Whitepaper bezpieczeństwa

Enterprise Security Overview - AI Interview Analyzer

Dostawca:	AI Interview Analyzer Sp. z o.o.
Adres:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Klasyfikacja:	PUBLIC
Data:	24.06.2026

Contents

Whitepaper bezpieczeństwa

Dostawca: AI Interview Analyzer Sp. z o.o., Warszawa, Poland

Odbiorcy: Zespoły ds. bezpieczeństwa przedsiębiorstw, IT oraz zakupów

Klasyfikacja: Publiczna

1. Podsumowanie wykonawcze

AI Interview Analyzer to korporacyjna platforma rekrutacyjna, która za wyraźną zgodą kandydata rejestruje rozmowy kwalifikacyjne, transkrybuje je i porządkuje, a następnie dostarcza rekruterom oparte na dowodach wsparcie w ocenie. Ponieważ platforma przetwarza dane osobowe kandydatów i wspiera procesy zatrudnienia, bezpieczeństwo i prywatność są traktowane jako podstawowe ograniczenia projektowe, a nie funkcje dodane później.

Niniejszy whitepaper opisuje w sposób konkretny i weryfikowalny, jak chronimy dane klientów i kandydatów. Został przygotowany z myślą o osobach oceniających dostawców: inżynierach bezpieczeństwa, administratorach IT, inspektorach ochrony danych oraz działach zakupów. Każda wartość liczbowa w tym dokumencie pochodzi bezpośrednio z naszych własnych systemów inżynieryjnych, a nie z materiałów marketingowych.

Główny przekaz jest prosty: **nie tylko deklarujemy, że platforma jest bezpieczna — my to stale testujemy.** Nasza baza kodu zawiera **3,171 zautomatyzowanych testów**, w tym dedykowany zestaw testów bezpieczeństwa obejmujący uwierzytelnianie, autoryzację, izolację między organizacjami, zabezpieczenia przed atakami typu injection oraz usuwanie danych. Dodatkowo uruchamiamy powtarzalny mechanizm testów penetracyjnych względem aktywnych wdrożeń i sporządzamy pisemne raporty z audytu. W siedmiu wewnętrznych audytach bezpieczeństwa przeprowadzonych w marcu i kwietniu 2026 odnotowaliśmy **zero krytycznych ustaleń**, a nasz najnowszy audyt zakończył się werdyktem **PASS**. (Formalna certyfikacja tych zabezpieczeń przez stronę trzecią znajduje się na naszej mapie drogowej; zob. Sekcja 18.)

Cecha bezpieczeństwa	Podsumowanie
Hosting	Microsoft Azure, wyłącznie regiony UE
Model sieciowy	Private endpoints, segmentacja sieci w modelu default-deny, brak publicznej bazy danych
Szyfrowanie	AES-256 w spoczynku, TLS 1.2 lub nowszy w tranzycie
Tożsamość	Krótkotrwałe podpisane tokeny, haszowanie haseł bcrypt, obsługa SSO
Kontrola dostępu	Kontrola dostępu oparta na rolach z rygorystyczną izolacją per organizacja
Sekrety	Scentralizowany sejf sekretów z dostępem opartym na managed identity
Prywatność	Wyraźna zgoda, konfigurowalna retencja, usuwanie jako jednej jednostki
Responsible AI	Wyłącznie wsparcie decyzji, człowiek zawsze uczestniczy w procesie
Zapewnienie	3,171 zautomatyzowanych testów oraz cykliczne testy penetracyjne i audyty

1.1 Jak czytać ten dokument

Sekcje 3 do 11 opisują mechanizmy zabezpieczające dane: architekturę, sieć, tożsamość, aplikację, ochronę danych, prywatność oraz bezpieczny cykl życia wytwarzania oprogramowania. Sekcje 12 i 13 obejmują nasz wyróżniający się program ciągłego testowania oraz historię audytów. Sekcje 14 do 17 dotyczą operacji, modelowania zagrożeń, zarządzania podatnościami oraz mapowania zgodności. Aneksy zawierają katalog mechanizmów kontrolnych, FAQ dla audytorów oraz słownik, z którego zespół bezpieczeństwa może korzystać bezpośrednio podczas oceny.

2. Zakres dokumentu i podejście

2.1 Co obejmuje ten dokument

Niniejszy whitepaper obejmuje architekturę bezpieczeństwa i praktyki usługi AI Interview Analyzer: środowisko hostingowe, projekt sieci, zarządzanie tożsamością i dostępem, mechanizmy kontroli na poziomie aplikacji, ochronę danych, zgodność z prywatnością i regulacjami, bezpieczny cykl życia wytwarzania oprogramowania oraz nasz program ciągłego testowania bezpieczeństwa.

2.2 Co czyni go weryfikowalnym

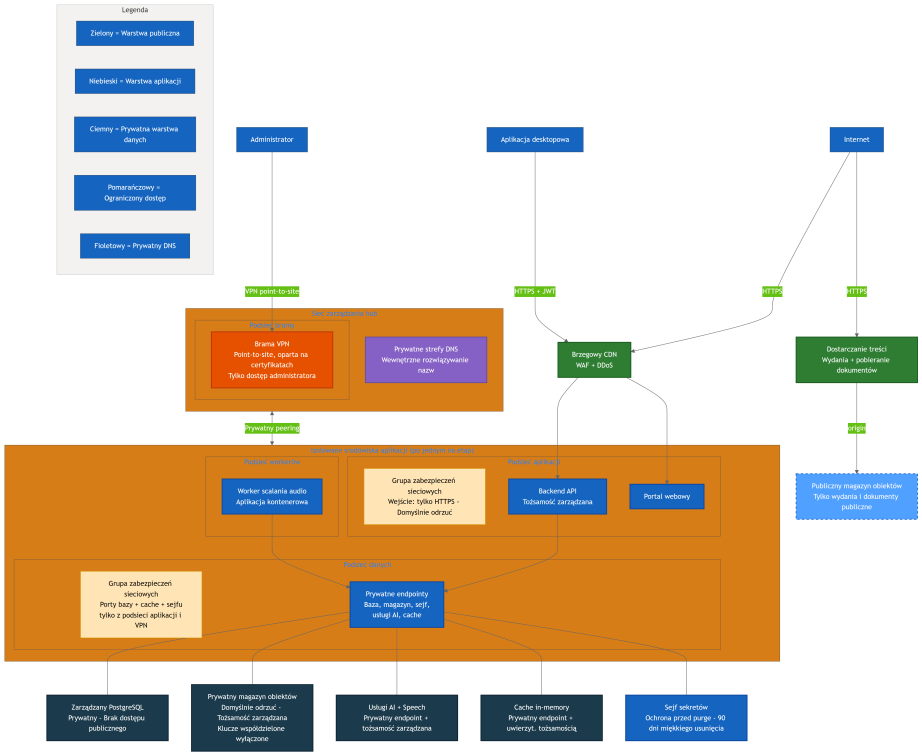
Deklaracje dostawców dotyczące bezpieczeństwa łatwo napisać, ale trudno im zaufać. Dlatego każdą główną tezę tego dokumentu powiązaliśmy z czymś konkretnym i mierzalnym w naszych systemach inżynieryjnych: mechanizmem kontrolnym zaimplementowanym w kodzie, testem potwierdzającym działanie tego mechanizmu, definicją infrastruktury wymuszającą jego stosowanie lub raportem z audytu dokumentującym przeprowadzoną kontrolę. Gdy dany mechanizm znajduje się na naszej przyszłej mapie drogowej, a nie jest jeszcze wdrożony, wskazujemy to wprost. Wolimy zadeklarować mniej i być wiarygodni, niż zadeklarować zbyt wiele i zostać na tym przyłapani.

2.3 Współdzielona odpowiedzialność

Platforma jest dostarczana jako software as a service. Odpowiadamy za infrastrukturę, aplikację, pipeline AI oraz przetwarzanie danych. Klient odpowiada za zarządzanie własnymi kontami użytkowników i rolami, konfigurowanie okien retencji danych zgodnie z własną polityką wewnętrzną oraz zapewnienie uzyskania zgody kandydata za pośrednictwem przepływu zgody udostępnianego przez platformę. Sekcja 14 opisuje ten podział bardziej szczegółowo.

3. Przegląd architektury bezpieczeństwa

Platforma została zbudowana jako niewielka liczba współpracujących usług, a nie jako pojedynczy monolit. Klientami są aplikacja desktopowa oraz portal webowy. Centralne backend API obsługuje całą trwałość danych, uwierzytelnianie, rozliczenia, pipeline AI, zgodę, pocztę e-mail, obsługę plików oraz dashboardy. Worker łączenia audio przetwarza nagrania asynchronicznie. Cały wrażliwy stan znajduje się za backend API; klienci nigdy nie komunikują się bezpośrednio z bazą danych, storage ani usługami AI.



Powyższy diagram przedstawia topologię produkcyjną z celowo uogólnionymi nazwami zasobów. Widoczne są w nim trzy zasady:

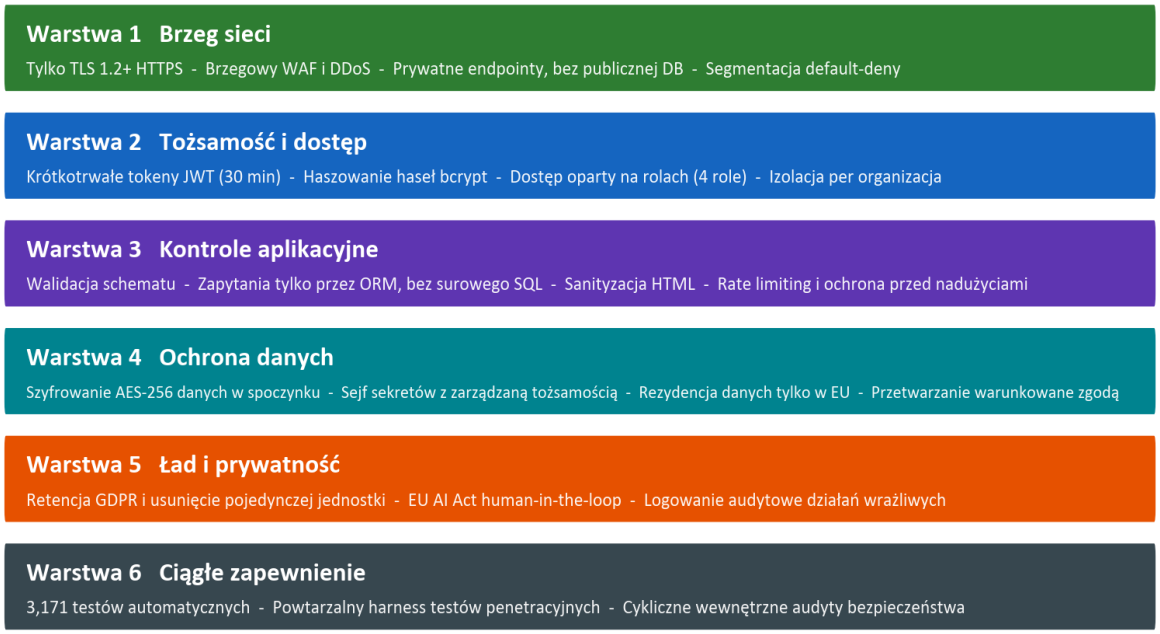
- **Brak bezpośredniej ekspozycji usług danych.** Baza danych, prywatny object storage, usługi AI oraz cache mają wyłączony publiczny dostęp sieciowy i są osiągalne wyłącznie przez private endpoints wewnątrz odizolowanej sieci wirtualnej. Sejf sekretów jest osiągany przez aplikację przez private endpoint i dodatkowo chroniony uwierzytelnianiem tożsamości platformowej oraz politykami dostępu o najmniejszych uprawnieniach, tak że każdy dostęp wymaga ważnej, autoryzowanej tożsamości niezależnie od ścieżki sieciowej.
- **Oddzielona powierzchnia publiczna.** Jedyny publiczny object storage przechowuje pliki wydań i dokumenty publiczne. Nigdy nie zawiera danych kandydatów. Ruch aplikacyjny skierowany do klientów przechodzi przez warstwę brzegową zapewniającą web application firewall, ochronę przed distributed-denial-of-service oraz dostarczanie treści.
- **Dostęp administracyjny jest kontrolowany.** Operatorzy uzyskują dostęp do zasobów wewnętrznych wyłącznie przez point-to-site VPN oparty na certyfikatach do sieci zarządzającej typu hub, a nie przez publiczny internet.

Każdy etap wdrożenia (development i production) jest w pełni odizolowanym środowiskiem z własną siecią, kontami storage, bazą danych i sekretami. Dane produkcyjne klientów nigdy nie występują w środowiskach niższych. Współdzielony hub zarządzający zawiera wyłącznie bramę VPN i prywatny DNS, prywatnie sparowany z każdym środowiskiem.

4. Defense in Depth

Żaden pojedynczy mechanizm kontrolny nie jest uznawany za wystarczający do powstrzymania każdego ataku. Platforma stosuje warstwowe, niezależne zabezpieczenia, tak aby awaria jednej warstwy nie prowadziła do ujawnienia danych. Warstwy poniżej są każda zaimplementowana i, jak opisano w Sekcji 12, testowana indywidualnie.

Warstwowy model bezpieczeństwa: niezależne kontrole na każdym poziomie



Warstwa	Reprezentatywne mechanizmy kontrolne
Brzeg sieci	Transport wyłącznie TLS, brzegowy WAF i ochrona DDoS, private endpoints, segmentacja default-deny
Tożsamość i dostęp	Krótkotrwałe podpisane tokeny, haszowanie bcrypt, kontrola dostępu oparta na rolach, izolacja per organizacja
Aplikacja	Walidacja schematu dla wszystkich danych wejściowych, dostęp do danych wyłącznie przez ORM, kodowanie danych wyjściowych, rate limiting
Ochrona danych	Szyfrowanie w spoczynku, sejf sekretów z managed identity, rezydencja danych w UE, przetwarzanie warunkowane zgodą
Nadzór i prywatność	Konfigurowalna retencja, usuwanie jako jednej jednostki, human-in-the-loop AI, rejestrowanie audytowe
Ciągłe zapewnienie	Zautomatyzowany zestaw testów, powtarzalne testy penetracyjne, cykliczne wewnętrzne audyty bezpieczeństwa

Dalsza część dokumentu omawia kolejno każdą warstwę, a następnie opisuje, jak stale udowadniamy, że te warstwy pozostają skuteczne.

5. Bezpieczeństwo sieci

5.1 Prywatność domyślnie

Warstwa danych jest prywatna z założenia. Zarządzana baza PostgreSQL ma wyłączony publiczny dostęp sieciowy i jest osiągalna wyłącznie przez private endpoint. Prywatny object storage jest skonfigurowany tak, aby domyślnie odmawiać dostępu sieciowego, całkowicie wyłącza współdzielone klucze dostępu i jest dostępny wyłącznie przez managed identity z podsieci aplikacyjnej. Cache, usługi AI oraz sejf sekretów są analogicznie osiągane przez private endpoints z prywatnym rozwiązywaniem DNS.

W praktyce oznacza to, że nie istnieje internet-facing connection string do bazy danych ani publiczny URL storage dla audio kandydatów: publiczny dostęp sieciowy do bazy danych i prywatnego storage jest całkowicie wyłączony. Sejf sekretów jest osiągany przez aplikację przez private endpoint i chroniony uwierzytelnianiem tożsamości platformowej oraz politykami dostępu o najmniejszych uprawnieniach, przy czym tożsamości aplikacyjne otrzymują wyłącznie uprawnienia odczytu do sekretów, których potrzebują, więc sekretów nie można pobrać bez ważnej, autoryzowanej tożsamości. Powierzchnia ataku, której zewnętrzny przeciwnik może w ogóle dotknąć, ogranicza się do endpointów HTTPS aplikacji za warstwą brzegową.

5.2 Segmentacja sieci

Każde środowisko jest podzielone na oddzielne podsieci dla warstwy aplikacyjnej, warstwy danych oraz workera asynchronicznego. Każda podsieć jest zarządzana przez network security group, której końcowa reguła odrzuca cały ruch przychodzący. Podsieć aplikacyjna akceptuje wyłącznie przychodzący HTTPS. Podsieć danych akceptuje wyłącznie określone porty bazy danych, cache i sejfu oraz tylko z podsieci aplikacyjnej lub administracyjnego VPN. Oznacza to, że nawet napastnik, który w jakiś sposób dotarłby do warstwy aplikacyjnej, nie może swobodnie przemieszczać się do warstwy danych; dozwolone są tylko te ścieżki, z których aplikacja korzysta zgodnie z przeznaczeniem.

5.3 Warstwa brzegowa

Publiczny ruch aplikacyjny jest obsługiwany przez warstwę brzegową zapewniającą web application firewall, ochronę DDoS oraz content delivery network. Pobieranie wydań i dokumentów jest obsługiwane z dedykowanego publicznego konta storage przez front door dostarczania treści, całkowicie oddzielonego od prywatnego storage przechowującego dane kandydatów. Te dwie płaszczyzny storage nigdy się nie mieszają: błędna konfiguracja płaszczyzny publicznej nie może ujawnić prywatnych danych kandydatów, ponieważ są to różne konta z różnymi regułami sieciowymi.

5.4 Dostęp administracyjny

Nie istnieje publiczny administracyjny endpoint do sieci prywatnej. Operatorzy łączą się przez bramę point-to-site VPN wykorzystującą uwierzytelnianie oparte na certyfikatach. Administracyjny dostęp do bazy danych i cache jest możliwy wyłącznie wewnątrz tego tunelu, ponieważ usługi te mają wyłączony publiczny dostęp sieciowy. Dzięki temu codzienne operacje są całkowicie odseparowane od publicznego internetu.

6. Zarządzanie tożsamością i dostępem

6.1 Uwierzytelnianie

Sesje użytkowników są ustanawiane przy użyciu podpisanego tokenu dostępu ważnego przez trzydzieści minut, sparowanego z oddzielnym, nieprzezroczystym, przechowywanym po stronie serwera tokenem odświeżania. Tokeny dostępu są weryfikowane przy każdym żądaniu, a użytkownik jest ponownie walidowany względem bazy danych (w tym pod kątem aktywności konta), zamiast polegać wyłącznie na zawartości tokenu. Wylogowanie natychmiast unieważnia sesję odświeżania po stronie serwera, więc przechwycony token odświeżania nie może pozostać ważny po wylogowaniu.

Hasła nigdy nie są przechowywane w postaci jawnego tekstu. Są haszowane z użyciem bcrypt i unikalnej soli dla każdego hasła. Dla organizacji preferujących single sign-on platforma obsługuje logowanie OAuth z Microsoft i Google; w takim przypadku żadne hasło nie jest w ogóle przechowywane.

Własność adresu e-mail jest weryfikowana przy użyciu jednorazowego, ograniczonego czasowo linku weryfikacyjnego, zanim samodzielnie zarejestrowane konto zostanie uznane za zweryfikowane, a ponowne wysyłki wiadomości weryfikacyjnych podlegają rate limiting, aby zapobiegać nadużyciom.

6.2 Kontrola dostępu oparta na rolach

Autoryzacja jest egzekwowana przez model ról z czterema rolami o rosnącym poziomie uprawnień: interviewer, hiring manager, recruiter oraz administrator. Dostęp do operacji uprzywilejowanych jest wymuszany przez zależności po stronie serwera sprawdzające zarówno rolę, jak i status weryfikacji wywołującego. Te kontrole ról zabezpieczają znacznie ponad sto odrębnych operacji API.

Rola	Typowe uprawnienia
Interviewer	Prowadzi przypisane rozmowy; widzi wyłącznie rozmowy przypisane do siebie
Hiring manager	Zarządza rekrutacjami, które posiada lub których jest członkiem
Recruiter	Pełne zarządzanie rekrutacjami i kandydatami w ramach organizacji
Administrator	Ustawienia organizacji, rozliczenia, administracja użytkownikami i kluczami API

Poza ogólnymi kontrolami ról platforma stosuje zasady widoczności na poziomie danych. Hiring managerowie widzą wyłącznie rekrutacje, które utworzyli lub których są członkami; interviewerzy widzą wyłącznie przypisane im rozmowy. Uprawnienia są więc egzekwowane zarówno na poziomie „jaką akcję”, jak i „które rekordy”.

6.3 Izolacja per organizacja

Platforma jest wielodostępna (multi-tenant), a izolacja tenantów jest traktowana jako mechanizm bezpieczeństwa pierwszej klasy. Każda uwierzytelniona tożsamość zawiera identyfikator organizacji, a zapytania o dane są ograniczane do tej organizacji. Gdy użytkownik żąda rekordu należącego do innej organizacji, platforma zwraca odpowiedź „not found” zamiast ujawniać, że taki rekord istnieje. Wewnętrzne identyfikatory bazy danych nigdy nie są eksponowane na interfejsie; API prezentuje identyfikatory wyświetlane i mapuje je ponownie dla każdego żądania, co eliminuje powszechną klasę ataków enumeracyjnych między tenantami.

Nie jest to wyłącznie założenie projektowe. Jak opisano w Sekcji 12, nasz zautomatyzowany zestaw uruchamia szeroką macierz międzyorganizacyjną, która próbuje uzyskać dostęp do danych jednej organizacji przy użyciu poświadczeń innej organizacji i potwierdza, że każda taka próba kończy się niepowodzeniem.

6.4 Dostęp programistyczny

Na potrzeby integracji organizacje w kwalifikujących się planach mogą wydawać klucze API. Klucze używają rozpoznawalnego prefiksu, zawierają 128 bitów entropii i są przechowywane wyłącznie jako hash; surowy klucz jest wyświetlany jednorazowo przy utworzeniu i nigdy ponownie. Każdy klucz ma jawnie zdefiniowany zakres uprawnień (odczyt, zapis lub integracja ATS), może być

ograniczony do określonych sieci źródłowych, może zostać natychmiast unieważniony oraz podlega limitom szybkości per klucz wynikającym z poziomu planu organizacji. Weryfikacja klucza używa porównania timing-safe, aby zapobiec ujawnianiu informacji przez czasy odpowiedzi.

7. Bezpieczeństwo aplikacji

Aplikacja została napisana tak, aby eliminować całe kategorie podatności, a nie łatać je przypadek po przypadku.

- **Injection.** Cały dostęp do bazy danych odbywa się przez object-relational mapper z parametryzowanymi zapytaniami. Baza kodu nie zawiera surowego SQL formatowanego jako string. Taka konstrukcja strukturalnie eliminuje SQL injection.
- **Walidacja danych wejściowych.** Każde ciało żądania jest walidowane względem ścisłego schematu, zanim trafi do logiki biznesowej. Nadmiernie duże ładunki są odrzucane, a endpointy listujące są stronicowane, aby ograniczać zużycie zasobów.
- **Kodowanie danych wyjściowych i cross-site scripting.** Tekst dostarczony przez użytkownika i wygenerowany przez AI jest traktowany jako niezaufany. Tam, gdzie treść musi zostać wyrenderowana jako HTML, przechodzi przez sanitizer oparty na liście dozwolonych elementów w momencie zapisu, a dedykowany zestaw testów potwierdza, że tagi script, event handlery oraz URL-e javascript są usuwane.
- **Mass assignment.** Operacje aktualizacji korzystają z jawnych schematów, które wykluczają uprzywilejowane pola, takie jak rola, organizacja i saldo kredytów, dzięki czemu klient nie może eskalować uprawnień przez przesłanie dodatkowych pól.
- **Rate limiting.** Endpointy uwierzytelniania i podatne na nadużycia podlegają rate limiting przy użyciu trwałego limitera opartego na bazie danych, który przetrwa restarty i działa poprawnie w wielu instancjach aplikacji. Logowanie, rejestracja, reset hasła i ponowne wysyłki weryfikacji mają własne limity. Rozpoznawanie adresu IP klienta zostało utwardzone przeciw spoofingowi nagłówków przekierowujących.
- **Webhooki.** Przychodzące webhooki od dostawców płatności i e-mail są weryfikowane względem podpisów dostawcy na surowym ciele żądania przed przetworzeniem.
- **Przesyłanie plików.** Uploady mają ograniczony rozmiar, są walidowane, przechowywane pod wygenerowanymi identyfikatorami zamiast nazw dostarczonych przez użytkownika oraz ograniczane per żądanie i per organizacja.
- **Nagłówki bezpieczeństwa.** W środowisku produkcyjnym odpowiedzi zawierają strict transport security, opcje content-type i frame, politykę referrer oraz restrykcyjną politykę permissions, a także ukrywają bannery serwera i frameworka.

8. Ochrona danych

8.1 Szyfrowanie

Wszystkie dane są szyfrowane w spoczynku z użyciem AES-256 przez warstwy szyfrowania storage i bazy danych platformy Azure. Cały ruch sieciowy jest obsługiwany wyłącznie przez HTTPS z użyciem TLS 1.2 lub nowszego; jawny HTTP jest przekierowywany do HTTPS na każdej warstwie. W środowisku produkcyjnym API i portal webowy emitują nagłówki strict transport security wraz z zestawem nagłówków utwardzających oraz ukrywają bannery wersji serwera i frameworka.

8.2 Zarządzanie sekretami

Sekrety aplikacyjne są przechowywane w scentralizowanym sejfie sekretów z włączoną ochroną purge protection i dziewięćdziesięciodniowym oknem soft-delete. Aplikacje uwierzytelniają się do zasobów Azure przy użyciu system-assigned managed identities zamiast długowiecznych kluczy; na przykład prywatny storage ma całkowicie wyłączone współdzielone klucze dostępu, więc dostęp jest możliwy wyłącznie przez przypisania ról oparte na tożsamości, ograniczone do konkretnego zasobu. Polityki dostępu do sejfu przyznają podmiotom aplikacyjnym wyłącznie uprawnienia odczytu do określonych sekretów, których potrzebują, zgodnie z zasadą najmniejszych uprawnień.

8.3 Rezydencja danych

Wszystkie dane klientów i kandydatów są przechowywane i przetwarzane na terenie Unii Europejskiej. Hosting aplikacji, baza danych, storage, cache i sekrety znajdują się w West Europe, a przetwarzanie AI odbywa się w regionach UE. Dostawca AI nie wykorzystuje danych klientów do trenowania swoich modeli.

8.4 Cykl życia pojedynczej rozmowy

Najbardziej przejrzystym sposobem zrozumienia mechanizmów ochrony danych jest prześledzenie jednej rozmowy od początku do końca. Zgoda jest pozyskiwana i rejestrowana przed rozpoczęciem jakiegokolwiek przetwarzania. Przesyłanie jest szyfrowane w tranzycie. Transkrypcja i analiza odbywają się w centrach danych w UE. Wyniki są zapisywane do szyfrowanego storage. Każdy rekord podlega następnie jednemu zegarowi retencji, który kończy się rejestrowanym, kaskadowym usunięciem. W dowolnym momencie prawa kandydata, takie jak wycofanie zgody, usunięcie, dostęp czy przenoszalność, mogą ten przepływ przerwać.

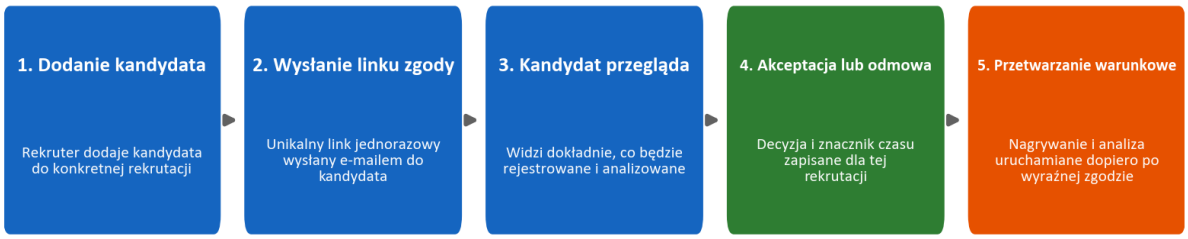
9. Privacy by Design i GDPR

Prywatność jest wbudowana w model danych i przepływ pracy, a nie dołączona wyłącznie przez politykę.

9.1 Zgoda

Żadna rozmowa nie jest nagrywana ani analizowana bez wyraźnej zgody kandydata. Gdy kandydat zostaje dodany do rekrutacji, platforma wysyła unikalny, jednorazowy link zgody e-mailem. Kandydat zapoznaje się z tym, co się wydarzy, i akceptuje lub odmawia. Stan zgody, w tym czas odpowiedzi, jest rejestrowany względem tej konkretnej rekrutacji, tak aby zgoda zawsze była ograniczona do konkretnego procesu zatrudnienia, a nie udzielana globalnie.

Zgoda kandydata: jawna i zarejestrowana przed jakimkolwiek przetwarzaniem

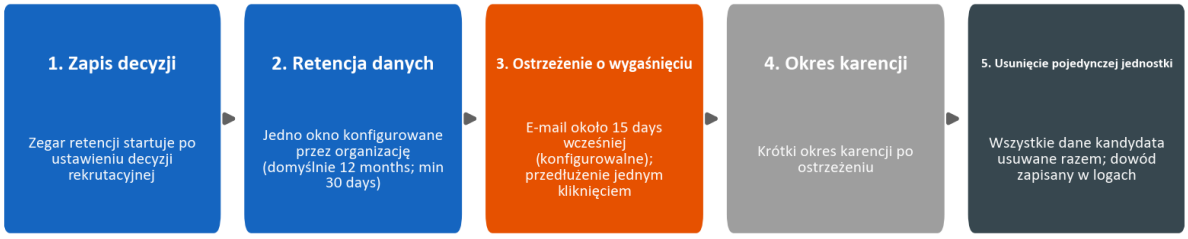


9.2 Retencja i usuwanie

Retencja danych jest konfigurowalna per organizacja, z domyślnym okresem dwunastu miesięcy i konfigurowalnym minimum trzydziestu dni, oraz może być nadpisana per kandydat. Istnieje jeden zegar retencji dla danych kandydata, a nie osobny licznik dla każdego artefaktu. Zegar rozpoczyna się w momencie zarejestrowania decyzji rekrutacyjnej. Przed wygaśnięciem danych platforma wysyła ostrzeżenie (domyślnie około piętnastu dni wcześniej) i oferuje przedłużenie jednym kliknięciem. Gdy dane są usuwane, usuwane są jako jedna jednostka: rekord kandydata, rozmowy, transkrypcje, nagrania audio, dokumenty i porównania są usuwane łącznie, a usunięcie jest rejestrowane w dzienniku audytowym. Nie pozostają żadne częściowe ani osierocone pozostałości.

Poniższy cykl życia pokazuje ten pojedynczy zegar i sposób, w jaki prowadzi on do jednego kaskadowego usunięcia z rejestrowanym dowodem usunięcia.

Retencja danych: jeden zegar na kandydata, usunięcie pojedynczej jednostki



9.3 Prawa osób, których dane dotyczą, i subprocesorzy

Platforma wspiera prawa osób, których dane dotyczą, wymagane przez GDPR, w tym dostęp, usunięcie, przenoszalność, sprzeciw i wyjaśnienie. Przetwarzanie odbywa się na podstawie umowy powierzenia przetwarzania danych, którą klienci akceptują

podczas rejestracji i która jest wersjonowana per organizacja. Nasi subprocesorzy oraz ich role, wszyscy w UE lub objęci odpowiednimi zabezpieczeniami, są ujawnieni w tej umowie, a klienci otrzymują wcześniejsze powiadomienie o każdej zmianie. Sekcja 17 zawiera rejestr subprocesorów i mapowanie zgodności artykuł po artykule.

10. Responsible AI i EU AI Act

Platforma należy do kategorii wysokiego ryzyka zgodnie z EU AI Act, ponieważ wspiera decyzje dotyczące zatrudnienia, i traktujemy tę klasyfikację poważnie.

Definiującą zasadą produktu jest to, że **AI stanowi wsparcie decyzji, a nie podejmuje decyzje.** System nigdy automatycznie nie akceptuje ani nie odrzuca kandydata. Transkrybuje mowę, porządkuje pytania i odpowiedzi, ocenia odpowiedzi względem kryteriów zdefiniowanych przez rekrutera oraz przygotowuje projekt informacji zwrotnej, a człowiek przegląda każdy wynik przed jego użyciem. Dzięki temu człowiek pozostaje jednoznacznie w pętli decyzyjnej.

Równie istotne jest to, czego AI nie robi. Nie ocenia osobowości, „dopasowania kulturowego", stanu emocjonalnego, tonu głosu, akcentu, płci, wieku, pochodzenia etnicznego, wyglądu ani mowy ciała. Ocena jest zakotwiczona w dowodach z transkryptu oraz w kryteriach zdefiniowanych przez rekrutera, a imiona kandydatów są wyłączane z danych wejściowych do oceny, aby ograniczać bias. Publikujemy kartę przejrzystości, dokumentację użytkownika oraz deklarację zgodności opisujące system, jego ograniczenia i zabezpieczenia.

Mechanizm Responsible-AI	Jak działa
Human in the loop	Każda ocena i każdy fragment informacji zwrotnej są przeglądane przez rekrutera przed użyciem
Brak zautomatyzowanych decyzji	System nigdy automatycznie nie akceptuje ani nie odrzuca kandydata
Ocena oparta na dowodach	Oceny odwołują się do potwierdzających dowodów z transkryptu
Projekt ograniczający bias	Imiona wyłączone z oceny; oceniana jest treść ponad styl
Ograniczenia zakresu	Osobowość, emocje, akcent i cechy chronione nigdy nie są oceniane
Bezpieczeństwo informacji zwrotnej dla kandydata	Prywatna informacja zwrotna dla kandydata przechodzi przez zabezpieczenie generation-and-validation

Te ograniczenia są nie tylko opisane w dokumentacji; są zakodowane w warstwie promptów AI i testowane przez dedykowany program testów bezpieczeństwa AI opisany w Sekcji 12.3.

11. Bezpieczny cykl życia wytwarzania oprogramowania

Bezpieczeństwo jest egzekwowane w sposobie, w jaki budujemy i dostarczamy oprogramowanie, a nie wyłącznie w działającym systemie.

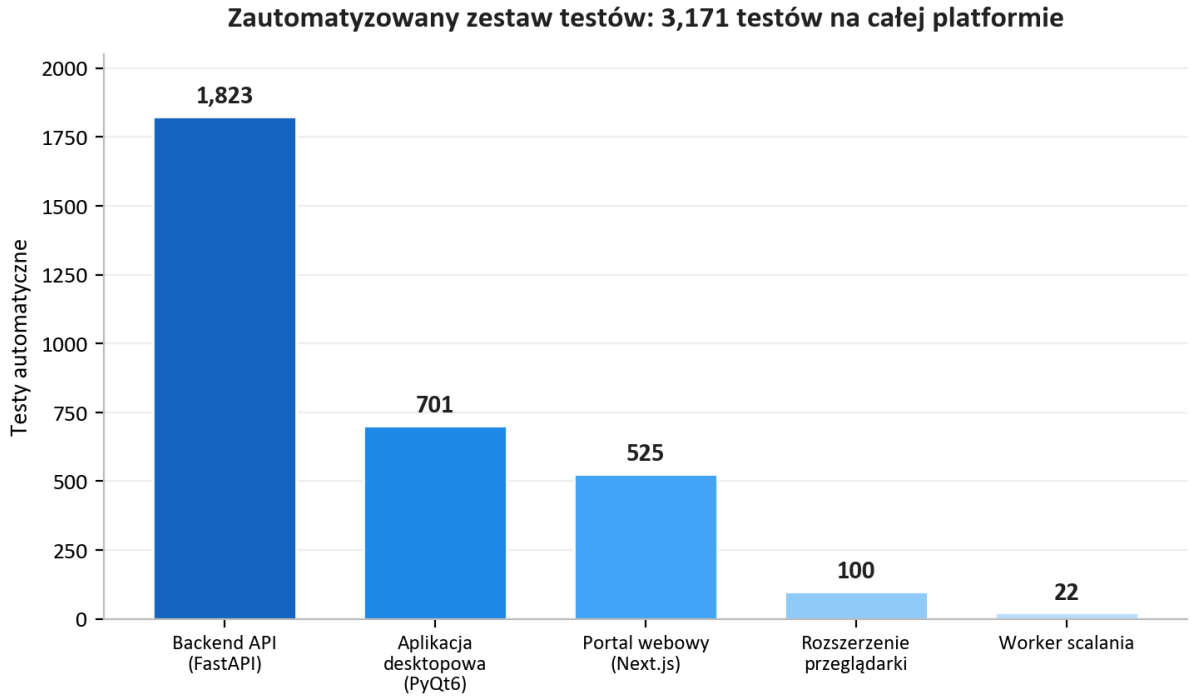
- **Separacja środowisk.** Development i production są całkowicie oddzielone, każde z własną infrastrukturą, kontami storage, bazą danych, sekretami i subdomenami. Nie istnieje żaden współdzielony stan.
- **Infrastructure as code.** Całe środowisko chmurowe jest definiowane jako kod i przeglądane jako kod, co sprawia, że postawa bezpieczeństwa jest audytowalna i powtarzalna. Audytor może dokładnie odczytać, które porty są otwarte, które zasoby są prywatne i które tożsamości mają jakie uprawnienia.
- **Przypięte, kontrolowane wdrożenia.** Każdy krok w pipeline continuous-integration jest przypięty do dokładnej, niezmiennej wersji. Wdrożenia produkcyjne są oparte na tagach, uruchamiane wyłącznie przez chroniony pipeline produkcyjny i objęte wymaganą aprobatą. Zautomatyzowany zestaw testów działa jako brama wydania: wdrożenie nie może zostać opublikowane, jeśli testy zakończą się niepowodzeniem.
- **Higiena zależności.** Zautomatyzowane monitorowanie zależności proponuje aktualizacje co tydzień w backendzie, desktopie, warstwie webowej, infrastrukturze i definicjach pipeline, a audyty zależności są częścią naszego okresowego przeglądu bezpieczeństwa.
- **Podpisane artefakty.** Instalatory desktopowe są podpisywane cyfrowo, dzięki czemu klienci mogą zweryfikować, że instalowane oprogramowanie rzeczywiście pochodzi od nas.
- **Dyscyplina sekretów.** Sekrety znajdują się w sejfie oraz w chronionych sekretach pipeline, nigdy w kodzie źródłowym.

12. Ciągłe testowanie bezpieczeństwa

To jest sedno naszej narracji dotyczącej zapewnienia bezpieczeństwa i obszar, którego większość dostawców nie potrafi wykazać. Traktujemy bezpieczeństwo jako coś, co należy stale mierzyć za pomocą wykonywalnych kontroli, a nie jednorazowo deklarować.

12.1 Zautomatyzowany zestaw testów

Platforma jest objęta **3,171 zautomatyzowanymi testami** obejmującymi backend API, aplikację desktopową, portal webowy, rozszerzenie przeglądarki oraz worker łączenia audio.



Nie są to wyłącznie testy funkcjonalne. Znacząca, dedykowana część testów bezpieczeństwa wykonuje mechanizmy kontrolne opisane wcześniej w tym dokumencie. Poniższy wykres przedstawia podział testów bezpieczeństwa w backend API według domen.

Wśród wielu innych ten zestaw obejmuje rozbudowaną macierz publicznego API, która uruchamia każdy endpoint jako legalny użytkownik, jako własny klucz API organizacji oraz jako klucz API konkurencyjnej organizacji, potwierdzając, że każda próba międzyorganizacyjna jest blokowana. Obejmuje dziesiątki testów powierzchni ataku o charakterze adwersarialnym dla spoofingu forwarding headers, header injection i wycieku identyfikatorów, ukierunkowany zestaw sanitizacji HTML dla cross-site scripting, testy egzekwowania ról dla pełnego modelu ról oraz testy dowodzące, że dane kandydata są rzeczywiście usuwane jako jedna jednostka. Ponieważ testy te działają jako brama wydania, regresja osłabiająca którykolwiek z tych mechanizmów kontrolnych zatrzyma wydanie, zamiast trafić do klientów.

12.2 Testy penetracyjne na żywym środowisku

Zautomatyzowane testy jednostkowe dowodzą, że mechanizmy kontrolne zachowują się poprawnie w izolacji. Aby wykazać, że współdziałają one poprawnie w rzeczywistym wdrożeniu, utrzymujemy powtarzalną metodologię testów penetracyjnych, która uruchamia rzeczywiste skrypty ataków przeciwko aktywnemu środowisku. Jest ona zorganizowana w sześciu fazach:

Faza	Obszar	Przykłady wykonywanych kontroli
1. Analiza statyczna	Kod źródłowy	Sekrety, wzorce injection, niebezpieczne funkcje, brak auth, niebezpieczny HTML
2. Przegląd architektury	Infrastruktura	Private endpoints, segmentacja, TLS, konfiguracja sekretów
3. Analiza wektorów ataku	Kontrola źródła i chmura	Ochrona branchy, zakres tożsamości, ekspozycja publiczna
4. Testy penetracyjne na żywo	Działające środowisko	Sondowanie bez uwierzytelnienia, dostęp między organizacjami, injection, manipulacja tokenami, SSRF, bursty limitów szybkości
5. Punktacja korporacyjna	Dojrzałość	Szesnaście kategorii bezpieczeństwa ocenianych względem korporacyjnej linii bazowej
6. Zależności i supply chain	Ryzyko stron trzecich	Audyt CVE zależności, przypięte akcje pipeline, integralność lock-file

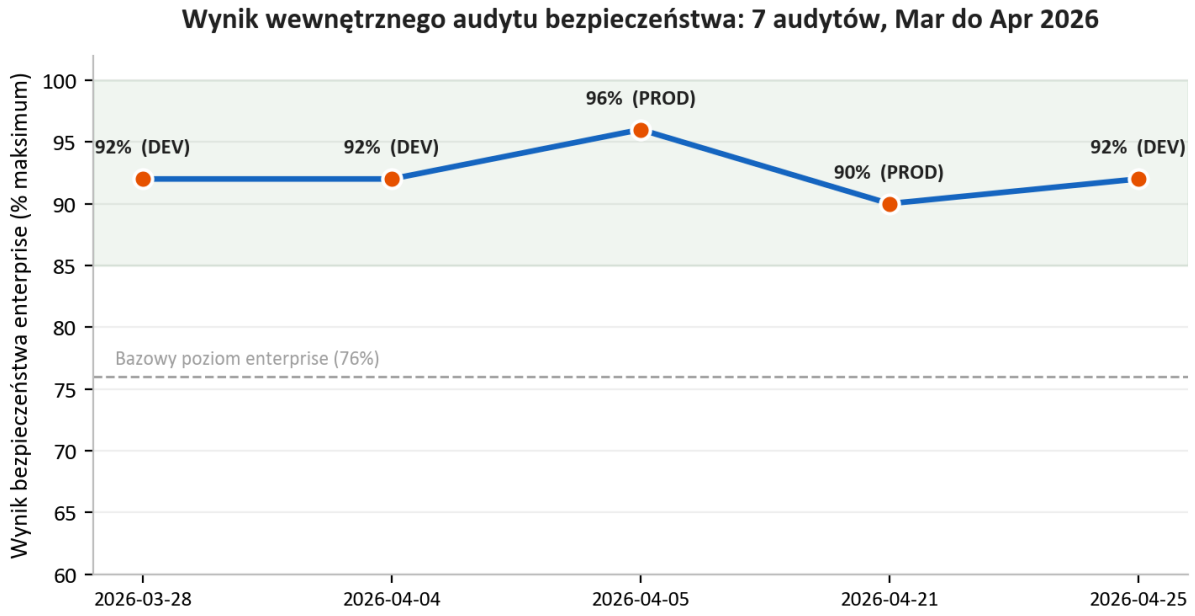
Faza 4 to rzeczywiste testy adwersarialne względem wdrożonego systemu, a nie lista kontrolna. Obejmuje sondowanie chronionych endpointów bez poświadczeń i potwierdzanie odmowy dostępu; rejestrację dwóch organizacji i próby dostępu do rekordów jednej organizacji z konta drugiej; wstrzykiwanie ładunków cross-site-scripting i server-side-template oraz potwierdzanie ich neutralizacji; manipulowanie tokenami uwierzytelniającymi i potwierdzanie ich odrzucenia; próby server-side request forgery względem cloud metadata endpoints; oraz bursty żądań do endpointów uwierzytelniania w celu potwierdzenia, że rate limiting rzeczywiście uruchamia się w aktywnym środowisku, a nie tylko teoretycznie.

12.3 Testowanie bezpieczeństwa informacji zwrotnej dla kandydata

Ponieważ platforma może generować prywatną rozwojową informację zwrotną dla kandydatów, prowadzimy osobny adwersarialny program bezpieczeństwa dla tej funkcji. Celowo dostarcza on systemowi ostre i wrogie notatki rekrutera i potwierdza, że treść skierowana do kandydata nigdy nie zawiera wulgarności, nigdy nie ujawnia ani nie przypisuje tożsamości rekrutera lub jego prywatnej opinii oraz nigdy nie stosuje oceniających etykiet osobowości. Chroni to zarówno kandydata, który powinien otrzymać konstruktywną i pełną szacunku informację zwrotną, jak i klienta, którego wewnętrzna opinia nigdy nie powinna wyciec na zewnątrz.

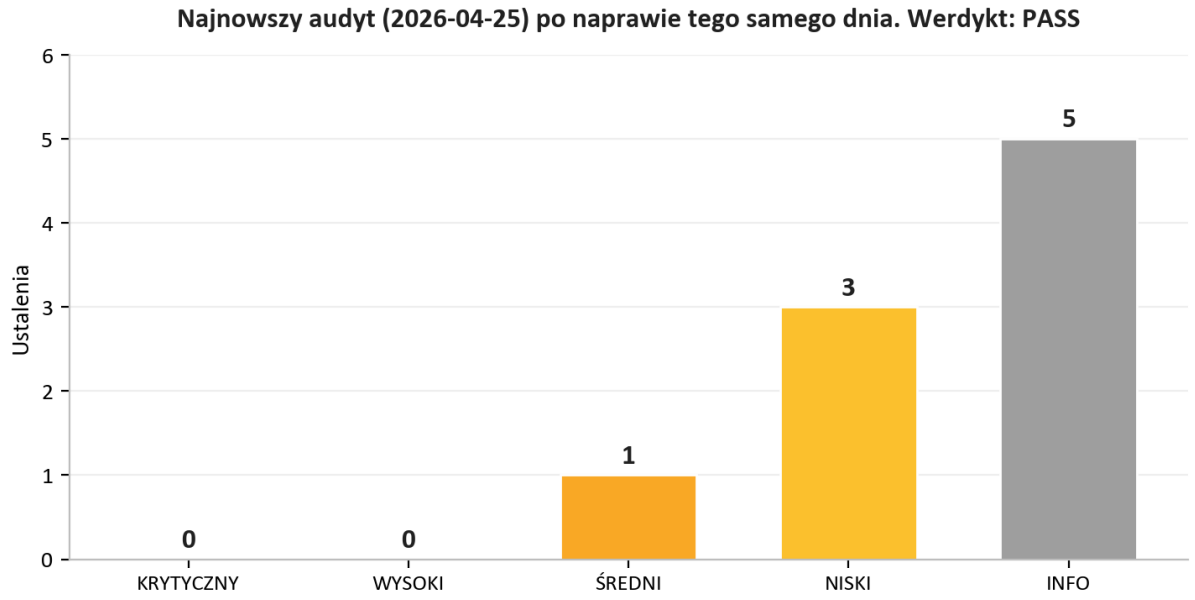
13. Wyniki audytów bezpieczeństwa

Prowadzimy cykliczne audyty bezpieczeństwa z użyciem ustrukturyzowanej, powtarzalnej metodologii testów penetracyjnych i sporządzamy z każdego raport datowany, zawierający ustalenia sklasyfikowane według ważności, materiał dowodowy i działania naprawcze. Są to audyty wewnętrzne realizowane w ramach naszego własnego procesu bezpieczeństwa; formalna certyfikacja tych samych mechanizmów przez stronę trzecią znajduje się na naszej mapie drogowej. Pomiędzy końcem marca a końcem kwietnia 2026 ukończyliśmy **siedem takich audytów** w środowiskach development i production.



Najistotniejszy dla potencjalnego klienta jest wynik dotyczący spójności: **we wszystkich siedmiu audytach odnotowano zero krytycznych ustaleń.** W rzadkich przypadkach, gdy pojawiał się problem o wyższej ważności, był on szybko usuwany, często tego samego dnia, i ponownie weryfikowany. Skala ocen została celowo zaostrzona w tym okresie (maksymalny możliwy wynik został podniesiony wraz z dodawaniem kolejnych kategorii do oceny), dlatego znormalizowana linia wyniku pozostaje wysoka, mimo że poprzeczka została podniesiona.

Nasz najnowszy audyt, z 25 April 2026, dobrze pokazuje, jak ten proces działa w praktyce. Zidentyfikowano dwa problemy o wyższej ważności, oba naprawiono i ponownie zweryfikowano tego samego dnia, a audyt zakończono werdyktem **PASS**, bez pozostających problemów gotowych do wykorzystania w ramach aktualnego modelu zagrożeń.



Audyt	Środowisko	Krytyczne	Werdykt
2026-03-28	Development	0	Gotowe do production
2026-04-04	Development	0	Gotowe dla enterprise
2026-04-05	Production	0	Gotowe dla enterprise
2026-04-20	Development	0	Gotowe do production, uwagi
2026-04-20	Development	0	Pass z uwagami
2026-04-21	Production	0	Bezpieczne, brak możliwych do wykorzystania ustaleń
2026-04-25	Development	0	Pass

Wzorzec widoczny w tych audytach stanowi najbardziej uczciwy dowód, jaki możemy zaoferować: problemy są znajdowane, ponieważ aktywnie ich szukamy, i są szybko zamykane, ponieważ proces został zbudowany właśnie po to, by je zamykać. Dostawca, który nigdy nie raportuje żadnego ustalenia, to zazwyczaj dostawca, który po prostu nie szuka.

14. Odporność operacyjna i współdzielona odpowiedzialność

14.1 Monitorowanie i logowanie

Telemetria aplikacyjna i platformowa trafia do scentralizowanego obszaru roboczego log analytics oraz usługi monitorowania aplikacji, co zapewnia nam wgląd w dostępność i zachowanie systemu. Wrażliwe działania, takie jak usuwanie danych, akceptacja umów prawnych i wywołania AI, są rejestrowane w dedykowanych tabelach audytowych, dzięki czemu istnieje trwały zapis tego, kto zrobił co z istotnymi danymi.

14.2 Kopie zapasowe i odtwarzanie

Zarządzana baza danych przechowuje automatyczne kopie zapasowe, a prywatny storage jest chroniony retencją soft-delete zarówno dla blobów, jak i kontenerów, dzięki czemu przypadkowe lub złośliwe usunięcie może zostać odtworzone w ramach okna retencji. Krytyczna infrastruktura posiada blokady usunięcia zapobiegające przypadkowemu usunięciu zasobów produkcyjnych.

14.3 Podsumowanie współdzielonej odpowiedzialności

Obszar	AI Interview Analyzer	Klient
Infrastruktura, sieć, patching	Tak	-
Bezpieczeństwo aplikacji i pipeline AI	Tak	-
Szyfrowanie, sekrety, rezydencja danych	Tak	-
Administracja użytkownikami i rolami	Zapewnia mechanizmy kontrolne	Zarządza użytkownikami i rolami
Konfiguracja polityki retencji	Zapewnia mechanizmy kontrolne	Ustawia okno retencji
Zgoda kandydata	Zapewnia workflow	Zapewnia jego użycie
Silne poświadczenia użytkowników końcowych i SSO	Obsługuje SSO i politykę	Egzekwuje politykę wewnętrzną

15. Model zagrożeń i mapowanie OWASP

Projektujemy zabezpieczenia pod kątem konkretnego zestawu przeciwników: zewnętrznego atakującego bez poświadczeń, ciekawskiego lub złośliwego uwierzytelnionego użytkownika jednej organizacji próbującego uzyskać dostęp do danych innej organizacji, skompromitowanej zależności oraz błędu wewnętrznego. Poniższa tabela mapuje powszechnie używane kategorie ryzyka OWASP Top 10 na konkretne mechanizmy kontrolne stosowane w tej platformie, z których każdy jest testowany w sposób opisany w Sekcji 12.

Ryzyko OWASP	Jak platforma je ogranicza
Broken access control	Kontrola dostępu oparta na rolach dla każdego uprzywilejowanego endpointu; ograniczanie per organizacja; „not found” przy dostępie cross-org; remapowanie identyfikatorów; macierz testów cross-org
Cryptographic failures	TLS 1.2+ w tranzycie; AES-256 w spoczynku; haszowanie haseł bcrypt; sekrety w zarządzanym sejfie
Injection	Parametryzowane zapytania wyłącznie przez ORM; ścisła walidacja schematów; sanitizacja HTML w momencie zapisu
Insecure design	Warstwowe defense in depth; modelowanie zagrożeń i przegląd architektury w każdym audycie
Security misconfiguration	Infrastructure as code; grupy sieciowe default-deny; nagłówki bezpieczeństwa; wyłączone współdzielone klucze storage; schemat API nie jest eksponowany w production
Vulnerable components	Cotygodniowe zautomatyzowane monitorowanie zależności; audyty CVE zależności w okresowym przeglądzie
Identification and authentication failures	Krótkotrwałe tokeny; login z rate limiting; weryfikacja e-mail; obsługa SSO; brak haseł w postaci jawnej
Software and data integrity failures	Przypięte, niezmienne kroki pipeline; podpisane instalatory desktopowe; weryfikacja podpisów webhooków; wdrożenia produkcyjne kontrolowane tagami
Security logging and monitoring failures	Scentralizowana telemetria; dedykowane tabele audytowe dla działań wrażliwych
Server-side request forgery	Połączenia wychodzące ograniczone do zaufanych endpointów; sondy SSRF w mechanizmie testów penetracyjnych

To mapowanie stanowi kręgosłup naszej argumentacji dotyczącej zapewnienia bezpieczeństwa: dla każdej dobrze znanej klasy ataku istnieje nazwany mechanizm kontrolny, a dla każdego nazwanego mechanizmu kontrolnego istnieje test.

16. Zarządzanie podatnościami i odpowiedzialne ujawnianie

Bezpieczeństwo nigdy nie jest ukończone, dlatego prowadzimy ciągłą pętlę wykrywania i remediacji.

- **Wykrywanie.** Podatności są ujawniane z czterech źródeł: zautomatyzowanego zestawu testów, cyklicznych audytów testów penetracyjnych, zautomatyzowanego monitorowania zależności oraz zgłoszeń od klientów lub badaczy.
- **Triaging.** Każdemu ustaleniu przypisywana jest ważność (critical, high, medium, low lub informational) wraz z materiałem dowodowym i właścicielem remediacji, dokładnie tak jak jest to odnotowywane w naszych raportach audytowych.
- **Cele remediacyjne.** Ustalenia critical i high są priorytetyzowane do natychmiastowej remediacji; w naszej historii audytów problemy o wyższej ważności były zazwyczaj usuwane i ponownie weryfikowane tego samego dnia. Ustalenia medium i niższe są planowane w regularnym cyklu utrzymaniowym.
- **Weryfikacja.** Poprawki są testowane ponownie, a tam, gdzie ma to znaczenie, wykonywana jest kontrola na aktywnym środowisku w celu potwierdzenia, że problem został rzeczywiście zamknięty, a nie tylko usunięty w kodzie.
- **Ujawnianie.** Problemy bezpieczeństwa można zgłaszać bezpośrednio do nas. Potwierdzamy przyjęcie zgłoszeń, prowadzimy analizę i informujemy zgłaszającego aż do momentu rozwiązania problemu.

17. Mapowanie zgodności

17.1 GDPR

Obszar GDPR	Implementacja na platformie
Podstawa prawna (Art. 6)	Wyraźna zgoda kandydata pozyskana przed przetwarzaniem
Minimalizacja danych i ograniczenie przechowywania (Art. 5)	Przetwarzane są wyłącznie dane istotne dla rozmowy; konfigurowalna retencja z automatycznym usuwaniem
Prawo do usunięcia (Art. 17)	Usuwanie wszystkich danych kandydata jako jednej jednostki, z rejestrowanym dowodem usunięcia
Prawa osób, których dane dotyczą (Art. 15 do 20)	Obsługiwane są dostęp, usunięcie, przenoszalność i sprzeciw
Obowiązki procesora (Art. 28)	Umowa powierzenia przetwarzania danych akceptowana przy rejestracji i wersjonowana per organizacja
Bezpieczeństwo przetwarzania (Art. 32)	Szyfrowanie, kontrola dostępu, izolacja i ciągłe testowanie opisane w tym dokumencie
Przejrzystość subprocesorów	Ujawnieni w umowie powierzenia przetwarzania danych z wcześniejszym powiadomieniem o zmianie

17.2 EU AI Act

Platforma jest traktowana jako system AI wysokiego ryzyka wspierający decyzje dotyczące zatrudnienia i utrzymujemy dokumentację zgodną z regulacją, w tym kartę przejrzystości, dokumentację użytkownika oraz deklarację zgodności. Główne zabezpieczenia — nadzór człowieka, przejrzystość, ocena oparta na dowodach oraz ścisłe ograniczenia zakresu tego, co AI ocenia — opisano w Sekcji 10. Kontynuujemy rozwijanie naszej formalnej dokumentacji zgodności wraz z postępem harmonogramu wdrażania regulacji.

17.3 Certyfikacje hostingu

Platforma działa w całości na Microsoft Azure, którego centra danych posiadają niezależne certyfikacje, w tym ISO 27001 oraz SOC 2. Certyfikacje te obejmują warstwy fizyczne i platformowe znajdujące się poniżej naszej aplikacji; mechanizmy kontrolne warstwy aplikacyjnej to te opisane w całym niniejszym dokumencie.

17.4 Rejestr subprocesorów

Sub-procesor	Cel	Region
Microsoft Azure	Hosting, przetwarzanie AI i mowy, storage, transakcyjna poczta e-mail	EU (West Europe, Sweden Central)
Stripe	Przetwarzanie subskrypcji i płatności	EU (Ireland)
Fakturownia	Fakturowanie	EU (Poland)
ATS connector (opcjonalnie)	Integracja z systemem śledzenia kandydatów, włączana wyłącznie na żądanie	EU

18. Mapa drogowa bezpieczeństwa

Traktujemy bezpieczeństwo jako program stale doskonalony. Obecne inicjatywy na naszej mapie drogowej obejmują wzmacnianie opcji multi-factor authentication dla kont administracyjnych, rozbudowę scentralizowanego audytowego logowania dostępu do danych, dalsze regularne zaostrzanie aktualności zależności oraz postęp w formalnej certyfikacji przez stronę trzecią mechanizmów kontrolnych opisanych w tym dokumencie. Żadna z tych inicjatyw nie oznacza luki narażającej dziś dane klientów; każda stanowi ulepszenie już warstwowej postawy bezpieczeństwa.

19. Podsumowanie

AI Interview Analyzer chroni dane kandydatów i klientów za pomocą architektury warstwowej: sieci prywatnej domyślnie, bez publicznych usług danych, silnej tożsamości i izolacji per organizacja, kodu aplikacyjnego eliminującego całe klasy podatności, szyfrowania i rezydencji danych w UE oraz mechanizmów prywatności wbudowanych w model danych. To, co wyróżnia platformę, to dowody stojące za tymi deklaracjami. Dzięki 3,171 zautomatyzowanym testom, powtarzalnej metodologii testów penetracyjnych na żywych środowiskach, dedykowanemu programowi bezpieczeństwa AI oraz historii siedmiu wewnętrznych audytów bezpieczeństwa z zerową liczbą krytycznych ustaleń, możemy pokazać — a nie tylko powiedzieć — że platforma jest bezpieczna.

Aneks A: Katalog mechanizmów kontroli bezpieczeństwa

Skrócone zestawienie głównych mechanizmów kontrolnych i dowodów potwierdzających każdy z nich.

Mechanizm kontrolny	Mechanizm	Dowód
Szyfrowanie transportowe	Wyłącznie HTTPS, TLS 1.2+, przekierowanie HTTP	Infrastructure as code; audyt architektury
Szyfrowanie w spoczynku	Szyfrowanie platformowe AES-256 dla storage i bazy danych	Konfiguracja platformy; audyt architektury
Ochrona haseł	bcrypt z solą per hasło	Kontrola źródła; testy uwierzytelniania
Zarządzanie sesją	30-minute signed tokens, odwoływalne odświeżanie po stronie serwera	Kontrola źródła; testy uwierzytelniania
Autoryzacja	Kontrola dostępu z czterema rolami na uprzywilejowanych endpointach	Zestaw testów egzekwowania ról
Izolacja tenantów	Ograniczanie zapytań per organizacja; 404 przy cross-org	Macierz testów międzyorganizacyjnych
Bezpieczeństwo kluczy API	Przechowywanie w postaci hashy, zakresy uprawnień, limity per klucz	Zestaw testów kluczy API
Ochrona przed injection	Parametryzowane zapytania wyłącznie przez ORM	Analiza statyczna; testy injection
Ochrona przed cross-site scripting	Sanitizacja HTML w momencie zapisu	Zestaw testów sanitizacji HTML
Rate limiting	Trwały limiter oparty na bazie danych dla endpointów auth	Testy limitów szybkości; kontrole burstów na żywo
Integralność webhooków	Weryfikacja podpisu dostawcy na surowym body	Zestaw testów webhooków
Zarządzanie sekretami	Zarządzany sejf, purge protection, managed identity	Infrastructure as code; audyt architektury
Izolacja sieci	Private endpoints; segmentacja default-deny	Infrastructure as code; audyt architektury
Usuwanie danych	Kaskadowe usuwanie jako jednej jednostki z dziennikiem audytowym	Zestaw testów usuwania GDPR
Supply chain	Przypięte kroki pipeline; cotygodniowe monitorowanie zależności	Konfiguracja pipeline; audyt zależności

Aneks B: Najczęściej zadawane pytania dla audytorów bezpieczeństwa

Gdzie przechowywane są nasze dane? W całości na terenie Unii Europejskiej, na Microsoft Azure, w West Europe, z przetwarzaniem AI w regionach UE. Dane kandydatów nigdy nie opuszczają UE.

Czy nasze dane są wykorzystywane do trenowania modeli AI? Nie. Dostawca AI nie wykorzystuje danych klientów do treningu.

Czy baza danych jest osiągalna z internetu? Nie. Publiczny dostęp sieciowy jest wyłączony, a baza danych jest osiągalna wyłącznie przez private endpoint wewnątrz sieci wirtualnej.

Czy jeden klient może zobaczyć dane innego klienta? Nie. Każde zapytanie jest ograniczane do organizacji wywołującego, dostęp między organizacjami zwraca „not found", a zautomatyzowana macierz stale testuje tę izolację.

Jak przechowywane są hasła? W postaci hashy z użyciem bcrypt i unikalnej soli per hasło. Obsługiwane jest również single sign-on z Microsoft i Google, w którym przypadku żadne hasło nie jest przechowywane.

Czy obsługujecie single sign-on? Tak, przez Microsoft i Google OAuth.

Jak długo ważne są tokeny dostępu? Trzydzieści minut, w parze z odwoływalną sesją odświeżania po stronie serwera, która jest unieważniana przy wylogowaniu.

Jak obsługiwana jest zgoda kandydata? Każdy kandydat otrzymuje unikalny, jednorazowy link zgody i musi zaakceptować go przed jakimkolwiek nagrywaniem lub analizą. Zgoda jest rejestrowana względem konkretnego procesu zatrudnienia.

Jak usuwane są dane? Jako jedna jednostka obejmująca rekord kandydata, rozmowy, transkrypcje, audio, dokumenty i porównania, zgodnie z konfigurowalnym harmonogramem retencji, z rejestrowanym dowodem usunięcia. Kandydaci mogą także bezpośrednio zażądać usunięcia.

Czy posiadacie umowę powierzenia przetwarzania danych? Tak, akceptowaną przy rejestracji i wersjonowaną per organizacja, w tym z rejestrem subprocesorów.

Czy AI podejmuje decyzje rekrutacyjne? Nie. Zapewnia wyłącznie wsparcie decyzji; człowiek przegląda każdy wynik i podejmuje wszystkie decyzje.

Jak dowodzicie swoich deklaracji dotyczących bezpieczeństwa? Poprzez 3,171 zautomatyzowanych testów, w tym dedykowany zestaw testów bezpieczeństwa, powtarzalną sześciostopniową metodologię testów penetracyjnych uruchamianą przeciw aktywnym środowiskom, program testów bezpieczeństwa AI oraz cykliczne pisemne raporty z audytów.

Co się dzieje, gdy znajdziecie podatność? Otrzymuje ona ważność wraz z materiałem dowodowym i właścicielem, jest usuwana zgodnie z harmonogramem priorytetów, ponownie weryfikowana — w tym poprzez kontrole na żywo tam, gdzie to istotne — i odnotowywana w raporcie audytowym.

Czy możemy przeprowadzić własny test penetracyjny? Oceny bezpieczeństwa mogą zostać zorganizowane przez opiekuna konta przy odpowiednim zakresie i harmonogramie.

Aneks C: Słownik

Termin	Znaczenie
AES-256	Silny standard szyfrowania symetrycznego stosowany do ochrony danych w spoczynku
bcrypt	Funkcja haszowania haseł zaprojektowana specjalnie do tego celu, z soleniem per hasło
Managed identity	Tożsamość wydawana przez platformę, która pozwala usłudze uwierzytelniać się bez przechowywanych kluczy
Private endpoint	Prywatny adres sieciowy, który utrzymuje usługę chmurową poza publicznym internetem
Network security group	Zestaw reguł zezwalających i odrzucających filtrujących ruch sieciowy do podsieci
RBAC	Kontrola dostępu oparta na rolach, przydzielająca uprawnienia zgodnie z rolą użytkownika
IDOR	Insecure direct object reference, wada kontroli dostępu, przed którą platforma się broni
SSRF	Server-side request forgery, klasa ataku badana w naszych testach penetracyjnych
Web application firewall	Mechanizm brzegowy filtrujący złośliwy ruch webowy
Data processing agreement	Umowa regulująca sposób, w jaki procesor przetwarza dane osobowe w imieniu administratora

Aneks D: Kontakt i kontrola dokumentu

AI Interview Analyzer Sp. z o.o.

ul. Jedrusik 6/53, 01-748 Warszawa, Poland

NIP: 5253079974

W celu przeprowadzenia przeglądu bezpieczeństwa, uzyskania kopii naszej umowy powierzenia przetwarzania danych lub naszej dokumentacji zgodności z EU AI Act prosimy o kontakt z opiekunem konta.

Ten dokument opisuje postawę bezpieczeństwa usługi AI Interview Analyzer na dzień wygenerowania wskazany w stopce. Jest udostępniany do celów ewaluacyjnych i nie stanowi części żadnej umowy. Szczegółowe zobowiązania kontraktowe dotyczące bezpieczeństwa są określone w odpowiedniej umowie oraz umowie powierzenia przetwarzania danych.