Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo systemów automatyki – SCADA pod ochroną – poziom 1 (CB1)

Numer usługi 2026/07/07/5274/3674308

5 630,94 PLN brutto
4 578,00 PLN netto
268,14 PLN brutto/h
218,00 PLN netto/h
183,33 PLN cena rynkowa

EMT-SYSTEMS Spółka z ograniczoną odpowiedzialnością

4,6 / 5

3 244 oceny

Gliwice
Usługa szkoleniowa
stacjonarna
Zajęcia grupowe
21:00 h
06.10.2026 do 08.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Aplikacje biznesowe
Grupa docelowa usługi	Szkolenie przeznaczone dla działów IT, działów bezpieczeństwa oraz automatyki firm produkcyjnych, a także wszystkich osób, które chcą zdobyć lub podnieść swoje kompetencje w danej dziedzinie. Szkolenie nastawione jest na budowanie świadomości oraz kompetencji zespołu w zakresie bezpieczeństwa sieci przemysłowych. **Usługa również adresowana dla uczestników projektu** • **"Opolskie Kształcenie Ustawiczne",** • **"Kierunek – Rozwój",** • **MP i/lub dla Uczestników Projektu NSE,** • **Lubuskie Bony Rozwojowe.** *Usługa rozwojowa skierowana jest również do uczestników innych projektów.* **Wymagania wstępne:** Ogólna wiedza techniczna, podstawowa znajomość systemów automatyki oraz zagadnień sieciowych.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	05-10-2026
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

Szkolenie przygotowuje do samodzielnej pracy w zakresie bezpieczeństwa cybernetycznego sieci przemysłowych, w tym działania sieci ETHERNET oraz monitorowania infrastruktury sieciowej systemu IDS.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Dba o bezpieczeństwo cybernetyczne sieci przemysłowych	omawia zasadę działania sieci ETHERNET	Test teoretyczny z wynikiem generowanym automatycznie
	monitoruje infrastrukturę sieciową systemu IDS	Test teoretyczny z wynikiem generowanym automatycznie
	samodzielnie rozwiązuje elementarne problemy dotyczące cyberbezpieczeństwa systemów automatyki	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

Niniejsze szkolenie ma na celu kompleksowe wsparcie osób dorosłych, które z własnej inicjatywy planują podnieść swoje kompetencje, umożliwiające rozwój w kierunku umiejętności zawodowych, niezbędnych do podjęcia pracy w sektorze zielonej gospodarki, ponadto niezbędnych z punktu widzenia regionalnych/lokalnych specjalizacji dla Śląska (RIS, PRT) przykładowo z branży: 7.1 Automatyka

przemysłowa, zautomatyzowane linie produkcyjne.

Program usługi obejmuje 21 godzin zegarowych. Przerwy wliczają się w czas trwania usługi szkoleniowej.

Dzień 1: 7 godzin

Dzień 2: 7 godzin

Dzień 3: 7 godzin

Czas trwania zajęć teoretycznych: 6h.

Czas trwania zajęć praktycznych: 15h.

Walidacja:

Wybrana metoda walidacji szkolenia: „Test teoretyczny z wynikiem generowanym automatycznie", dla której nie jest wymagane wprowadzenie osoby walidującej usługę w sekcji osób prowadzących. Uczestnik szkolenia wypełnia test pod koniec szkolenia w aplikacji dostępnej na komputerze w sali szkoleniowej EMT-Systems.

Program szkolenia:

zień 1

1. **Wprowadzenie do sieci przemysłowych.**
2. Jak działa sieć w standardzie ETHERNET?
3. Sieciowy model ISO/OSI.
4. Komunikacja w sieci Ethernet – podstawy.
5. Komunikacja w warstwie trzeciej (L3).
6. Protokoły warstwy transportowej (L4).
7. Protokoły warstwy aplikacji (L7).

Dzień 2

1. **Jak zadbać o bezpieczeństwo cybernetyczne sieci przemysłowych?**
2. Wprowadzenie – informacje podstawowe.
   - Przegląd podatności i źródeł zagrożeń.
   - Normy, dobre praktyki, polityki bezpieczeństwa (Defence in depth, NIST, IEC 62443, Reagowanie na incydenty).
   - Inwentaryzacja podstawą bezpieczeństwa.
   - Audyty bezpieczeństwa - badanie bezpieczeństwa sieci.
   - Bezpieczna transmisja.
3. Ochrona pasywna – jak monitorować sieć SCADA.
   - Podstawowe zagadnienia (SOC, SIEM, SOAR, IDS, Honeypot).
   - IDS – kluczowy system monitorowania sieci SCADA.
4. Ochrona aktywna – Jak zabezpieczać systemy sterowania czyli PLC pod ochroną?
   - Podstawowe zagadnienia (koncepcja Defence in Depth, Cyber Killchain).
   - Stosowane technologie (Firewall, IPS, Dioda danych, NG Firewall, DPI Firewall).
   - DPI Firewall – ochrona sterowników PLC i HMI.

Dzień 3

1. **Monitorowania infrastruktury sieciowej system IDS - praktyczne warsztaty.**

- Architektura systemu monitorowania.
- Wprowadzenie do interfejsu systemu IDS.

1. **Dashboard, alarmy, inwentaryzacja, raportowanie, reguły bezpieczeństwa itd.**

- Analiza przypadku.
  - Identyfikacja nowego urządzenia w sieci.
  - Wykrycie aktywnego rekonesansu sieci.
  - Identyfikacja niewłaściwej komendy wybranego protokołu (np. Modbus, S7+, PROFINET).
  - Atak Man in the middle.
  - Wykrywanie malware.
  - Tworzenie polityk bezpieczeństwa.
    - Wykrycie nieautoryzowanego zapytania o wartość rejestru sterownika.

- Wykrycie nieautoryzowanej zmiany parametrów rejestru.

1. Podsumowanie.
2. Walidacja

Warunki niezbędne do osiągnięcia celu usługi

Ogólna wiedza techniczna, podstawowa znajomość systemów automatyki oraz zagadnień sieciowych.

Warunki organizacyjne:

Szkolenia prowadzone są w Laboratoriach Centrum Szkoleń Inżynierskich EMT-Systems wyposażonych w rzutnik multimedialny i tablicę suchościeralną, laptopy dla uczestników kursu oraz prowadzącego.

Sale i laboratoria szkoleniowa - klimatyzowane, duże i przestronne. Stanowiska dla kursantów zostały specjalistycznie wyposażone.

Uczestnicy szkolenia nie są dzieleni na sekcje. W przypadku osiągnięcia pełnej grupy uczestników szkolenia każdy z uczestników ma możliwość wykonania ćwiczenia indywidualnie. Każdy Uczestnik szkolenia ma do dyspozycji stanowisko przeznaczone do nauki i rozwiązywania zadań opartych o przemysłowe sieci komunikacyjne ETHERNET.

Zestawy umożliwiają tworzenie rozbudowanych sieci, pozwalają na wykonywanie zadań i ćwiczeń w szerokim zakresie tematycznym.

Harmonogram

Liczba pozycji harmonogramu: 30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 30 Wprowadzenie do sieci przemysłowych	Zajęcia	Stefan Bednarczyk	06-10-2026	09:00	09:45	00:45
2 z 30 Jak działa sieć w standardzie ETHERNET?	Zajęcia	Stefan Bednarczyk	06-10-2026	09:45	10:30	00:45
3 z 30 -	Przerwa	-	06-10-2026	10:30	10:45	00:15
4 z 30 Sieciowy model ISO/OSI.	Zajęcia	Stefan Bednarczyk	06-10-2026	10:45	11:45	01:00
5 z 30 Komunikacja w sieci Ethernet – podstawy.	Zajęcia	Stefan Bednarczyk	06-10-2026	11:45	12:30	00:45
6 z 30 -	Przerwa	-	06-10-2026	12:30	13:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 30 Komunikacja w warstwie trzeciej (L3).	Zajęcia	Stefan Bednarczyk	06-10-2026	13:00	14:15	01:15
8 z 30 Protokoły warstwy transportowej (L4).	Zajęcia	Stefan Bednarczyk	06-10-2026	14:15	15:00	00:45
9 z 30 -	Przerwa	-	06-10-2026	15:00	15:15	00:15
10 z 30 Protokoły warstwy aplikacji (L7).	Zajęcia	Stefan Bednarczyk	06-10-2026	15:15	16:00	00:45
11 z 30 Jak zadbać o bezpieczeństwo cybernetyczne sieci przemysłowych?, Wprowadzenie – informacje podstawowe.	Zajęcia	Stefan Bednarczyk	07-10-2026	09:00	09:45	00:45
12 z 30 Przegląd podatności i źródeł zagrożeń. Normy, dobre praktyki, polityki bezpieczeństwa (Defence in depth, NIST, IEC 62443, Reagowanie na incydenty).	Zajęcia	Stefan Bednarczyk	07-10-2026	09:45	10:30	00:45
13 z 30 -	Przerwa	-	07-10-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 30 Inwentaryzacja podstawą bezpieczeństwa. Audyty bezpieczeństwa - badanie bezpieczeństwa sieci. Bezpieczna transmisja.	Zajęcia	Stefan Bednarczyk	07-10-2026	10:45	11:45	01:00
15 z 30 Ochrona pasywna – jak monitorować sieć SCADA. Podstawowe zagadnienia (SOC, SIEM, SOAR, IDS, Honeypot).	Zajęcia	Stefan Bednarczyk	07-10-2026	11:45	12:30	00:45
16 z 30 -	Przerwa	-	07-10-2026	12:30	13:00	00:30
17 z 30 IDS – kluczowy system monitorowania sieci SCADA.	Zajęcia	Stefan Bednarczyk	07-10-2026	13:00	14:15	01:15
18 z 30 Ochrona aktywna – Jak zabezpieczać systemy sterowania czyli PLC pod ochroną? Podstawowe zagadnienia (koncepcja Defence in Depth, Cyber Killchain).	Zajęcia	Stefan Bednarczyk	07-10-2026	14:15	15:00	00:45
19 z 30 -	Przerwa	-	07-10-2026	15:00	15:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 30 Stosowane technologie (Firewall, IPS, Dioda danych, NG Firewall, DPI Firewall). DPI Firewall – ochrona sterowników PLC i HMI.	Zajęcia	Stefan Bednarczyk	07-10-2026	15:15	16:00	00:45
21 z 30 Monitorowania infrastruktury sieciowej system IDS - praktyczne warsztaty. Architektura systemu monitorowania.	Zajęcia	Stefan Bednarczyk	08-10-2026	09:00	09:45	00:45
22 z 30 Wprowadzenie do interfejsu systemu IDS. Dashboard, alarmy, inwentaryzacja, raportowanie, reguły bezpieczeństwa itd.	Zajęcia	Stefan Bednarczyk	08-10-2026	09:45	10:30	00:45
23 z 30 -	Przerwa	-	08-10-2026	10:30	10:45	00:15
24 z 30 Analiza przypadku. Identyfikacja nowego urządzenia w sieci.	Zajęcia	Stefan Bednarczyk	08-10-2026	10:45	11:45	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
25 z 30 Wykrycie aktywnego rekonesansu sieci. Identyfikacja niewłaściwej komendy wybranego protokołu (np. Modbus, S7+, PROFINET).	Zajęcia	Stefan Bednarczyk	08-10-2026	11:45	12:30	00:45
26 z 30 -	Przerwa	-	08-10-2026	12:30	13:00	00:30
27 z 30 Atak Man in the middle. Wykrywanie malware. Tworzenie polityk bezpieczeństwa.	Zajęcia	Stefan Bednarczyk	08-10-2026	13:00	14:15	01:15
28 z 30 -	Przerwa	-	08-10-2026	14:15	14:30	00:15
29 z 30 Wykrycie nieautoryzowanego zapytania o wartość rejestru sterownika. Wykrycie nieautoryzowanej zmiany parametrów rejestru. Podsumowanie.	Zajęcia	Stefan Bednarczyk	08-10-2026	14:30	15:45	01:15
30 z 30 -	Walidacja	Stefan Bednarczyk	08-10-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	21:00
w tym suma godzin zajęć	17:45

Rodzaj godzin	Liczba godzin
w tym suma godzin walidacji	00:15
w tym suma przerw	03:00
Suma godzin dydaktycznych bez przerw	24:00

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	5 630,94 PLN
Koszt przypadający na 1 uczestnika netto	4 578,00 PLN
Koszt osobogodziny brutto	268,14 PLN
Koszt osobogodziny netto	218,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	21:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Stefan Bednarczyk

Specjalista z dziedziny Systemy sterowania i wizualizacji, dedykowany prowadzący z zakresu Cyberbezpieczeństwo w automatyce. W EMT-Systems posiada 3-letnie doświadczenie w prowadzeniu zajęć dydaktycznych. W ciągu ostatnich trzech lat z zakresu Cyberbezpieczeństwo w automatyce przeprowadził następującą liczbę szkoleń: ok. 4. Trener posiadający doświadczenie w prowadzeniu zajęć dydaktycznych z zakresu cyberbezpieczeństwa. Elektronik, projektant systemów informatycznych, specjalista ds. cyberbezpieczeństwa przemysłowego. Certyfikowany ekspert z zakresu cyberbezpieczeństwa przemysłowego: GIAC GICSP (Global Industrial Cyber Security Professional). Certyfikaty dot. administracji sieciami: Certified StormShield Network Administrator (CSNA), Cisco CCNA. Szkolenia: CEH v10 (Certified Ethical Hacker), Cisco CCNP. Specjalizacja: Systemy sterowania i wizualizacji. Wykształcenie: Wyższe techniczne.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały szkoleniowe przekazywane są kursantom w postaci autorskiego skryptu. Kursanci otrzymują również materiały piśmiennicze (notes, długopis).

Warunki uczestnictwa

Po dokonaniu zgłoszenia skontaktujemy się w celu potwierdzenia możliwości uczestnictwa i podpisania umowy na realizację szkolenia.

Informacje dodatkowe

Przed zgłoszeniem na usługę prosimy o kontakt w celu potwierdzenia dostępności wolnych miejsc.

EMT-Systems Sp. z o. o. zastrzega sobie prawo do nieuruchomienia szkolenia w przypadku niewystarczającej liczby zgłoszeń (min. 6 uczestników).

Istnieje możliwość zwolnienia usługi z podatku VAT na podstawie § 3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (DZ.U.2013, poz. 1722 z późn. zm.), w przypadku, gdy Przedsiębiorca/Uczestnik otrzyma dofinansowanie na poziomie co najmniej 70% ze środków publicznych. Warunkiem zwolnienia jest dostarczenie do firmy szkoleniowej stosownego oświadczenia na co najmniej 1 dzień roboczy przed szkoleniem. W innej sytuacji należy doliczyć podatek VAT w wysokości 23%.

Została podpisana umowa z WUP Kraków.

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój.

Poczęstunek kawowy i obiadowy nie jest wliczony w cenę kursu.

Adres

ul. Bojkowska 35A

44-100 Gliwice

woj. śląskie

Siedziba Centrum Szkoleń Inżynierskich, na którą składają się biura, pracownie i laboratoria szkoleniowe – znajduje się w doskonałej lokalizacji, niedaleko zjazdu z A4 (zjazd Sośnica). Szkolenia prowadzone są w budynku nr 3 Cechownia przy ulicy Bojkowskiej 35A na terenie kompleksu inwestycyjnego "Nowe Gliwice".

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe

Kontakt

AGNIESZKA FRANC

E-mail agnieszka.franc@emt-systems.pl
Telefon (+48) 501 322 109