



The Synergy of Artificial Intelligence and Cybersecurity

Numer usługi 2026/04/18/200144/3496929

9 955,00 PLN brutto

9 955,00 PLN netto

248,88 PLN brutto/h

248,88 PLN netto/h

332,00 PLN cena rynkowa ⓘ

Marketing Minds
Academy Dawid
Chlebus

Brak ocen dla tego dostawcy

📍 Gdańsk

🏢 Usługa szkoleniowa

📄 stacjonarna

🕒 40:00 h

📅 24.08.2026 do 28.08.2026

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.

The Synergy of Artificial Intelligence and Cybersecurity 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

8

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji

21-08-2026

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

Celem szkolenia jest wyposażenie uczestnika w kompetencje niezbędne do samodzielnej pracy na stanowisku specjalisty ds. bezpieczeństwa IT z elementami AI.

Uczestnik nauczy się oceniać poziom ryzyka cyfrowego w strukturach organizacyjnych.

Uczestnik pozna kluczowe komponenty infrastruktury IT istotne dla utrzymania ciągłości bezpieczeństwa.

Uczestnik nabędzie umiejętność tworzenia i wdrażania dokumentacji polityk bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia techniki inżynierii społecznej wspomagane przez AI (Deepfake, Vishing).	Wyjaśnia różnice między tradycyjnym phishingiem a atakiem typu AI-Generated.	Test teoretyczny
Projektuje bezpieczne i etyczne zapytania (prompty) do analizy danych wrażliwych.	Przeprowadza skuteczną anonimizację dokumentu biurowego przed procesowaniem w AI	Obserwacja w warunkach symulowanych
Wdraża procedury reagowania na incydenty naruszenia bezpieczeństwa danych	Opracowuje plan mitygacji skutków wycieku danych do publicznych modeli AI.	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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Filar I: Fundamenty Cyber-Higieny i Architektura Bezpieczeństwa w Erze AI

Ten moduł koncentruje się na budowie solidnej bazy technicznej, niezbędnej do zrozumienia zaawansowanych mechanizmów obronnych.

- **Architektura systemów operacyjnych (OS Security):** Analiza bezpiecznych konfiguracji systemów Windows i Linux, zarządzanie uprawnieniami oraz izolacja procesów w celu minimalizacji powierzchni ataku.
- **Zarządzanie tożsamością i dostępem (IAM/MFA):** Wdrażanie rygorystycznych polityk uwierzytelniania wieloskładnikowego (MFA) oraz modelu *Least Privilege* w celu zapobiegania nieautoryzowanemu przejęciu kont przez boty i algorytmy AI.
- **Psychologia bezpieczeństwa i czynnik ludzki:** Analiza błędów poznawczych wykorzystywanych w inżynierii społecznej; kształtowanie postawy „Human-Firewall” w organizacji.
- **Zarządzanie (Management Principles):** Wprowadzenie do standardów zarządzania bezpieczeństwem informatycznym i ocena wagi ryzyka w strukturze organizacyjnej.

Filar II: Compliance, RODO i Zarządzanie Danymi w Procesach AI

Moduł dedykowany prawnym i operacyjnym aspektom przetwarzania danych w nowoczesnej administracji.

- **RODO w automatyzacji:** Implementacja mechanizmów ochrony danych osobowych (*Privacy by Design*) w systemach wykorzystujących uczenie maszynowe; zarządzanie ryzykiem wycieku danych do modeli publicznych.
- **Audyt i AI Act:** Analiza zgodności stosowanych narzędzi z nadchodzącymi regulacjami Unii Europejskiej dotyczącymi sztucznej inteligencji; ocena ryzyka systemów AI.
- **Zaawansowane techniki ochrony prywatności:** Praktyczne zastosowanie pseudonimizacji i anonimizacji dokumentacji służbowej przed procesowaniem jej przez algorytmy zewnętrzne.
- **Polityki bezpieczeństwa:** Projektowanie i wdrażanie sformalizowanych dokumentów regulujących zasady ochrony informacji wewnątrz podmiotu.

Filar III: Threat Intelligence i Ofensywne Zastosowania AI

Zaawansowana analiza ekosystemu zagrożeń i rozpoznawanie metod stosowanych przez wyspecjalizowane grupy przestępcze.

- **Analiza grup APT (Advanced Persistent Threats):** Profilowanie motywacji, celów i unikalnych taktyk stosowanych przez państwowe i komercyjne grupy hakerskie.
- **Operacyjny Threat Intelligence:** Wykorzystanie danych strategicznych i taktycznych do przewidywania kierunków ataków; wstęp do białego wywiadu (OSINT) w identyfikacji zagrożeń.
- **Detekcja Deepfake i manipulacji:** Metody identyfikacji zmanipulowanych komunikatów audio-wizualnych (vishing, impersonacja) tworzonych przy pomocy AI w celach dezinformacyjnych i wyłudzeń.

Filar IV: Monitoring, Systemy SIEM i Analityka Logistyki Danych

Skoncentrowanie się na technicznych aspektach nadzoru nad infrastrukturą sieciową w czasie rzeczywistym.

- **Agregacja i korelacja logów:** Potęga logistyki danych w wykrywaniu incydentów; nauka łączenia rozproszonych zdarzeń systemowych w spójne scenariusze ataków.
- **Narzędzia klasy SIEM i monitoring:** Przegląd i konfiguracja systemów do zarządzania informacją i zdarzeniami bezpieczeństwa (np. Splunk).
- **Analiza ruchu sieciowego:** Wykorzystanie analizatorów protokołów (np. Wireshark) do identyfikacji anomalii, tunelowania danych i prób exfiltracji informacji.

Filar V: Warsztat Operacyjny – Incident Response i Forensics

Praktyczne zastosowanie wiedzy w symulowanych warunkach kryzysowych i analizie powłamaniowej.

- **Symulacja Incydentu (Blue Team Workshop):** Udział w praktycznych ćwiczeniach odzwierciedlających realny atak na organizację; nauka mitygacji skutków i komunikacji kryzysowej.
- **Zarządzanie cyklem życia incydentu:** Fazy detekcji, izolacji (Containment), eliminacji zagrożenia (Eradication) oraz odzyskiwania sprawności systemów (Recovery).
- **Informatyka śledcza (Forensics Fundamentals):** Zasady zabezpieczania dowodów cyfrowych; analiza śladów pozostawionych w systemach Windows i Linux (analiza powłamaniowa).
- **Analiza Forensyczna:** Korzystanie ze specjalistycznego oprogramowania (np. Autopsy) w celu identyfikacji i dokumentacji przebiegu włamania

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	9 955,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	9 955,00 PLN
Koszt osobogodziny brutto	248,88 PLN
Koszt osobogodziny netto	248,88 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

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

prezentacji, materiałów poglądowych, wideo tutorialów, 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 dostępna 24/7, 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 miesiące po zakończeniu kursu.

Informacje dodatkowe

Zapewniamy rozwój i bezpieczną przyszłość każdemu człowiekowi w świecie nowych technologii. Dzięki autorskim rozwiązaniom dopasowujemy sposób nauczania przez Internet do indywidualnych potrzeb, a nasi Mentorzy i Mentorki są niezawodnym wsparciem w zdobywaniu umiejętności potrzebnych na współczesnym rynku pracy.

Kursant otrzymuje dostęp do platformy, na której są zamieszczone wszystkie niezbędne materiały dzięki czemu może uczyć się w dowolnym dla siebie momencie. Kluczową przewagą szkolenia jest nauka zdalna, elastyczna, dopasowana do zajęć podopiecznych, bez względu na miejsce zamieszkania.

Mentorzy, bazując na wieloletnim doświadczeniu w branży, wprowadzają w świat pracy w IT oraz zapewniają kursantom wsparcie podczas lekcji na żywo, prowadzonych dwa razy w tygodniu, w formie: videochatu live i codziennych konsultacji na chacie pisanim.

Adres

Gdańsk
Gdańsk
woj. pomorskie

Kontakt



GRZEGORZ CHLEBUS

E-mail chlebusek@wp.pl

Telefon (+48) 798 009 221