Możliwość dofinansowania

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

Numer usługi 2026/01/30/5274/3296899

5 760,09 PLN brutto
4 683,00 PLN netto
274,29 PLN brutto/h
223,00 PLN netto/h

EMT-SYSTEMS Spółka z ograniczoną odpowiedzialnością

4,6 / 5

3 066 ocen

Gliwice / stacjonarna
Usługa szkoleniowa
21 h
19.05.2026 do 21.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Aplikacje biznesowe
Grupa docelowa usługi	Szkolenie przeznaczone dla działów IT, działów bezpieczeństwa oraz automatyki firm produkcyjnych. 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	15-05-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	21

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 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

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.

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.

Program szkolenia:

Szkolenie trwa 21 godzin dydaktycznych (1 godzina dydaktyczna to 45 min). Przerwy nie wliczają się w czas trwania usługi szkoleniowej.

Dzień 1: 7 godzin dydaktycznych

Dzień 2: 7 godzin dydaktycznych

Dzień 3: 7 godzin dydaktycznych

Program:

Dzień 1

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

Dzień 2

1. **Jak zadbać o bezpieczeństwo cybernetyczne sieci przemysłowych?**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.

2. Ochrona pasywna – jak monitorować sieć SCADA.
   - Podstawowe zagadnienia (SOC, SIEM, SOAR, IDS, Honeypot).
   - IDS – kluczowy system monitorowania sieci SCADA.

3. 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. 1. **Monitorowania infrastruktury sieciowej system IDS - praktyczne warsztaty.**Architektura systemu monitorowania.
   2. Wprowadzenie do interfejsu systemu IDS.

2. **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.

3. Podsumowanie.
4. 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 przedmiotów/zajęć: 24

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 24 Wprowadzenie do sieci przemysłowych. Jak działa sieć w standardzie ETHERNET?	Stefan Bednarczyk	19-05-2026	09:00	10:30	01:30
2 z 24 Przerwa kawowa	Stefan Bednarczyk	19-05-2026	10:30	11:00	00:30
3 z 24 Sieciowy model ISO/OSI. Komunikacja w sieci Ethernet – podstawy.	Stefan Bednarczyk	19-05-2026	11:00	12:30	01:30
4 z 24 Przerwa obiadowa	Stefan Bednarczyk	19-05-2026	12:30	13:30	01:00
5 z 24 Komunikacja w warstwie trzeciej (L3).	Stefan Bednarczyk	19-05-2026	13:30	15:00	01:30
6 z 24 Przerwa kawowa	Stefan Bednarczyk	19-05-2026	15:00	15:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 24 Protokoły warstwy transportowej (L4). Protokoły warstwy aplikacji (L7).	Stefan Bednarczyk	19-05-2026	15:15	16:00	00:45
8 z 24 Jak zadbać o bezpieczeństwo cybernetyczne sieci przemysłowych? Wprowadzenie – informacje podstawowe. Przegląd podatności i źródeł zagrożeń.	Stefan Bednarczyk	20-05-2026	09:00	10:30	01:30
9 z 24 Przerwa kawowa	Stefan Bednarczyk	20-05-2026	10:30	11:00	00:30
10 z 24 Normy, dobre praktyki, polityki bezpieczeństwa (Defence in depth, NIST, IEC 62443, Reagowanie na incydenty). Inwentaryzacja podstawą bezpieczeństwa.	Stefan Bednarczyk	20-05-2026	11:00	11:45	00:45
11 z 24 Audyty bezpieczeństwa - badanie bezpieczeństwa sieci. Bezpieczna transmisja.	Stefan Bednarczyk	20-05-2026	11:45	12:30	00:45
12 z 24 Przerwa obiadowa	Stefan Bednarczyk	20-05-2026	12:30	13:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 24 Ochrona pasywna – jak monitorować sieć SCADA. Podstawowe zagadnienia (SOC, SIEM, SOAR, IDS, Honeypot). IDS – kluczowy system monitorowania sieci SCADA.	Stefan Bednarczyk	20-05-2026	13:30	14:15	00:45
14 z 24 Ochrona aktywna – Jak zabezpieczać systemy sterowania czyli PLC pod ochroną? Podstawowe zagadnienia (koncepcja Defence in Depth, Cyber Killchain).	Stefan Bednarczyk	20-05-2026	14:15	15:00	00:45
15 z 24 Przerwa kawowa	Stefan Bednarczyk	20-05-2026	15:00	15:15	00:15
16 z 24 Stosowane technologie (Firewall, IPS, Dioda danych, NG Firewall, DPI Firewall). DPI Firewall – ochrona sterowników PLC i HMI.	Stefan Bednarczyk	20-05-2026	15:15	16:00	00:45
17 z 24 Monitorowania infrastruktury sieciowej system IDS - praktyczne warsztaty. Architektura systemu monitorowania. Wprowadzenie do interfejsu systemu IDS.	Stefan Bednarczyk	21-05-2026	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 24 Przerwa kawowa	Stefan Bednarczyk	21-05-2026	10:30	11:00	00:30
19 z 24 Dashboard, alarmy, inwentaryzacja, raportowanie, reguły bezpieczeństwa itd. Analiza przypadku. Identyfikacja nowego urządzenia w sieci. Wykrycie aktywnego rekonesansu sieci.	Stefan Bednarczyk	21-05-2026	11:00	12:30	01:30
20 z 24 Przerwa obiadowa	Stefan Bednarczyk	21-05-2026	12:30	13:30	01:00
21 z 24 Identyfikacja niewłaściwej komendy wybranego protokołu (np. Modbus, S7+, PROFINET). Atak Man in the middle. Wykrywanie malware. Tworzenie polityk bezpieczeństwa.	Stefan Bednarczyk	21-05-2026	13:30	14:15	00:45
22 z 24 Przerwa kawowa	Stefan Bednarczyk	21-05-2026	14:15	14:30	00:15
23 z 24 Wykrycie nieautoryzowanego zapytania o wartość rejestru sterownika. Wykrycie nieautoryzowanej zmiany parametrów rejestru. Podsumowanie.	Stefan Bednarczyk	21-05-2026	14:30	15:45	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 24 Walidacja - test teoretyczny z wynikiem generowanym automatycznie	Stefan Bednarczyk	21-05-2026	15:45	16:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 760,09 PLN
Koszt przypadający na 1 uczestnika netto	4 683,00 PLN
Koszt osobogodziny brutto	274,29 PLN
Koszt osobogodziny netto	223,00 PLN

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 5-letnie doświadczenie w prowadzeniu zajęć dydaktycznych. W ciągu ostatnich pięciu lat do nadal 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 (Cyberbezpieczeństwo w automatyce). Wykształcenie: mgr inż.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników szkolenia otrzymuje skrypt szkoleniowy, notes i 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