Sigurnosni whitepaper

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Sigurnosni whitepaper

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

Publika: Timovi za sigurnost u poduzećima, IT i nabavu

Klasifikacija: Javno

1. Izvršni sažetak

AI Interview Analyzer je platforma za zapošljavanje za poduzeća koja, uz izričitu privolu kandidata, snima intervjue, transkribira ih i strukturira te proizvodi podršku za evaluaciju utemeljenu na dokazima za regrutere. Budući da platforma obrađuje osobne podatke kandidata i podržava procese zapošljavanja, sigurnost i privatnost tretiraju se kao primarna projektna ograničenja, a ne kao značajke dodane naknadno.

Ovaj whitepaper opisuje, konkretnim i provjerljivim pojmovima, kako štitimo podatke korisnika i kandidata. Napisana je za osobe koje provode pregled dobavljača: sigurnosne inženjere, IT administratore, službenike za zaštitu podataka i nabavu. Svaka brojka u ovom dokumentu preuzeta je izravno iz naših vlastitih inženjerskih sustava, a ne iz marketinških materijala.

Središnja poruka je jednostavna: **ne tvrdimo samo da je platforma sigurna, već to neprekidno testiramo.** Naša baza koda sadrži **3,171 automatiziranih testova**, uključujući namjenski sigurnosni paket koji provjerava autentikaciju, autorizaciju, izolaciju između organizacija, obrane od injekcija i brisanje podataka. Povrh toga, provodimo ponovljiv okvir za penetracijsko testiranje nad aktivnim implementacijama i izrađujemo pisana izvješća o reviziji. Tijekom sedam internih sigurnosnih revizija u ožujku i travnju 2026. zabilježili smo **zero critical findings**, pri čemu je naša najnovija revizija zaključena presudom **PASS**. (Formalna certifikacija ovih kontrola od strane treće strane nalazi se na našem planu razvoja; vidjeti Odjeljak 18.)

Sigurnosna karakteristika	Sažetak
Hosting	Microsoft Azure, samo EU regije
Mrežni model	Privatne krajnje točke, segmentacija mreže sa zadanim uskraćivanjem, bez javne baze podataka
Enkripcija	AES-256 u mirovanju, TLS 1.2 ili viši u prijenosu
Identitet	Kratkotrajni potpisani tokeni, bcrypt hashiranje lozinki, podrška za SSO
Kontrola pristupa	RBAC s strogom izolacijom po organizaciji
Tajne	Centralizirani trezor tajni s pristupom putem upravljanog identiteta
Privatnost	Izričita privola, prilagodljivo zadržavanje, brisanje jedne cjeline
Odgovorni AI	Samo podrška pri odlučivanju, čovjek je uvijek uključen
Jamstvo	3,171 automatiziranih testova plus periodična penetracijska testiranja i revizije

1.1 Kako čitati ovaj dokument

Odjeljci 3 do 11 opisuju kontrole koje štite podatke: arhitekturu, mrežu, identitet, aplikaciju, zaštitu podataka, privatnost i životni ciklus sigurnog razvoja. Odjeljci 12 i 13 pokrivaju naš prepoznatljiv program kontinuiranog testiranja i našu povijest revizija. Odjeljci 14 do 17 obuhvaćaju operacije, modeliranje prijetnji, upravljanje ranjivostima i mapiranje usklađenosti. Dodaci pružaju katalog kontrola, FAQ za pregledavatelje i glosar koji sigurnosni tim može izravno koristiti tijekom procjene.

2. Opseg i pristup dokumenta

2.1 Što ovaj dokument pokriva

Ovaj whitepaper pokriva sigurnosnu arhitekturu i prakse usluge AI Interview Analyzer: okruženje hostinga, mrežni dizajn, upravljanje identitetom i pristupom, kontrole na razini aplikacije, zaštitu podataka, privatnost i regulatorno usklađivanje, životni ciklus sigurnog razvoja i naš program kontinuiranog sigurnosnog testiranja.

2.2 Što ga čini provjerljivim

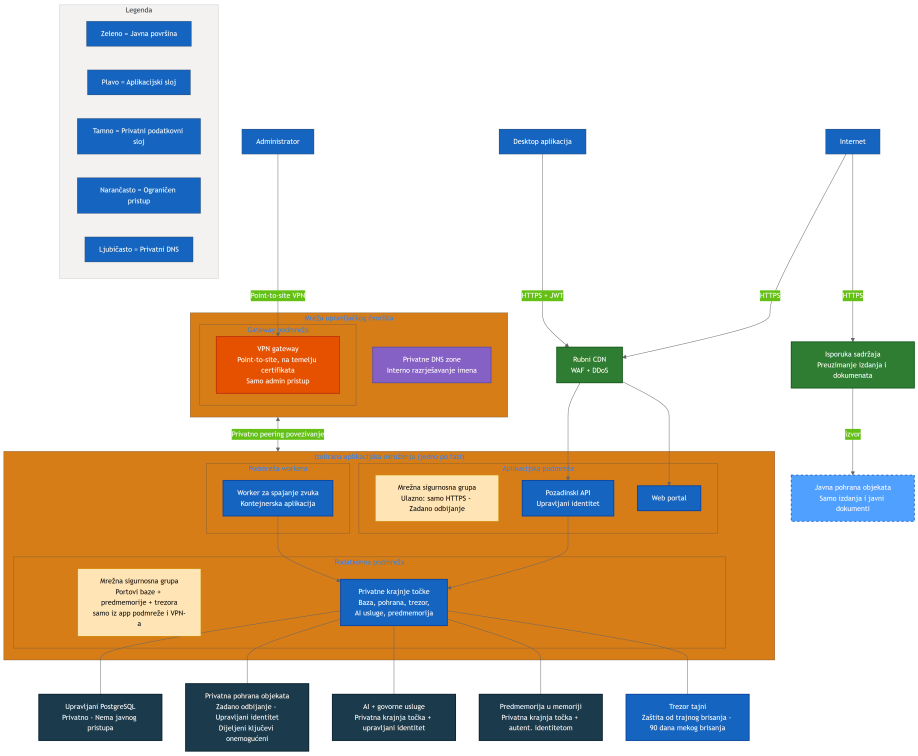
Tvrdnje dobavljača o sigurnosti lako je napisati, a teško im je vjerovati. Stoga smo svaku glavnu tvrdnju u ovom dokumentu povezali s nečim konkretnim i mjerljivim unutar naših inženjerskih sustava: kontrolom implementiranom u kodu, testom koji dokazuje da kontrola radi, infrastrukturnom definicijom koja je provodi ili revizorskim izvješćem koje bilježi dokumentiranu provjeru. Gdje je kontrola dio našeg budućeg plana razvoja, a ne današnje isporuke, to izričito navodimo. Radije ćemo iznijeti manje tvrdnji i biti pouzdani nego iznijeti previše i biti razotkriveni.

2.3 Podijeljena odgovornost

Platforma se isporučuje kao softver kao usluga. Mi upravljamo infrastrukturom, aplikacijom, AI cjevovodom i rukovanjem podacima. Korisnik je odgovoran za upravljanje vlastitim korisničkim računima i ulogama, konfiguriranje razdoblja zadržavanja podataka u skladu sa svojom internom politikom i osiguravanje da se privola kandidata pribavlja putem tijeka privole koji platforma pruža. Odjeljak 14 detaljnije opisuje ovu podjelu.

3. Pregled sigurnosne arhitekture

Platforma je izgrađena kao mali broj međusobno surađujućih usluga, a ne kao jedan monolit. Desktop aplikacija i web portal djeluju kao klijenti. Središnji backend API upravlja cjelokupnom pohranom, autentikacijom, naplatom, AI cjevovodom, privolom, e-poštom, rukovanjem datotekama i nadzornim pločama. Radnik za spajanje audiosnimki obrađuje snimke asinkrono. Sve osjetljivo stanje nalazi se iza backend API-ja; klijenti nikada ne komuniciraju izravno s bazom podataka, pohranom ili AI uslugama.



Gornji dijagram prikazuje produkcijsku topologiju s namjerno generaliziranim nazivima resursa. U njemu su vidljiva tri načela:

- **Bez izravnog izlaganja podatkovnih usluga.** Baza podataka, privatna objektna pohrana, AI usluge i predmemorija imaju onemogućen javni mrežni pristup i dostupni su samo putem privatnih krajnjih točaka unutar izolirane virtualne mreže. Trezor tajni aplikacija dohvaća putem privatne krajnje točke, a dodatno je zaštićen autentikacijom identiteta platforme i politikama pristupa s najmanjim privilegijama, tako da svaki pristup zahtijeva valjan, autoriziran identitet neovisno o mrežnoj putanji.
- **Odvojena javna površina.** Jedina javna objektna pohrana sadrži preuzimanja izdanja i javne dokumente. Nikada ne sadrži podatke kandidata. Promet aplikacije okrenut korisnicima prolazi kroz rubni sloj koji pruža web application firewall, zaštitu od distributed-denial-of-service napada i isporuku sadržaja.
- **Administrativni pristup je kontroliran.** Operateri pristupaju internim resursima samo putem point-to-site VPN veze temeljene na certifikatima prema upravljačkoj hub mreži, a ne preko javnog interneta.

Svaka faza implementacije (razvoj i produkcija) potpuno je izolirano okruženje sa svojom mrežom, računima za pohranu, bazom podataka i tajnama. Produkcijski podaci korisnika nikada nisu prisutni u nižim okruženjima. Zajednički upravljački hub sadrži samo VPN pristupnik i privatni DNS, privatno uparen sa svakim okruženjem.

4. Višeslojna obrana

Nijednoj pojedinačnoj kontroli ne vjeruje se da će zaustaviti svaki napad. Platforma slaže neovisne kontrole tako da kvar bilo kojeg sloja ne izloži podatke. Svaki od slojeva u nastavku implementiran je i, kako je opisano u Odjeljku 12, pojedinačno testiran.

Slojeviti sigurnosni model: neovisne kontrole na svakoj razini

Sloj	Reprezentativne kontrole
Rub mreže	Samo TLS promet, rubni WAF i DDoS zaštita, privatne krajnje točke, segmentacija sa zadanim uskraćivanjem
Identitet i pristup	Kratkotrajni potpisani tokeni, bcrypt hashiranje, RBAC, izolacija po organizaciji
Aplikacija	Validacija sheme na svim ulazima, pristup podacima samo putem ORM, kodiranje izlaza, ograničavanje brzine
Zaštita podataka	Enkripcija u mirovanju, trezor tajni s upravljanim identitetom, rezidentnost podataka u EU, obrada uvjetovana privolom
Upravljanje i privatnost	Prilagodljivo zadržavanje, brisanje jedne cjeline, AI s čovjekom u petlji, revizijsko bilježenje
Kontinuirano jamstvo	Automatizirani paket testova, ponovljiva penetracijska testiranja, periodične interne sigurnosne revizije

Ostatak ovog dokumenta prolazi kroz svaki sloj redom, a zatim opisuje kako kontinuirano dokazujemo da ti slojevi ostaju čvrsti.

5. Mrežna sigurnost

5.1 Privatno prema zadanim postavkama

Podatkovni sloj privatan je po konstrukciji. Upravljana PostgreSQL baza podataka ima onemogućen javni mrežni pristup i dostupna je samo putem privatne krajnje točke. Privatna objektna pohrana konfigurirana je tako da prema zadanim postavkama uskraćuje mrežni pristup, u potpunosti onemogućuje shared access ključeve i dostupna je samo putem upravljanog identiteta iz podmreže aplikacije. Predmemorija, AI usluge i trezor tajni također su dostupni putem privatnih krajnjih točaka uz privatno DNS razrješenje.

U praksi to znači da ne postoji internetski dostupan connection string do baze podataka niti javni URL pohrane za audio kandidata: baza podataka i privatna pohrana imaju izričito onemogućen javni mrežni pristup. Trezor tajni aplikacija dohvaća putem privatne krajnje točke i zaštićen je autentikacijom identiteta platforme i politikama pristupa s najmanjim privilegijama, pri čemu identiteti aplikacije imaju odobren samo pristup za čitanje onih tajni koje su im potrebne, tako da se tajne ne mogu dohvatiti bez valjanog, autoriziranog identiteta. Površina napada koju vanjski protivnik uopće može dosegnuti ograničena je na HTTPS krajnje točke aplikacije iza rubnog sloja.

5.2 Segmentacija mreže

Svako je okruženje podijeljeno na zasebne podmreže za aplikacijski sloj, podatkovni sloj i asinkronog radnika. Svakom podmrežom upravlja network security group čije završno pravilo uskraćuje sav ulazni promet. Podmreža aplikacije prihvaća samo ulazni HTTPS. Podatkovna podmreža prihvaća samo specifične portove za bazu podataka, predmemoriju i trezor, i to samo iz podmreže aplikacije ili administrativnog VPN-a. To znači da čak ni napadač koji bi nekako dosegnuo aplikacijski sloj ne može slobodno pivotirati prema podatkovnom sloju; dopuštene su samo putanje koje aplikacija legitimno koristi.

5.3 Rub

Javni promet aplikacije postavljen je iza rubnog sloja koji pruža web application firewall, DDoS zaštitu i content delivery network. Preuzimanja izdanja i dokumenata poslužuju se iz namjenskog javnog računa za pohranu putem front door sloja za isporuku sadržaja, potpuno odvojeno od privatne pohrane koja sadrži podatke kandidata. Te dvije ravnine pohrane nikada se ne miješaju: pogrešna konfiguracija javne ravnine ne može izložiti privatne podatke kandidata, jer se radi o različitim računima s različitim mrežnim pravilima.

5.4 Administrativni pristup

Ne postoji javna administrativna krajnja točka prema privatnoj mreži. Operateri se povezuju putem point-to-site VPN pristupnika koji koristi autentikaciju temeljenu na certifikatima. Administrativni pristup bazi podataka i predmemoriji moguć je samo iz tog tunela, budući da te usluge imaju onemogućen javni mrežni pristup. Time se svakodnevne operacije u potpunosti drže izvan javnog interneta.

6. Upravljanje identitetom i pristupom

6.1 Autentikacija

Korisničke sesije uspostavljaju se potpisanim pristupnim tokenom koji vrijedi trideset minuta, uparenim s odvojenim neprozirnim tokenom za osvježavanje na strani poslužitelja. Pristupni tokeni provjeravaju se pri svakom zahtjevu, a korisnik se ponovno validira prema bazi podataka (uključujući provjeru aktivnog računa) umjesto da se vjeruje isključivo sadržaju tokena. Odjava odmah opoziva sesiju osvježavanja na strani poslužitelja, tako da ukradeni token za osvježavanje ne može nadživjeti odjavu.

Lozinke se nikada ne pohranjuju u čistom tekstu. Hashiraju se pomoću bcrypt uz jedinstveni salt za svaku lozinku. Za organizacije koje preferiraju single sign-on, platforma podržava OAuth prijavu s Microsoft i Google, u kojem slučaju se lozinka uopće ne pohranjuje.

Vlasništvo nad adresom e-pošte verificira se putem jednokratne, vremenski ograničene poveznice za verifikaciju prije nego što se samoregistrirani račun smatra verificiranim, a ponovno slanje verifikacijskih poruka e-pošte ograničeno je kako bi se spriječila zlouporaba.

6.2 RBAC

Autorizacija se provodi kroz model uloga s četiri uloge rastuće razine privilegija: interviewer, hiring manager, recruiter i administrator. Pristup privilegiranim operacijama provodi se putem ovisnosti na strani poslužitelja koje provjeravaju i ulogu i status verifikacije pozivatelja. Ove provjere uloga štite znatno više od stotinu različitih API operacija.

Uloga	Tipične mogućnosti
Interviewer	Provodi dodijeljene intervjue; vidi samo intervjue dodijeljene njemu
Hiring manager	Upravlja zapošljavanjima kojima je vlasnik ili njihov član
Recruiter	Potpuno upravljanje zapošljavanjem i kandidatima unutar organizacije
Administrator	Postavke organizacije, naplata, upravljanje korisnicima i API ključevima

Uz grube provjere uloga, platforma primjenjuje pravila vidljivosti na razini podataka. Hiring manager vidi samo zapošljavanja koja je stvorio ili čiji je član; interviewer vidi samo intervjue dodijeljene njemu. Privilegije se stoga provode i na razini pitanja "koja radnja" i na razini pitanja "koji zapisi".

6.3 Izolacija po organizaciji

Platforma je multitenantna, a izolacija tenanata tretira se kao sigurnosna kontrola prve klase. Svaki autentificirani identitet nosi identifikator organizacije, a upiti nad podacima ograničeni su na tu organizaciju. Kada korisnik zatraži zapis koji pripada drugoj organizaciji, platforma vraća odgovor "not found" umjesto da otkrije postojanje tog zapisa. Interni identifikatori baze podataka nikada se ne izlažu na komunikacijskom sloju; API prikazuje identifikatore za prikaz i ponovno ih mapira po zahtjevu, čime se uklanja česta klasa napada enumeracije između tenanata.

To nije samo projektna namjera. Kao što je opisano u Odjeljku 12, naš automatizirani paket pokreće veliku matricu između organizacija koja pokušava pristupiti podacima jedne organizacije koristeći vjerodajnice druge i potvrđuje da svaki takav pokušaj ne uspijeva.

6.4 Programski pristup

Za integracije organizacije na odgovarajućim planovima mogu izdavati API ključeve. Ključevi koriste prepoznatljiv prefiks, sadrže 128 bita entropije i pohranjuju se samo kao hash; sirovi ključ prikazuje se jednom pri stvaranju i nikada više. Svaki ključ nosi izričit opseg dozvola (čitanje, pisanje ili ATS integracija), može biti ograničen na određene izvorne mreže, može se trenutačno opozvati i podliježe ograničenjima brzine po ključu izvedenima iz razine plana organizacije. Verifikacija ključeva koristi usporedbu sigurnu na vremenske razlike kako bi se izbjeglo curenje informacija kroz vrijeme odgovora.

7. Sigurnost aplikacije

Aplikacija je napisana tako da ukloni cijele kategorije ranjivosti, a ne da ih krpa pojedinačno.

• **Injekcija.** Sav pristup bazi podataka odvija se kroz object-relational mapper s parametriziranim upitima. Baza koda ne sadrži sirovi SQL formatiran nizovima. Time se strukturno eliminira SQL injection.

• **Validacija ulaza.** Svako tijelo zahtjeva validira se prema strogoj shemi prije nego što dosegne poslovnu logiku. Preveliki payloadi se odbijaju, a krajnje točke za popise paginiraju se kako bi se ograničila potrošnja resursa.

• **Kodiranje izlaza i cross-site scripting.** Tekst koji dostavi korisnik i tekst koji generira AI tretiraju se kao nepouzdani. Gdje se sadržaj mora prikazati kao HTML, prolazi kroz sanitizer s popisom dopuštenih elemenata u trenutku upisa, a namjenski paket testova potvrđuje da se script tagovi, event handleri i javascript URL-ovi uklanjaju.

• **Masovno dodjeljivanje.** Operacije ažuriranja koriste izričite sheme koje isključuju privilegirana polja kao što su uloga, organizacija i stanje kredita, tako da klijent ne može eskalirati privilegije slanjem dodatnih polja.

• **Ograničavanje brzine.** Autentikacija i krajnje točke sklone zlouporabi ograničene su pomoću trajnog limitera temeljenog na bazi podataka koji preživljava restart i ispravno radi kroz više instanci aplikacije. Prijava, registracija, resetiranje lozinke i ponovno slanje verifikacije imaju vlastita ograničenja. Razrješenje IP adrese klijenta učvršćeno je protiv lažiranja forwarding zaglavlja.

• **Webhookovi.** Ulazni webhookovi od pružatelja plaćanja i e-pošte verificiraju se prema potpisima pružatelja na sirovom tijelu zahtjeva prije obrade.

• **Prijenosi datoteka.** Prijenosi imaju ograničenje veličine, validiraju se, pohranjuju pod generiranim identifikatorima umjesto korisnički zadanih naziva i ograničeni su po zahtjevu i po organizaciji.

• **Sigurnosna zaglavlja.** U produkciji odgovori sadrže strict transport security, opcije za content-type i frame, politiku referrera i restriktivnu permissions policy te potiskuju bannere poslužitelja i frameworka.

8. Zaštita podataka

8.1 Enkripcija

Svi podaci enkriptirani su u mirovanju pomoću AES-256 kroz platformne Azure slojeve za enkripciju pohrane i baze podataka. Sav mrežni promet poslužuje se isključivo preko HTTPS koristeći TLS 1.2 ili viši; nekriptirani HTTP preusmjerava se na HTTPS na svakoj razini. U produkciji API i web portal emitiraju strict transport security zaglavlja zajedno sa skupom zaglavlja za učvršćivanje te potiskuju bannere verzija poslužitelja i frameworka.

8.2 Upravljanje tajnama

Tajne aplikacije čuvaju se u centraliziranom trezoru tajni s uključenom purge protection i prozorom soft-delete od devedeset dana. Aplikacije se autentificiraju prema Azure resursima koristeći system-assigned managed identities umjesto dugotrajnih ključeva; na primjer, privatna pohrana ima shared access ključeve potpuno onemogućene, pa je pristup moguć samo kroz dodjele uloga temeljene na identitetu ograničene na pojedinačni resurs. Politike pristupa trezoru daju aplikacijskim principalima pristup samo za čitanje točno onih tajni koje su im potrebne, slijedeći načelo najmanjih privilegija.

8.3 Rezidentnost podataka

Svi podaci korisnika i kandidata pohranjuju se i obrađuju unutar Europske unije. Hosting aplikacije, baza podataka, pohrana, predmemorija i tajne nalaze se u West Europe, a AI obrada radi u EU regijama. Pružatelj AI usluge ne koristi podatke korisnika za treniranje svojih modela.

8.4 Životni ciklus jednog intervjua

Najjasniji način razumijevanja kontrola zaštite podataka jest pratiti jedan intervju od početka do kraja. Privola se prikuplja i bilježi prije bilo kakve obrade. Prijenos je enkriptiran tijekom prijenosa. Transkripcija i analiza odvijaju se unutar podatkovnih centara u EU. Rezultati se upisuju u enkriptiranu pohranu. Svaki zapis zatim je pod upravljanjem jedinstvenog sata zadržavanja koji završava evidentiranim kaskadnim brisanjem. U bilo kojem trenutku prava kandidata poput povlačenja privole, brisanja, pristupa ili prenosivosti mogu prekinuti ovaj tijek.

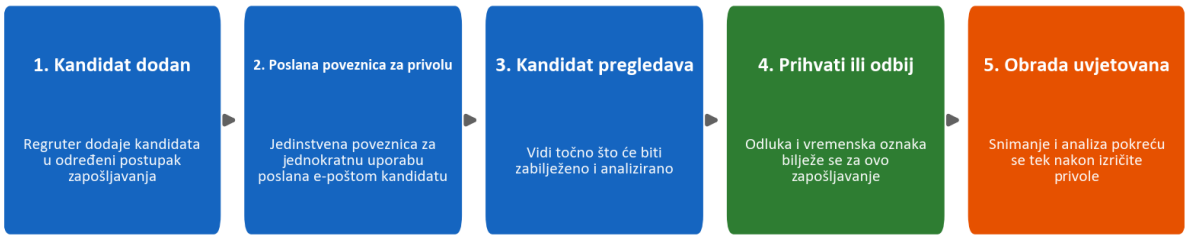
9. Privatnost po dizajnu i GDPR

Privatnost je ugrađena u podatkovni model i tijek rada, a nije naknadno dodana samo kroz politiku.

9.1 Privola

Nijedan intervju ne snima se niti analizira bez izričite privole kandidata. Kada se kandidat doda u proces zapošljavanja, platforma e-poštom izdaje jedinstvenu, jednokratnu poveznicu za privolu. Kandidat pregledava što će se dogoditi i zatim prihvaća ili odbija. Stanje privole, uključujući vrijeme odgovora, bilježi se uz taj konkretni proces zapošljavanja, tako da je privola uvijek vezana uz konkretan postupak zapošljavanja, a ne globalno dana.

Privola kandidata: izričita i zabilježena prije svake obrade



9.2 Zadržavanje i brisanje

Zadržavanje podataka prilagodljivo je po organizaciji, sa zadanih dvanaest mjeseci i prilagodljivim minimumom od trideset dana, a može se nadjačati po kandidatu. Postoji jedan jedinstveni sat zadržavanja za podatke kandidata, a ne zaseban mjerač vremena po artefaktu. Sat počinje kada se zabilježi odluka o zapošljavanju. Prije isteka podataka, platforma šalje upozorenje (prema zadanim postavkama otprilike petnaest dana unaprijed) i nudi produljenje jednim klikom. Kada se podaci brišu, brišu se kao jedna cjelina: zapis kandidata, intervjui, transkripti, audiosnimke, dokumenti i usporedbe uklanjaju se zajedno, a brisanje se bilježi u revizijskom dnevniku. Nema djelomičnih ili napuštenih ostataka.

Životni ciklus u nastavku prikazuje ovaj jedinstveni sat i način na koji se spaja u jedno kaskadno brisanje s evidentiranim dokazom brisanja.

Zadržavanje podataka: jedan sat po kandidatu, brisanje pojedinačne jedinice

9.3 Prava ispitanika i podizvršitelji obrade

Platforma podržava prava ispitanika zahtijevana prema GDPR, uključujući pristup, brisanje, prenosivost, prigovor i objašnjenje. Obrada se provodi u skladu s ugovorom o obradi podataka koji korisnici prihvaćaju pri registraciji i koji je verzioniran po organizaciji. Naši podizvršitelji obrade i njihove uloge, svi unutar EU ili uz odgovarajuće zaštitne mjere, objavljeni su u tom

ugovoru, a korisnici dobivaju prethodnu obavijest o svakoj promjeni. Odjeljak 17 sadrži registar podizvršitelja obrade i mapiranje usklađenosti članak po članak.

10. Odgovorni AI i EU AI Act

Platforma pripada kategoriji visokog rizika prema EU AI Act jer podržava odluke o zapošljavanju, i tu klasifikaciju shvaćamo ozbiljno.

Definirajuće pravilo proizvoda jest da je **AI podrška pri odlučivanju, a ne donositelj odluka.** Sustav nikada automatski ne prihvaća niti odbija kandidata. On transkribira govor, strukturira pitanja i odgovore, ocjenjuje odgovore prema kriterijima koje je definirao regruter i sastavlja povratne informacije, a čovjek pregledava svaki izlaz prije njegove uporabe. Time se čovjek čvrsto zadržava u petlji.

Jednako je važno i ono što AI ne radi. Ne procjenjuje osobnost, "kulturalnu usklađenost", emocionalno stanje, ton glasa, naglasak, spol, dob, etničku pripadnost, izgled ili govor tijela. Ocjenjivanje je usidreno u dokazima iz transkripta i kriterijima koje definira regruter, a imena kandidata isključena su iz ulaza za evaluaciju kako bi se smanjila pristranost. Objavljujemo karticu transparentnosti, korisničku dokumentaciju i izjavu o sukladnosti koja opisuje sustav, njegova ograničenja i njegove zaštitne mjere.

Kontrola odgovornog AI	Kako funkcionira
Čovjek u petlji	Svaku ocjenu i svaki dio povratne informacije pregledava regruter prije uporabe
Bez automatiziranih odluka	Sustav nikada automatski ne prihvaća niti automatski ne odbija kandidata
Ocjenjivanje utemeljeno na dokazima	Ocjene upućuju na potkrepljujuće dokaze iz transkripta
Dizajn protiv pristranosti	Imena su isključena iz evaluacije; sadržaj se ocjenjuje ispred stila
Ograničenja opsega	Osobnost, emocija, naglasak i zaštićena obilježja nikada se ne procjenjuju
Sigurnost povratnih informacija kandidatu	Privatne povratne informacije kandidatu prolaze zaštitnu ogradu sigurnosti generiranja i validacije

Ta ograničenja nisu samo navedena u dokumentaciji; ona su kodirana u prompt sloju AI-ja i provjeravaju se namjenskim programom testiranja AI sigurnosti opisanim u Odjeljku 12.3.

11. Životni ciklus sigurnog razvoja

Sigurnost se provodi kroz način na koji gradimo i isporučujemo softver, a ne samo u sustavu koji radi.

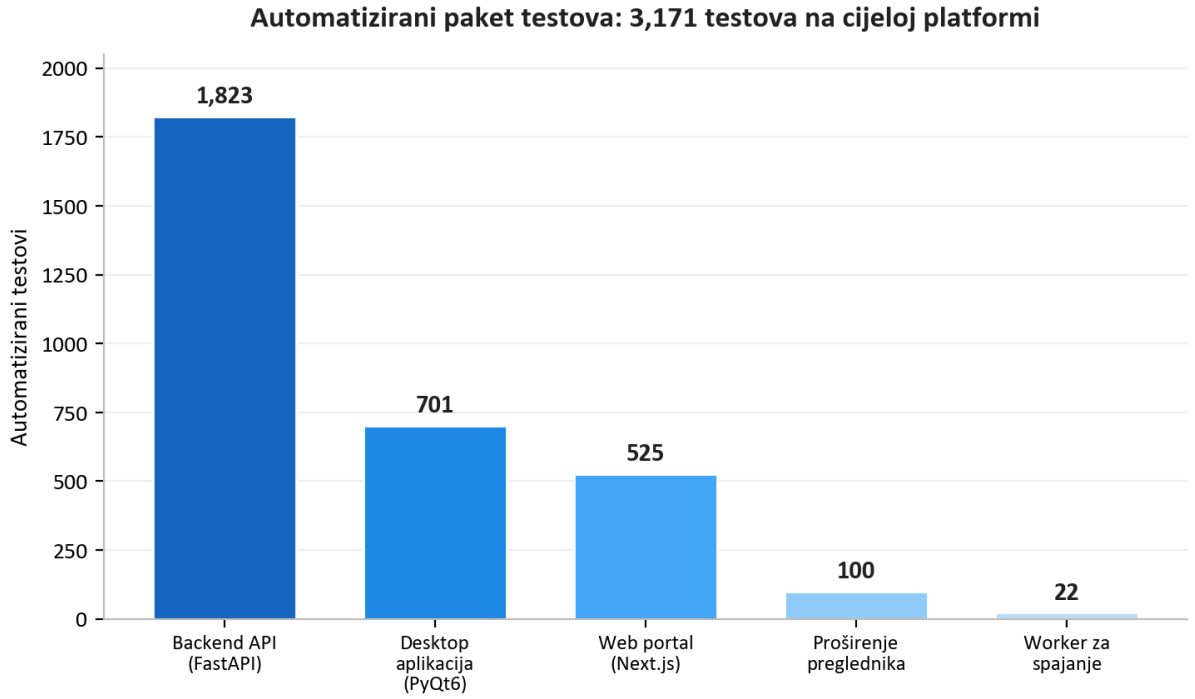
- **Odvajanje okruženja.** Razvoj i produkcija potpuno su odvojeni, svaki sa svojom infrastrukturom, računima za pohranu, bazom podataka, tajnama i poddomenama. Ne postoji zajedničko stanje.
- **Infrastruktura kao kod.** Cijelo cloud okruženje definirano je kao kod i pregledava se kao kod, što sigurnosni položaj čini revizibilnim i ponovljivim. Pregledavatelj može točno vidjeti koji su portovi otvoreni, koji su resursi privatni i koji identiteti imaju koje dozvole.
- **Fiksirane i kontrolirane implementacije.** Svaki korak u CI/CD cjevovodu fiksiran je na točnu, nepromjenjivu verziju. Produkcijske implementacije temelje se na oznakama, izvode se samo kroz zaštićeni produkcijski cjevovod i kontrolirane su obveznim odobrenjem. Automatizirani paket testova radi kao kontrolna točka izdanja: implementacija se ne može isporučiti ako testovi ne uspiju.
- **Higijena ovisnosti.** Automatizirani nadzor ovisnosti tjedno predlaže ažuriranja kroz backend, desktop, web, infrastrukturu i definicije cjevovoda, a revizije ovisnosti dio su našeg periodičnog sigurnosnog pregleda.
- **Potpisani artefakti.** Instalacijski paketi desktop aplikacije digitalno su potpisani, tako da korisnici mogu provjeriti da softver koji instaliraju doista dolazi od nas.
- **Disciplina tajni.** Tajne se nalaze u trezoru i u zaštićenim tajnama cjevovoda, nikada u izvornom kodu.

12. Kontinuirano sigurnosno testiranje

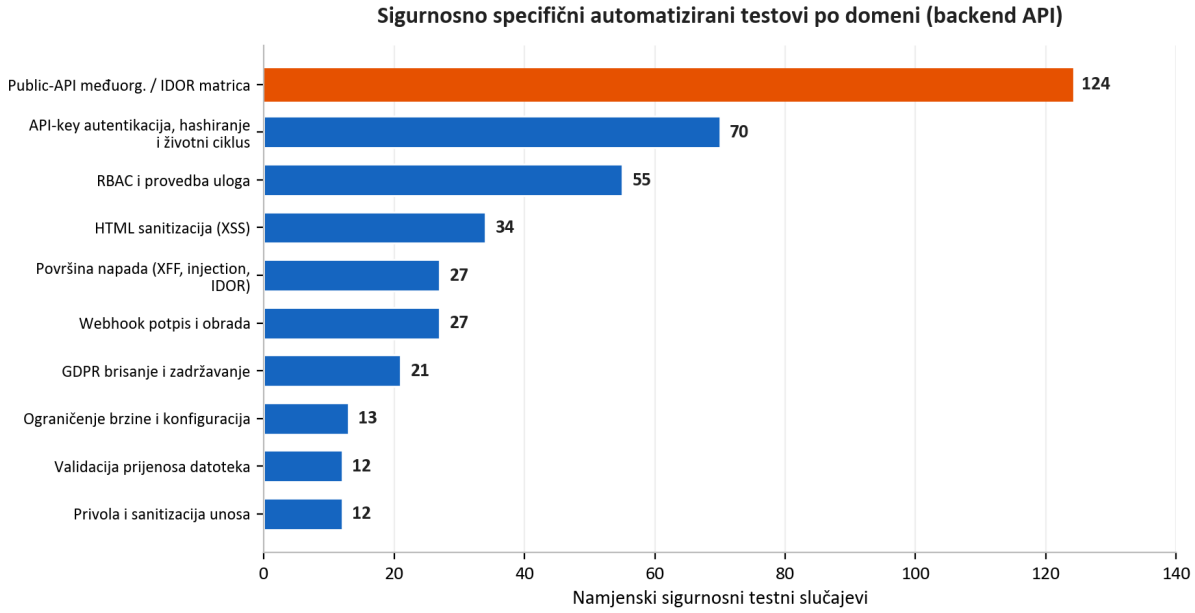
Ovo je srce naše priče o jamstvu i dio koji većina dobavljača ne može pokazati. Sigurnost tretiramo kao nešto što se kontinuirano mjeri izvršivim provjerama, a ne kao tvrdnju iznesenu jednom.

12.1 Automatizirani paket testova

Platforma je pokrivena s **3,171 automatiziranih testova** koji obuhvaćaju backend API, desktop aplikaciju, web portal, proširenje preglednika i radnika za spajanje audiosnimki.



To nisu samo funkcionalni testovi. Značajan, namjenski sigurnosni paket provjerava kontrole opisane ranije u ovom dokumentu. Donji grafikon raščlanjuje sigurnosno specifične testove u backend API-ju po domenama.



Između mnogih drugih, ovaj paket uključuje veliku matricu javnog API-ja koja pokreće svaku krajnju točku kao legitimni korisnik, kao vlastiti API ključ organizacije i kao API ključ suparničke organizacije, potvrđujući da je svaki pokušaj između organizacija blokiran. Uključuje desetke testova površine napada s protivničkim pristupom za lažiranje forwarding zaglavlja, injection zaglavlja i curenje identifikatora, fokusirani paket HTML sanitizacije za cross-site scripting, testove provedbe uloga za puni model uloga i testove koji dokazuju da se podaci kandidata doista brišu kao cjelina. Budući da se ti testovi izvršavaju kao kontrolna točka izdanja, regresija koja oslabi bilo koju od tih kontrola zaustavila bi izdanje umjesto da dođe do korisnika.

12.2 Aktivno penetracijsko testiranje

Automatizirani jedinični testovi dokazuju da se kontrole ispravno ponašaju u izolaciji. Kako bismo dokazali da zajedno funkcioniraju u stvarnoj implementaciji, održavamo ponovljivu metodologiju penetracijskog testiranja koja pokreće stvarne napadačke skripte protiv aktivnog okruženja. Organizirana je u šest faza:

Faza	Fokus	Primjeri onoga što se provjerava
1. Statička analiza	Izvorni kod	Tajne, obrasci injekcije, opasne funkcije, nedostajuća autentikacija, nesiguran HTML
2. Pregled arhitekture	Infrastruktura	Privatne krajnje točke, segmentacija, TLS, konfiguracija tajni
3. Analiza vektora napada	Source control i cloud	Zaštita grana, opseg identiteta, javna izloženost
4. Aktivno penetracijsko testiranje	Aktivno okruženje	Ispitivanje bez autentikacije, pristup između organizacija, injekcija, manipulacija tokenima, SSRF, rafali ograničenja brzine
5. Ocjenjivanje za poduzeća	Zrelost	Šesnaest sigurnosnih kategorija ocijenjenih prema osnovici za poduzeća
6. Ovisnosti i opskrbni lanac	Rizik trećih strana	Revizija CVE-ova ovisnosti, fiksirane akcije cjevovoda, integritet lock datoteka

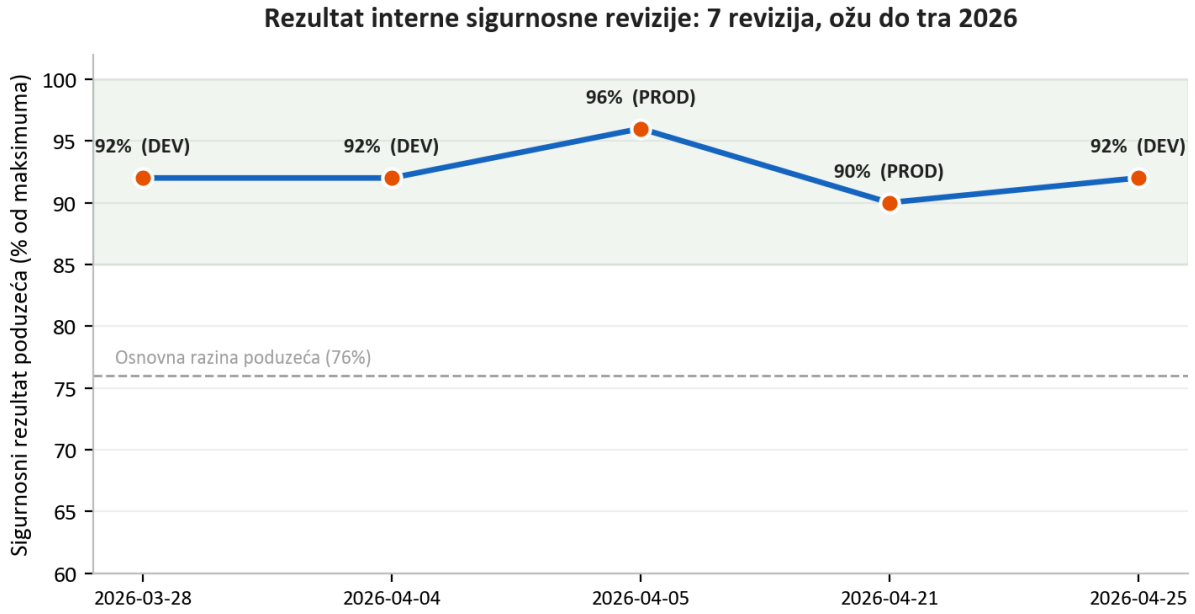
Faza 4 predstavlja stvarno protivničko testiranje nad implementiranim sustavom, a ne kontrolni popis. Ona ispituje zaštićene krajnje točke bez vjerodajnica i potvrđuje da odbijaju pristup; registrira dvije organizacije i pokušava pristupiti zapisima jedne organizacije koristeći račun druge; ubacuje cross-site-scripting i server-side-template payloadove i potvrđuje da su neutralizirani; manipulira autentikacijskim tokenima i potvrđuje da su odbijeni; pokušava server-side request forgery protiv cloud metadata krajnjih točaka; i izaziva rafalni promet na autentikacijskim krajnjim točkama kako bi potvrdila da ograničavanje brzine doista radi u aktivnom okruženju, a ne samo teorijski.

12.3 Testiranje sigurnosti povratnih informacija kandidatu

Budući da platforma može generirati privatne razvojne povratne informacije za kandidate, provodimo zaseban protivnički sigurnosni program nad tom značajkom. On namjerno sustavu daje grube i neprijateljske bilješke regrutera i potvrđuje da izlaz okrenut kandidatu nikada ne sadrži vulgarnosti, nikada ne otkriva niti pripisuje identitet regrutera ili privatno mišljenje i nikada ne primjenjuje osuđujuće etikete osobnosti. Time se štite i kandidat, koji treba dobiti konstruktivne i uvažavajuće povratne informacije, i korisnik, kojem interno mišljenje nikada ne bi smjelo procuriti prema van.

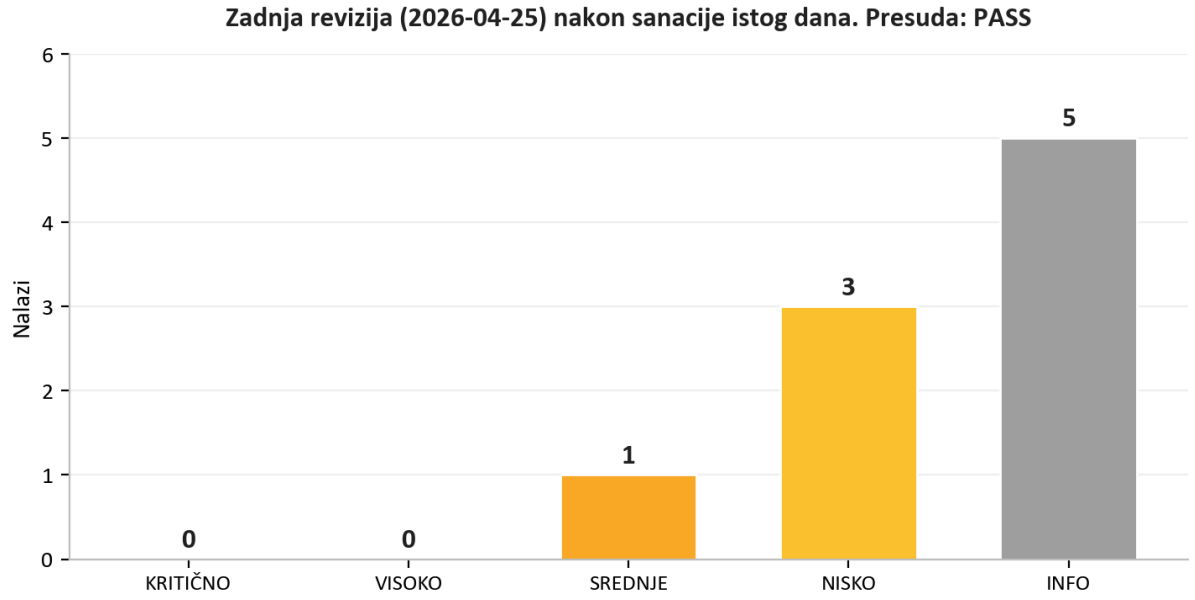
13. Rezultati sigurnosnih revizija

Provodi se periodične sigurnosne revizije koristeći strukturiranu, ponovljivu metodologiju penetracijskog testiranja, a svaka se dokumentira kao datirano izvješće s nalazima ocijenjenima po ozbiljnosti, dokazima i sanacijom. To su interne revizije koje provodi naš vlastiti sigurnosni proces; formalna certifikacija istih kontrola od strane treće strane nalazi se na našem planu razvoja. Između kraja ožujka i kraja travnja 2026. dovršili smo **seven such audits** kroz razvoj i produkciju.



Rezultat koji je potencijalnom korisniku najvažniji jest dosljednost: **across all seven audits there were zero critical findings.** U rijetkim slučajevima kada bi se pojavio problem više ozbiljnosti, on bi bio brzo saniran, često istoga dana, i ponovno verificiran. Rubrika ocjenjivanja tijekom tog je razdoblja namjerno pooštrena (maksimalni mogući rezultat povećan je kako smo dodavali više kategorija za procjenu), zbog čega linija normaliziranog rezultata ostaje visoka čak i kada je ljestvica podignuta.

Naša najnovija revizija, 25 April 2026, ilustrira kako proces funkcionira u praksi. Identificirana su dva problema više ozbiljnosti, oba su ispravljena i ponovno verificirana istoga dana, a revizija je zaključena presudom **PASS** bez preostalih problema spremnih za iskorištavanje unutar aktualnog modela prijetnji.



Revizija	Okruženje	Kritično	Presuda
2026-03-28	Razvoj	0	Spremno za produkciju
2026-04-04	Razvoj	0	Spremno za poduzeća
2026-04-05	Produkcija	0	Spremno za poduzeća
2026-04-20	Razvoj	0	Spremno za produkciju, napomene
2026-04-20	Razvoj	0	Prolaz uz napomene
2026-04-21	Produkcija	0	Sigurno, bez iskoristivih nalaza
2026-04-25	Razvoj	0	Prolaz

Uzorak kroz ove revizije najiskreniji je dokaz koji možemo ponuditi: problemi se pronalaze, jer ih aktivno tražimo, i brzo se zatvaraju, jer je proces izgrađen da ih zatvori. Dobavljač koji nikada ne prijavi nalaz obično je dobavljač koji ih ne traži.

14. Operativna otpornost i podijeljena odgovornost

14.1 Nadzor i zapisivanje

Telemetrija aplikacije i platforme ulijeva se u centralizirani workspace za analitiku zapisnika i uslugu nadzora aplikacije, što nam daje vidljivost u dostupnost i ponašanje. Osjetljive radnje poput brisanja podataka, prihvaćanja pravnih ugovora i AI poziva bilježe se u namjenskim revizijskim tablicama, tako da postoji trajan zapis o tome tko je što učinio s važnim podacima.

14.2 Sigurnosne kopije i oporavak

Upravljana baza podataka zadržava automatizirane sigurnosne kopije, a privatna pohrana zaštićena je soft-delete zadržavanjem i za blobove i za kontejnere, tako da se slučajno ili zlonamjerno brisanje može oporaviti unutar prozora zadržavanja. Kritična infrastruktura ima zaključavanja brisanja kako bi se spriječilo slučajno uklanjanje produkcijskih resursa.

14.3 Sažetak podijeljene odgovornosti

Područje	AI Interview Analyzer	Korisnik
Infrastruktura, mreža, patchiranje	Da	-
Sigurnost aplikacije i AI cjevovod	Da	-
Enkripcija, tajne, rezidentnost podataka	Da	-
Upravljanje korisnicima i ulogama	Pruža kontrole	Upravlja korisnicima i ulogama
Konfiguracija politike zadržavanja	Pruža kontrole	Postavlja razdoblje zadržavanja
Privola kandidata	Pruža tijek rada	Osigurava da se koristi
Snažne vjerodajnice krajnjih korisnika i SSO	Podržava SSO i politiku	Provodi internu politiku

15. Model prijetnji i OWASP mapiranje

Projektiramo protiv konkretnog skupa protivnika: vanjskog napadača bez vjerodajnica, znatiželjnog ili zlonamjernog autentificiranog korisnika jedne organizacije koji pokušava dosegnuti podatke druge organizacije, kompromitiranu ovisnost i internu pogrešku. Donja tablica mapira široko korištene kategorije rizika OWASP Top 10 na specifične kontrole koje ih rješavaju u ovoj platformi, a svaka od njih provjerava se testiranjem opisanim u Odjeljku 12.

OWASP rizik	Kako ga platforma ublažava
Neispravna kontrola pristupa	RBAC na svakoj privilegiranoj krajnjoj točki; ograničavanje po organizaciji; "not found" pri pristupu između organizacija; ponovno mapiranje identifikatora; matrica testiranja između organizacija
Kriptografski propusti	TLS 1.2+ u prijenosu; AES-256 u mirovanju; bcrypt hashiranje lozinki; tajne u upravljanom trezoru
Injekcija	Parametrizirani upiti samo putem ORM; stroga validacija sheme; HTML sanitizacija u trenutku upisa
Nesiguran dizajn	Slojevita višeslojna obrana; modeliranje prijetnji i pregled arhitekture u svakoj reviziji
Sigurnosna pogrešna konfiguracija	Infrastruktura kao kod; mrežne grupe sa zadanim uskraćivanjem; sigurnosna zaglavlja; onemogućeni shared storage ključevi; API shema nije izložena u produkciji
Ranjive komponente	Tjedni automatizirani nadzor ovisnosti; revizije CVE-ova ovisnosti u periodičnom pregledu
Propusti identifikacije i autentikacije	Kratkotrajni tokeni; prijava s ograničenjem brzine; verifikacija e-pošte; podrška za SSO; bez lozinki u čistom tekstu
Propusti integriteta softvera i podataka	Fiksirani, nepromjenjivi koraci cjevovoda; potpisani desktop instalacijski paketi; verifikacija potpisa webhookova; produkcijske implementacije kontrolirane oznakama
Propusti sigurnosnog zapisivanja i nadzora	Centralizirana telemetrija; namjenske revizijske tablice za osjetljive radnje
Server-side request forgery	Izlazni pozivi ograničeni na pouzdane krajnje točke; SSRF probe u okviru za penetracijsko testiranje

Ovo mapiranje čini okosnicu našeg argumenta jamstva: za svaku dobro poznatu klasu napada postoji imenovana kontrola, a za svaku imenovanu kontrolu postoji test.

16. Upravljanje ranjivostima i odgovorno otkrivanje

Sigurnost nikada nije dovršena, pa provodimo kontinuiranu petlju otkrivanja i sanacije.

• **Otkrivanje.** Ranjivosti se otkrivaju iz četiri izvora: automatiziranog paketa testova, periodičnih revizija penetracijskog testiranja, automatiziranog nadzora ovisnosti i prijava korisnika ili istraživača.

• **Trijaža.** Svakom nalazu dodjeljuje se razina ozbiljnosti (critical, high, medium, low ili informational) s dokazima i vlasnikom sanacije, točno kako je zabilježeno u našim revizijskim izvješćima.

• **Ciljevi sanacije.** Critical i high nalazi imaju prioritet za trenutačnu sanaciju; u našoj povijesti revizija nalazi veće ozbiljnosti obično su rješavani i ponovno verificirani istoga dana. Medium i niži nalazi planiraju se u redovni ciklus održavanja.

• **Verifikacija.** Ispravci se ponovno testiraju, a kada je relevantno provodi se i aktivna provjera nad implementiranim okruženjem kako bi se potvrdilo da je problem doista zatvoren, a ne samo zatvoren u kodu.

• **Otkrivanje.** Sigurnosni problemi mogu nam se prijaviti izravno. Potvrđujemo primitak prijava, istražujemo ih i obavještavamo prijavitelja do razrješenja.

17. Mapiranje usklađenosti

17.1 GDPR

GDPR područje	Implementacija platforme
Pravna osnova (Art. 6)	Izričita privola kandidata prikupljena prije obrade
Minimizacija podataka i ograničenje pohrane (Art. 5)	Obrađuju se samo podaci relevantni za intervju; prilagodljivo zadržavanje s automatskim brisanjem
Pravo na brisanje (Art. 17)	Brisanje svih podataka kandidata kao jedne cjeline, uz evidentirani dokaz brisanja
Prava ispitanika (Art. 15 to 20)	Podržani su pristup, brisanje, prenosivost i prigovor
Obveze izvršitelja obrade (Art. 28)	Ugovor o obradi podataka prihvaća se pri registraciji i verzioniran je po organizaciji
Sigurnost obrade (Art. 32)	Enkripcija, kontrola pristupa, izolacija i kontinuirano testiranje kako je opisano u ovom dokumentu
Transparentnost podizvršitelja obrade	Objavljeno u ugovoru o obradi podataka uz prethodnu obavijest o promjeni

17.2 EU AI Act

Platforma se tretira kao visokorizični AI sustav koji podržava odluke o zapošljavanju, i održavamo dokumentaciju usklađenu s regulativom, uključujući karticu transparentnosti, korisničku dokumentaciju i izjavu o sukladnosti. Temeljne zaštitne mjere, ljudski nadzor, transparentnost, ocjenjivanje utemeljeno na dokazima i stroga ograničenja opsega onoga što AI procjenjuje opisani su u Odjeljku 10. Nastavljamo razvijati našu formalnu dokumentaciju o sukladnosti kako implementacijski rok regulative napreduje.

17.3 Certifikacije hostinga

Platforma radi u cijelosti na Microsoft Azure, čiji podatkovni centri posjeduju neovisne certifikacije uključujući ISO 27001 i SOC 2. Te certifikacije pokrivaju fizičke i platformne slojeve ispod naše aplikacije; kontrole na razini aplikacije opisane su kroz cijeli ovaj dokument.

17.4 Registar podizvršitelja obrade

Podizvršitelj obrade	Svrha	Regija
Microsoft Azure	Hosting, AI i obrada govora, pohrana, transakcijska e-pošta	EU (West Europe, Sweden Central)
Stripe	Obrada pretplata i plaćanja	EU (Ireland)
Fakturownia	Fakturiranje	EU (Poland)
ATS connector (optional)	Integracija za praćenje kandidata, omogućena samo na zahtjev	EU

18. Sigurnosni plan razvoja

Sigurnost tretiramo kao program kontinuiranog poboljšavanja. Trenutačne inicijative na našem planu razvoja uključuju jačanje opcija višefaktorske autentikacije za administrativne račune, proširenje centraliziranog revizijskog zapisivanja pristupa podacima, nastavak redovitog pooštravanja ažurnosti ovisnosti i napredovanje prema formalnoj certifikaciji kontrola opisanih u ovom dokumentu od strane treće strane. Ništa od navedenog nije praznina koja danas izlaže podatke korisnika; svaka stavka predstavlja poboljšanje već slojevito postavljenog sigurnosnog stanja.

19. Sažetak

AI Interview Analyzer štiti podatke kandidata i korisnika kroz slojevitu arhitekturu: privatnu mrežu prema zadanim postavkama bez javnih podatkovnih usluga, snažan identitet i izolaciju po organizaciji, aplikacijski kod koji projektno uklanja cijele klase ranjivosti, enkripciju i rezidentnost podataka u EU te kontrole privatnosti ugrađene u podatkovni model. Ono što platformu izdvaja jesu dokazi iza tih tvrdnji. S 3,171 automatiziranih testova, ponovljivom metodologijom aktivnog penetracijskog testiranja, namjenskim programom sigurnosti AI-ja i evidencijom od sedam internih sigurnosnih revizija s zero critical findings, možemo pokazati, a ne samo reći, da je platforma sigurna.

Dodatak A: Katalog sigurnosnih kontrola

Sažeta referenca primarnih kontrola i dokaza koji podupiru svaku od njih.

Kontrola	Mehanizam	Dokaz
Enkripcija prijenosa	Samo HTTPS, TLS 1.2+, HTTP preusmjeren	Infrastruktura kao kod; revizija arhitekture
Enkripcija u mirovanju	AES-256 platformna enkripcija pohrane i baze podataka	Konfiguracija platforme; revizija arhitekture
Zaštita lozinki	bcrypt sa saltom za svaku lozinku	Source control; testovi autentikacije
Upravljanje sesijama	30-minutni potpisani tokeni, opozivo osvježavanje na strani poslužitelja	Source control; testovi autentikacije
Autorizacija	Kontrola pristupa s četiri uloge na privilegiranim krajnjim točkama	Paket testova provedbe uloga
Izolacija tenanata	Ograničavanje upita po organizaciji; 404 pri pristupu između organizacija	Matrica testiranja između organizacija
Sigurnost API ključeva	Pohrana kao hash, ograničene dozvole, ograničenja brzine po ključu	Paket testova API ključeva
Obrana od injekcije	Parametrizirani upiti samo putem ORM	Statička analiza; testovi injekcije
Obrana od cross-site scripting	HTML sanitizacija u trenutku upisa	Paket testova HTML sanitizacije
Ograničavanje brzine	Trajni limiter temeljen na bazi podataka na autentikacijskim krajnjim točkama	Testovi ograničenja brzine; aktivne provjere rafala
Integritet webhookova	Verifikacija potpisa pružatelja na sirovom tijelu	Paket testova webhookova
Upravljanje tajnama	Upravljani trezor, purge protection, upravljani identitet	Infrastruktura kao kod; revizija arhitekture
Mrežna izolacija	Privatne krajnje točke; segmentacija sa zadanim uskraćivanjem	Infrastruktura kao kod; revizija arhitekture
Brisanje podataka	Kaskadno brisanje jedne cjeline uz revizijski dnevnik	Paket GDPR testova brisanja
Opskrbni lanac	Fiksirani koraci cjevovoda; tjedni nadzor ovisnosti	Konfiguracija cjevovoda; revizija ovisnosti

Dodatak B: Često postavljana pitanja za sigurnosne pregledavatelje

Gdje se pohranjuju naši podaci? U cijelosti unutar Europske unije, na Microsoft Azure, u West Europe uz AI obradu u EU regijama. Podaci kandidata nikada ne napuštaju EU.

Koriste li se naši podaci za treniranje AI modela? Ne. Pružatelj AI usluge ne koristi podatke korisnika za treniranje.

Je li baza podataka dostupna s interneta? Ne. Javni mrežni pristup je onemogućen, a baza podataka dostupna je samo putem privatne krajnje točke unutar virtualne mreže.

Može li jedan korisnik vidjeti podatke drugog korisnika? Ne. Svaki upit ograničen je na organizaciju pozivatelja, pristup između organizacija vraća "not found", a automatizirana matrica kontinuirano testira ovu izolaciju.

Kako se pohranjuju lozinke? Hashirane pomoću bcrypt i jedinstvenog salta za svaku lozinku. Podržan je single sign-on s Microsoft i Google, u kojem slučaju se lozinka ne pohranjuje.

Podržavate li single sign-on? Da, putem Microsoft i Google OAuth.

Koliko dugo vrijede pristupni tokeni? Trideset minuta, upareni s opozivom sesijom osvježavanja na strani poslužitelja koja se poništava pri odjavi.

Kako se upravlja privolom kandidata? Svaki kandidat prima jedinstvenu, jednokratnu poveznicu za privolu i mora je prihvatiti prije bilo kakvog snimanja ili analize. Privola se bilježi uz konkretni proces zapošljavanja.

Kako se brišu podaci? Kao jedna cjelina koja obuhvaća zapis kandidata, intervjue, transkripte, audio, dokumente i usporedbe, prema prilagodljivom rasporedu zadržavanja, uz evidentirani dokaz brisanja. Kandidati također mogu izravno zatražiti brisanje.

Imate li ugovor o obradi podataka? Da, prihvaća se pri registraciji i verzioniran je po organizaciji, uključujući registar podizvršitelja obrade.

Donosi li AI odluke o zapošljavanju? Ne. Pruža samo podršku pri odlučivanju; čovjek pregledava svaki izlaz i donosi sve odluke.

Kako dokazujete svoje sigurnosne tvrdnje? Kroz 3,171 automatiziranih testova uključujući namjenski sigurnosni paket, ponovljivu metodologiju penetracijskog testiranja u šest faza koja se provodi nad aktivnim okruženjima, program testiranja sigurnosti AI-ja i periodična pisana revizijska izvješća.

Što se događa kada pronađete ranjivost? Dodjeljuje joj se razina ozbiljnosti s dokazima i vlasnikom, sanira se prema prioritetnom rasporedu, ponovno verificira uključujući aktivne provjere gdje je relevantno i bilježi u revizijskom izvješću.

Možemo li provesti vlastito penetracijsko testiranje? Sigurnosne procjene mogu se dogovoriti putem vašeg predstavnika računa uz odgovarajući opseg i raspored.

Dodatak C: Glosar

Pojam	Značenje
AES-256	Snažan standard simetrične enkripcije koji se koristi za zaštitu podataka u mirovanju
bcrypt	Namjenski izrađena funkcija za hashiranje lozinki sa saltanjem za svaku lozinku
Managed identity	Identitet koji izdaje platforma i koji omogućuje usluzi autentikaciju bez pohranjenih ključeva
Private endpoint	Privatna mrežna adresa koja cloud uslugu drži izvan javnog interneta
Network security group	Skup pravila dopuštanja i uskraćivanja koja filtriraju mrežni promet prema podmreži
RBAC	Kontrola pristupa temeljena na ulogama, koja dodjeljuje dozvole prema ulozi korisnika
IDOR	Insecure direct object reference, propust kontrole pristupa od kojeg se platforma brani
SSRF	Server-side request forgery, klasa napada koja se ispituje u našim penetracijskim testovima
Web application firewall	Rubna kontrola koja filtrira zlonamjerni web promet
Data processing agreement	Ugovor koji uređuje kako izvršitelj obrade rukuje osobnim podacima u ime voditelja obrade

Dodatak D: Kontakt i upravljanje dokumentom

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Za sigurnosni pregled, kopiju našeg ugovora o obradi podataka ili naše dokumentacije o sukladnosti s EU AI Act, obratite se svojem predstavniku računa.

Ovaj dokument opisuje sigurnosni položaj usluge AI Interview Analyzer na datum generiranja prikazan u podnožju. Dostavlja se u svrhe procjene i ne čini dio bilo kojeg ugovora. Specifične ugovorne sigurnosne obveze utvrđene su u primjenjivom ugovoru i ugovoru o obradi podataka.