege),
- zarządzanie tożsamością użytkowników (IAM),
- uwierzytelnianie wieloskładnikowe (MFA),
- kontrola dostępu do systemów i danych,
- praktyczna konfiguracja mechanizmów uwierzytelniania.

Moduł II. Zarządzanie ryzykiem oraz bezpieczeństwo łańcucha dostaw

Liczba godzin: 3 godziny 30 minut (1,5 godziny teorii / 2 godziny praktyki)

Moduł poświęcony jest identyfikacji zagrożeń związanych z łańcuchem dostaw oprogramowania oraz metodom zarządzania ryzykiem cyberbezpieczeństwa. Uczestnicy nauczą się identyfikować aktywa organizacji, klasyfikować ryzyko oraz oceniać bezpieczeństwo dostawców i wykorzystywanego oprogramowania. Praktyczne ćwiczenia obejmują analizę ryzyka oraz ocenę podatności środowiska informatycznego.

Zakres

- bezpieczeństwo łańcucha dostaw (Supply Chain Security),
- ataki na dostawców usług i oprogramowania,
- weryfikacja integralności oprogramowania,
- identyfikacja i klasyfikacja aktywów,
- zarządzanie ryzykiem cyberbezpieczeństwa,
- analiza podatności infrastruktury,
- opracowanie planu ograniczania ryzyka.

Moduł III. Wykrywanie zagrożeń i monitorowanie bezpieczeństwa

Liczba godzin: 2 godziny 30 minut (1 godzina teorii / 1,5 godziny praktyki)

Celem modułu jest rozwój kompetencji związanych z wykrywaniem nowoczesnych zagrożeń oraz monitorowaniem infrastruktury informatycznej. Uczestnicy poznają działanie systemów SIEM, metody analizy logów, mechanizmy korelacji zdarzeń oraz sposoby identyfikacji zaawansowanych zagrożeń. W części praktycznej skonfigurują podstawowe reguły monitorowania i analizę incydentów.

Zakres

- zagrożenia APT i Insider Threat,
- analiza behawioralna zagrożeń,
- EDR/XDR i nowoczesna ochrona punktów końcowych,
- identyfikacja podatności systemów,
- podstawy działania systemów SIEM,
- analiza logów bezpieczeństwa,
- konfiguracja reguł korelacji i alertów.

Moduł IV. Reagowanie na incydenty oraz organizacja bezpieczeństwa informacji

Liczba godzin: 2 godziny 30 minut(1 godzina teorii / 1,5 godziny praktyki)

Moduł obejmuje przygotowanie uczestników do skutecznego reagowania na incydenty bezpieczeństwa oraz organizowania pracy zgodnie z zasadami ochrony informacji. Uczestnicy poznają procedury reagowania na ataki DDoS, dokumentowania incydentów, współpracy z zespołami IT oraz komunikowania zaleceń bezpieczeństwa. Ćwiczenia praktyczne obejmują analizę scenariuszy incydentów oraz opracowanie procedur postępowania.

Zakres

- proces reagowania na incydenty,
- procedury postępowania podczas ataków DDoS,
- filtrowanie ruchu sieciowego,
- dokumentowanie incydentów bezpieczeństwa,
- organizacja bezpiecznego stanowiska pracy,
- ochrona informacji i kontrola dostępu,
- współpraca zespołów IT podczas incydentów,
- komunikacja w zakresie cyberbezpieczeństwa,
- zarządzanie czasem i priorytetyzacja działań związanych z bezpieczeństwem.

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, licząc od kolejnego dnia roboczego po jej przeprowadzeniu.

Z uwagi na to, data zakończenia usługi została wydłużona.

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Moduł I. Zero Trust i zarządzanie tożsamością użytkowników	Zajęcia	Marcin Rał	08-12-2026	06:30	09:30	03:00
2 z 8 -	Przerwa	-	08-12-2026	09:30	10:30	01:00
3 z 8 Moduł II. Zarządzanie ryzykiem oraz bezpieczeństwo łańcucha dostaw	Zajęcia	Marcin Rał	08-12-2026	10:30	13:30	03:00
4 z 8 Moduł III. Wykrywanie zagrożeń i monitorowanie bezpieczeństwa	Zajęcia	Marcin Rał	09-12-2026	06:30	09:00	02:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 8 -	Przerwa	-	09-12-2026	09:00	09:30	00:30
6 z 8 Moduł IV. Reagowanie na incydenty oraz organizacja bezpieczeństwa informacji	Zajęcia	Marcin Rał	09-12-2026	09:30	12:00	02:30
7 z 8 -	Przerwa	-	09-12-2026	12:00	12:30	00:30
8 z 8 -	Walidacja	-	09-12-2026	12:30	13:30	01:00

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 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	4 477,20 PLN

Koszt przypadający na 1 uczestnika netto	3 640,00 PLN
Koszt osobogodziny brutto	319,80 PLN
Koszt osobogodziny netto	260,00 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	14:00

Prowadzący

Liczba prowadzących: 1

1 z 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 w formie PDF (przekazana najpóźniej w dniu rozpoczęcia szkolenia drogą e-mailową).

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 lipca2019 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%

Adres

ul. Kościuszki 8
42-300 Myszków
woj. śląskie

Oddział Magot, wjazd od strony Marketu Chińskiego

Kontakt

NIKOL WATOŁA

E-mail nikol.watola@ernabo.com
Telefon (+48) 530 642 270