AI BUSINESS LAB

WERSJA 1.0 · WRZESIEŃ 2026

DOKUMENT PUBLICZNY

CYBERSECURITY CAPABILITIES

Zakres usług bezpieczeństwa

Zakres usług bezpieczeństwa AI Business Lab: co realizujemy sami, co z certyfikowanymi partnerami i na jakich standardach się opieramy.

DOSTAWCA

CLEARWISE sp. z o.o.

marka AI Business Lab · NIP 5833541389 · KRS 0001181410

KONTAKT

kontakt@aibusinesslab.pl

umowy, NDA i DPA: legal@aibusinesslab.pl

01 Zakres usług

- **Audyt cyberbezpieczeństwa**
  Poczta i domena, Microsoft 365 lub Google Workspace, strona, dostępy i kopie zapasowe. Lista ryzyk z priorytetami.
- **Audyt agentów AI, LLM, MCP i RAG**
  Testy prompt injection, wycieków danych i uprawnień narzędzi w chatbotach, agentach i bazach wiedzy.
- **Bezpieczne AI w organizacji**
  Shadow AI, polityka korzystania z AI, firmowe konta i szkolenie wymagane przez AI Act.
- **NIS2 i ustawa o KSC**
  Kwalifikacja podmiotu, przegląd gotowości, plan wdrożenia. Audyt ustawowy z certyfikowanym partnerem.
- **Monitoring i zabezpieczanie**
  Stała opieka: domena i poczta, strona, aktualizacje, kopie zapasowe, wycieki haseł, raport okresowy.
- **Testy penetracyjne**
  Aplikacje, API i infrastruktura. Realizuje certyfikowany partner, my prowadzimy zakres i wdrożenie poprawek.
- **Pomoc po incydencie**
  Zhakowana strona, przejęta poczta lub konto, ransomware. Ograniczenie skutków, zgłoszenia i zalecenia.

02 Realizacja: sami i z partnerami

Realizujemy sami	Z certyfikowanym partnerem
Audyt cyberbezpieczeństwa	Testy penetracyjne aplikacji, API i infrastruktury
Audyt agentów AI, LLM, MCP i RAG	Audyt ustawowy KSC
Shadow AI, polityka AI, szkolenia	Informatyka śledcza i odzyskiwanie danych po ransomware
NIS2: kwalifikacja, przegląd gotowości, plan	Socjotechnika (kampanie phishingowe)
Monitoring i zabezpieczanie	Całodobowe centrum SOC / EDR

Realizujemy sami	Z certyfikowanym partnerem
Pomoc po incydentach (strony, poczta, konta)	

Partnera i kwalifikacje osób wykonujących prace partnerskie przedstawiamy w ofercie, przed podpisaniem umowy. Odpowiadamy za zakres, koordynację, raport i weryfikację poprawek.

03 Audyt cyberbezpieczeństwa

Audyt cyberbezpieczeństwa AI Business Lab obejmuje siedem obszarów: domenę i pocztę (SPF, DKIM, DMARC, przekierowania, reguły skrzynek), tożsamość i dostęp w Microsoft 365 lub Google Workspace (uwierzytelnianie wieloskładnikowe, konta uprzywilejowane, aplikacje z dostępem do danych), stronę internetową i aplikacje udostępnione w internecie, stacje robocze i aktualizacje, kopie zapasowe i odtwarzanie, narzędzia AI używane w firmie oraz procedury reagowania na incydenty. Każde ustalenie ma dowód, ocenę ryzyka i rekomendację. Po wdrożeniu poprawek sprawdzamy ponownie ustalenia krytyczne i wysokie.

04 Audyt bezpieczeństwa systemów AI

Audyt bezpieczeństwa agentów AI to kontrolowane testy systemów opartych na modelach językowych: chatbotów dla klientów, wewnętrznych asystentów, agentów wykonujących działania przez narzędzia i serwery MCP (Model Context Protocol) oraz systemów RAG, które odpowiadają na podstawie dokumentów firmy. Sprawdzamy odporność na prompt injection bezpośredni i pośredni (przez treść maila, dokumentu lub strony), możliwość wycieku danych między użytkownikami i z bazy wiedzy, zakres uprawnień narzędzi, obsługę sekretów, rejestrowanie działań agenta i miejsca, w których decyzję musi zatwierdzić człowiek. Opieramy się na OWASP Top 10 for LLM Applications i MITRE ATLAS. Wynikiem jest raport z dowodami i plan zabezpieczeń.

05 Bezpieczeństwo AI w organizacji

Shadow AI to narzędzia sztucznej inteligencji używane w firmie bez wiedzy osób odpowiedzialnych za IT i dane: prywatne konta ChatGPT, darmowi asystenci, wtyczki do przeglądarki, nagrywarki spotkań. Usługa AI Business Lab obejmuje mapę narzędzi AI w organizacji i danych, które do nich trafiają, ocenę ryzyka każdego narzędzia, przeniesienie zespołu na konta firmowe z wyłączonym trenowaniem modeli na danych, krótką politykę korzystania z AI oraz szkolenie, które pomaga spełnić obowiązek zapewnienia wiedzy o AI z art. 4 AI Act (obowiązuje od 2 lutego 2025 r.).

06 Przygotowanie do NIS2 i ustawy o KSC

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (ustawa z 23 stycznia 2026 r., Dz.U. 2026 poz. 252) wdraża dyrektywę NIS2 i obowiązuje od 3 kwietnia 2026 r. Obejmuje podmioty kluczowe i ważne z kilkunastu sektorów, zwykle średnie i duże firmy, a w części sektorów niezależnie od wielkości. Nakłada m.in. obowiązek systemu zarządzania bezpieczeństwem informacji, zgłaszania poważnych incydentów i odpowiedzialność

kierownictwa. AI Business Lab ustala, czy i jako jaki podmiot firma podlega ustawie, przeprowadza przegląd gotowości (porównanie stanu firmy z wymaganiami) i przygotowuje plan wdrożenia. Audyt ustawowy wykonuje certyfikowany audytor partnera.

07 Monitoring bezpieczeństwa i utrzymanie

Monitoring bezpieczeństwa AI Business Lab to stała opieka nad elementami, które najczęściej prowadzą do incydentów w małych i średnich organizacjach: konfiguracją domeny i poczty (SPF, DKIM, DMARC i raporty o podszywaniu się), ważnością certyfikatów, aktualizacjami stron i systemów, kopiami zapasowymi z okresowym testem odtworzenia, wyciekami haseł firmowych kont, kontami z uprawnieniami administratora oraz narzędziami AI z dostępem do danych. Klient dostaje alerty o problemach i okresowy raport z listą zmian. Usługa nie jest całodobowym centrum SOC. Zakres reakcji i czasy obsługi zapisujemy w umowie.

08 Testy penetracyjne (z partnerem)

Test penetracyjny to kontrolowana, uzgodniona z klientem próba ataku na wybrane systemy: aplikacje webowe i mobilne, API, infrastrukturę sieciową, środowiska chmurowe i systemy AI. AI Business Lab realizuje testy penetracyjne z certyfikowanym partnerem specjalizującym się w testach ofensywnych. Przed umową przedstawiamy partnera i kwalifikacje osób wykonujących testy. Odpowiadamy za ustalenie zakresu i zasad testów, koordynację, raport z dowodami i oceną ryzyka oraz retest poprawek. Testy agentów AI, LLM i MCP prowadzimy sami jako część audytu systemów AI.

09 Reagowanie na incydenty bezpieczeństwa

AI Business Lab pomaga firmom po czterech najczęstszych incydentach: zainfekowanej lub podmienionej stronie WordPress (czyszczenie plików i bazy, usunięcie obcych kont, aktualizacje, prośba do Google o ponowne sprawdzenie), przejętej skrzynce Microsoft 365, Google Workspace lub u dostawcy hostingu (odzyskanie dostępu, wylogowanie obcych sesji, usunięcie ukrytych reguł przekierowań, uwierzytelnianie wieloskładnikowe), przejętym koncie w mediach społecznościowych oraz zaszyfrowanych plikach po ataku ransomware. Przy ransomware ustalamy pierwsze kroki, zabezpieczamy ślady i angażujemy partnera specjalizującego się w reagowaniu na incydenty i odzyskiwaniu danych. Zgłoszenia przyjmujemy formularzem i mailem. Nie świadczymy jeszcze całodobowej interwencji.

10 Standardy i punkty odniesienia

- CIS Controls: przegląd zabezpieczeń organizacji
- OWASP WSTG i API Security Top 10: aplikacje i API
- OWASP Top 10 for LLM Applications, MITRE ATLAS: systemy AI

- MITRE ATT&CK: scenariusze ataków
- Ustawa o krajowym systemie cyberbezpieczeństwa (NIS2), RODO, AI Act (art. 4)

11 Certyfikaty i kwalifikacje

Pozycja	Status
OpenAI Select Partner	Program OpenAI Partner Network, od 25 września 2026 r.
Certyfikaty specjalistów (np. OSCP, CISSP, CEH)	**[DO UZUPEŁNIENIA: Do uzupełnienia imiennie po uzyskaniu lub przy zespołach partnerskich w ofercie.]**
Uprawnienia audytora KSC	Audyt ustawowy KSC wykonuje audytor partnera z uprawnieniami z art. 16 ustawy o KSC, przedstawiany imiennie w ofercie.
ISO/IEC 27001 (organizacja)	W przygotowaniu do certyfikacji. Jednostkę certyfikującą i datę podamy po uzyskaniu certyfikatu.

Kontakt

Zakres i harmonogram przygotowujemy po krótkiej rozmowie.

PROJEKTY I DOKUMENTY
kontakt@aibusinesslab.pl

UMOWY, NDA, DPA
legal@aibusinesslab.pl

SPÓŁKA
CLEARWISE sp. z o.o., ul. Zawodzie 20, 80-726 Gdańsk

REJESTR
KRS 0001181410 · NIP 5833541389 · REGON 542127749