Możliwość dofinansowania

Cyberbezpieczeństwo i AI: Od fundamentów i obrony przed atakami do automatyzacji procesów - szkolenie.

Numer usługi 2025/11/19/177993/3158709

2 400,00 PLN brutto
2 400,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

ŁÓDZKI DOM BIZNESU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ SPÓŁKA KOMANDYTOWA

★★★★★ 5,0 / 5

2 oceny

Łódź / stacjonarna
Usługa szkoleniowa
24 h
25.11.2025 do 28.11.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do pracowników działów IT, administratorów systemów, kadry zarządzającej oraz wszystkich pracowników biurowych, którzy chcą podnieść swoje kompetencje w zakresie cyfrowego bezpieczeństwa. Zaprojektowana dla osób odpowiedzialnych za ochronę danych w firmie, chcących zrozumieć mechanizmy współczesnych cyberzagrożeń (phishing, ransomware, ataki sieciowe) oraz nauczyć się wykorzystywać sztuczną inteligencję (AI) do automatyzacji procesów obronnych.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	21-11-2025
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	24
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Uczestnik po zakończeniu szkolenia jest w pełni przygotowany do praktycznego zabezpieczania siebie i organizacji przed cyber zagrożeniami. Po zakończeniu usługi uczestnik potrafi rozpoznawać wektory ataków (socjotechnika, ataki sieciowe), wdrażać mechanizmy obronne (MFA, higiena haseł) oraz wykorzystywać narzędzia AI do automatyzacji monitoringu bezpieczeństwa i reagowania na incydenty.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozpoznaje i charakteryzuje główne typy zagrożeń cybernetycznych.	Identyfikuje co najmniej 5 typów ataków (np. phishing, ransomware, man-in-the-middle).	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje adekwatny mechanizm obronny do zidentyfikowanego zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera i konfiguruje podstawowe zabezpieczenia systemowe i tożsamości.	Wskazuje zasady tworzenia silnych haseł i konfiguracji uwierzytelniania dwuskładnikowego (2FA/MFA).	Test teoretyczny z wynikiem generowanym automatycznie
	Rozróżnia wiadomości phishingowe od legalnej komunikacji na podstawie analizy nagłówków i treści.	Test teoretyczny z wynikiem generowanym automatycznie
Opisuje procedury testów penetracyjnych i analizy podatności.	Identyfikuje luki bezpieczeństwa w przykładowej aplikacji webowej (zgodnie z OWASP Top 10).	Test teoretyczny z wynikiem generowanym automatycznie
	Wyjaśnia etapy reagowania na incydent (Incident Response) i podstawy informatyki śledczej.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje zastosowanie AI i automatyzacji w cyberbezpieczeństwie.	Wskazuje przykłady użycia modeli AI do detekcji zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie
	Opisuje wymagania formalne (RODO/GDPR, NIS2) w kontekście ochrony danych.	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

Warunki organizacyjne

- **Czas trwania usługi:** 24 godziny zegarowe (60 min), realizowane przez 3 dni (8h/dzień).
- **Przerwy:** Wliczone w czas usługi rozwojowej.
- **Warunki techniczne:** Uczestnicy pracują na komputerach własnych (wymagane środowisko do wirtualizacji). Sala wyposażona w rzutnik i szybkie łącze internetowe.
- **Walidacja:** Walidacja (15 minut na uczestnika) przeprowadzana jest w formie **Testu teoretycznego z wynikiem generowanym automatycznie**.

Usługa realizowana jest w formie warsztatu praktycznego (Hands-on Labs) z elementami wykładu [T/P/M].

Dzień 1: Fundamenty Cyberbezpieczeństwa i Ataki na Użytkowników

09.00 - 10.30:

Wprowadzenie i krajobraz współczesnych zagrożeń.

- 10.30 - 10.45: Przerwa

10.45 - 12.15:

Phishing i Social Engineering – symulacje ataków i analiza psychologiczna.

- 12.15 - 13.00: Przerwa

13.00 - 14.00:

Bezpieczeństwo tożsamości: Hasła, MFA i łamanie haseł (pokaz na żywo).

14.00 - 15.30:

Malware i Ransomware – analiza działania złośliwego oprogramowania w bezpiecznym środowisku (sandbox).

- 15.30 - 15.45: Przerwa

15.45 - 17.00

Test cyberhigieny i podsumowanie dnia.

Dzień 2: Zaawansowane Ataki, Sieci i Informatyka Śledcza

09.00 - 10.30

Network Security – bezpieczeństwo sieci WiFi i analiza pakietów (Wireshark).

- 10.30 - 10.45: Przerwa

10.45 - 12.15

WebApp Security – bezpieczeństwo aplikacji webowych (OWASP Top 10, środowisko DVWA).

- 12.15 - 13.00: Przerwa

13.00 - 15.00:

- Incident Response & Forensics – reagowanie na incydenty, analiza logów i śladów cyfrowych.

15.00 - 15.15: Przerwa

15.15 - 17.00

Supply Chain & Third-Party Risk – ryzyka łańcucha dostaw i skanowanie podatności.

Dzień 3: AI w Cybersec, Automatyzacja i CTF

09.00 - 10.30:

AI & ML w Security – wykorzystanie modeli językowych i GANs w obronie i ataku.

- 10.30 - 10.45: Przerwa

10.45 - 12.15:

Automatyzacja procesów bezpieczeństwa (workflows, threat intelligence API).

- 12.15 - 13.00: Przerwa

13.00 - 14.30

Compliance i regulacje – Zero Trust, RODO/GDPR, dyrektywa NIS2.

- 14.30 - 14.45: Przerwa

14.45 - 16.45

Red Teaming & Capture The Flag (CTF) – finałowe ćwiczenie praktyczne (symulacja ataku i obrony).

16.45 - 17.00

Walidacja efektów uczenia się.

Harmonogram

Liczba przedmiotów/zajęć: 23

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 23 Wprowadzenie + Krajobraz zagrożeń	David Michel	25-11-2025	09:00	10:30	01:30
2 z 23 przerwa	David Michel	25-11-2025	10:30	10:45	00:15
3 z 23 Phishing & Social Engineering (Warsztat)	David Michel	25-11-2025	10:45	12:15	01:30
4 z 23 przerwa	David Michel	25-11-2025	12:15	13:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 23 Hasła, MFA, Password Cracking (Live)	David Michel	25-11-2025	13:00	14:00	01:00
6 z 23 Malware & Ransomware (Demo)	David Michel	25-11-2025	14:00	15:30	01:30
7 z 23 przerwa	David Michel	25-11-2025	15:30	15:45	00:15
8 z 23 Test cyberhigieny i Q&A	David Michel	25-11-2025	15:45	17:00	01:15
9 z 23 Network Security & WiFi (Wireshark)	David Michel	27-11-2025	09:00	10:30	01:30
10 z 23 przerwa	David Michel	27-11-2025	10:30	10:45	00:15
11 z 23 WebApp Security (OWASP, DVWA)	David Michel	27-11-2025	10:45	12:15	01:30
12 z 23 Przerwa	David Michel	27-11-2025	12:15	13:00	00:45
13 z 23 Incident Response & Forensics	David Michel	27-11-2025	13:00	15:00	02:00
14 z 23 Przerwa	David Michel	27-11-2025	15:00	15:15	00:15
15 z 23 •Supply Chain & Third-Party Risk	David Michel	27-11-2025	15:15	17:00	01:45
16 z 23 AI & ML w Security (Demo modeli)	David Michel	28-11-2025	09:00	10:30	01:30
17 z 23 Przerwa	David Michel	28-11-2025	10:30	10:45	00:15
18 z 23 Automatyzacje (Workflows, API)	David Michel	28-11-2025	10:45	12:15	01:30
19 z 23 Przerwa	David Michel	28-11-2025	12:15	13:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 23 Compliance: NIS2, GDPR, Zero Trust	David Michel	28-11-2025	13:00	14:30	01:30
21 z 23 Przerwa	David Michel	28-11-2025	14:30	14:45	00:15
22 z 23 Red Teaming & Capture The Flag (CTF)	David Michel	28-11-2025	14:45	16:45	02:00
23 z 23 Walidacja	-	28-11-2025	16:45	17:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 400,00 PLN
Koszt przypadający na 1 uczestnika netto	2 400,00 PLN
Koszt osobogodziny brutto	100,00 PLN
Koszt osobogodziny netto	100,00 PLN

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" (Stanford Online 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

Informacje o materiałach dla uczestników usługi Uczestnicy otrzymują komplet materiałów dydaktycznych (cyfrowych):

- Skrypty szkoleniowe z opisem typów ataków i metod obrony.
- Szablony checklist bezpieczeństwa i procedur reagowania na incydenty.
- Dostęp do środowiska laboratoryjnego (wirtualne maszyny) na czas szkolenia.
- Dostęp do platformy testowej w celu przeprowadzenia walidacji.

Warunki uczestnictwa

Znajomość podstaw obsługi komputera i Internetu.

Warunkiem uzyskania zaświadczenia/certyfikatu jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej oraz uzyskanie pozytywnej oceny na podstawie wyniku walidacji.

Zapis na usługę musi nastąpić najpóźniej na 1 dzień przed datą jej rozpoczęcia.

Adres

ul. Walerego Wróblewskiego 18

93-578 Łódź

woj. łódzkie

Kontakt

Mateusz Świąder

E-mail swiadermateusz@gmail.com

Telefon (+48) 733 058 666