Możliwość dofinansowania

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

Numer usługi 2024/04/03/5274/2112388

5 535,00 PLN brutto
4 500,00 PLN netto
263,57 PLN brutto/h
214,29 PLN netto/h

EMT-SYSTEMS Spółka z ograniczoną odpowiedzialnością

★★★★½

Gliwice / stacjonarna
Usługa szkoleniowa
21 h
28.10.2024 do 30.10.2024

Informacje podstawowe

Kategoria	Techniczne / Automatyka i robotyka
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
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".** **Wymagania wstępne:** Ogólna wiedza techniczna, podstawowa znajomość systemów automatyki oraz zagadnień sieciowych.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	8
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
	monitoruje infrastrukturę sieciową systemu IDS	Test teoretyczny
	dba odpowiednio o bezpieczeństwo cybernetyczne sieci przemysłowych zgodnie z poznanymi sposobami	Test teoretyczny
	widzi potrzebę samokształcenia się z obszaru cyberbezpieczeństwa w automatyce	Test teoretyczny
	identyfikuje i szuka rozwiązań problemów technicznych związanych z pracą na zajmowanym stanowisku	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, opis efektów uczenia się znajduje się na certyfikacie.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Tak, certyfikat potwierdza przeprowadzenie walidacji w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Tak, certyfikat potwierdza rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

Program szkolenia:

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

Dzień 1	**Wprowadzenie do sieci przemysłowych.** 1. 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	**Jak zadbać o bezpieczeństwo cybernetyczne sieci przemysłowych?** 1. 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	**Monitorowania infrastruktury sieciowej system IDS - praktyczne warsztaty.** 1. 1. Architektura systemu monitorowania. 2. Wprowadzenie do interfejsu systemu IDS. **Dashboard, alarmy, inwentaryzacja, raportowanie, reguły bezpieczeństwa itd.** 1. 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. 2. Podsumowanie. 3. 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?	Piotr Urbańczyk	28-10-2024	09:00	10:00	01:00
2 z 24 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	28-10-2024	10:00	10:15	00:15
3 z 24 Sieciowy model ISO/OSI. Komunikacja w sieci Ethernet – podstawy.	Piotr Urbańczyk	28-10-2024	10:15	12:30	02:15
4 z 24 Przerwa obiadowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	28-10-2024	12:30	13:00	00:30
5 z 24 Komunikacja w warstwie trzeciej (L3).	Piotr Urbańczyk	28-10-2024	13:00	14:30	01:30
6 z 24 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	28-10-2024	14:30	14:45	00:15
7 z 24 Protokoły warstwy transportowej (L4). Protokoły warstwy aplikacji (L7).	Piotr Urbańczyk	28-10-2024	14:45	16:00	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 24 Jak zadbać o bezpieczeństwo cybernetyczne sieci przemysłowych? Wprowadzenie – informacje podstawowe. Przegląd podatności i źródeł zagrożeń.	Piotr Urbańczyk	29-10-2024	09:00	10:00	01:00
9 z 24 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	29-10-2024	10:00	10:15	00:15
10 z 24 Normy, dobre praktyki, polityki bezpieczeństwa (Defence in depth, NIST, IEC 62443, Reagowanie na incydenty). Inwentaryzacja podstawą bezpieczeństwa.	Piotr Urbańczyk	29-10-2024	10:15	11:30	01:15
11 z 24 Audyty bezpieczeństwa - badanie bezpieczeństwa sieci. Bezpieczna transmisja.	Piotr Urbańczyk	29-10-2024	11:30	12:30	01:00
12 z 24 Przerwa obiadowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	29-10-2024	12:30	13:00	00:30
13 z 24 Ochrona pasywna – jak monitorować sieć SCADA. Podstawowe zagadnienia (SOC, SIEM, SOAR, IDS, Honeypot). IDS – kluczowy system monitorowania sieci SCADA.	Piotr Urbańczyk	29-10-2024	13:00	14:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 24 Ochrona aktywna – Jak zabezpieczać systemy sterowania czyli PLC pod ochroną? Podstawowe zagadnienia (koncepcja Defence in Depth, Cyber Killchain).	Piotr Urbańczyk	29-10-2024	14:00	14:30	00:30
15 z 24 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	29-10-2024	14:30	14:45	00:15
16 z 24 Stosowane technologie (Firewall, IPS, Dioda danych, NG Firewall, DPI Firewall). DPI Firewall – ochrona sterowników PLC i HMI.	Piotr Urbańczyk	29-10-2024	14:45	16:00	01:15
17 z 24 Monitorowania infrastruktury sieciowej system IDS - praktyczne warsztaty. Architektura systemu monitorowania. Wprowadzenie do interfejsu systemu IDS.	Piotr Urbańczyk	30-10-2024	09:00	10:00	01:00
18 z 24 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	30-10-2024	10:00	10:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 24 Dashboard, alarmy, inwentaryzacja, raportowanie, reguły bezpieczeństwa itd. Analiza przypadku. Identyfikacja nowego urządzenia w sieci. Wykrycie aktywnego rekonesansu sieci.	Piotr Urbańczyk	30-10-2024	10:15	12:30	02:15
20 z 24 Przerwa obiadowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	30-10-2024	12:30	13:00	00:30
21 z 24 Identyfikacja niewłaściwej komendy wybranego protokołu (np. Modbus, S7+, PROFINET). Atak Man in the middle. Wykrywanie malware. Tworzenie polityk bezpieczeństwa.	Piotr Urbańczyk	30-10-2024	13:00	14:30	01:30
22 z 24 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	30-10-2024	14:30	14:45	00:15
23 z 24 Wykrycie nieautoryzowanego zapytania o wartość rejestru sterownika. Wykrycie nieautoryzowanej zmiany parametrów rejestru. Podsumowanie.	Piotr Urbańczyk	30-10-2024	14:45	15:45	01:00
24 z 24 Walidacja	-	30-10-2024	15:45	16:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 535,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	263,57 PLN
Koszt osobogodziny netto	214,29 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Urbańczyk

Specjalista z dziedziny Systemy sterowania i wizualizacji, dedykowany prowadzący z zakresu Cyberbezpieczeństwo w automatyce. W EMT-Systems posiada 4-letnie doświadczenie w prowadzeniu zajęć dydaktycznych. W ciągu ostatnich czterech lat z zakresu Cyberbezpieczeństwo w automatyce przeprowadził następującą liczbę szkoleń: ok. 9. Trener posiadający doświadczenie w prowadzeniu zajęć dydaktycznych z zakresu cyberbezpieczeństwa. Ponadto wieloletni praktyk w dziedzinie cyberbezpieczeństwa dzięki pracy na rzecz przedsiębiorstw. Specjalizacja: Systemy sterowania i wizualizacji. Wykształcenie: Wyższe techniczne.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników szkolenia otrzymuje skrypt szkoleniowy, notes i długopis.

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). W tej sytuacji uczestnik zostanie poinformowany o najbliższym możliwym do zrealizowania terminie.

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 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%.

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