Możliwość dofinansowania

Instalacje ekologiczne a cyberbezpieczeństwo – wprowadzenie i dobre praktyki

Numer usługi 2025/12/30/199110/3232476

5 000,00 PLN brutto
5 000,00 PLN netto
312,50 PLN brutto/h
312,50 PLN netto/h

GAWOS SZKOLENIA I DORADZTWO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Wisła / stacjonarna
Usługa szkoleniowa
16 h
07.02.2026 do 08.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Grupą docelową szkolenia są: - pasjonaci ekologii i świadomego prowadzenia firm wyposażonych w instalacje ekologiczne - osoby chcące poznać zasady prawidłowego zabezpieczania urządzeń i systemów, które są wykorzystywane w instalacjach wytwarzających energię elektryczną, produkujących biogaz, zapewniających odprowadzanie ścieków bytowych, stacji uzdatniania wody - osoby zajmujące się utrzymaniem systemów monitorowania i wizualizacji, automatyki przemysłowej, - osoby chcące pogłębić wiedzę z zakresu cyberbezpieczeństwa
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	06-02-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
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 samodzielnego korzystania i wdrażania zasad cyberbezpieczeństwa dla instalacji ekologicznych. Uczestnik rozpoznaje typy zagrożeń, analizy sieci komunikacyjnych i przemysłowych, określania słabych punktów sieci a także wykonania analizy ryzyka sieci. Jest świadomy zagrożeń dla środowiska w przypadku ingerencji w układy zdalnego sterowania i potrafi wdrożyć zasady cyberbezpieczeństwa ze szczególnym uwzględnieniem minimalizacji start środowiskowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
rozróżnia podstawowe pojęcia bezpieczeństwa sieci przemysłowych oraz obowiązujące normy i skutki incydentów bezpieczeństwa.	wymienia definicje pojęć, normy oraz określa skutki incydentów	Test teoretyczny
rozpoznaje zagrożenia sieci przemysłowych oraz podstawowe metody diagnostyki.	klasyfikuje zagrożenia do sytuacji oraz wybiera właściwe metody diagnostyczne	Test teoretyczny
analizuje strukturę sieci przemysłowej i IoT oraz rolę jej elementów.	analizuje schemat sieci i wylicza jej kluczowe elementy	Test teoretyczny
rozróżnia zasady analizy dokumentacji technicznej sieci.	analizuje dokumentację i wymienia potencjalne zagrożenia bezpieczeństwa.	Test teoretyczny
wymienia metody analizy ryzyka sieci przemysłowej	określa analizę ryzyka oraz poziom ryzyka.	Test teoretyczny
wylicza zasady projektowania bezpiecznych sieci przemysłowych.	omawia projekt sieci zgodny z dobrymi praktykami	Test teoretyczny
analizuje projekty innych uczestników pod kątem zgodności z założeniami i celam	trafnie i spójnie analizuje projekty, ocenia projekty innych uczestników według ustalonych kryteriów identyfikuje obszary wymagające poprawy i projektuje usprawnienia	Wywiad swobodny
analizuje wyniki prac, definiuje wnioski, identyfikuje obszary wymagające poprawy oraz określa działania usprawniające wynikające z przeprowadzonej analizy projektów	analizuje i wyjaśnia wyniki w sposób logiczny i spójny, dobiera adekwatne działania usprawniające	Wywiad swobodny
wyjaśnia znaczenie cyberbezpieczeństwa w organizacji	wymienia podstawowe zagrożenia cyberbezpieczeństwa w organizacji, omawia przykłady doświadczeń własnych lub innych związanych z cyberbezpieczeństwem	Test teoretyczny

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

Program szkolenia skupia się na :

- identyfikacji zagrożeń bezpieczeństwa w sieciach przemysłowych i sieciach IoT,

- analizie sieci przemysłowych z naciskiem na bezpieczeństwo tych sieci,

- umiejętności identyfikowania potencjalnych zagrożeń na podstawie dokumentacji,

- wykonywania analizy ryzyka i wstępnego określania metod zabezpieczenia sieci,

- realizacji wstępnego projektu sieci przemysłowej zgodnie z zasadami dobrych praktyk

Każdy moduł szkolenia będzie podsumowany testem teoretycznym sprawdzającym wiedzę. Dzień 1: 09:00 – 17:00

1 Moduł: Wprowadzenie do bezpieczeństwa sieci przemysłowych:- definicja bezpieczeństwa- przepisy i normy obowiązujące- przykłady udanych ataków na infrastrukturę sieciową

2 Moduł: Identyfikacja zagrożeń i narzędzia diagnostyczne: - identyfikacja zagrożeń – typy ataków i metody obrony, - dostępne podstawowe narzędzia do diagnostyki sieci

3 Moduł: Analiza struktury sieci przemysłowej i IoT:- ćwiczenia praktyczne – analiza sieci

4 Moduł: Identyfikacja potencjalnych zagrożeń na podstawie struktury sieci i dokumentacji:- ćwiczenia praktyczne – analiza sieci na podstawie dokumentacji i identyfikacji potencjalnych zagrożeń bezpieczeństwa

5 Moduł: Analiza ryzyka sieci przemysłowej: - ćwiczenia praktyczne Dzień 2: 9:00-17:00

6 Moduł: Wykonanie projektu sieci przemysłowej w organizacji z uwzględnieniem dobrych praktyk:- ćwiczenia praktyczne

7 Moduł: Analiza projektów uczestników:-praca warsztatowa polegająca na wzajemnej analizie wykonanych projektów przez uczestników

8 Moduł: Omówienie wyników prac

9 Moduł: Dyskusja grupowa na temat doświadczeń uczestników w zakresie cyberbezpieczeństwa

10 Moduł: Podsumowanie szkolenia

11 Moduł: Walidacja

WALIDACJA EFEKTÓW UCZENIA SIĘ

W ramach szkolenia, w drugim dniu, zostanie przeprowadzona walidacja osiągniętych efektów uczenia się. Walidacja jest wliczona w czas trwania szkolenia i obejmuje test wiedzy teoretycznej sprawdzający znajomość samodzielnego korzystania i wdrażania zasad cyberbezpieczeństwa dla instalacji ekologicznych.

Walidacja efektów uczenia się została zaplanowana do przeprowadzenia przez walidatora zewnętrznego, w miejscu realizacji usługi rozwojowej, zgodnie ze Standardami Usług Rozwojowych.

Walidacja obejmuje dwa etapy:

1. Test teoretyczny

W godzinach od 15:15 do 16:00 przeprowadzony zostanie test teoretyczny w formie pisemnej. Test będzie składał się z 20 pytań.Odpowiedzi będą udzielane w formie pisemnej. Ocena testu zostanie dokonana przez walidatora zewnętrznego na podstawie wcześniej opracowanego klucza odpowiedzi. Test służy weryfikacji wiedzy nabytej przez uczestników w trakcie realizacji usługi rozwojowej.

2. Wywiad swobodny

W godzinach od 16:00 do 17:00 przeprowadzony zostanie wywiad swobodny realizowany w grupie z każdym uczestnikiem usługi rozwojowej. Wywiad ma na celu potwierdzenie osiągnięcia efektów uczenia się w zakresie umiejętności, w szczególności: analizy projektów, oceny projektów innych uczestników według ustalonych kryteriów, identyfikowania obszarów wymagających poprawy oraz proponowania usprawnień.

Pytania zadawane w trakcie wywiadu mają charakter otwarty. Nie stosuje się wcześniej przygotowanej listy pytań ani narzuconej kolejności ich zadawania. W razie potrzeby walidator zewnętrzny zadaje pytania uzupełniające. Każdy uczestnik odpowiada na dwa pytania**.**

Wręczenie certyfikatów uczestnictwa.

Czas trwania szkolenia: 16 godzin zegarowych.

Szkolenie dzieli się na część praktyczną 12h i część teoretyczną 4h

Przerwy wliczone w czas trwania usługi W trakcie szkolenia będą krótsze przerwy w zależności od kondycji uczestników.

Zielone umiejętności i kompetencje zawarte w kursie:

- Świadomość i szacunek dla środowiska,
- Umiejętności pracy zespołowej odzwierciedlające potrzebę wspólnej pracy wewnątrz organizacji nad poszukiwaniem rozwiązań ograniczających wpływ cyberzagrożeń dla środowiska poprzez ingerencję w systemy sterowania i monitorowania
- Budowa zabezpieczeń systemów monitorujących z uwzględnieniem ich wpływu na środowisko
- Digitalizacja dokumentów i procesów co redukuje zużycie papierów i energii
- Minimalizowanie ryzyka negatywnego wpływu działania instalacji ekologicznych na środowisko w przypadku ingerencji osób nie powołanych,
- Planowanie oparte na logicznym myśleniu, analizowanie efektywności pracowniczej, przygotowywanie raportów

TEMATYKA SZKOLENIA JEST ZGODNA Z PROGRAMEM REGIONALNYM TECHNOLOGII NA LATA 2019 -2030 W OBSZARZE TECHNOLOGIE TELEKOMUNIKACYJNE I INFORMACYJNE, OBSZAR 4.1 TECHNOLOGIE TELEKOMUNIKACYJNE

Treści szkoleniowe pozostają w spójności z zielonymi kompetencjami wskazanymi przez Komisję Europejską w bazie ESCO

Uczestnicy rozwijają m.in. umiejętności: analitycznego myślenia, świadomość wpływu zagrożeń cyfrowych na instalacje ekologiczne, włączania narzędzi cyfrowych w procesy usprawniające zarządzanie i zabezpieczanie instalacji ekologicznych, wspierania odpowiedzialnej transformacji cyfrowo-ekologicznej, przystosowywania swoich działań do potrzeb rynku pracy w kontekście zielonej i cyfrowej zmiany.

Harmonogram

Liczba przedmiotów/zajęć: 22

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 22 Rejestracja i powitanie uczestników	Artur Dylong	07-02-2026	09:00	09:45	00:45
2 z 22 Wprowadzenie co to jest cyberbezpioeczeństwo, definicje	Artur Dylong	07-02-2026	09:45	10:30	00:45
3 z 22 Przepisy i normy obowiązujące	Artur Dylong	07-02-2026	10:30	11:15	00:45
4 z 22 Identyfikacja zagrożeń – typy ataków	Artur Dylong	07-02-2026	11:15	12:00	00:45
5 z 22 Przerwa kawowa	Artur Dylong	07-02-2026	12:00	12:15	00:15
6 z 22 Omówienie narzędzi do diagnostyki sieci przemysłowych	Artur Dylong	07-02-2026	12:15	13:00	00:45
7 z 22 Omówienie dobrych praktyk w zakresie budowy sieci przemysłowych	Artur Dylong	07-02-2026	13:00	14:00	01:00
8 z 22 Przerwa obiadowa	Artur Dylong	07-02-2026	14:00	14:30	00:30
9 z 22 Analiza sieci przemysłowej warsztaty praktyczne	Artur Dylong	07-02-2026	14:30	15:15	00:45
10 z 22 Identyfikacja zagrożeń na podstawie struktury i dokumentacji sieci – warsztaty praktyczne	Artur Dylong	07-02-2026	15:15	16:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 22 Omówienie i podsumowanie pierwszego dnia szkolenia	Artur Dylong	07-02-2026	16:00	17:00	01:00
12 z 22 Powtórzenie wiedzy z dnia pierwszego	Artur Dylong	08-02-2026	09:00	09:45	00:45
13 z 22 Wykonanie analizy ryzyka sieci przemysłowej warsztaty praktyczne część 1	Artur Dylong	08-02-2026	09:45	10:30	00:45
14 z 22 Wykonanie analizy ryzyka sieci przemysłowej warsztaty praktyczne część 2	Artur Dylong	08-02-2026	10:30	11:15	00:45
15 z 22 Wykonanie projektu sieci przemysłowej w organizacji z uwzględnieniem dobrych praktyk	Artur Dylong	08-02-2026	11:15	12:00	00:45
16 z 22 Przerwa kawowa	Artur Dylong	08-02-2026	12:00	12:15	00:15
17 z 22 Wzajemna analiza opracowanych projektów	Artur Dylong	08-02-2026	12:15	13:00	00:45
18 z 22 Dyskusja i omówienie wyników projektu i analizy część 1	Artur Dylong	08-02-2026	13:00	14:00	01:00
19 z 22 Przerwa obiadowa	Artur Dylong	08-02-2026	14:00	14:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 22 Dyskusja i omówienie wyników projektu i analizy część 2	Artur Dylong	08-02-2026	14:30	15:15	00:45
21 z 22 Walidacja - test teoretyczny	-	08-02-2026	15:15	16:00	00:45
22 z 22 Walidacja - wywiad swobodny	-	08-02-2026	16:00	17:00	01:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	312,50 PLN
Koszt osobogodziny netto	312,50 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Artur Dylong

Wieloletni pracownik Instytutu EMAG w Katowicach. Praktyk w zakresie projektowania i wdrażania systemów przemysłowych. Doświadczenie zdobyte w Polsce i za granicą. Autor i współautor artykułów naukowych z zakresu automatyki przemysłowej, systemów gazometrycznych, rozwiązań sieciowych i komunikacyjnych. Obecnie wykładowca Politechniki Śląskiej. Na co dzień zajmuje się zagadnieniami związanymi z bezpieczeństwa sieci przemysłowych wykorzystywanych w systemach automatyki i monitorowania. Od ponad 20 lat prowadzi szkolenia i wykłady dla pracowników zakładów przemysłowych w zakresie systemów monitorowania i automatyki przemysłowej. Autor i współautor systemów monitorowania wykorzystywanych w przemyśle i jednostkach gospodarki komunalnej. Od 5 lat, wykładowca akademicki, prowadzi zajęcia na studiach pierwszego i drugiego stopnia oraz na studiach podyplomowych w zakresie cyberbezpieczeństwa systemów OT

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe:

Warsztaty realizowane są na postawie dostarczonej kursantom dokumentacji sieci przemysłowej w postaci prezentacji multimedialnej i drukowanych materiałów. Materiały drukowane zawierają skrócony opis instalacji ekologicznej, schematy połączeń sieci przemysłowej oraz wymagań funkcjonalnych w stosunku do systemu jako całości. Zadaniem kursantów jest realizacja wymaganych zdań na podstawie w/w materiałów

Warunki uczestnictwa

Warunek ukończenia: obecność na co najmniej 80% zajęć.

Tryb szkolenia: stacjonarny, warsztatowy

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 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%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych

Informacje dodatkowe

Szkolenie zostanie zrealizowane w przypadku zebrania się grupy min. 6 - osobowej.

Aby wziąć udział w szkoleniu należy skontaktować się przed datą zakończenia rekrutacji z organizatorem szkolenia drogą mailową lub telefoniczną.

Treści szkoleniowe pozostają w spójności z zielonymi kompetencjami wskazanymi przez Komisję Europejską w bazie ESCO

Adres

ul. Czarne 3/-
43-460 Wisła
woj. śląskie

Aries Hotel&Spa Wisła

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt

KATARZYNA ANDERKA

E-mail anderka.katarzyna@interia.pl
Telefon (+48) 515 077 796