Możliwość dofinansowania

Cyberbezpieczeństwo & Sztuczna Inteligencja

Numer usługi 2026/04/19/200144/3497446

13 530,00 PLN brutto
11 000,00 PLN netto
338,25 PLN brutto/h
275,00 PLN netto/h
332,00 PLN cena rynkowa

Marketing Minds Academy Dawid Chlebus

Brak ocen dla tego dostawcy

Gdańsk
Usługa szkoleniowa
mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
40:00 h
15.07.2026 do 19.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	Szkolenie z zakresu synergii sztucznej inteligencji i cyberbezpieczeństwa dedykowane jest osobom zainteresowanym nowoczesnymi technologiami, które pragną zdobyć umiejętności wykrywania zagrożeń cyfrowych, minimalizowania ryzyka oraz podejmowania właściwych działań naprawczych w środowisku firmowym.To propozycja dla uczestników bez wcześniejszego doświadczenia, którzy chcą poznać praktyczne metody zabezpieczania organizacji w obliczu dynamicznie rosnącej aktywności cyberprzestępczej wspomaganej sztuczną inteligencją.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	13-07-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
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

Szkolenie przygotowuje uczestnika do kompleksowego pełnienia obowiązków na stanowisku specjalisty ds. cyberbezpieczeństwa z uwzględnieniem technologii AI.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik po zakończeniu szkolenia posiada wiedzę w zakresie:Mechanizmów Deepfake i Vishing: Zna zasady działania algorytmów syntezy obrazu oraz klonowania głosu (Voice Cloning) wykorzystywanych do impersonacji. Ewolucji Phishingu: Rozumie, jak modele LLM automatyzują tworzenie spersonalizowanych, bezbłędnych wiadomości typu Spear-Phishing. Psychologii manipulacji AI: Definiuje techniki wywierania wpływu (presja czasu, reguła autorytetu) wzmocnione przez technologie generatywne. Procedur weryfikacji: Zna techniczne i operacyjne metody potwierdzania tożsamości rozmówcy oraz autentyczności treści cyfrowych.	Uczestnik udowadnia osiągnięcie efektu, jeśli:Wymienia min. 3 symptomy manipulacji wideo/audio (np. artefakty obrazu, nienaturalna intonacja). Opisuje procedurę „Call-back” oraz stosowanie haseł bezpieczeństwa w komunikacji głosowej. Wskazuje różnice między masowym spamem a atakiem celowanym generowanym przez AI	Test teoretyczny
Uczestnik po zakończeniu usługi szkoleniowej posiada praktyczną biegłość w zakresie:Tworzenia bezpiecznych struktur zapytań: Buduje prompty w oparciu o zaawansowane ramy (np. kontekst, zadanie, ograniczenia), które minimalizują ryzyko wycieku informacji niejawnych.Operacyjnej anonimizacji danych: Samodzielnie identyfikuje i zastępuje dane wrażliwe (identyfikatory osobowe, dane finansowe, dane medyczne) tagami syntetycznymi przed ich wprowadzeniem do interfejsu AI.Stosowania barier etycznych: Konstruuje zapytania w sposób zapobiegający generowaniu treści stronniczych, dyskryminujących lub niezgodnych z etyką zawodową i polityką organizacji.Weryfikacji wyników pod kątem wycieków: Analizuje odpowiedzi wygenerowane przez AI w celu sprawdzenia, czy model nie ujawnia w sposób niejawny informacji, które powinny pozostać chronione	Opracowuje prompt do analizy obszernego dokumentu urzędowego, stosując technikę usuwania danych osobowych (PII - Personally Identifiable Information) przy jednoczesnym zachowaniu kontekstu merytorycznego.Demonstruje proces weryfikacji i „czyszczenia” zapytania z elementów mogących sugerować tożsamość osób, których dotyczy sprawa (np. zmiana lokalizacji, dat, unikalnych cech zdarzeń).Tworzy zestaw instrukcji systemowych (System Prompts), które wymuszają na modelu AI odmowę przetwarzania danych niezgodnych z procedurą bezpieczeństwa organizacji.	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik po zakończeniu usługi szkoleniowej wykazuje gotowość do:Odpowiedzialnego działania w sytuacjach stresowych: Przyjmuje postawę opartą na spokoju i rzetelności podczas identyfikacji naruszenia, co pozwala na skuteczne powstrzymanie skutków incydentu.Transparentnej komunikacji kryzysowej: Rozumie wagę niezwłocznego raportowania anomalii do odpowiednich jednostek (np. IOD, dział IT) zgodnie z etyką zawodową i dobrem organizacji.Promowania kultury bezpieczeństwa: Wykazuje inicjatywę w uświadamianiu współpracowników o ryzykach i współdziała w zespole w celu minimalizacji skutków błędów ludzkich.Etycznego podejścia do danych: Przestrzega zasad poufności i integralności informacji, kierując się interesem publicznym oraz ochroną prywatności osób, których dane dotyczą	Demonstruje postawę zgodną z procedurą zgłaszania incydentów podczas symulowanego ataku, nie ulegając presji czasu wywieranej przez napastnika.Uzasadnia konieczność podjęcia natychmiastowych działań mitygujących (np. izolacja zainfekowanego urządzenia) w kontekście odpowiedzialności za zasoby cyfrowe firmy.Proponuje usprawnienia w komunikacji międzyzespołowej na wypadek wystąpienia cyberataku, wykazując troskę o ciągłość procesów administracyjnych	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

Filar I: Architektura Oporności i Higiena Cyfrowa 2.0

Moduł koncentruje się na budowie technicznych fundamentów „Defense in Depth" (obrony głębokiej) w nowoczesnych środowiskach pracy.

- **Hardening Systemów i Środowisk:** Metodyka uszczelniania konfiguracji OS (Windows/Linux), segmentacja procesów oraz zarządzanie uprawnieniami w celu redukcji powierzchni ataku (Attack Surface Management).
- **Ekosystem Tożsamości (Identity Security):** Projektowanie systemów uwierzytelniania progresywnego. Implementacja strategii *Zero Trust* oraz kontrola dostępów uprzywilejowanych w relacji człowiek-algorytm.
- **Behawioralne Aspekty Bezpieczeństwa:** Neurobiologia manipulacji w socjotechnice. Budowa odporności organizacji poprzez modelowanie nawyków bezpieczeństwa i przeciwdziałanie inżynierii społecznej.
- **Governance w IT:** Ramy strategicznego nadzoru nad infrastrukturą oraz metodyka szacowania ryzyk operacyjnych i technologicznych.

Filar II: Ramy Normatywne, Prywatność i AI Governance

Zorientowanie na aspekty prawne, etyczne i proceduralne przetwarzania danych w zautomatyzowanym świecie.

- **Inżynieria Prywatności (Privacy Engineering):** Wdrażanie standardów RODO w algorytmach uczenia maszynowego. Zarządzanie integralnością danych i zapobieganie ich niekontrolowanemu wyciekowi do sieci neuronowych.
- **Zgodność i Etyka Algorytmiczna:** Przygotowanie organizacji do wymogów *EU AI Act*. Audytowanie narzędzi pod kątem transparentności, stronniczości i bezpieczeństwa prawnego.
- **Operacyjna Ochrona Informacji:** Praktyczne wykorzystanie technologii deidentyfikacji, syntetyzacji danych i zaawansowanego maskowania treści w obiegach dokumentacji.
- **Standardy Dokumentacji Systemowej:** Tworzenie i implementacja polityk bezpieczeństwa informacji (PBI) oraz instrukcji bezpiecznej eksploatacji systemów IT.

Filar III: Rozpoznawanie Zagrożeń i Wywiad Technologiczny (Threat Intel)

Proaktywne podejście do identyfikacji metod stosowanych przez zaawansowanych adwersarzy.

- **Analiza Taktyk i Procedur (TTPs):** Badanie schematów działania grup APT. Zrozumienie łańcucha ataku (*Cyber Kill Chain*) w kontekście specyficznych celów administracyjnych i biznesowych.
- **Rozpoznanie Operacyjne (OSINT & HUMINT):** Wykorzystanie metod wywiadu jawnoźródłowego do monitorowania zagrożeń i wykrywania prób infiltracji systemów organizacji.
- **Kryminalistyczna Detekcja Manipulacji:** Techniki identyfikacji syntetycznych treści audio-wizualnych (Deepfake). Metody weryfikacji autentyczności komunikatów w kanałach zdalnych.

Filar IV: Telemetria, Nadzór Sieciowy i Analityka Zdarzeń

Techniczne aspekty wykrywania anomalii i ciągłego monitoringu stanu bezpieczeństwa.

- **Analityka Logistyki Informacji:** Zaawansowana korelacja danych z rozproszonych źródeł. Wykorzystanie matematyki statystycznej w wykrywaniu wczesnych sygnałów włamania.
- **Operacyjne Systemy Nadzoru (SOC/SIEM):** Architektura systemów monitorowania zdarzeń. Konfiguracja reguł detekcji i automatyzacja alertów w środowiskach hybrydowych.
- **Audyt Przepływów Sieciowych:** Analiza ruchu na poziomie pakietów. Wykrywanie kanałów exfiltracji danych i nieautoryzowanych połączeń przy użyciu profesjonalnych analizatorów ruchu.

Filar V: Zarządzanie Kryzysowe i Informatyka Śledcza (Incident & Forensics)

Przekucie wiedzy w sprawne działania reakcyjne i zabezpieczenie materiału dowodowego.

- **Scenariusze Reagowania (Incident Response Plans):** Ćwiczenia typu *Tabletop* i symulacje "Live-Fire" odzwierciedlające realne scenariusze naruszeń. Zarządzanie komunikacją wewnątrz i na zewnątrz podmiotu.
- **Neutralizacja i Rekonstrukcja:** Metodyka izolowania zagrożeń, usuwania skutków infekcji oraz przywracania integralności systemów po incydencie.
- **Metodyka Śledztw Cyfrowych (Digital Forensics):** Zabezpieczanie ulotnych dowodów cyfrowych zgodnie z procedurami kryminalistycznymi. Analiza artefaktów systemowych (pamięć RAM, rejestry, systemy plików).
- **Ekspertyza Powłamaniowa:** Wykorzystanie narzędzi do ekstrakcji i analizy danych (np. Autopsy, Magnet) w celu odtworzenia chronologii zdarzeń i identyfikacji sprawcy.

Harmonogram

Liczba pozycji harmonogramu: 0

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

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	13 530,00 PLN
Koszt przypadający na 1 uczestnika netto	11 000,00 PLN
Koszt osobogodziny brutto	338,25 PLN
Koszt osobogodziny netto	275,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Grzegorz Chlebus

Trener biznesu, przedsiębiorca i specjalista w zakresie zarządzania, audytów oraz energetyki odnawialnej.
Certyfikowany trener VCC z ponad 1500 godzin przeprowadzonych szkoleń, w tym autorskich programów edukacyjnych skierowanych do młodego pokolenia przedsiębiorców – ze szczególnym uwzględnieniem tematyki sukcesji w firmach rodzinnych, cyberbezpieczeństwa oraz gospodarki o obiegu zamkniętym (GOZ). Twórca innowacyjnych warsztatów edukacyjnych łączących kompetencje cyfrowe, ekologiczne i strategiczne podejście do zarządzania.
Od wielu lat aktywnie działa jako wspólnik kilku firm, specjalizujących się w usługach marketingowych oraz wsparciu osób fizycznych i przedsiębiorstw znajdujących się w trudnej sytuacji finansowej. Łączy kompetencje doradcze z umiejętnością zarządzania kryzysowego, pomagając klientom odzyskać stabilność i rozwinąć działalność.
Posiada szeroką wiedzę w obszarze systemów zarządzania jakością – jako audytor wewnętrzny systemu zarządzania jakością wg normy PN-EN ISO 9001:2015 wdraża i ocenia skuteczność procesów w organizacjach.
Ekspert w branży nieruchomości – zarządca nieruchomości wielkopowierzchniowych, a także audytor energetyczny i remontowy budynków. Dysponuje tytułem technika urządzeń i systemów energetyki odnawialnej, co pozwala mu łączyć podejście inżynierskie z doradztwem energetycznym i optymalizacją kosztów utrzymania obiektów.

Równolegle rozwija swoją wiedzę prawniczą jako student III roku prawa, dzięki czemu skutecznie łączy wiedzę biznesową

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Skrypt szkoleniowy

Warunki techniczne

Platforma Zoom

Adres

Gdańsk
Gdańsk
woj. pomorskie

Kontakt

GRZEGORZ CHLEBUS

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