Możliwość dofinansowania

SOVERANO

SOVERANO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,6 / 5

180 ocen

Bezpieczeństwo Przemysłowe i Ochrona Obiektów Krytycznych – szkolenie.

Numer usługi 2026/08/06/217200/3733528

1 600,00 PLN brutto
1 600,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h
154,44 PLN cena rynkowa

Łódź
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
16:00 h
07.12.2026 do 08.12.2026

Informacje podstawowe

Kategoria	Biznes / Organizacja
Grupa docelowa usługi	Szkolenie skierowane jest do inżynierów automatyki przemysłowej (OT/SCADA), dyrektorów do spraw bezpieczeństwa oraz kadry odpowiedzialnej za zarządzanie ciągłością działania w zakładach energetycznych, a także do dostawców technologii obronnych oraz rozwiązań podwójnego zastosowania (Dual-Use), dążących do spełnienia wymagań dyrektyw NIS2 oraz CER.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	04-12-2026
Forma prowadzenia usługi	stacjonarna
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Usługa prowadzi osobę uczestniczącą do samodzielnego zabezpieczania sieci automatyki przemysłowej przed sabotażem, zapewniania bezpiecznego transferu danych technologicznych oraz wdrażania procedur ciągłości działania zgodnych z dyrektywami NIS2 i CER w obiektach infrastruktury krytycznej.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. Analizuje podatności sieci automatyki przemysłowej oraz sterowników PLC pod kątem podatności na sabotaż i cyfrowe ataki hybrydowe.	Identyfikuje wektory ataku wynikające z podłączenia nieautoryzowanych nośników pamięci do magistrali OT.	Test teoretyczny z wynikiem generowanym automatycznie
	Klasyfikuje wymogi dyrektyw NIS2 i CER w odniesieniu do zabezpieczenia obiektów infrastruktury krytycznej.	Test teoretyczny z wynikiem generowanym automatycznie
2. Konfiguruje sprzętowe mechanizmy izolacji oraz ochrony transmisji danych w systemach SCADA i urządzeniach diagnostycznych.	Przeprowadza instalację blokad przesyłu danych USB oraz ekranowania elektromagnetycznego modemów transmisyjnych przy użyciu pokrowca ochronnego.	Test teoretyczny z wynikiem generowanym automatycznie
3. Projektuje procedury przywracania retencji kodu oraz awaryjnego sterowania infrastrukturą przemysłową w warunkach blokady systemów dostępowych.	Przeprowadza wgrywanie bezpiecznego oprogramowania układowego z szyfrowanego nośnika pamięci z klawiaturą PIN.	Test teoretyczny z wynikiem generowanym automatycznie
	Formułuje algorytm przywracania sygnału telemetrycznego sterowników PLC po wystąpieniu incydentu bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
4. Wdraża procedury bezpiecznego transferu danych technologicznych oraz zarządzania ciągłością działania w zakładach przemysłowych i energetycznych.	Opracowuje taktyczny rejestr decyzji operacyjnych w formie dokumentacji analogowej na wypadek awarii sieci cyfrowych.	Test teoretyczny z wynikiem generowanym automatycznie
	Stosuje sprzętowe klucze bezpieczeństwa w procesie uwierzytelniania dostępu do węzłów sieci OT.	Test teoretyczny z wynikiem generowanym automatycznie
	Ocenia poziom odporności fizycznej i cyfrowej obiektu krytycznego w oparciu o zestaw wytycznych prawnych i technicznych.	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

WARUNKI ORGANIZACYJNE:

- Forma usługi: Stacjonarna.
- Czas trwania usługi: 16 godzin zegarowych (60 min). Przerwy wliczane są w czas trwania całej usługi.
- Klauzula Dostępności: W oparciu o zasadę racjonalnych usprawnień i dostępności (wynikającą z Ustawy o dostępności) orazstandardy równego traktowania, organizator zapewnia wsparcie dla osób ze szczególnymi potrzebami. W celu skorzystania zracjonalnych usprawnień, uczestnik proszony jest o wcześniejsze zgłoszenie swoich potrzeb organizatorowi szkolenia.
- Walidacja przeprowadzana jest w formie testu teoretycznego generowanego wynikiem automatycznym. W celu zapewnieniaobiektywności oceny, proces walidacji jest prowadzony zgodnie z zasadą rozdzielności procesów kształcenia i walidacji.
- Typy zajęć: [T] Teoretyczne: Wykłady, prezentacje, analiza koncepcji. [P] Praktyczne: Ćwiczenia, zadania, praca z narzędziami podokiem trenera. [M] Mieszane: Łączą wprowadzenie teoretyczne z zadaniami praktycznymi.

PROGRAM SZKOLENIA

Program szkolenia skonstruowany jest wokół praktycznych wyzwań związanych z wdrażaniem europejskich wymogów prawnych NIS2 i CER oraz zabezpieczaniem infrastruktury krytycznej przed zaawansowanymi atakami hybrydowymi i sabotażem. Osoba uczestnicząca przechodzi przez złożony cykl dydaktyczny, podczas którego poddaje szczegółowej analizie realistyczny scenariusz zainfekowania urządzeń diagnostycznych oraz przerwania sygnałów telemetrycznych w sterownikach PLC elektrociepłowni i zakładów zbrojeniowych. W ramach bloku warsztatowego kadra inżynieryjna oraz zarządzająca ćwiczy techniki fizycznej izolacji hardware'owej, wykorzystując blokady przesyłu danych oraz pokrowce ekranujące przed impulsami elektromagnetycznymi i geolokalizacją. Zajęcia obejmują również procedury bezpiecznej retencji kodu, wgrywanie czystego oprogramowania układowego z szyfrowanych nośników pamięci oraz tworzenie analogowych rejestrów decyzyjnych w warunkach całkowitego zablokowania cyfrowych systemów kontroli dostępu.

HARMONOGRAM SZCZEGÓŁOWY

Dzień 1 (07.12.2026 r.)

- **08:00 – 10:00** Scenariusz kryzysowy: sabotaż SCADA, incydent w sieci OT i wymogi dyrektyw NIS2/CER [M/T] – Osoba prowadząca: David Michel
- **10:00 – 10:15** Przerwa
- **10:15 – 12:15** Hardware'owa izolacja urządzeń, stosowanie blokad USB oraz pokrowców ekranujących [P] – Osoba prowadząca: David Michel
- **12:15 – 12:45** Przerwa
- **12:45 – 14:30** Procedury retencji kodu i wgrywanie oprogramowania układowego ze szyfrowanych nośników [P] – Osoba prowadząca: David Michel
- **14:30 – 14:45** Przerwa
- **14:45 – 16:00** Zabezpieczanie sterowników PLC i przywracanie sygnałów telemetrycznych w zakładzie [P] – Osoba prowadząca: David Michel

Dzień 2 (08.12.2026 r.)

- **08:00 – 10:00** Ochrona obiektów krytycznych i transferu danych technologicznych Dual-Use [M/P] – Osoba prowadząca: David Michel
- **10:00 – 10:15** Przerwa
- **10:15 – 12:15** Ćwiczenia symulacyjne: reakcja na zablokowanie cyfrowych systemów kontroli dostępu [P] – Osoba prowadząca: David Michel
- **12:15 – 12:45** Przerwa

- **12:45 – 14:30** Zarządzanie ciągłością działania oraz tworzenie taktycznych rejestrów decyzji [P] – Osoba prowadząca: David Michel
- **14:30 – 14:45** Przerwa
- **14:45 – 15:45** Konfiguracja sprzętowych kluczy bezpieczeństwa dla sieci przemysłowych [P] – Osoba prowadząca: David Michel
- **15:45 – 16:00** Walidacja efektów uczenia się (Test wiedzy pod nadzorem) [T] – Osoba wykonująca walidację: Mateusz Świąder

Harmonogram

Liczba pozycji harmonogramu: 15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Scenariusz kryzysowy: sabotaż SCADA, incydent w sieci OT i wymogi dyrektyw NIS2/CER	Zajęcia	David Michel	07-12-2026	08:00	10:00	02:00
2 z 15 -	Przerwa	-	07-12-2026	10:00	10:15	00:15
3 z 15 Hardware'owa izolacja urządzeń, stosowanie blokad USB oraz pokrowców ekranujących	Zajęcia	David Michel	07-12-2026	10:15	12:15	02:00
4 z 15 -	Przerwa	-	07-12-2026	12:15	12:45	00:30
5 z 15 Procedury retencji kodu i wgrywanie oprogramowania układowego ze szyfrowanych nośników	Zajęcia	David Michel	07-12-2026	12:45	14:30	01:45
6 z 15 -	Przerwa	-	07-12-2026	14:30	14:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 15 Zabezpieczanie sterowników PLC i przywracanie sygnałów telemetrycznych w zakładzie	Zajęcia	David Michel	07-12-2026	14:45	16:00	01:15
8 z 15 Ochrona obiektów krytycznych i transferu danych technologicznych Dual-Use	Zajęcia	David Michel	08-12-2026	08:00	10:00	02:00
9 z 15 -	Przerwa	-	08-12-2026	10:00	10:15	00:15
10 z 15 Ćwiczenia symulacyjne: reakcja na zablokowanie cyfrowych systemów kontroli dostępu	Zajęcia	David Michel	08-12-2026	10:15	12:15	02:00
11 z 15 -	Przerwa	-	08-12-2026	12:15	12:45	00:30
12 z 15 Zarządzanie ciągłością działania oraz tworzenie taktycznych rejestrów decyzji	Zajęcia	David Michel	08-12-2026	12:45	14:30	01:45
13 z 15 -	Przerwa	-	08-12-2026	14:30	14:45	00:15
14 z 15 Konfiguracja sprzętowych kluczy bezpieczeństwa dla sieci przemysłowych	Zajęcia	David Michel	08-12-2026	14:45	15:45	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 15 -	Walidacja	-	08-12-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:45
w tym suma godzin walidacji	00:15
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 600,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	1 600,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1

1 z 1

David Michel

David Michel jest dwujęzycznym (PL/DE) ekspertem w zakresie praktycznego zastosowania sztucznej inteligencji w biznesie. Posiada doświadczenie w automatyzacji procesów, integracji narzędzi AI z systemami firmowymi i ocenie kompetencji cyfrowych zespołów. Jego kwalifikacje są potwierdzone aktualnymi certyfikatami, takimi jak "AI Trainer Certificate" (Fraunhofer Institute 2024),"Microsoft Azure AI Fundamentals AI-900" (2024), "AI in Healthcare, Business & Society" (StanfordOnline 2023) oraz "AI for Everyone" (DeepLearning.AI 2023). Regularnie doradza firmom w Polsce i Austrii w zakresie wdrażania rozwiązań opartych na LLM i automatyzacji raportowania. Posiadane przez niego doświadczenie i kwalifikacje zostały nabyte w ciągu ostatnich pięciu lat, co spełnia wymogi BUR.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każda osoba uczestnicząca otrzymuje imienny zestaw wyposażenia technicznego „Sprzęt do Łączności i Ciągłości Działania (BCM)”:

- - Pokrowiec Faradaya na urządzenia mobilne i modemy transmisyjne (ochrona przed impulsami elektromagnetycznymi EMP, lokalizacją i podsłuchem).
  - Hardware’owy klucz bezpieczeństwa (np. YubiKey) do ochrony dostępu do infrastruktury OT/SCADA.
  - Blokada przesyłu danych USB („USB Condom”) do bezpiecznego podłączania urządzeń w strefach chronionych.
  - Cyfrowy pendrive ze szyfrowaniem hardware’owym (z klawiaturą PIN) z Bazą Wdrożeniową dla Przemysłu i Energetyki.
  - Taktyczny, wodoodporny notes (Rite in the Rain) do prowadzenia analogowego rejestru decyzji.
  - Radio awaryjne na korbkę z panelem fotowoltaicznym i funkcją zasilacza przenośnego.
  - Talia Kart Scenariuszowych (Wargaming Operacyjno-Edukacyjny) obejmująca incydenty w obiektach krytycznych.

Warunki uczestnictwa

Aby wziąć udział w szkoleniu, uczestnik powinien być zainteresowany tematem, otwarty na naukę, gotowy do pracy w grupie, posiadać podstawowe umiejętności komunikacyjne. Warunkiem udziału w usłudze jest dokonanie zapisu na usługę co najmniej 1 dzień (do godziny 14.00), przed jej rozpoczęciem i uzyskanie akceptacji ze strony Dostawcy Usługi. Warunkiem uzyskania zaświadczenia/certyfikatu jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz uzyskanie pozytywnej oceny dla każdego uczestnika na podstawie wyniku walidacji przeprowadzonej przez podmiot walidujący/Walidatora.

Uczestnik zobowiązany jest do okazania się dokumentem potwierdzającym tożsamość ze zdjęciem, przed zespołem monitorującym usługę rozwojową.

Walidacja jest prowadzona w formie testu z wynikiem generowanym automatycznie, co zapewnia obiektywną weryfikację nabytych kompetencji. Proces ten odbywa się pod nadzorem niezależnego walidatora, zgodnie z zasadą rozdzielności funkcji dydaktycznej od oceniającej.

Informacje dodatkowe

Korzystając 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 możliwe jest skorzystanie ze 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 od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Adres

ul. Juliana Tuwima 48/11
90-021 Łódź
woj. łódzkie

Kontakt

MATEUSZ ŚWIĄDER

E-mail swiadermateusz@gmail.com
Telefon (+48) 733 058 666