Możliwość dofinansowania

Cyberbezpieczeństwo

Numer usługi 2026/04/18/200144/3496918

10 000,00 PLN brutto
10 000,00 PLN netto
250,00 PLN brutto/h
250,00 PLN netto/h
261,33 PLN cena rynkowa

Marketing Minds Academy Dawid Chlebus

Brak ocen dla tego dostawcy

Gdańsk
Usługa szkoleniowa
stacjonarna
40:00 h
03.08.2026 do 07.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane do pracowników administracyjnych pasjonujących się technologią, chcących nauczyć się rozpoznawania cyberataków, zapobiegania im i reagowania na incydenty w organizacji. To intensywny kurs dla osób początkujących, które chcą skutecznie chronić firmę przed rosnącym zagrożeniem ze strony cyberprzestępców przy użyciu narzędzi AI. Pracownicy biurowi, administracja publiczna, specjaliści HR i finansów pracujący na komputerach.
Minimalna liczba uczestników	10
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	31-07-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	40
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

Kurs przygotowuje uczestnika do samodzielnego rozpoznawania nowoczesnych cyberzagrożeń wykorzystujących sztuczną inteligencję oraz do bezpiecznego stosowania narzędzi AI w codziennej pracy administracyjno-biurowej. Uczestnik po zakończeniu szkolenia będzie przygotowany do podejmowania działań w zakresie ochrony danych osobowych (RODO) w interakcji z modelami językowymi, skutecznego identyfikowania ataków typu AI-phishing i Deepfake oraz wdrażania proced

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje kluczowe zagrożenia cybernetyczne nowej generacji, w tym ataki typu AI-phishing oraz technologię Deepfake. Wyjaśnia zasady bezpiecznego przetwarzania danych służbowych i osobowych (RODO) w kontekście korzystania z publicznych modeli językowych. Rozróżnia bezpieczne narzędzia AI od rozwiązań niosących wysokie ryzyko dla bezpieczeństwa informacji w organizacji.	Uczestnik poprawnie wskazuje min. 3 cechy charakterystyczne wiadomości phishingowej wygenerowanej przez AI w teście wiedzy. Uczestnik wymienia co najmniej 5 rodzajów danych, których nie wolno wprowadzać do publicznych czatów AI. Uczestnik prawidłowo klasyfikuje narzędzia AI pod kątem ich bezpieczeństwa w pytaniach testowych.	Test teoretyczny
Samodzielnie przeprowadza anonimizację dokumentów biurowych przed poddaniem ich analizie przez algorytmy AI. Skutecznie weryfikuje prawdziwość informacji wygenerowanych przez AI, stosując techniki fact-checkingu i wykrywania halucynacji modelu. Tworzy bezpieczne i efektywne zapytania (prompty), które automatyzują zadania biurowe bez narażania zasobów firmy.	Zadanie praktyczne: Uczestnik poprawnie usuwa dane wrażliwe z przygotowanego szablonu pisma urzędowego. Zadanie praktyczne: Uczestnik znajduje błędy merytoryczne w tekście wygenerowanym przez AI na podstawie źródłowej bazy wiedzy. Zadanie praktyczne: Uczestnik redaguje pismo urzędowe z pomocą AI, wykorzystując bezpieczny prompt.	Obserwacja w warunkach symulowanych
Wykazuje postawę ograniczonego zaufania do komunikatów cyfrowych i treści generowanych automatycznie. Przyjmuje odpowiedzialność za bezpieczeństwo cyfrowe organizacji, promując etyczne wykorzystanie sztucznej inteligencji.	Obserwacja podczas symulacji: Uczestnik krytycznie ocenia wiarygodność przedstawionego nagrania audio/video. Dyskusja moderowana: Uczestnik proponuje co najmniej jedną zasadę do wewnętrznego dekalogu bezpieczeństwa AI w biurze.	Obserwacja w warunkach symulowanych

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

Program Ramowy Usługi Rozwojowej

Tytuł: The Intersection of Cybersecurity and AI: Integracja bezpieczeństwa cyfrowego i sztucznej inteligencji w procesach administracyjnych.

MODUŁ I: Ekosystem AI w środowisku biurowym – architektura i ryzyka

- **Taksonomia Sztucznej Inteligencji:** Klasyfikacja narzędzi LLM (Large Language Models) i ich rola w transformacji cyfrowej administracji.
- **Analiza wektorów zagrożeń:** Potencjalne podatności wynikające z implementacji narzędzi AI w infrastrukturze biurowej.
- **Inżynieria zapytań (Prompt Engineering):** Zaawansowane techniki komunikacji z AI (Few-shot prompting, Chain-of-thought) w celu optymalizacji procesów redakcyjnych.
- **Higiena tożsamości cyfrowej:** Zarządzanie dostępem (IAM) i rola uwierzytelniania wieloskładnikowego (MFA) w zabezpieczaniu kont asystentów AI.

MODUŁ II: Compliance, RODO i ramy prawne eksploatacji AI

- **Zgodność z AI Act:** Analiza obowiązków wynikających z europejskiego rozporządzenia o sztucznej inteligencji w sektorze publicznym i prywatnym.
- **Ochrona danych osobowych (GDPR/RODO):** Ryzyka re-identyfikacji danych i zasada minimalizacji w kontekście interakcji z algorytmami uczenia maszynowego.
- **Metodologia anonimizacji i pseudonimizacji:** Praktyczne zastosowanie technik deidentyfikacji danych przed procesowaniem w chmurze obliczeniowej.
- **Własność intelektualna:** Analiza statusu prawnego utworów wygenerowanych przy udziale AI oraz kwestie licencyjne (SaaS vs. On-premise).

MODUŁ III: Inżynieria społeczna i ataki nowej generacji (Social Engineering 2.0)

- **Ewolucja Phishingu:** Analiza porównawcza tradycyjnych kampanii oraz ataków generatywnych (Precision Phishing).
- **Technologia Deepfake w atakach na ciągłość biznesową:** Metody detekcji manipulacji audio-wizualnej oraz procedury weryfikacji tożsamości (Challenge-Response).
- **Zagrożenia typu Adversarial AI:** Zrozumienie mechanizmów wprowadzania modeli w błąd (Input Injection) i ochrony przed manipulacją wynikami.
- **Studium przypadku (Case Studies):** Krytyczna analiza incydentów naruszenia bezpieczeństwa z wykorzystaniem AI w administracji.

MODUŁ IV: Operacyjna weryfikacja danych i automatyzacja procesów

- **Weryfikacja integralności informacji:** Strategie przeciwdziałania halucynacjom modeli (Cross-referencing) i techniki weryfikacji faktograficznej.

- **Analityka deskryptywna w biurze:** Wykorzystanie AI do bezpiecznej interpretacji zbiorów danych i generowania raportów bez naruszania poufności (Data Leakage Prevention).
- **Automatyzacja procesów (RPA + AI):** Projektowanie bezpiecznych pętli automatyzacji zadań powtarzalnych.
- **Narzędzia wspomagające (Sourcing):** Przegląd bezpiecznych repozytoriów i weryfikacja wtyczek (Plugins) pod kątem złośliwego oprogramowania.

MODUŁ V: Zarządzanie incydentem i audyt kompetencji

- **Incident Response w erze AI:** Opracowanie algorytmów postępowania w przypadku podejrzenia kompromitacji danych lub systemów.
- **Kultura Security-First:** Budowa świadomości organizacyjnej i rola pracownika jako "ludzkiego sensora" w systemie bezpieczeństwa.
- **Governance w obszarze AI:** Opracowanie polityki akceptowalnego użytkowania (Acceptable Use Policy – AUP) dla narzędzi AI w organizacji.
- **Walidacja efektów uczenia się:**
  - **Panel ekspercki:** Test wiedzy teoretycznej z zakresu Cybersecurity i AI.
  - **Egzamin praktyczny:** Symulacja reagowania na atak socjotechniczny oraz audyt bezpieczeństwa przygotowanego promptu.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	10 000,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	10 000,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	250,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Grzegorz Chlebus

Specjalista od cyberbezpieczeństwa

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypty szkoleniowe. Praca na komputerach zapewnionych przez organizatora.

Informacje dodatkowe

Materiały opracowane są przez mentorów z wieloletnim doświadczeniem na rynku pracy w branży IT. Kursant otrzymuje dostęp doplatformy edukacyjnej, na której zamieszczone są wszystkie niezbędne materiały i może uczyć się w dowolnym momencie. Materiały sądostępne na platformie Future Collars w formie:

prezentacji, materiałów poglądowych, wideotutorialów, slajdów, plików pdf, filmów z lekcji na żywo.

Użytkownik otrzymuje dostęp do platformy, na której odbywać się będą lekcje online w czasie rzeczywistym. Platforma jest dostępna24/7, więc kursant może z niej korzystać w dowolnym momencie.

Kursant ma dostęp do tych materiałów i lekcji, które są zapisywane na platformie po lekcji online i może z nich korzystać jeszcze przez 3 miesięcy po zakończeniu kursu.

Adres

Gdańsk
Gdańsk
woj. pomorskie

Kontakt

GRZEGORZ CHLEBUS

E-mail chlebusek@wp.pl
Telefon (+48) 798 009 221