Możliwość dofinansowania

AI w cyberbezpieczeństwie

Numer usługi 2026/04/15/198554/3490083

2 500,00 PLN brutto
2 500,00 PLN netto
156,25 PLN brutto/h
156,25 PLN netto/h
261,33 PLN cena rynkowa

Centrum Szkoleniowe EDU-PROGRES JOLANTA ROSSA

Brak ocen dla tego dostawcy

Usługa szkoleniowa
zdalna w czasie rzeczywistym
16:00 h
18.05.2026 do 19.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	pracownicy firm, kierownictwo
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	10-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Szkolenie to ma na celu nie tylko przekazanie wiedzy teoretycznej, ale także praktyczne przygotowanie uczestników do wyzwań, jakie niesie ze sobą dynamicznie rozwijająca się dziedzina cyberbezpieczeństwa w kontekście sztucznej inteligencji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnicy zdobędą umiejętności w zakresie identyfikacji zagrożeń, analizy ryzyk oraz implementacji rozwiązań opartych na AI, które wspierają obronę przed cyberatakami.	3. Elementy praktyczne Obecność laboratoriów, ćwiczeń lub case studies Możliwość pracy z narzędziami (np. systemy detekcji zagrożeń, modele ML) Symulacje rzeczywistych ataków (np. phishing, malware detection) 👷 4. Kompetencje prowadzącego Doświadczenie w cyberbezpieczeństwie i AI Certyfikaty branżowe (np. CISSP, CEH, AI-related certs) Doświadczenie praktyczne (np. praca w SOC, red teaming)	Debata swobodna

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

DZIEŃ 1 – Podstawy i zastosowania AI (8h)

🔷 Moduł 1: Wprowadzenie do AI i cyberbezpieczeństwa (2h)

- Podstawy sztucznej inteligencji i uczenia maszynowego
- Typy modeli (supervised, unsupervised, deep learning)
- Rola AI w cyberbezpieczeństwie (SOC, SIEM, EDR)
- Aktualne trendy i kierunki rozwoju

Efekt: zrozumienie podstaw AI i jej zastosowań w bezpieczeństwie

🔷 Moduł 2: AI w detekcji zagrożeń (2h)

- Wykrywanie anomalii w ruchu sieciowym
- Analiza logów i zdarzeń bezpieczeństwa
- Systemy antyfraudowe i antyphishingowe
- Automatyzacja reakcji na incydenty

Warsztat: analiza logów i identyfikacja anomalii

🔷 Moduł 3: Narzędzia i technologie (2h)

- Python w cyberbezpieczeństwie (podstawy)
- Biblioteki ML (np. scikit-learn)
- Narzędzia SIEM/EDR z elementami AI
- Integracja AI z infrastrukturą IT

Warsztat: prosty model detekcji zagrożeń

🔷 Moduł 4: AI w SOC – case studies (2h)

- Zastosowanie AI w Security Operations Center
- Analiza rzeczywistych incydentów
- Automatyzacja alertów i priorytetyzacja zdarzeń

Case study: analiza incydentu bezpieczeństwa

📅 DZIEŃ 2 – Zagrożenia, bezpieczeństwo i wdrożenia (8h)

🔷 Moduł 5: Zagrożenia związane z AI (2h)

- Adversarial attacks
- Data poisoning i model evasion
- Zagrożenia związane z modelami językowymi (np. prompt injection)
- Deepfake i manipulacja informacją

Efekt: identyfikacja nowych typów zagrożeń

🔷 Moduł 6: Bezpieczeństwo systemów AI (2h)

- Zabezpieczanie modeli ML
- Zarządzanie danymi i dostępem
- Monitorowanie modeli i ich podatności
- Secure AI lifecycle

Warsztat: analiza podatności modelu

🔷 Moduł 7: Aspekty prawne i etyczne (2h)

- RODO / GDPR w kontekście AI
- Standardy (ISO 27001, NIST)
- Etyka AI i odpowiedzialność
- Ryzyka biznesowe i organizacyjne

Dyskusja: scenariusze decyzyjne

🔷 Moduł 8: Projekt końcowy i podsumowanie (2h)

- Opracowanie mini projektu (zastosowanie AI w cyberbezpieczeństwie)
- Prezentacja wyników
- Test końcowy i omówienie

Harmonogram

Liczba pozycji harmonogramu: 8

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Wprowadzenie do AI i cyberbezpieczeństwa (2h)	DAWID PAWLICKI	18-05-2026	08:00	10:00	02:00
2 z 8 AI w detekcji zagrożeń (2h)	DAWID PAWLICKI	18-05-2026	10:00	12:00	02:00
3 z 8 Narzędzia i technologie (2h)	DAWID PAWLICKI	18-05-2026	12:00	14:00	02:00
4 z 8 AI w SOC – case studies (2h)	DAWID PAWLICKI	18-05-2026	14:00	16:00	02:00
5 z 8 Zagrożenia związane z AI (2h)	DAWID PAWLICKI	19-05-2026	08:00	10:00	02:00
6 z 8 Bezpieczeństwo systemów AI (2h)	DAWID PAWLICKI	19-05-2026	10:00	12:00	02:00
7 z 8 Aspekty prawne i etyczne (2h)	DAWID PAWLICKI	19-05-2026	12:00	14:00	02:00
8 z 8 Projekt końcowy i podsumowanie (2h)	DAWID PAWLICKI	19-05-2026	14:00	16:00	02:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 500,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
Koszt przypadający na 1 uczestnika netto	2 500,00 PLN

Koszt osobogodziny brutto	156,25 PLN
Koszt osobogodziny netto	156,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

DAWID PAWLICKI

Dawid Pawlicki – trener AI i cyberbezpieczeństwa

Dawid Pawlicki jest trenerem specjalizującym się w obszarze sztucznej inteligencji oraz cyberbezpieczeństwa, z doświadczeniem w prowadzeniu szkoleń dla pracowników biznesu i IT. W swojej pracy koncentruje się na praktycznym wykorzystaniu technologii AI w kontekście ochrony informacji oraz zarządzania ryzykiem cybernetycznym.

Prowadzi szkolenia obejmujące m.in.:

zastosowanie narzędzi AI (np. modele językowe, automatyzacja) w środowisku pracy,
identyfikację zagrożeń wynikających z wykorzystania AI (np. prompt injection, phishing wspierany AI),
budowanie świadomości cyberbezpieczeństwa w organizacjach,
bezpieczne wdrażanie rozwiązań opartych na sztucznej inteligencji.

Posiada doświadczenie w pracy z różnymi grupami odbiorców – od kadry menedżerskiej po specjalistów IT – oraz umiejętność przekładania złożonych zagadnień technologicznych na praktyczne zastosowania biznesowe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

prezentacja, materiały szkoleniowe

Warunki techniczne

dostęp do komputera

Kontakt

JOLANTA ROSSA

E-mail j.rossa@edu-progres.pl
Telefon (+48) 607 805 066