AI BUSINESS LAB

WERSJA 1.0 · WRZESIEŃ 2026

DOKUMENT PUBLICZNY

SECURITY ASSESSMENT METHODOLOGY

Metodologia audytu

Jak prowadzimy audyty cyberbezpieczeństwa i AI Security: etapy, zasady testów, skala ocen ryzyka, format raportu i ochrona danych klienta.

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 Etapy audytu

Etap	Opis
1. Zakres i zasady	Ustalamy cel, systemy, osoby kontaktowe, okno prac i to, czego nie dotykamy. Podpisujemy NDA i, jeśli przetwarzamy dane osobowe, umowę powierzenia.
2. Zebranie informacji	Rozmowa z IT i właścicielami procesów, przegląd konfiguracji i dokumentów. Pracujemy na dostępach tylko do odczytu, chyba że zakres mówi inaczej.
3. Weryfikacja techniczna	Sprawdzamy konfigurację i zachowanie systemów: domena i poczta, tożsamość i uprawnienia, strona i aplikacje, kopie zapasowe, narzędzia AI.
4. Ocena ryzyka	Każde ustalenie ma dowód, ocenę wpływu i prawdopodobieństwa oraz poziom: krytyczny, wysoki, średni, niski lub informacyjny.
5. Raport i omówienie	Podsumowanie dla zarządu, szczegóły dla IT, plan naprawczy z kolejnością i właścicielami. Omawiamy wyniki na spotkaniu.
6. Weryfikacja poprawek	Po wdrożeniu zmian sprawdzamy ponownie ustalenia krytyczne i wysokie. Raport dostaje aktualizację statusu.

02 Skala ocen ryzyka

Poziom	Definicja
Krytyczny	Możliwe przejęcie kont, systemów lub danych bez dodatkowych warunków. Naprawa natychmiast.
Wysoki	Poważny wpływ przy realnym scenariuszu ataku. Naprawa w najbliższym cyklu prac.
Średni	Wpływ ograniczony albo wymaga dodatkowych warunków. Naprawa planowa.
Niski	Utrudnienie dla atakującego lub dobra praktyka. Do rozważenia.
Informacyjny	Obserwacja bez bezpośredniego ryzyka, przydatna przy planowaniu.

Poziom wynika z oceny wpływu (skutek wykorzystania) i prawdopodobieństwa (łatwość wykorzystania, wymagane warunki). Przy ustaleniach z oceną CVSS podajemy ją dodatkowo.

03 Zasady testów

- Pisemna zgoda właściciela systemów i zakres z listą systemów, adresów i kont.
- Okno prac i osoby kontaktowe po obu stronach, kanał pilnego kontaktu.
- Działania nieodwracalne (wysyłka, zapis, usuwanie) wyłącznie na kopii, środowisku testowym lub po zgodzie.
- Ustalenia krytyczne zgłaszamy od razu, nie czekając na raport.
- Zakaz testów obciążeniowych i socjotechniki bez osobnej zgody.

04 Ochrona danych klienta

- NDA i umowa powierzenia przed startem.
- Dostępy tylko do odczytu, gdy to możliwe; konta imienne, bez współdzielenia haseł.
- Dowody (zrzuty, logi, zapisy rozmów z systemami AI) w szyfrowanej lokalizacji, dostęp tylko dla zespołu projektu.
- Usunięcie danych i dowodów po zakończeniu, w terminie z umowy, z potwierdzeniem.

05 Format raportu

Część	Zawartość
Podsumowanie dla zarządu	Najważniejsze ryzyka, skutki biznesowe, decyzje do podjęcia (1-2 strony)
Zakres i metoda	Systemy, okres, ograniczenia, wykorzystane standardy
Ustalenia	Opis, dowód, wpływ, prawdopodobieństwo, poziom, rekomendacja, odniesienie do standardu
Plan naprawczy	Kolejność, właściciel po stronie klienta, szacowana pracochłonność
Weryfikacja	Status ustaleń krytycznych i wysokich po poprawkach

06 Audyt systemów AI

- Model i polecenia systemowe: prompt injection, obchodzenie instrukcji, ujawnienie promptu.
- Dane i RAG: uprawnienia do dokumentów, wycieki między użytkownikami, zatrute źródła.
- Narzędzia i MCP: zakres uprawnień, działania bez zgody, zaufanie do serwerów zewnętrznych.
- Operacje: sekrety, rejestrowanie działań agenta, limity kosztów, akceptacja człowieka.
- Punkty odniesienia: OWASP Top 10 for LLM Applications, MITRE ATLAS.

Kontakt

Metodologię dopasowujemy do zakresu i wymagań organizacji klienta.

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