Bezpečnostný whitepaper

Enterprise Security Overview - AI Interview Analyzer

Poskytovateľ:	AI Interview Analyzer Sp. z o.o.
Adresa:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Klasifikácia:	PUBLIC
Dátum:	24.06.2026

Contents

Bezpečnostný whitepaper

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

Cieľová skupina: Tímy enterprise security, IT a procurement

Klasifikácia: Verejné

1. Zhrnutie pre vedenie

AI Interview Analyzer je enterprise platforma pre nábor, ktorá so zreteľným súhlasom kandidáta nahráva pohovory, prepisuje ich a štruktúruje a vytvára podporu hodnotenia pre recruiterov založenú na dôkazoch. Keďže platforma spracúva osobné údaje kandidátov a podporuje náborové procesy, bezpečnosť a súkromie sa považujú za primárne návrhové obmedzenia, nie za funkcie doplnené neskôr.

Tento whitepaper konkrétnym a overiteľným spôsobom opisuje, ako chránime údaje zákazníkov a kandidátov. Je napísaný pre ľudí, ktorí hodnotia dodávateľov: bezpečnostných inžinierov, IT administrátorov, pracovníkov ochrany osobných údajov a procurement. Každý údaj v tomto dokumente pochádza priamo z našich vlastných inžinierskych systémov, nie z marketingových materiálov.

Ústredné posolstvo je jednoduché: **netvrdíme iba, že je platforma bezpečná, ale priebežne testujeme, že bezpečná skutočne je.** Náš codebase obsahuje **3,171 automatizovaných testov**, vrátane vyhradenej bezpečnostnej sady, ktorá preveruje authentication, authorization, izoláciu medzi organizáciami, ochranu proti injection a mazanie dát. Okrem toho prevádzkujeme opakovateľný harness na penetration testing proti živým nasadeniam a vytvárame písomné auditné správy. V priebehu siedmich interných bezpečnostných auditov v marci a apríli 2026 sme zaznamenali **zero critical findings**, pričom náš najnovší audit bol uzavretý s verdiktom **PASS**. (Formálna third-party certification týchto kontrol je súčasťou nášho roadmap; pozri časť 18.)

Bezpečnostná charakteristika	Zhrnutie
Hosting	Microsoft Azure, iba regióny EÚ
Sieťový model	Private endpoints, default-deny network segmentation, žiadna verejná database
Šifrovanie	AES-256 v pokoji, TLS 1.2 alebo vyšší pri prenose
Identity	Krátkodobé signed tokens, bcrypt password hashing, podpora SSO
Riadenie prístupu	Role-based access control s prísnou izoláciou podľa organizácie
Secrets	Centralizovaný secrets vault s prístupom cez managed identity
Súkromie	Výslovný súhlas, konfigurovateľná retencia, vymazanie ako jednej jednotky
Responsible AI	Iba podpora rozhodovania, človek vždy v procese
Zabezpečenie	3,171 automatizovaných testov plus opakované penetration tests a audity

1.1 Ako čítať tento dokument

Časti 3 až 11 opisujú kontroly, ktoré chránia dáta: architektúru, sieť, identity, aplikáciu, ochranu dát, súkromie a secure development lifecycle. Časti 12 a 13 pokrývajú náš charakteristický program priebežného testovania a históriu auditov. Časti 14 až 17 sa venujú operations, threat modeling, vulnerability management a mapovaniu compliance. Prílohy poskytujú katalóg kontrol, FAQ pre hodnotiteľov a glosár, ktorý môže bezpečnostný tím priamo použiť počas hodnotenia.

2. Rozsah a prístup dokumentu

2.1 Čo tento dokument pokrýva

Tento whitepaper pokrýva bezpečnostnú architektúru a postupy služby AI Interview Analyzer: hosting environment, návrh siete, identity and access management, kontroly na aplikačnej úrovni, ochranu dát, súlad so súkromím a reguláciami, secure development lifecycle a náš program priebežného bezpečnostného testovania.

2.2 Čo ho robí overiteľným

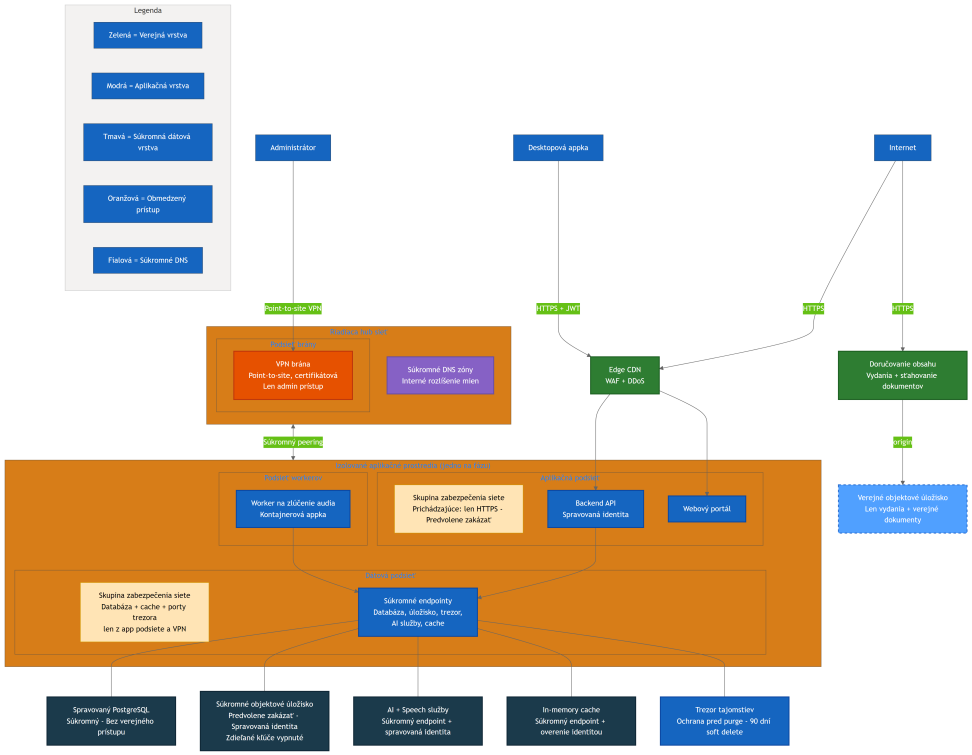
Bezpečnostné tvrdenia dodávateľov sa píšu ľahko a dôveruje sa im ťažko. Každé hlavné tvrdenie v tomto dokumente sme preto naviazali na niečo konkrétne a merateľné v našich inžinierskych systémoch: kontrolu implementovanú v kóde, test dokazujúci, že kontrola funguje, definíciu infraštruktúry, ktorá ju vynucuje, alebo auditnú správu zaznamenávajúcu zdokumentovanú kontrolu. Ak je kontrola súčasťou nášho budúceho roadmap a nie dnešného produkčného stavu, uvádzame to výslovne. Radšej budeme tvrdiť menej a získať dôveru, než tvrdiť priveľa a byť usvedčení z nepresnosti.

2.3 Shared Responsibility

Platforma je poskytovaná ako software as a service. Prevádzkujeme infraštruktúru, aplikáciu, AI pipeline a spracovanie dát. Zákazník je zodpovedný za správu vlastných používateľských účtov a rolí, konfiguráciu retention windows pre dáta podľa svojej internej politiky a za zabezpečenie, že súhlas kandidáta je získaný prostredníctvom workflow na súhlas, ktorý platforma poskytuje. Časť 14 opisuje toto rozdelenie podrobnejšie.

3. Prehľad bezpečnostnej architektúry

Platforma je postavená ako malý počet spolupracujúcich služieb, nie ako jeden monolit. Desktop aplikácia a web portal fungujú ako klienti. Centrálne backend API spravuje všetku persistenciu, authentication, billing, AI pipeline, consent, email, file handling a dashboards. Audio merge worker spracúva nahrávky asynchrónne. Všetok citlivý stav sa nachádza za backend API; klienti nikdy nekomunikujú priamo s database, storage ani AI services.



Vyššie uvedený diagram zobrazuje produkčnú topológiu so zámerne zovšeobecnenými názvami zdrojov. Viditeľné sú v ňom tri princípy:

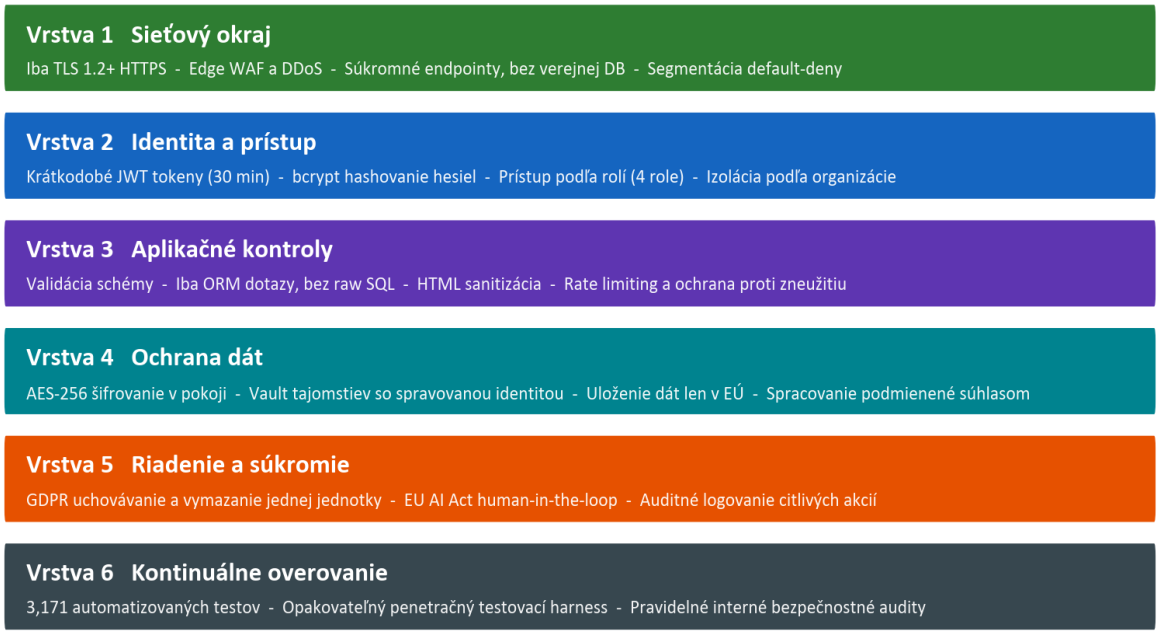
- **Žiadne priame vystavenie dátových služieb.** Database, private object storage, AI services a cache majú vypnutý public network access a sú dostupné iba cez private endpoints v rámci izolovanej virtual network. Secrets vault je aplikáciou dosahovaný cez private endpoint a je dodatočne chránený authentication pomocou platform identity a least-privilege access policies, takže akýkoľvek prístup vyžaduje platnú autorizovanú identitu bez ohľadu na sieťovú cestu.
- **Oddelená verejná plocha.** Jediný public object storage uchováva release downloads a verejné dokumenty. Nikdy neobsahuje údaje kandidátov. Prevádzka aplikácie smerom k zákazníkom prechádza cez edge layer, ktorá poskytuje web application firewall, distributed-denial-of-service protection a content delivery.
- **Administratívny prístup je kontrolovaný.** Operátori pristupujú k interným zdrojom iba prostredníctvom certificate-based point-to-site VPN do management hub network, nie cez verejný internet.

Každá deployment stage (development a production) je plne izolované prostredie s vlastnou sieťou, storage accounts, database a secrets. Produkčné dáta zákazníkov sa nikdy nenachádzajú v nižších prostrediach. Shared management hub obsahuje iba VPN gateway a private DNS, privátne peered do každého prostredia.

4. Defense in Depth

Žiadnej jednej kontrole sa nedôveruje natoľko, aby zastavila každý útok. Platforma vrství nezávislé kontroly tak, aby zlyhanie ktorejkoľvek jednej vrstvy neviedlo k odhaleniu dát. Nižšie uvedené vrstvy sú každá implementovaná a, ako je opísané v časti 12, samostatne testovaná.

Vrstvený bezpečnostný model: nezávislé kontroly v každej vrstve



Vrstva	Reprezentatívne kontroly
Network edge	Prenos iba cez TLS, edge WAF a DDoS protection, private endpoints, default-deny segmentation
Identity and access	Krátkodobé signed tokens, bcrypt hashing, role-based access control, izolácia podľa organizácie
Aplikácia	Schema validation na všetkých vstupoch, prístup k dátam iba cez ORM, output encoding, rate limiting
Ochrana dát	Šifrovanie v pokoji, secrets vault s managed identity, rezidencia dát v EÚ, spracovanie podmienené consent
Governance a súkromie	Konfigurovateľná retencia, vymazanie ako jednej jednotky, human-in-the-loop AI, audit logging
Continuous assurance	Automatizovaná sada testov, opakovateľné penetration tests, pravidelné interné security audits

Zvyšok tohto dokumentu postupne prechádza jednotlivými vrstvami a potom opisuje, ako priebežne dokazujeme, že tieto vrstvy fungujú.

5. Bezpečnosť siete

5.1 Súkromné v predvolenom stave

Dátová vrstva je súkromná už svojou konštrukciou. Spravovaná PostgreSQL database má vypnutý public network access a je dostupná iba cez private endpoint. Private object storage je nakonfigurovaný tak, aby v predvolenom stave zamietal sieťový prístup, úplne vypína shared access keys a je dostupný iba cez managed identity z application subnet. Cache, AI services a secrets vault sú podobne dostupné cez private endpoints s private DNS resolution.

V praxi to znamená, že neexistuje žiadny internetovo dostupný connection string do database a žiadne verejné storage URL pre candidate audio: database a private storage majú public network access úplne vypnutý. Secrets vault je aplikáciou dosahovaný cez private endpoint a je chránený authentication pomocou platform identity a least-privilege access policies, pričom aplikačné identity majú iba read-only access iba k secrets, ktoré potrebujú, takže secrets nie je možné získať bez platnej autorizovanej identity. Attack surface, ktorej sa externý útočník môže vôbec dotknúť, je obmedzený na HTTPS endpoints aplikácie za edge layer.

5.2 Segmentácia siete

Každé prostredie je rozdelené na samostatné subnety pre application tier, data tier a asynchronous worker. Každý subnet je riadený network security group, ktorej posledné pravidlo zamieta všetku inbound traffic. Application subnet prijíma iba inbound HTTPS. Data subnet prijíma iba konkrétne porty pre database, cache a vault, a to iba z application subnet alebo administratívnej VPN. To znamená, že aj útočník, ktorý by sa nejakým spôsobom dostal do application tier, nemôže voľne pivotovať do data tier; povolené sú iba cesty, ktoré aplikácia legitímne používa.

5.3 Edge

Verejná aplikačná prevádzka je umiestnená za edge layer poskytujúcou web application firewall, DDoS protection a content delivery network. Downloads release verzií a dokumentov sú obsluhované z vyhradeného public storage account prostredníctvom content-delivery front door, úplne oddelene od private storage, ktorý uchováva údaje kandidátov. Tieto dve storage planes sa nikdy nemiešajú: nesprávna konfigurácia verejnej roviny nemôže vystaviť súkromné údaje kandidátov, pretože ide o odlišné accounts s odlišnými network rules.

5.4 Administratívny prístup

Do private network neexistuje žiadny verejný administratívny endpoint. Operátori sa pripájajú cez point-to-site VPN gateway, ktorá používa certificate-based authentication. Administratívny prístup k database a cache je možný iba zvnútra tohto tunela, pretože tieto služby majú public network access vypnutý. Vďaka tomu každodenné operations prebiehajú úplne mimo verejného internetu.

6. Identity and Access Management

6.1 Authentication

Používateľské sessions sa vytvárajú pomocou signed access token platného tridsať minút, spárovaného so samostatným opaque server-side refresh token. Access tokens sa overujú pri každej request a používateľ sa znovu validuje voči database (vrátane kontroly active-account) namiesto toho, aby sa dôverovalo iba obsahu tokenu. Odhlásenie okamžite revokuje server-side refresh session, takže ukradnutý refresh token neprežije logout.

Passwords sa nikdy neukladajú v plain text. Sú hashované pomocou bcrypt s jedinečným per-password salt. Pre organizácie, ktoré preferujú single sign-on, platforma podporuje OAuth login cez Microsoft a Google; v takom prípade sa žiadne password vôbec neuchováva.

Vlastníctvo email adresy sa overuje prostredníctvom single-use, time-limited verification link predtým, než sa self-registered account považuje za overený, a opätovné odosielanie verification emailov je rate limited, aby sa zabránilo zneužitiu.

6.2 Role-Based Access Control

Authorization je vynucovaná cez model rolí so štyrmi rolami so stúpajúcou úrovňou oprávnení: interviewer, hiring manager, recruiter a administrator. Prístup k privilegovaným operáciám je vynucovaný server-side dependencies, ktoré kontrolujú rolu aj verification status volajúceho. Tieto role checks chránia výrazne viac než sto odlišných API operations.

Rola	Typické oprávnenia
Interviewer	Vedie priradené pohovory; vidí iba pohovory, ktoré sú mu priradené
Hiring manager	Spravuje recruitmenty, ktoré vlastní alebo ktorých je členom
Recruiter	Úplná správa recruitmentov a kandidátov v rámci organizácie
Administrator	Nastavenia organizácie, billing, správa používateľov a API keys

Okrem hrubých kontrol rolí platforma uplatňuje pravidlá viditeľnosti na úrovni dát. Hiring managers vidia iba recruitmenty, ktoré vytvorili alebo ktorých sú členmi; interviewers vidia iba pohovory, ktoré sú im priradené. Oprávnenia sa teda vynucujú tak na úrovni „aká akcia“, ako aj na úrovni „ktoré záznamy“.

6.3 Izolácia podľa organizácie

Platforma je multi-tenant a tenant isolation sa považuje za bezpečnostnú kontrolu prvej triedy. Každá authenticated identity nesie identifier organizácie a dátové queries sú ohraničené na túto organizáciu. Keď používateľ požiada o záznam patriaci inej organizácii, platforma vráti odpoveď „not found“ namiesto odhalenia, že záznam existuje. Interné database identifiers sa nikdy nevystavujú na wire; API prezentuje display identifiers a pri každej request ich znovu mapuje, čím eliminuje bežnú triedu útokov cross-tenant enumeration.

Nejde iba o návrhový zámer. Ako je opísané v časti 12, naša automatizovaná sada spúšťa rozsiahlu cross-organization matrix, ktorá sa pokúša pristúpiť k dátam jednej organizácie pomocou credentials druhej organizácie, a potvrdzuje, že každý takýto pokus zlyhá.

6.4 Programmatic Access

Pre integrations môžu organizácie v oprávnených plánoch vydávať API keys. Keys používajú rozpoznateľný prefix, nesú 128 bits of entropy a ukladajú sa iba ako hash; surový key sa zobrazí raz pri vytvorení a už nikdy znova. Každý key nesie explicit permission scope (read, write alebo ATS integration), môže byť obmedzený na konkrétne source networks, možno ho okamžite revokovať a podlieha per-key rate limits odvodeným od plan tier organizácie. Verifikácia key používa timing-safe comparison, aby sa zabránilo úniku informácií cez response timing.

7. Bezpečnosť aplikácie

Aplikácia je napísaná tak, aby odstraňovala celé kategórie zraniteľností namiesto ich záplatovania po jednom prípade.

- **Injection.** Všetok prístup k database prebieha cez object-relational mapper s parameterized queries. Codebase neobsahuje žiadne raw string-formatted SQL. Tým sa štrukturálne eliminuje SQL injection.
- **Validácia vstupu.** Každé request body sa pred vstupom do business logic validuje voči striktnej schema. Predimenzované payloads sa zamietajú a list endpoints používajú pagination na obmedzenie spotreby zdrojov.
- **Output encoding a cross-site scripting.** Text dodaný používateľom aj text generovaný AI sa považuje za nedôveryhodný. Tam, kde musí byť obsah renderovaný ako HTML, prechádza pri zápise cez sanitizer založený na allow-list a vyhradená sada testov potvrdzuje, že script tags, event handlers a javascript URLs sa odstraňujú.
- **Mass assignment.** Update operations používajú explicit schemas, ktoré vylučujú privilegované polia ako role, organization a credit balance, takže klient nemôže eskalovať oprávnenia odoslaním dodatočných polí.
- **Rate limiting.** Authentication a endpoints náchylné na zneužitie sú rate limited pomocou durable limiter backed by database, ktorý prežíva restarts a funguje správne naprieč viacerými application instances. Login, registration, password reset a verification resends majú každé vlastné limity. Resolving client IP je spevnený proti spoofing forwarding headers.
- **Webhooks.** Inbound webhooks od payment a email providers sa pred spracovaním overujú voči provider signatures nad raw request body.
- **File uploads.** Uploads majú obmedzenú veľkosť, sú validované, ukladajú sa pod generated identifiers namiesto názvov dodaných používateľom a sú obmedzené per request a per organization.
- **Security headers.** V production responses nesú strict transport security, content-type a frame options, referrer policy a restrictive permissions policy a potláčajú server a framework banners.

8. Ochrana dát

8.1 Šifrovanie

Všetky dáta sú šifrované v pokoji pomocou AES-256 prostredníctvom platformových vrstiev šifrovania storage a database v Azure. Všetka sieťová komunikácia je obsluhovaná výhradne cez HTTPS s použitím TLS 1.2 alebo vyššieho; plaintext HTTP je na každej vrstve presmerovaný na HTTPS. V production API a web portal odosielajú strict transport security headers spolu so sadou headers na spevnenie a potláčajú version banners servera a frameworku.

8.2 Správa secrets

Application secrets sa uchovávajú v centralizovanom secrets vault s aktivovanou purge protection a ninety-day soft-delete window. Aplikácie sa autentifikujú k Azure resources pomocou system-assigned managed identities namiesto long-lived keys; napríklad private storage má shared access keys úplne vypnuté, takže prístup je možný iba cez identity-based role assignments s rozsahom na individuálny resource. Vault access policies udeľujú aplikačným principalom read-only access iba k tým secrets, ktoré potrebujú, v súlade so zásadou least privilege.

8.3 Rezidencia dát

Všetky údaje zákazníkov a kandidátov sú ukladané a spracúvané v rámci Európskej únie. Hosting aplikácie, database, storage, cache a secrets sa nachádzajú vo West Europe a AI processing beží v regiónoch EÚ. Poskytovateľ AI nepoužíva údaje zákazníkov na trénovanie svojich models.

8.4 Životný cyklus jedného pohovoru

Najzreteľnejším spôsobom, ako pochopiť kontroly ochrany dát, je sledovať jeden pohovor od začiatku do konca. Pred akýmkoľvek spracovaním sa zachytí a zaznamená consent. Upload je pri prenose šifrovaný. Transcription a analysis prebiehajú v dátových centrách EÚ. Výsledky sa zapisujú do šifrovaného storage. Každý záznam je potom riadený jednými retention clock, ktoré sa končia zaznamenaným cascading deletion. V ktoromkoľvek okamihu môžu práva kandidáta, ako withdrawal, deletion, access alebo portability, tento tok prerušiť.

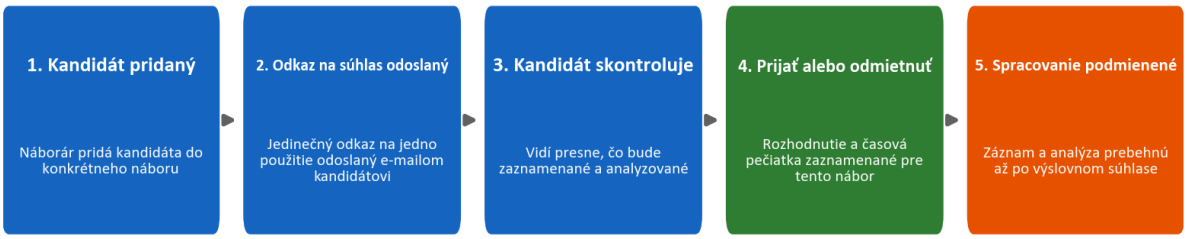
9. Privacy by Design a GDPR

Súkromie je zabudované do dátového modelu a workflow, nie je doplnené iba prostredníctvom politiky.

9.1 Consent

Žiadny pohovor sa nenahráva ani neanalyzuje bez explicit consent kandidáta. Keď je kandidát pridaný do recruitmentu, platforma emailom odošle jedinečný single-use consent link. Kandidát si prečíta, čo sa bude diať, a buď súhlasí, alebo odmietne. Stav consent, vrátane času odpovede, sa zaznamenáva k tomuto konkrétnemu recruitmentu, takže consent je vždy viazaný na konkrétny hiring process a nie je udelený globálne.

Súhlas kandidáta: výslovný a zaznamenaný pred akýmkoľvek spracovaním



9.2 Retencia a vymazanie

Retencia dát je konfigurovateľná pre každú organizáciu, s predvolenou hodnotou dvanásť mesiacov a konfigurovateľným minimom tridsať dní, pričom môže byť prepísaná pre jednotlivého kandidáta. Pre údaje kandidáta existujú jedny retention clock, nie samostatný časovač pre každý artifact. Clock sa spustia po zaznamenaní hiring decision. Pred vypršaním dát platforma odošle upozornenie (predvolene približne pätnásť dní vopred) a ponúkne predĺženie jedným kliknutím. Keď sa dáta vymažú, vymažú sa ako jedna jednotka: záznam kandidáta, pohovory, transcripts, audio recordings, documents a comparisons sa odstránia spoločne a vymazanie sa zaznamená do audit log. Nezostávajú žiadne čiastočné ani orphaned residues.

Nižšie uvedený lifecycle zobrazuje tieto jedny clock a to, ako sa zbiehajú do jedného cascading deletion s logged proof of erasure.

Uchovávanie dát: jeden časovač na kandidáta, vymazanie jednej jednotky

9.3 Práva dotknutých osôb a sub-processors

Platforma podporuje práva dotknutých osôb požadované podľa GDPR vrátane access, deletion, portability, objection a explanation. Spracúvanie sa vykonáva na základe data processing agreement, ktorú zákazníci akceptujú pri registrácii a ktorá je versioned per organization. Naši sub-processors a ich úlohy, všetci v EÚ alebo pod primeranými safeguards, sú zverejnení v tejto agreement a zákazníci dostávajú vopred oznámenie o každej zmene. Časť 17 obsahuje register sub-processors a mapovanie

compliance po jednotlivých článkoch.

10. Responsible AI a EU AI Act

Platforma spadá do high-risk category podľa EU AI Act, pretože podporuje rozhodnutia v oblasti zamestnania, a túto klasifikáciu berieme vážne.

Definujúcim pravidlom produktu je, že **AI je podpora rozhodovania, nie rozhodovateľ.** Systém nikdy kandidáta automaticky neprijíma ani neodmieta. Prepisuje reč, štruktúruje otázky a odpovede, skóruje odpovede voči kritériám definovaným recruiterom a pripravuje návrhy feedbacku, pričom človek každé output skontroluje pred jeho použitím. Tým sa človek pevne udržiava v procese.

Rovnako dôležité je aj to, čo AI nerobí. Nehodnotí osobnosť, „cultural fit“, emočný stav, tón hlasu, prízvuk, pohlavie, vek, etnicitu, vzhľad ani body language. Skórovanie je ukotvené v dôkazoch z transcriptu a v kritériách definovaných recruiterom a mená kandidátov sú z evaluation input vylúčené, aby sa znížilo bias. Zverejňujeme transparency card, user documentation a declaration of conformity opisujúce systém, jeho obmedzenia a safeguards.

Kontrola Responsible AI	Ako funguje
Human in the loop	Každé skóre a každý feedback pred použitím kontroluje recruiter
Žiadne automatizované rozhodnutia	Systém nikdy kandidáta automaticky neprijme ani automaticky neodmietne
Skórovanie založené na dôkazoch	Skóre odkazujú na podporné dôkazy z transcriptu
Návrh proti bias	Mená sú vylúčené z evaluation; hodnotí sa obsah nad štýlom
Obmedzenie rozsahu	Osobnosť, emócie, prízvuk a chránené charakteristiky sa nikdy nehodnotia
Bezpečnosť candidate feedback	Súkromný feedback pre kandidáta prechádza cez safety guardrail pre generation-and-validation

Tieto obmedzenia nie sú uvedené iba v dokumentácii; sú zakódované v AI prompt layer a preverované vyhradeným programom AI-safety tests opísaným v časti 12.3.

11. Secure Development Lifecycle

Bezpečnosť sa vynucuje v spôsobe, akým softvér vytvárame a vydávame, nie iba v bežiacom systéme.

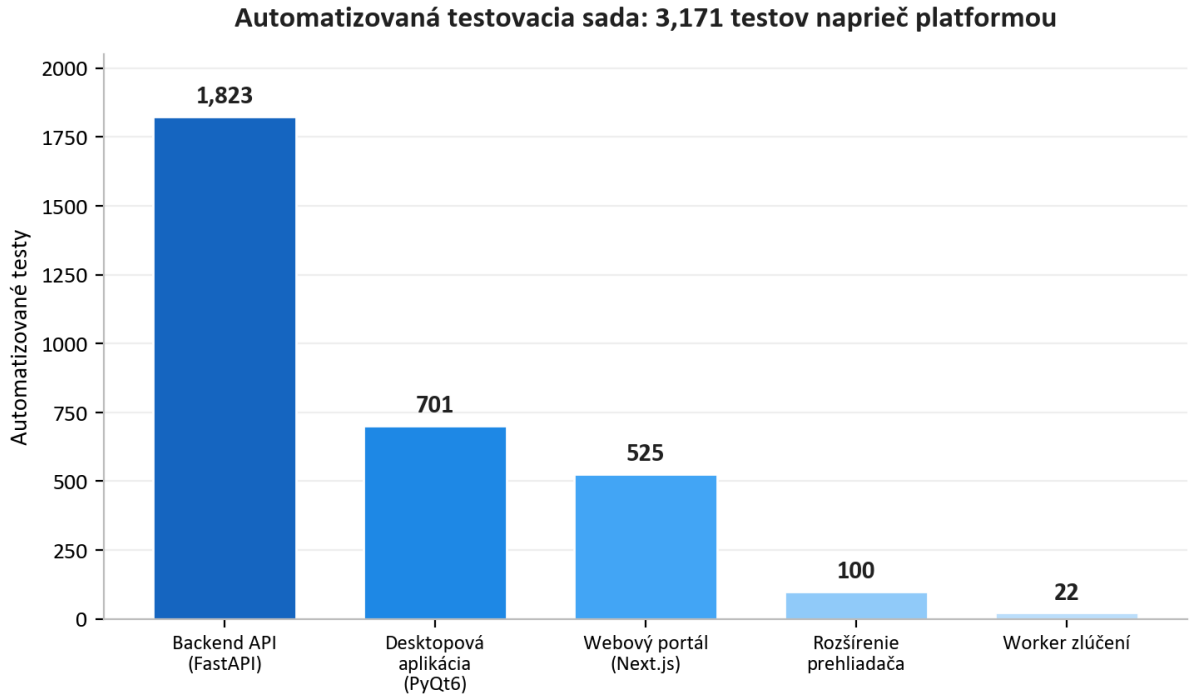
- **Oddelenie prostredí.** Development a production sú plne oddelené, každé s vlastnou infraštruktúrou, storage accounts, database, secrets a subdomains. Neexistuje žiadny shared state.
- **Infrastructure as code.** Celé cloud environment je definované ako code a kontrolované ako code, čo robí bezpečnostné nastavenie auditovateľným a reprodukovateľným. Hodnotiteľ si môže presne prečítať, ktoré ports sú otvorené, ktoré resources sú private a ktoré identity majú aké permissions.
- **Pinned, gated deployments.** Každý krok v continuous-integration pipeline je pinned na presnú immutable version. Production deployments sú založené na tagoch, bežia iba cez chránený production pipeline a sú gated povinným approval. Automatizovaná sada testov funguje ako release gate: deployment nemôže byť vydaný, ak testy zlyhajú.
- **Hygiena dependencies.** Automatizované dependency monitoring navrhuje weekly updates naprieč backendom, desktopom, webom, infraštruktúrou a definíciami pipeline a dependency audits sú súčasťou našej periodickej security review.
- **Signed artifacts.** Desktop installers sú code-signed, takže zákazníci môžu overiť, že softvér, ktorý inštalujú, skutočne pochádza od nás.
- **Disciplinované zaobchádzanie so secrets.** Secrets sa nachádzajú vo vault a v chránených pipeline secrets, nikdy nie v source code.

12. Priebežné bezpečnostné testovanie

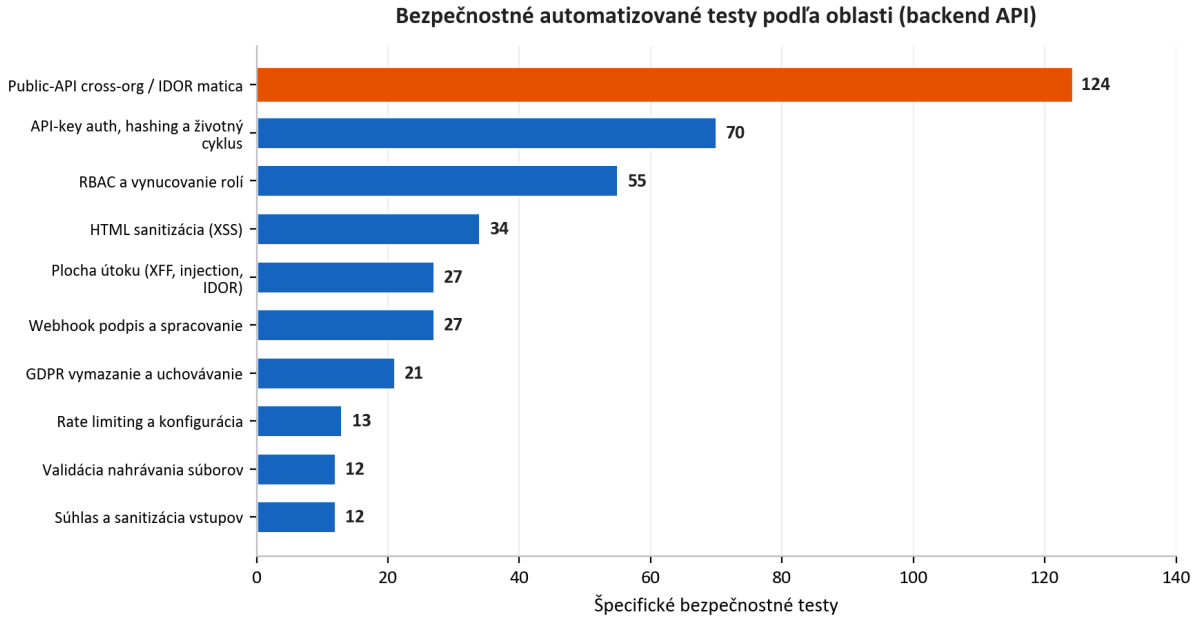
Toto je jadro nášho príbehu o assurance a časť, ktorú väčšina dodávateľov nedokáže ukázať. Bezpečnosť považujeme za niečo, čo sa má priebežne merať pomocou spustiteľných kontrol, nie za niečo, čo sa raz vyhlási.

12.1 Automatizovaná sada testov

Platformu pokrýva **3,171 automatizovaných testov** naprieč backend API, desktop application, web portal, browser extension a audio merge worker.



Nejde iba o funkčné testy. Podstatná vyhradená bezpečnostná sada preveruje kontroly opísané vyššie v tomto dokumente. Graf nižšie rozdeľuje bezpečnostne špecifické testy v backend API podľa domény.



Táto sada okrem mnohých iných obsahuje rozsiahlu public-API matrix, ktorá spúšťa každý endpoint ako legitímny používateľ, ako vlastný API key organizácie a ako API key konkurenčnej organizácie, pričom potvrdzuje, že každý cross-organization pokus je zablokovaný. Zahŕňa desiatky adversarial attack-surface tests pre spoofing forwarding headers, header injection a leakage identifiers, cielenú HTML-sanitization suite pre cross-site scripting, role-enforcement tests pre celý model rolí a testy dokazujúce, že údaje kandidáta sa skutočne vymažú ako jednotka. Keďže tieto testy bežia ako release gate, regression, ktorá by oslabila ktorúkoľvek z týchto kontrol, by zastavila release a nedostala sa k zákazníkom.

12.2 Live Penetration Testing

Automatizované unit tests dokazujú, že kontroly sa izolovane správajú korektne. Aby sme dokázali, že držia pohromade v reálnom deployment, udržiavame opakovateľnú metodiku penetration testing, ktorá spúšťa skutočné attack scripts proti živému prostrediu. Je organizovaná do šiestich fáz:

Fáza	Zameranie	Príklady toho, čo sa preveruje
1. Static analysis	Source code	Secrets, injection patterns, dangerous functions, missing auth, unsafe HTML
2. Architecture review	Infrastructure	Private endpoints, segmentation, TLS, konfigurácia secrets
3. Attack-vector analysis	Source control a cloud	Branch protection, scope identít, public exposure
4. Live penetration testing	Bežiace prostredie	Unauthenticated probing, cross-org access, injection, token tampering, SSRF, rate-limit bursts
5. Enterprise scoring	Maturity	Šestnásť bezpečnostných kategórií skórovaných voči enterprise baseline
6. Dependency and supply chain	Third-party risk	Dependency CVE audit, pinned pipeline actions, integrity lock-file

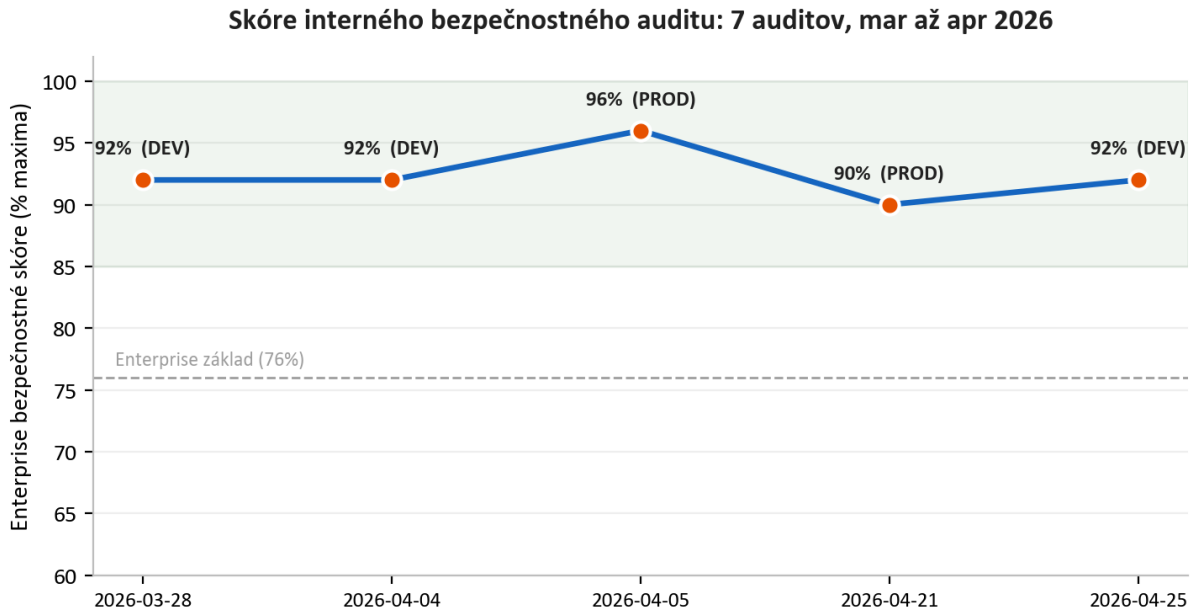
Fáza 4 je skutočné adversarial testing proti nasadenému systému, nie checklist. Preveruje chránené endpoints bez credentials a potvrdzuje, že odmietajú prístup; registruje dve organizácie a pokúša sa pristúpiť k záznamom jednej organizácie pomocou účtu druhej; vkladá payloads pre cross-site-scripting a server-side-template a potvrdzuje, že sú neutralizované; manipuluje authentication tokens a potvrdzuje, že sú odmietnuté; pokúša sa o server-side request forgery proti cloud metadata endpoints; a generuje bursts proti authentication endpoints, aby potvrdila, že rate limiting sa skutočne spúšťa v živom prostredí, nielen teoreticky.

12.3 Safety Testing pre feedback kandidátom

Keďže platforma môže generovať súkromný rozvojový feedback pre kandidátov, prevádzkujeme pre túto funkcionalitu samostatný adversarial safety program. Zámerne dodáva systému tvrdé a nepriateľské poznámky recruitera a potvrdzuje, že output smerujúci ku kandidátovi nikdy neobsahuje vulgarizmy, nikdy neodhaľuje ani nepripisuje identitu recruitera alebo jeho súkromný názor a nikdy nepoužíva hodnotiace osobnostné nálepky. Chráni to kandidáta, ktorý má dostať konštruktívny a rešpektujúci feedback, aj zákazníka, ktorému sa interný názor nesmie dostať navonok.

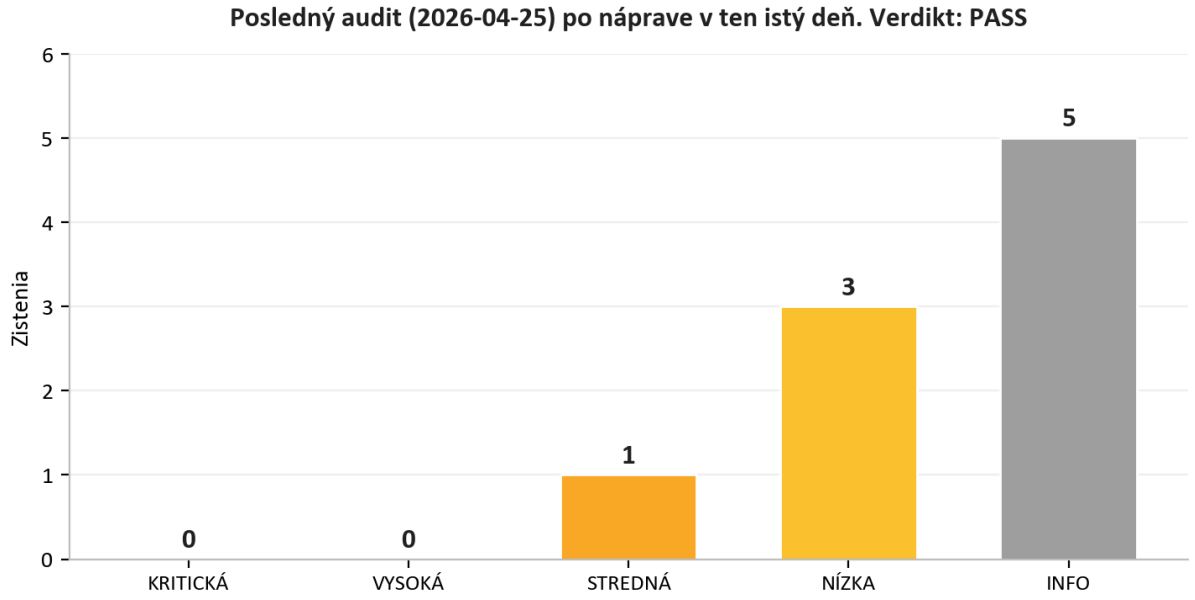
13. Výsledky bezpečnostných auditov

Vykonávame pravidelné security audits s použitím štruktúrovanej, opakovateľnej metodiky penetration testing a každý z nich spracúvame ako datovanú správu so zisteniami hodnotenými podľa severity, evidence a remediation. Ide o interné audity realizované naším vlastným security process; formálna third-party certification tých istých kontrol je súčasťou nášho roadmap. Medzi koncom marca a koncom apríla 2026 sme dokončili **seven such audits** naprieč development a production.



Výsledok, ktorý je pre potenciálneho zákazníka najdôležitejší, je konzistentnosť: **across all seven audits there were zero critical findings.** V zriedkavých prípadoch, keď sa objavil problém vyššej severity, bol rýchlo odstránený, často ešte v ten istý deň, a znovu overený. Scoring rubric bol počas tohto obdobia zámerne sprísnený (maximálne možné score bolo zvýšené, keď sme pridali ďalšie hodnotené kategórie), preto normalizovaná línia score zostáva vysoká, aj keď sa latka posúvala nahor.

Náš najnovší audit z 25 April 2026 ilustruje, ako proces funguje v praxi. Boli identifikované dva problémy vyššej severity, oba boli v ten istý deň opravené a znovu overené a audit bol uzavretý s verdiktom **PASS** bez zostávajúcich issues pripravených na exploit v rámci aktuálneho threat model.



Audit	Prostredie	Critical	Verdikt
2026-03-28	Development	0	Pripravené na production
2026-04-04	Development	0	Pripravené pre enterprise
2026-04-05	Production	0	Pripravené pre enterprise
2026-04-20	Development	0	Pripravené na production, poznámky
2026-04-20	Development	0	Pass s poznámkami
2026-04-21	Production	0	Bezpečné, bez exploitovateľných zistení
2026-04-25	Development	0	Pass

Vzorec naprieč týmito auditmi je najpoctivejším dôkazom, ktorý môžeme ponúknuť: issues sa nachádzajú, pretože ich intenzívne hľadáme, a rýchlo sa uzatvárajú, pretože proces je postavený tak, aby ich uzatváral. Dodávateľ, ktorý nikdy nehlási žiadne finding, je zvyčajne dodávateľ, ktorý nehľadá.

14. Prevádzková odolnosť a Shared Responsibility

14.1 Monitoring a logging

Telemetry aplikácie a platformy prúdia do centralizovaného log analytics workspace a služby application-monitoring, čo nám dáva prehľad o dostupnosti a správaní. Citlivé akcie, ako mazanie dát, prijatie legal-agreement a AI invocations, sa zaznamenávajú do vyhradených audit tables, takže existuje trvalý záznam o tom, kto čo vykonal s dôležitými dátami.

14.2 Zálohovanie a obnova

Spravovaná database uchováva automatizované backups a private storage je chránený soft-delete retention na úrovni blobs aj containers, takže náhodné alebo škodlivé vymazanie možno obnoviť v rámci retention window. Kritická infraštruktúra nesie deletion locks, aby sa zabránilo náhodnému odstráneniu produkčných resources.

14.3 Súhrn Shared Responsibility

Oblasť	AI Interview Analyzer	Zákazník
Infraštruktúra, sieť, patching	Áno	-
Bezpečnosť aplikácie a AI pipeline	Áno	-
Šifrovanie, secrets, rezidencia dát	Áno	-
Správa používateľov a rolí	Poskytuje kontroly	Spravuje používateľov a roly
Konfigurácia retention policy	Poskytuje kontroly	Nastavuje retention window
Súhlas kandidáta	Poskytuje workflow	Zabezpečuje jeho používanie
Silné credentials koncových používateľov a SSO	Podporuje SSO a policy	Vynucuje internú policy

15. Threat Model a mapovanie na OWASP

Navrhujeme proti konkrétnemu súboru protivníkov: externému útočníkovi bez credentials, zvedavému alebo škodlivému authenticated používateľovi jednej organizácie, ktorý sa snaží pristúpiť k dátam inej organizácie, compromised dependency a chybe insidera. Nižšie uvedená tabuľka mapuje široko používané rizikové kategórie OWASP Top 10 na konkrétne kontroly, ktoré ich v tejto platforme riešia, pričom každá z nich je preverovaná testovaním opísaným v časti 12.

Riziko OWASP	Ako ho platforma zmierňuje
Broken access control	Role-based access control na každom privilegovanom endpoint; scope podľa organizácie; „not found“ pri cross-org access; remapping identifierov; cross-org test matrix
Cryptographic failures	TLS 1.2+ pri prenose; AES-256 v pokoji; bcrypt password hashing; secrets v managed vault
Injection	Iba ORM parameterized queries; strict schema validation; HTML sanitization pri zápise
Insecure design	Vrstvená defense in depth; threat modeling a architecture review v každom audite
Security misconfiguration	Infrastructure as code; default-deny network groups; security headers; disabled shared storage keys; API schema nie je v production vystavená
Vulnerable components	Weekly automated dependency monitoring; dependency CVE audits pri periodickom review
Identification and authentication failures	Krátkodobé tokens; rate-limited login; email verification; podpora SSO; žiadne plaintext passwords
Software and data integrity failures	Pinned, immutable pipeline steps; signed desktop installers; webhook signature verification; production deploys gated tagmi
Security logging and monitoring failures	Centralizovaná telemetry; vyhradené audit tables pre citlivé akcie
Server-side request forgery	Outbound calls obmedzené na trusted endpoints; SSRF probes v penetration-test harness

Toto mapovanie je kostrou nášho argumentu pre assurance: pre každú známu triedu útokov existuje pomenovaná kontrola a pre každú pomenovanú kontrolu existuje test.

16. Vulnerability Management a Responsible Disclosure

Bezpečnosť nikdy nie je dokončená, preto prevádzkujeme priebežný cyklus objavovania a remediation.

- **Discovery.** Vulnerabilities sa identifikujú zo štyroch zdrojov: automatizovaná sada testov, pravidelné penetration-test audits, automatizované dependency monitoring a reporty od zákazníkov alebo výskumníkov.
- **Triage.** Každému finding sa priradí severity (critical, high, medium, low alebo informational) spolu s evidence a vlastníkom remediation, presne tak, ako sa zaznamenáva v našich audit reports.
- **Ciele remediation.** Critical a high findings dostávajú prioritu na okamžitú remediation; v našej audit history boli findings vyššej severity typicky vyriešené a znovu overené ešte v ten istý deň. Medium a nižšie findings sa plánujú do bežnej maintenance cadence.
- **Verification.** Opravy sa znovu testujú a tam, kde je to relevantné, sa proti nasadenému prostrediu vykoná live check, aby sa potvrdilo, že issue je skutočne uzavretá, nielen uzavretá v kóde.
- **Disclosure.** Bezpečnostné obavy nám možno nahlásiť priamo. Prijatie reportov potvrdíme, vyšetríme ich a priebežne informujeme oznamovateľa až do vyriešenia.

17. Mapovanie compliance

17.1 GDPR

Oblasť GDPR	Implementácia v platforme
Zákonný základ (Art. 6)	Explicit consent kandidáta získaný pred spracovaním
Minimalizácia dát a obmedzenie uchovávania (Art. 5)	Spracúvajú sa iba dáta relevantné pre pohovor; konfigurovateľná retencia s automatickým vymazaním
Právo na vymazanie (Art. 17)	Vymazanie všetkých dát kandidáta ako jednej jednotky, s logged proof of erasure
Práva dotknutých osôb (Art. 15 to 20)	Podporované sú access, deletion, portability a objection
Povinnosti sprostredkovateľa (Art. 28)	Data processing agreement akceptovaná pri registrácii a versioned per organization
Bezpečnosť spracovania (Art. 32)	Šifrovanie, riadenie prístupu, izolácia a priebežné testovanie, ako je opísané v tomto dokumente
Transparentnosť sub-processorov	Zverejnené v data processing agreement s vopred oznámenou zmenou

17.2 EU AI Act

Platforma sa považuje za high-risk AI system podporujúci rozhodnutia v oblasti zamestnania a udržiavame dokumentáciu zosúladenú s reguláciou vrátane transparency card, user documentation a declaration of conformity. Základné safeguards, human oversight, transparentnosť, evidence-based scoring a prísne scope limits na to, čo AI vyhodnocuje, sú opísané v časti 10. Ako sa posúva implementation timeline regulácie, pokračujeme v rozvíjaní našej formálnej conformity documentation.

17.3 Hosting certifications

Platforma beží úplne na Microsoft Azure, ktorého dátové centrá majú nezávislé certifications vrátane ISO 27001 a SOC 2. Tieto certifications pokrývajú fyzické a platform layers pod našou aplikáciou; aplikačné kontroly sú tie, ktoré sú opísané v celom tomto dokumente.

17.4 Register sub-processorov

Sub-processor	Účel	Región
Microsoft Azure	Hosting, AI a speech processing, storage, transactional email	EU (West Europe, Sweden Central)
Stripe	Spracovanie subscriptions a payments	EU (Ireland)
Fakturownia	Fakturácia	EU (Poland)
ATS connector (optional)	Integrácia applicant-tracking, aktivovaná iba na požiadanie	EU

18. Security Roadmap

Bezpečnosť vnímame ako program neustáleho zlepšovania. Aktuálne iniciatívy v našom roadmap zahŕňajú posilnenie možností multi-factor authentication pre administratívne účty, rozšírenie centralizovaného audit logging prístupov k dátam, pokračovanie v sprísňovaní aktuálnosti dependencies v pravidelnej cadence a postup v oblasti formálnej third-party certification kontrol opísaných v tomto dokumente. Žiadna z týchto oblastí dnes nepredstavuje medzeru, ktorá by vystavovala zákaznícke dáta; každá z nich je vylepšením už teraz vrstveného bezpečnostného nastavenia.

19. Zhrnutie

AI Interview Analyzer chráni údaje kandidátov a zákazníkov prostredníctvom vrstvenej architektúry: siete private-by-default bez verejných dátových služieb, silných identít a izolácie podľa organizácie, aplikačného kódu, ktorý navrhuje mimo hry celé triedy zraniteľností, šifrovania a rezidencie dát v EÚ a kontrol súkromia zabudovaných do dátového modelu. To, čo platformu odlišuje, sú dôkazy za týmito tvrdeniami. S 3,171 automatizovanými testami, opakovateľnou metodikou live penetration testing, vyhradeným programom AI-safety a históriou siedmich interných security audits s zero critical findings môžeme ukázať, nielen tvrdiť, že platforma je bezpečná.

Príloha A: Katalóg bezpečnostných kontrol

Stručný referenčný prehľad primárnych kontrol a dôkazov, ktoré každú z nich podporujú.

Kontrola	Mechanizmus	Dôkaz
Šifrovanie prenosu	Iba HTTPS, TLS 1.2+, presmerovanie HTTP	Infrastructure as code; architecture audit
Šifrovanie v pokoji	Platformové šifrovanie AES-256 na storage a database	Platform configuration; architecture audit
Ochrana passwords	bcrypt s per-password salt	Source control; authentication tests
Session management	30-minute signed tokens, revocable server-side refresh	Source control; authentication tests
Authorization	Four-role access control na privilegovaných endpoints	Role-enforcement test suite
Tenant isolation	Scope queries podľa organizácie; 404 pri cross-org	Cross-organization test matrix
Bezpečnosť API keys	Hashed storage, scoped permissions, per-key rate limits	API-key test suite
Ochrana proti injection	Iba ORM parameterized queries	Static analysis; injection tests
Ochrana proti cross-site scripting	HTML sanitization pri zápise	HTML-sanitization test suite
Rate limiting	Durable limiter backed by database na auth endpoints	Rate-limit tests; live burst checks
Integrita webhooks	Provider signature verification na raw body	Webhook test suite
Správa secrets	Managed vault, purge protection, managed identity	Infrastructure as code; architecture audit
Izolácia siete	Private endpoints; default-deny segmentation	Infrastructure as code; architecture audit
Vymazanie dát	Cascading deletion ako jednej jednotky s audit log	GDPR deletion test suite
Supply chain	Pinned pipeline steps; weekly dependency monitoring	Pipeline configuration; dependency audit

Príloha B: Často kladené otázky pre security reviewerov

Kde sú uložené naše dáta? Úplne v rámci Európskej únie, na Microsoft Azure, vo West Europe s AI processing v regiónoch EÚ. Údaje kandidátov nikdy neopúšťajú EÚ.

Používajú sa naše dáta na trénovanie AI models? Nie. Poskytovateľ AI nepoužíva údaje zákazníkov na training.

Je database dostupná z internetu? Nie. Public network access je vypnutý a database je dostupná iba cez private endpoint v rámci virtual network.

Môže jeden zákazník vidieť dáta iného zákazníka? Nie. Každý query je ohraničený na organizáciu volajúceho, cross-organization access vracia „not found“ a automatizovaná matrix túto izoláciu priebežne testuje.

Ako sa ukladajú passwords? Hashované pomocou bcrypt a jedinečného per-password salt. Podporovaný je single sign-on cez Microsoft a Google, v takom prípade sa žiadne password neukladá.

Podporujete single sign-on? Áno, cez Microsoft a Google OAuth.

Ako dlho sú access tokens platné? Tridsať minút, v páre s revocable server-side refresh session, ktorá sa pri logout invaliduje.

Ako sa rieši consent kandidáta? Každý kandidát dostane jedinečný single-use consent link a musí súhlasiť pred akýmkoľvek recording alebo analysis. Consent sa zaznamenáva ku konkrétnemu hiring process.

Ako sa dáta mažú? Ako jedna jednotka zahŕňajúca záznam kandidáta, interviews, transcripts, audio, documents a comparisons, podľa konfigurovateľného retention schedule, s logged proof of erasure. Kandidáti môžu o deletion požiadať aj priamo.

Máte data processing agreement? Áno, akceptovanú pri registrácii a versioned per organization vrátane registra sub-processorov.

Robí AI rozhodnutia o prijímaní? Nie. Poskytuje iba decision support; človek kontroluje každý output a robí všetky rozhodnutia.

Ako dokazujete svoje bezpečnostné tvrdenia? Prostredníctvom 3,171 automatizovaných testov vrátane vyhradenej bezpečnostnej sady, opakovateľnej six-phase methodology penetration testing spúšťanej proti live environments, programu AI-safety tests a pravidelných písomných audit reports.

Čo sa stane, keď nájdete vulnerability? Priradí sa jej severity spolu s evidence a ownerom, opraví sa podľa priority, znovu overí vrátane live checks tam, kde je to relevantné, a zaznamená sa do audit report.

Môžeme vykonať vlastný penetration test? Security assessments možno dohodnúť prostredníctvom vášho account representative pri primeranom scope a scheduling.

Príloha C: Glosár

Pojem	Význam
AES-256	Silný symetrický štandard šifrovania používaný na ochranu dát v pokoji
bcrypt	Účelovo navrhnutá funkcia password hashing s per-password salting
Managed identity	Identita vydaná platformou, ktorá umožňuje službe autentifikovať sa bez uložených keys
Private endpoint	Súkromná sieťová adresa, ktorá drží cloud service mimo verejného internetu
Network security group	Súbor pravidiel allow a deny, ktoré filtrujú sieťovú prevádzku do subnetu
RBAC	Role-based access control, udeľovanie permissions podľa role používateľa
IDOR	Insecure direct object reference, chyba access control, proti ktorej sa platforma bráni
SSRF	Server-side request forgery, trieda útokov preverovaná v našich penetration tests
Web application firewall	Edge control, ktorá filtruje škodlivú webovú prevádzku
Data processing agreement	Zmluva upravujúca, ako processor spracúva osobné údaje v mene controllera

Príloha D: Kontakt a riadenie dokumentu

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Ak požadujete security review, kópiu našej data processing agreement alebo našu conformity documentation k EU AI Act, kontaktujte, prosím, svojho account representative.

Tento dokument opisuje security posture služby AI Interview Analyzer k dátumu vygenerovania uvedenému v päte. Poskytuje sa na účely hodnotenia a netvorí súčasť žiadnej zmluvy. Konkrétne zmluvné bezpečnostné záväzky sú uvedené v príslušnej zmluve a data processing agreement.