Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo: Ochrona sieci przemysłowych – poziom 2 (CB2)

Numer usługi 2024/04/03/5274/2112427

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
27.11.2024 do 29.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Aplikacje biznesowe
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:** Obsługa analizatora pakietów Wireshark, znajomość zagadnień Cyber Kill Chain, znajomość zagadnień OT: Model PERA, komponenty ICS, Znajomość działania sieci komputerowych (TCP/IP, Ethernet, Protokoły warstw wyższych)
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 wdrażania rozwiązań podnoszących bezpieczeństwo w sieciach przemysłowych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wdraża rozwiązania podnoszące bezpieczeństwo w sieciach przemysłowych	charakteryzuje typowe scenariusze naruszenia bezpieczeństwa instalacji przemysłowej	Test teoretyczny
	planuje implementację rozwiązań podnoszących bezpieczeństwo w sieciach zgodnie z poznanymi na szkoleniu metodami	Test teoretyczny
	reaguje w trakcie incydentu i działa pod presją czasu	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	• Minimalny kurs obsługi **Linux**:
	  • Podstawy niezbędne do poruszania się w środowisku laboratoryjnym
	• Aktywny Cykl Działań Cyberbezpieczeństwa
	• Analiza protokołów przemysłowych z wykorzystaniem **Wireshark**
	  • Narzędzia Wireshark, edytory szesnastkowe
	• Audytowanie stanu bezpieczeństwa konfiguracji systemów Windows Linux:
	  • Narzędzia **CIS-CAT**, **Lynis**, **Wynis**
	• Monitorowanie bezpieczeństwa sieci:
	  • Narzędzia **Radiflow iSID**, **Security Onion**, **Snort** v.2.9, **Snort** v 3.1

Dzień 2	• Elementy testów penetracyjnych:
	  • Elementy metodyki prowadzenia testów i aspekty związane z sieciami przemysłowymi
	  • Narzędzia: framework Metasploit, dystrybucja Kali Linux
	• Wstęp do **informatyki śledczej**:
	  • Metody zabezpieczania danych do analizy i proste techniki ich analizowania

Dzień 3	• Analiza ryzyka, IOC i TTP:
	  • Metody uzyskania IOC i TTP oraz wykorzystanie tych danych w procesie analizy ryzyka
	  • Rozwiązania **CIARA**
	• Praktyczne aspekty inwentaryzacji zasobów w sieci:
	  • Możliwości wykorzystania narzędzi Open Source do uzyskiwania danych inwentaryzacyjnych
	  • Narzędzia **snmpwalk**, **grassmarlin**, **nmap** i Wireshark
	• Praktyczne aspekty zwiększania bezpieczeństwa systemów przemysłowych:
	  • Zagadnienia powierzcgni ataku i jej ograniczania
	  • Możliwości i ograniczenia rozwiązań **Honeypot**
	• Praktyczne aspekty rozwiązań **SIEM**:
	  • Rodzaje rozwiązań SIEM
	  • Metody zbierania danych dla SIEM
	  • Zagadnienia reguł korelacji
	• Walidacja

Warunki niezbędne do osiągnięcia celu usługi: Obsługa analizatora pakietów Wireshark, znajomość zagadnień Cyber Kill Chain, znajomość zagadnień OT: Model PERA, komponenty ICS, Znajomość działania sieci komputerowych (TCP/IP, Ethernet, Protokoły warstw wyższych).

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: 21

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Minimalny kurs obsługi Linux. Aktywny Cykl Działań Cyberbezpieczeństwa.	Piotr Urbańczyk	27-11-2024	09:00	10:45	01:45
2 z 21 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	27-11-2024	10:45	11:00	00:15
3 z 21 Analiza protokołów przemysłowych z wykorzystaniem Wireshark	Piotr Urbańczyk	27-11-2024	11:00	12:30	01:30
4 z 21 Przerwa obiadowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	27-11-2024	12:30	13:00	00:30
5 z 21 Audytowanie stanu bezpieczeństwa konfiguracji systemów Windows Linux.	Piotr Urbańczyk	27-11-2024	13:00	14:30	01:30
6 z 21 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	27-11-2024	14:30	14:45	00:15
7 z 21 Monitorowanie bezpieczeństwa sieci	Piotr Urbańczyk	27-11-2024	14:45	16:00	01:15
8 z 21 Elementy testów penetracyjnych. Wstęp do informatyki śledczej.	Piotr Urbańczyk	28-11-2024	09:00	10:45	01:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 21 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	28-11-2024	10:45	11:00	00:15
10 z 21 Elementy testów penetracyjnych. Wstęp do informatyki śledczej.	Piotr Urbańczyk	28-11-2024	11:00	12:30	01:30
11 z 21 Przerwa obiadowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	28-11-2024	12:30	13:00	00:30
12 z 21 Elementy testów penetracyjnych. Wstęp do informatyki śledczej.	Piotr Urbańczyk	28-11-2024	13:00	14:30	01:30
13 z 21 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	28-11-2024	14:30	14:45	00:15
14 z 21 Elementy testów penetracyjnych. Wstęp do informatyki śledczej.	Piotr Urbańczyk	28-11-2024	14:45	16:00	01:15
15 z 21 Analiza ryzyka, IOC i TTP.	Piotr Urbańczyk	29-11-2024	09:00	10:45	01:45
16 z 21 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	29-11-2024	10:45	11:00	00:15
17 z 21 Praktyczne aspekty inwentaryzacji zasobów w sieci.	Piotr Urbańczyk	29-11-2024	11:00	13:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 21 Przerwa obiadowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	29-11-2024	13:00	13:30	00:30
19 z 21 Praktyczne aspekty zwiększania bezpieczeństwa systemów przemysłowych. Praktyczne aspekty rozwiązań SIEM.	Piotr Urbańczyk	29-11-2024	13:30	15:30	02:00
20 z 21 Przerwa kawowa (wliczona w czas trwania usługi)	Piotr Urbańczyk	29-11-2024	15:30	15:45	00:15
21 z 21 Walidacja	-	29-11-2024	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/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%.

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