Drošības baltais dokuments

Enterprise Security Overview - AI Interview Analyzer

Pakalpojumu sniedzējs:	AI Interview Analyzer Sp. z o.o.
Adrese:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Klasifikācija:	PUBLIC
Datums:	24.06.2026

Contents

Drošības baltais dokuments

Pakalpojuma sniedzējs: AI Interview Analyzer Sp. z o.o., Warszawa, Poland

Mērķauditorija: Uzņēmumu drošības, IT un iepirkumu komandas

Klasifikācija: Publisks

1. Kopsavilkums

AI Interview Analyzer ir uzņēmuma līmeņa personāla atlases platforma, kas ar nepārprotamu kandidāta piekrišanu ieraksta intervijas, tās transkribē un strukturē, kā arī nodrošina uz pierādījumiem balstītu novērtēšanas atbalstu personāla atlases speciālistiem. Tā kā platforma apstrādā kandidātu personas datus un atbalsta atlases procesus, drošība un privātums tiek uzskatīti par primāriem projektēšanas ierobežojumiem, nevis par vēlāk pievienotām funkcijām.

Šajā baltajā dokumentā konkrētos un pārbaudāmos terminos aprakstīts, kā mēs aizsargājam klientu un kandidātu datus. Tas ir rakstīts tiem, kuri izvērtē piegādātājus: drošības inženieriem, IT administratoriem, datu aizsardzības speciālistiem un iepirkumu komandām. Katrs skaitlis šajā dokumentā ir iegūts tieši no mūsu pašu inženiertehniskajām sistēmām, nevis no mārketinga materiāliem.

Centrālais vēstījums ir vienkāršs: **mēs ne tikai apgalvojam, ka platforma ir droša, mēs nepārtraukti pārbaudām, ka tā ir droša.** Mūsu koda bāzē ir **3,171 automatizēti testi**, tostarp īpaša drošības testu kopa, kas pārbauda autentifikāciju, autorizāciju, izolāciju starp organizācijām, aizsardzību pret injekcijām un datu dzēšanu. Papildus tam mēs īstenojam atkārtojamu ielaušanās testēšanas sistēmu pret aktīvajām izvietošanas vidēm un sagatavojam rakstiskus audita ziņojumus. Septiņos iekšējos drošības auditos 2026. gada martā un aprīlī mēs konstatējām **zero critical findings**, un mūsu jaunākais audits noslēdzās ar verdiktu **PASS**. (Šo kontroļu formāla trešās puses sertifikācija ir iekļauta mūsu attīstības plānā; skatiet 18. sadaļu.)

Drošības raksturlielums	Kopsavilkums
Mitināšana	Microsoft Azure, tikai ES reģioni
Tīkla modelis	Privāti galapunkti, noklusējuma-liegt tīkla segmentēšana, nav publiskas datubāzes
Šifrēšana	AES-256 glabāšanā, TLS 1.2 vai augstāka versija pārraidē
Identitāte	Īslaicīgi parakstīti tokeni, bcrypt paroļu jaukšana, SSO atbalsts
Piekļuves kontrole	Lomu balstīta piekļuves kontrole ar stingru izolāciju katrai organizācijai
Noslēpumi	Centralizēta noslēpumu glabātuve ar managed-identity piekļuvi
Privātums	Nepārprotama piekrišana, konfigurējama glabāšana, dzēšana kā vienotai vienībai
Atbildīgs AI	Tikai lēmumu atbalsts, cilvēks vienmēr ir procesā
Pārliecība	3,171 automatizēti testi, kā arī periodiski ielaušanās testi un auditi

1.1 Kā lasīt šo dokumentu

3. līdz 11. sadaļa apraksta kontroles mehānismus, kas aizsargā datus: arhitektūru, tīklu, identitāti, lietojumprogrammu, datu aizsardzību, privātumu un drošas izstrādes dzīves ciklu. 12. un 13. sadaļa aptver mūsu raksturīgo nepārtrauktās testēšanas programmu un auditu vēsturi. 14. līdz 17. sadaļa aptver operācijas, draudu modelēšanu, ievainojamību pārvaldību un atbilstības kartējumu. Pielikumos ir kontroles katalogs, FAQ izvērtētājiem un glosārijs, ko drošības komanda var izmantot tieši novērtēšanas laikā.

2. Dokumenta tvērums un pieeja

2.1 Ko šis dokuments aptver

Šis baltais dokuments aptver AI Interview Analyzer pakalpojuma drošības arhitektūru un praksi: mitināšanas vidi, tīkla dizainu, identitātes un piekļuves pārvaldību, lietojumprogrammas līmeņa kontroles, datu aizsardzību, privātuma un regulatīvo prasību atbilstību, drošas izstrādes dzīves ciklu un mūsu nepārtrauktās drošības testēšanas programmu.

2.2 Kas padara to pārbaudāmu

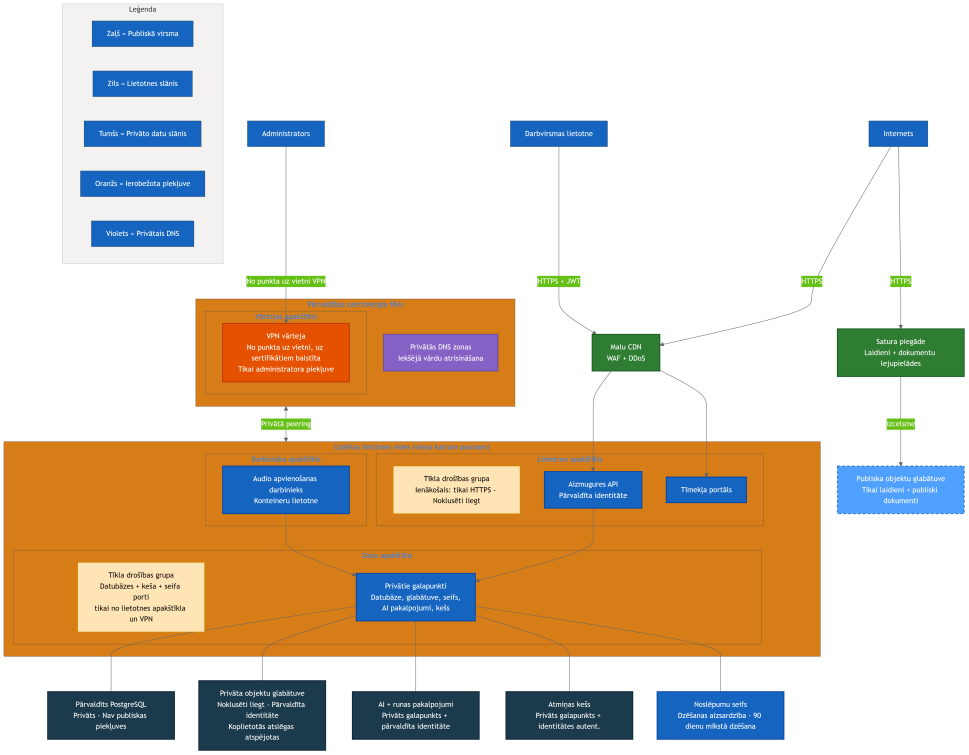
Piegādātāju drošības apgalvojumus ir viegli uzrakstīt un grūti uzticami novērtēt. Tāpēc katru galveno apgalvojumu šajā dokumentā esam sasaistījuši ar kaut ko konkrētu un izmērāmu mūsu inženiertehniskajās sistēmās: kontroli, kas ieviesta kodā, testu, kas pierāda, ka kontrole darbojas, infrastruktūras definīciju, kas to nodrošina, vai audita ziņojumu, kas fiksē dokumentētu pārbaudi. Ja kontrole ir daļa no mūsu nākotnes plāna, nevis šodien jau piegādāta funkcionalitāte, mēs to norādām nepārprotami. Mēs labāk apgalvosim mazāk un saglabāsim uzticību, nekā apgalvosim pārāk daudz un tiksim pieķerti.

2.3 Dalītā atbildība

Platforma tiek nodrošināta kā programmatūra kā pakalpojums. Mēs pārvaldām infrastruktūru, lietojumprogrammu, AI procesu plūsmu un datu apstrādi. Klients ir atbildīgs par savu lietotāju kontu un lomu pārvaldību, datu glabāšanas termiņu konfigurēšanu atbilstoši savām iekšējām politikām un par to, lai kandidāta piekrišana tiktu iegūta, izmantojot platformas nodrošināto piekrišanas darbplūsmu. 14. sadaļā šis sadalījums ir aprakstīts detalizētāk.

3. Drošības arhitektūras pārskats

Platforma ir izveidota kā neliels skaits savstarpēji sadarbojošos pakalpojumu, nevis kā viens monolīts. Darbvirsmas lietojumprogramma un tīmekļa portāls darbojas kā klienti. Centrālais backend API pārvalda visu noturīgo glabāšanu, autentifikāciju, norēķinus, AI procesu plūsmu, piekrišanu, e-pastu, failu apstrādi un informācijas paneļus. Audio apvienošanas darbinieks ierakstus apstrādā asinhroni. Visa sensitīvā informācija atrodas aiz backend API; klienti nekad nesazinās tieši ar datubāzi, glabātuvi vai AI pakalpojumiem.



Iepriekš redzamā diagramma parāda ražošanas topoloģiju, kur resursu nosaukumi ir apzināti vispārināti. Tajā ir redzami trīs principi:

- **Nav tiešas datu pakalpojumu publiskas pieejamības.** Datubāzei, privātajai objektu glabātuvei, AI pakalpojumiem un kešatmiņai ir atspējota publiskā tīkla piekļuve, un tie ir sasniedzami tikai caur privātajiem galapunktiem izolētā virtuālajā tīklā. Noslēpumu glabātuvei lietojumprogramma piekļūst caur privāto galapunktu, un to papildus aizsargā platformas identitātes autentifikācija un minimālo privilēģiju piekļuves politikas, tāpēc jebkurai piekļuvei ir nepieciešama derīga, autorizēta identitāte neatkarīgi no tīkla ceļa.
- **Atdalīta publiskā virsma.** Vienīgā publiskā objektu glabātuve satur laidienu lejupielādes un publiskus dokumentus. Tā nekad nesatur kandidātu datus. Klientiem paredzētā lietojumprogrammas datplūsma iet caur malas slāni, kas nodrošina web application firewall, distributed-denial-of-service aizsardzību un satura piegādi.
- **Administratīvā piekļuve ir kontrolēta.** Operatori sasniedz iekšējos resursus tikai caur uz sertifikātiem balstītu point-to-site VPN pārvaldības centrmezgla tīklā, nevis pa publisko internetu.

Katrs izvietošanas posms (izstrāde un ražošana) ir pilnībā izolēta vide ar savu tīklu, glabātuves kontiem, datubāzi un noslēpumiem. Klientu ražošanas dati nekad neatrodas zemākās vidēs. Koplietojams pārvaldības centrmezgls satur tikai VPN vārteju un privāto DNS, kas privāti savienots ar katru vidi.

4. Aizsardzība vairākos slāņos

Nevienai vienai kontrolei netiek uzticēts apturēt visus uzbrukumus. Platforma izmanto neatkarīgu kontroles slāņu kopumu, lai viena slāņa kļūme neatklātu datus. Zemāk norādītie slāņi katrs ir ieviesti un, kā aprakstīts 12. sadaļā, individuāli testēti.

Slāņots drošības modelis: neatkarīgas kontroles katrā līmenī

Slānis	Raksturīgas kontroles
Tīkla mala	Tikai TLS pārraide, malas WAF un DDoS aizsardzība, privātie galapunkti, noklusējuma-liegt segmentēšana
Identitāte un piekļuve	Īslaicīgi parakstīti tokeni, bcrypt jaukšana, lomu balstīta piekļuves kontrole, izolācija katrai organizācijai
Lietojumprogramma	Shēmas validācija visām ievadēm, tikai ORM datu piekļuve, izvades kodēšana, ātruma ierobežošana
Datu aizsardzība	Šifrēšana glabāšanā, noslēpumu glabātuve ar managed identity, datu rezidence ES, uz piekrišanu balstīta apstrāde
Pārvaldība un privātums	Konfigurējama glabāšana, dzēšana kā vienotai vienībai, human-in-the-loop AI, audita žurnalēšana
Nepārtraukta pārliecība	Automatizētu testu kopa, atkārtojami ielaušanās testi, periodiski iekšējie drošības auditi

Dokumenta atlikusī daļa secīgi izskaidro katru slāni un pēc tam apraksta, kā mēs nepārtraukti pierādām, ka šie slāņi ir efektīvi.

5. Tīkla drošība

5.1 Privāts pēc noklusējuma

Datu līmenis ir privāts jau pēc konstrukcijas. Pārvaldītajai PostgreSQL datubāzei ir atspējota publiskā tīkla piekļuve, un tā ir sasniedzama tikai caur privātu galapunktu. Privātā objektu glabātuve ir konfigurēta tā, lai pēc noklusējuma liegtu tīkla piekļuvi, pilnībā atspējotu koplietotās piekļuves atslēgas un būtu pieejama tikai ar managed identity starpniecību no lietojumprogrammas apakštīkla. Arī kešatmiņa, AI pakalpojumi un noslēpumu glabātuve tiek sasniegti caur privātiem galapunktiem ar privātu DNS izšķiršanu.

Praksē tas nozīmē, ka nav internetam pieejamas datubāzes savienojuma virknes un nav publiska glabātuves URL kandidātu audio failiem: datubāzei un privātajai glabātuvei publiskā tīkla piekļuve ir pilnībā atspējota. Noslēpumu glabātuvei lietojumprogramma piekļūst caur privātu galapunktu, un to aizsargā platformas identitātes autentifikācija un minimālo privilēģiju piekļuves politikas, kur lietojumprogrammu identitātēm ir piešķirta tikai lasīšanas piekļuve tikai tiem noslēpumiem, kas tām nepieciešami, tāpēc noslēpumus nav iespējams iegūt bez derīgas, autorizētas identitātes. Uzbrukuma virsma, kurai ārējs pretinieks vispār var pieskarties, aprobežojas ar lietojumprogrammas HTTPS galapunktiem aiz malas slāņa.

5.2 Tīkla segmentēšana

Katra vide ir sadalīta atsevišķos apakštīklos lietojumprogrammu līmenim, datu līmenim un asinhronajam darbiniekam. Katru apakštīklu pārvalda network security group, kuras pēdējais noteikums liedz visu ienākošo datplūsmu. Lietojumprogrammas apakštīkls pieņem tikai ienākošo HTTPS datplūsmu. Datu apakštīkls pieņem tikai konkrētos datubāzes, kešatmiņas un glabātuves portus, un tikai no lietojumprogrammas apakštīkla vai administratīvā VPN. Tas nozīmē, ka pat uzbrucējs, kurš kaut kādā veidā sasniegtu lietojumprogrammu līmeni, nevar brīvi pārvietoties uz datu līmeni; atļauti ir tikai tie ceļi, kurus lietojumprogramma likumīgi izmanto.

5.3 Mala

Publiskā lietojumprogrammas datplūsma tiek novirzīta caur malas slāni, kas nodrošina web application firewall, DDoS aizsardzību un content delivery network. Laidienu un dokumentu lejupielādes tiek apkalpotas no īpaša publiska glabātuves konta caur content-delivery front door, pilnībā atsevišķi no privātās glabātuves, kurā atrodas kandidātu dati. Šie divi glabāšanas slāņi nekad nesajaucas: nepareiza konfigurācija publiskajā slānī nevar atklāt privātos kandidātu datus, jo tie atrodas dažādos kontos ar atšķirīgiem tīkla noteikumiem.

5.4 Administratīvā piekļuve

Privātajā tīklā nav publiska administratīvā galapunkta. Operatori pieslēdzas caur point-to-site VPN vārteju, kas izmanto uz sertifikātiem balstītu autentifikāciju. Administratīva piekļuve datubāzei un kešatmiņai ir iespējama tikai no šī tuneļa iekšienes, jo šiem pakalpojumiem publiskā tīkla piekļuve ir atspējota. Tādējādi ikdienas darbības pilnībā tiek turētas ārpus publiskā interneta.

6. Identitātes un piekļuves pārvaldība

6.1 Autentifikācija

Lietotāju sesijas tiek izveidotas ar parakstītu piekļuves tokenu, kas ir derīgs trīsdesmit minūtes, pārī ar atsevišķu, necaurspīdīgu, servera pusē glabātu refresh token. Piekļuves tokeni tiek pārbaudīti pie katra pieprasījuma, un lietotājs tiek atkārtoti validēts pret datubāzi (tostarp aktīva konta pārbaudi), nevis uzticēts tikai tokena saturam. Izrakstīšanās nekavējoties atsauc servera puses refresh sesiju, tāpēc nozagts refresh token nevar palikt derīgs pēc izrakstīšanās.

Paroles nekad netiek glabātas atklātā tekstā. Tās tiek jauktas ar bcrypt, izmantojot unikālu sāli katrai parolei. Organizācijām, kas dod priekšroku single sign-on, platforma atbalsta OAuth pieteikšanos ar Microsoft un Google, un šādā gadījumā parole vispār netiek glabāta.

E-pasta īpašumtiesības tiek pārbaudītas, izmantojot vienreiz lietojamu, laikā ierobežotu verifikācijas saiti, pirms pašreģistrēts konts tiek uzskatīts par verificētu, un verifikācijas e-pasta atkārtotas nosūtīšanas pieprasījumi ir pakļauti ātruma ierobežojumiem, lai novērstu ļaunprātīgu izmantošanu.

6.2 Lomu balstīta piekļuves kontrole

Autorizācija tiek īstenota ar lomu modeli, kurā ir četras lomas ar pieaugošu privilēģiju līmeni: intervētājs, pieņemšanas vadītājs, personāla atlases speciālists un administrators. Piekļuve privileģētām darbībām tiek nodrošināta ar servera puses atkarībām, kas pārbauda gan lomu, gan pieprasītāja verifikācijas statusu. Šīs lomu pārbaudes aizsargā krietni vairāk nekā simts dažādas API darbības.

Loma	Tipiskās iespējas
Intervētājs	Veic piešķirtās intervijas; redz tikai sev piešķirtās intervijas
Pieņemšanas vadītājs	Pārvalda atlases procesus, kas viņam pieder vai kuros viņš ir dalībnieks
Personāla atlases speciālists	Pilnīga atlases un kandidātu pārvaldība organizācijas ietvaros
Administrators	Organizācijas iestatījumi, norēķini, lietotāju un API atslēgu administrēšana

Papildus vispārīgajām lomu pārbaudēm platforma piemēro datu līmeņa redzamības noteikumus. Pieņemšanas vadītāji redz tikai tos atlases procesus, ko viņi ir izveidojuši vai kuru dalībnieki ir; intervētāji redz tikai sev piešķirtās intervijas. Tādējādi privilēģijas tiek ieviestas gan līmenī “kāda darbība”, gan līmenī “kuri ieraksti”.

6.3 Izolācija katrai organizācijai

Platforma ir multi-tenant, un nomnieku izolācija tiek uzskatīta par pamatklases drošības kontroli. Katra autentificētā identitāte nes organizācijas identifikatoru, un datu vaicājumi tiek ierobežoti šīs organizācijas ietvaros. Ja lietotājs pieprasa ierakstu, kas pieder citai organizācijai, platforma atgriež atbildi “not found”, nevis atklāj, ka ieraksts eksistē. Iekšējie datubāzes identifikatori nekad netiek atklāti ārējā saskarnē; API uzrāda attēlojamos identifikatorus un katra pieprasījuma laikā tos pārveido atkārtoti, kas novērš izplatītu uzbrukumu klasi, kas saistīta ar uzskaitīšanu starp nomniekiem.

Tas nav tikai projektēšanas nodoms. Kā aprakstīts 12. sadaļā, mūsu automatizētā kopa izpilda plašu starporganizāciju matricu, kas mēģina piekļūt vienas organizācijas datiem, izmantojot citas organizācijas akreditācijas datus, un apstiprina, ka katrs šāds mēģinājums neizdodas.

6.4 Programmatiska piekļuve

Integrācijām organizācijas atbilstošos plānos var izveidot API atslēgas. Atslēgām ir atpazīstams prefikss, tās satur 128 bitu entropiju un tiek glabātas tikai jauktā veidā; neapstrādātā atslēga tiek parādīta vienreiz izveides brīdī un nekad vairs. Katrai atslēgai ir skaidri definēts atļauju tvērums (read, write vai ATS integration), to var ierobežot uz konkrētiem avota tīkliem, to var nekavējoties atsaukt, un uz to attiecas katrai atslēgai atsevišķi ātruma ierobežojumi, kas atvasināti no organizācijas plāna līmeņa. Atslēgas verifikācijā tiek izmantota pret laiku droša salīdzināšana, lai novērstu informācijas noplūdi caur atbildes laiku.

7. Lietojumprogrammu drošība

Lietojumprogramma ir rakstīta tā, lai novērstu veselas ievainojamību kategorijas, nevis tās labotu katru gadījumu atsevišķi.

• **Injekcija.** Visa piekļuve datubāzei notiek caur object-relational mapper ar parametrizētiem vaicājumiem. Koda bāzē nav neapstrādātu virkņu formatētu SQL. Tas strukturāli izslēdz SQL injection.

• **Ievades validācija.** Katrs pieprasījuma saturs tiek validēts pret stingru shēmu, pirms tas sasniedz biznesa loģiku. Pārmērīgi lieli pieprasījumi tiek noraidīti, un sarakstu galapunkti ir lapoti, lai ierobežotu resursu izmantošanu.

• **Izvades kodēšana un cross-site scripting.** Lietotāju ievadīts un AI ģenerēts teksts tiek uzskatīts par neuzticamu. Ja saturs jāattēlo kā HTML, tas rakstīšanas brīdī tiek izlaists caur atļauto elementu sanitizētāju, un īpaša testu kopa apstiprina, ka script tagi, notikumu apstrādātāji un javascript URL tiek noņemti.

• **Mass assignment.** Atjaunināšanas darbībās tiek izmantotas skaidri definētas shēmas, kas izslēdz privileģētus laukus, piemēram, lomu, organizāciju un kredītu bilanci, tāpēc klients nevar eskalēt privilēģijas, iesniedzot papildu laukus.

• **Ātruma ierobežošana.** Autentifikācijas un ļaunprātīgai izmantošanai pakļautie galapunkti tiek ierobežoti, izmantojot noturīgu, datubāzē balstītu ierobežotāju, kas pārdzīvo restartēšanu un korekti darbojas vairākās lietojumprogrammas instancēs. Pieteikšanās, reģistrācija, paroles atiestatīšana un verifikācijas atkārtota nosūtīšana katrai ir savi ierobežojumi. Klienta IP noteikšana ir nostiprināta pret forwarding header viltošanu.

• **Webhook.** Ienākošie webhook no maksājumu un e-pasta pakalpojumu sniedzējiem tiek pārbaudīti pret sniedzēja parakstiem uz neapstrādātā pieprasījuma satura, pirms tie tiek apstrādāti.

• **Failu augšupielādes.** Augšupielādēm ir izmēra ierobežojumi, tās tiek validētas, glabātas ar ģenerētiem identifikatoriem, nevis lietotāja dotajiem nosaukumiem, un ierobežotas gan katram pieprasījumam, gan katrai organizācijai.

• **Drošības galvenes.** Ražošanas vidē atbildes satur strict transport security, content-type un frame options, referrer policy un ierobežojošu permissions policy, kā arī apspiež servera un ietvara reklāmkarogus.

8. Datu aizsardzība

8.1 Šifrēšana

Visi dati tiek šifrēti glabāšanā, izmantojot AES-256 caur Azure platformas glabāšanas un datubāzes šifrēšanas slāņiem. Visa tīkla datplūsma tiek apkalpota tikai caur HTTPS, izmantojot TLS 1.2 vai augstāku versiju; atklātā teksta HTTP tiek pāradresēts uz HTTPS katrā līmenī. Ražošanas vidē API un tīmekļa portāls nosūta strict transport security galvenes kopā ar nostiprināšanas galveņu kopumu un apspiež servera un ietvara versiju reklāmkarogus.

8.2 Noslēpumu pārvaldība

Lietojumprogrammas noslēpumi tiek glabāti centralizētā noslēpumu glabātuvē ar iespējotu purge protection un deviņdesmit dienu soft-delete logu. Lietojumprogrammas autentificējas Azure resursiem, izmantojot system-assigned managed identities, nevis ilgtermiņa atslēgas; piemēram, privātajai glabātuvei koplietotās piekļuves atslēgas ir pilnībā atspējotas, tāpēc piekļuve ir iespējama tikai caur uz identitāti balstītām lomu piešķiršanām, kas attiecinātas uz konkrēto resursu. Glabātuves piekļuves politikas piešķir lietojumprogrammas principāliem tikai lasīšanas piekļuvi konkrētajiem nepieciešamajiem noslēpumiem, ievērojot minimālo privilēģiju principu.

8.3 Datu rezidence

Visi klientu un kandidātu dati tiek glabāti un apstrādāti Eiropas Savienībā. Lietojumprogrammas mitināšana, datubāze, glabātuve, kešatmiņa un noslēpumi atrodas West Europe, bet AI apstrāde notiek ES reģionos. AI pakalpojuma sniedzējs neizmanto klientu datus savu modeļu apmācībai.

8.4 Vienas intervijas dzīves cikls

Skaidrākais veids, kā izprast datu aizsardzības kontroles mehānismus, ir izsekot vienai intervijai no sākuma līdz beigām. Piekrišana tiek iegūta un reģistrēta pirms jebkādas apstrādes. Augšupielāde tiek šifrēta pārraides laikā. Transkripcija un analīze notiek ES datu centros. Rezultāti tiek ierakstīti šifrētā glabātuvē. Pēc tam katrs ieraksts tiek pārvaldīts ar vienu glabāšanas taimeri, kas beidzas ar reģistrētu, kaskadējošu dzēšanu. Jebkurā brīdī kandidāta tiesības, piemēram, atsaukums, dzēšana, piekļuve vai pārnesamība, var pārtraukt šo plūsmu.

9. Privātums pēc projektēšanas un GDPR

Privātums ir iestrādāts datu modelī un darbplūsmā, nevis pievienots tikai ar politiku palīdzību.

9.1 Piekrišana

Neviena intervija netiek ierakstīta vai analizēta bez kandidāta nepārprotamas piekrišanas. Kad kandidāts tiek pievienots atlases procesam, platforma nosūta unikālu, vienreiz lietojamu piekrišanas saiti pa e-pastu. Kandidāts iepazīstas ar to, kas notiks, un piekrīt vai atsakās. Piekrišanas statuss, ieskaitot atbildes laiku, tiek reģistrēts attiecībā uz konkrēto atlases procesu, tāpēc piekrišana vienmēr ir piesaistīta konkrētam darbā pieņemšanas procesam, nevis piešķirta globāli.

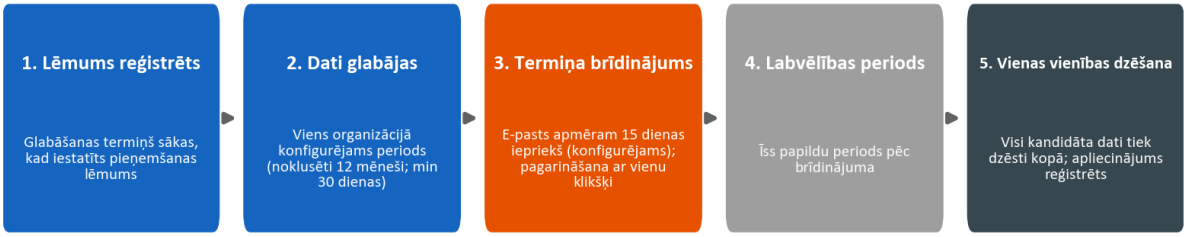
Kandidāta piekrišana: skaidra un reģistrēta pirms jebkādas apstrādes

9.2 Glabāšana un dzēšana

Datu glabāšanas termiņš ir konfigurējams katrai organizācijai, ar noklusējuma termiņu divpadsmit mēneši un konfigurējamu minimumu trīsdesmit dienas, un to var pārrakstīt katram kandidātam atsevišķi. Kandidāta datiem ir viens glabāšanas taimeris, nevis atsevišķs taimeris katram artefaktam. Taimeris sākas, kad tiek reģistrēts pieņemšanas lēmums. Pirms datu termiņa beigām platforma nosūta brīdinājumu (pēc noklusējuma apmēram piecpadsmit dienas iepriekš) un piedāvā pagarinājumu ar vienu klikšķi. Kad dati tiek dzēsti, tie tiek dzēsti kā viena vienība: kandidāta ieraksts, intervijas, transkripti, audio ieraksti, dokumenti un salīdzinājumi tiek noņemti kopā, un dzēšana tiek reģistrēta audita žurnālā. Nepaliek daļēji vai bāreņveida atlikumi.

Tālāk redzamais dzīves cikls parāda šo vienoto taimeri un to, kā tas noved pie vienas kaskadējošas dzēšanas ar reģistrētu dzēšanas pierādījumu.

Datu glabāšana: viens termiņš katram kandidātam, vienas vienības dzēšana



9.3 Datu subjekta tiesības un apakšapstrādātāji

Platforma atbalsta GDPR prasītās datu subjekta tiesības, tostarp piekļuvi, dzēšanu, pārnesamību, iebildumus un skaidrojuma saņemšanu. Apstrāde tiek veikta saskaņā ar datu apstrādes līgumu, ko klienti pieņem reģistrācijas laikā un kas ir versēts katrai organizācijai. Mūsu apakšapstrādātāji un to lomas, visi ES vai ar atbilstošiem aizsardzības pasākumiem, ir atklāti šajā līgumā, un

klienti iepriekš tiek informēti par jebkurām izmaiņām. 17. sadaļā ir ietverts apakšapstrādātāju reģistrs un atbilstības kartējums pa pantiem.

10. Atbildīgs AI un EU AI Act

Platforma ietilpst EU AI Act augsta riska kategorijā, jo tā atbalsta nodarbinātības lēmumus, un mēs šo klasifikāciju uztveram nopietni.

Produkta noteicošais princips ir, ka **AI ir lēmumu atbalsts, nevis lēmumu pieņēmējs.** Sistēma nekad automātiski nepieņem vai nenoraida kandidātu. Tā transkribē runu, strukturē jautājumus un atbildes, vērtē atbildes pret personāla atlases speciālista definētajiem kritērijiem un sagatavo atsauksmju projektu, un cilvēks pārskata katru rezultātu, pirms tas tiek izmantots. Tādējādi cilvēks stingri paliek procesa centrā.

Tikpat svarīgi ir tas, ko AI nedara. Tas nevērtē personību, "kultūras saderību", emocionālo stāvokli, balss toni, akcentu, dzimumu, vecumu, etnisko piederību, izskatu vai ķermeņa valodu. Vērtēšana ir balstīta uz pierādījumiem no transkripta un personāla atlases speciālista definētajiem kritērijiem, un kandidātu vārdi ir izslēgti no novērtēšanas ievades, lai mazinātu aizspriedumus. Mēs publicējam pārredzamības karti, lietotāja dokumentāciju un atbilstības deklarāciju, kurā aprakstīta sistēma, tās ierobežojumi un aizsardzības pasākumi.

Atbildīga AI kontrole	Kā tā darbojas
Human in the loop	Katru vērtējumu un katru atsauksmes daļu pirms izmantošanas pārskata personāla atlases speciālists
Nav automatizētu lēmumu	Sistēma nekad automātiski nepieņem un automātiski nenoraida kandidātu
Uz pierādījumiem balstīta vērtēšana	Vērtējumi atsaucas uz atbalstošiem pierādījumiem no transkripta
Dizains pret aizspriedumiem	Vārdi izslēgti no vērtēšanas; saturs tiek vērtēts augstāk par stilu
Tvēruma ierobežojumi	Personība, emocijas, akcents un aizsargājamās pazīmes nekad netiek vērtētas
Kandidātu atsauksmju drošība	Privātās kandidātu atsauksmes iziet ģenerēšanas un validācijas drošības aizsargbarjeru

Šie ierobežojumi ir ne tikai norādīti dokumentācijā; tie ir ieviesti AI prompt slānī un pārbaudīti ar īpašu AI drošības testēšanas programmu, kas aprakstīta 12.3 sadaļā.

11. Drošas izstrādes dzīves cikls

Drošība tiek īstenota tajā, kā mēs veidojam un piegādājam programmatūru, ne tikai darbojošajā sistēmā.

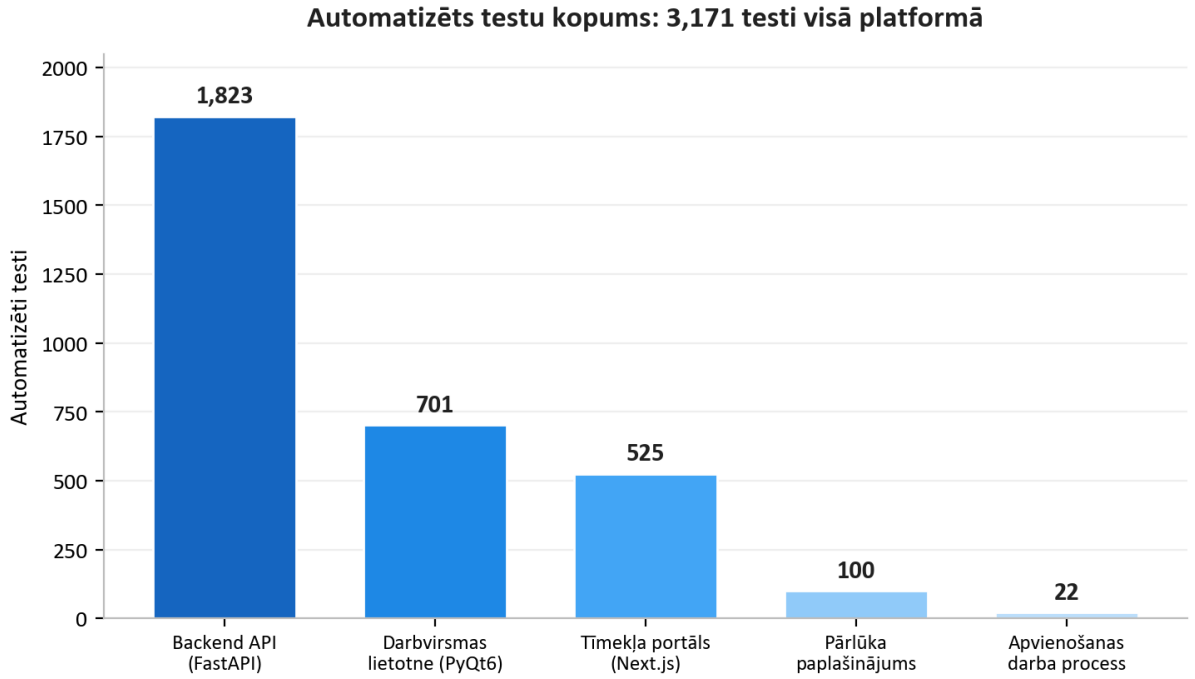
- **Vides nodalīšana.** Izstrādes un ražošanas vides ir pilnībā nodalītas, katrai ir sava infrastruktūra, glabātuves konti, datubāze, noslēpumi un apakšdomēni. Nav koplietota stāvokļa.
- **Infrastruktūra kā kods.** Visa mākoņvide ir definēta kā kods un pārskatīta kā kods, kas padara drošības stāvokli auditējamu un reproducējamu. Izvērtētājs var precīzi nolasīt, kuri porti ir atvērti, kuri resursi ir privāti un kurām identitātēm ir kādas atļaujas.
- **Piespraustas, kontrolētas izvietošanas.** Katrs nepārtrauktās integrācijas procesa solis ir piesaistīts precīzai, nemainīgai versijai. Ražošanas izvietošanas ir balstītas uz tagiem, tiek izpildītas tikai caur aizsargāto ražošanas procesu un ir pakļautas obligātam apstiprinājumam. Automatizēto testu kopa darbojas kā laidiena vārti: izvietošanu nevar izlaist, ja testi neizdodas.
- **Atkarību higiēna.** Automatizēta atkarību uzraudzība katru nedēļu piedāvā atjauninājumus backend, darbvirsmas lietotnei, tīmeklim, infrastruktūrai un procesu definīcijām, un atkarību auditi ir daļa no mūsu periodiskās drošības pārskatīšanas.
- **Parakstīti artefakti.** Darbvirsmas instalatori ir parakstīti ar kodu, lai klienti varētu pārbaudīt, ka instalētā programmatūra patiešām nāk no mums.
- **Noslēpumu disciplīna.** Noslēpumi atrodas glabātuvē un aizsargātajos procesu noslēpumos, nekad pirmkodā.

12. Nepārtraukta drošības testēšana

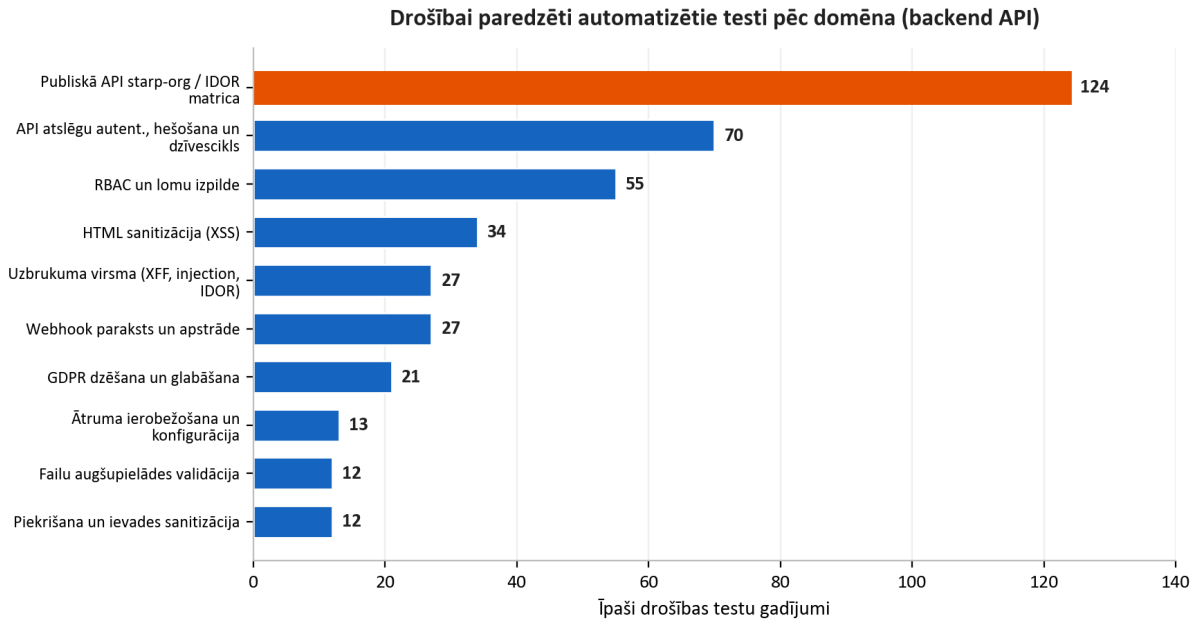
Tas ir mūsu pārliecības stāsta kodols un tā daļa, ko vairums piegādātāju nespēj parādīt. Mēs uzskatām drošību par kaut ko tādu, ko nepārtraukti mērīt ar izpildāmām pārbaudēm, nevis vienreiz apgalvot.

12.1 Automatizēto testu kopa

Platformu aptver **3,171 automatizēti testi**, kas aptver backend API, darbvirsmas lietojumprogrammu, tīmekļa portālu, pārlūkprogrammas paplašinājumu un audio apvienošanas darbinieku.



Tie nav tikai funkcionālie testi. Ievērojama, īpaši izveidota drošības testu kopa pārbauda kontroles, kas aprakstītas iepriekš šajā dokumentā. Zemāk redzamā diagramma parāda backend API drošībai specifisko testu sadalījumu pa domēniem.



Šajā kopā, starp daudziem citiem, ir iekļauta liela publiskā API matrica, kas izpilda katru galapunktu kā leģitīms lietotājs, kā pašas organizācijas API atslēga un kā konkurējošas organizācijas API atslēga, apstiprinot, ka katrs starporganizāciju mēģinājums tiek bloķēts. Tajā ietilpst desmitiem pretinieka skatījuma uzbrukuma virsmas testu forwarding header viltošanai, header injection un identifikatoru noplūdei, fokusēta HTML sanitizācijas kopa cross-site scripting pārbaudēm, lomu īstenošanas testi pilnam lomu modelim un testi, kas pierāda, ka kandidātu dati patiešām tiek dzēsti kā vienota vienība. Tā kā šie testi darbojas kā laidiena vārti, regresija, kas vājinātu jebkuru no šīm kontrolēm, apturētu laidienu, nevis nonāktu pie klientiem.

12.2 Aktīvās ielaušanās testēšana

Automatizētie vienību testi pierāda, ka kontroles pareizi uzvedas izolēti. Lai pierādītu, ka tās darbojas kopā reālā izvietojumā, mēs uzturam atkārtojamu ielaušanās testēšanas metodoloģiju, kas izpilda reālus uzbrukuma skriptus pret aktīvu vidi. Tā ir organizēta sešās fāzēs:

Fāze	Fokuss	Pārbaudāmo aspektu piemēri
1. Statiskā analīze	Pirmkods	Noslēpumi, injekciju paterni, bīstamas funkcijas, trūkstoša auth, nedrošs HTML
2. Arhitektūras pārskats	Infrastruktūra	Privātie galapunkti, segmentēšana, TLS, noslēpumu konfigurācija
3. Uzbrukuma vektoru analīze	Versiju kontrole un mākonis	Atzaru aizsardzība, identitātes tvērums, publiska ekspozīcija
4. Aktīvā ielaušanās testēšana	Darbojoša vide	Neautentificēta zondēšana, starporganizāciju piekļuve, injekcija, tokenu manipulācija, SSRF, ātruma ierobežojumu pārsniegšana
5. Uzņēmuma līmeņa vērtēšana	Briedums	Sešpadsmit drošības kategorijas, kas novērtētas pret uzņēmuma bāzlīniju
6. Atkarības un piegādes ķēde	Trešo pušu risks	Atkarību CVE audits, piespraustas procesu darbības, lock-file integritāte

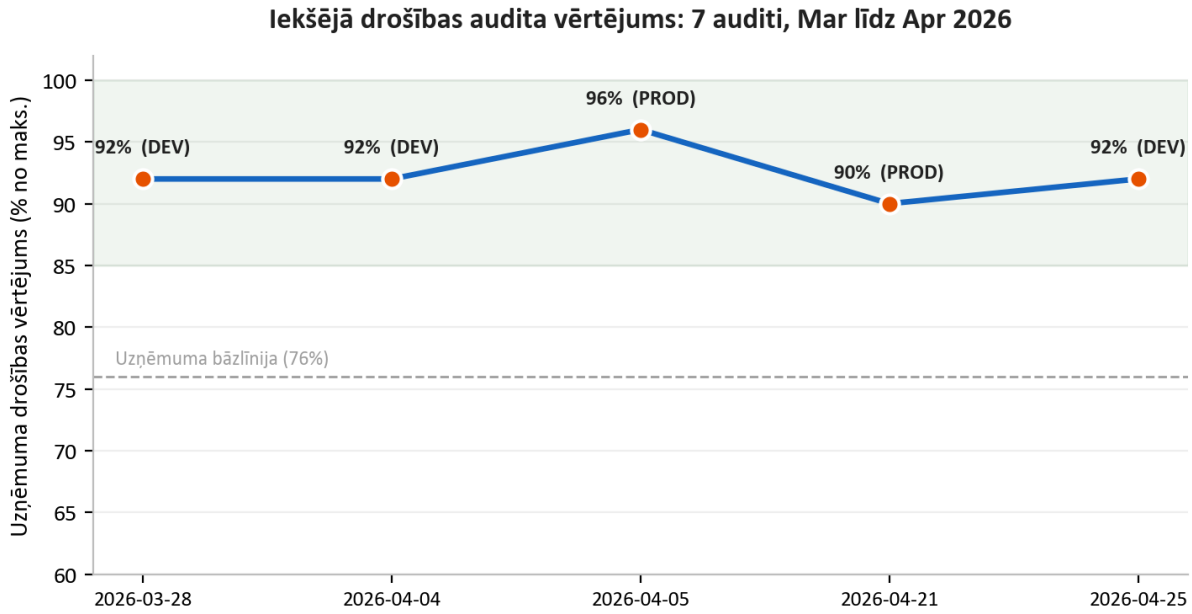
4. fāze ir īsta pretinieka testēšana pret izvietotu sistēmu, nevis kontrolsaraksts. Tā zondē aizsargātus galapunktus bez akreditācijas datiem un apstiprina, ka tie atsaka piekļuvi; tā reģistrē divas organizācijas un mēģina sasniegt vienas organizācijas ierakstus ar otras organizācijas kontu; tā injicē cross-site-scripting un server-side-template slodzes un apstiprina, ka tās tiek neitralizētas; tā manipulē ar autentifikācijas tokeniem un apstiprina, ka tie tiek noraidīti; tā mēģina veikt server-side request forgery pret mākoņa metadatu galapunktiem; un tā pārslogo autentifikācijas galapunktus, lai apstiprinātu, ka ātruma ierobežošana patiešām aktivizējas aktīvajā vidē, nevis tikai teorijā.

12.3 Kandidātu atsauksmju drošības testēšana

Tā kā platforma var ģenerēt privātas attīstības atsauksmes kandidātiem, mēs šai funkcijai īstenojam atsevišķu pretiniecisku drošības programmu. Tā apzināti ievada sistēmā skarbas un naidīgas personāla atlases speciālistu piezīmes un apstiprina, ka kandidātam paredzētajā izvadē nekad nav rupjību, nekad netiek atklāta vai piedēvēta personāla atlases speciālista identitāte vai privāts viedoklis un nekad netiek piemērotas nosodošas personības birkas. Tas aizsargā gan kandidātu, kuram jāsaņem konstruktīva un cieņpilna atsauksme, gan klientu, kuram nekad nevajadzētu pieļaut iekšēja viedokļa noplūdi uz āru.

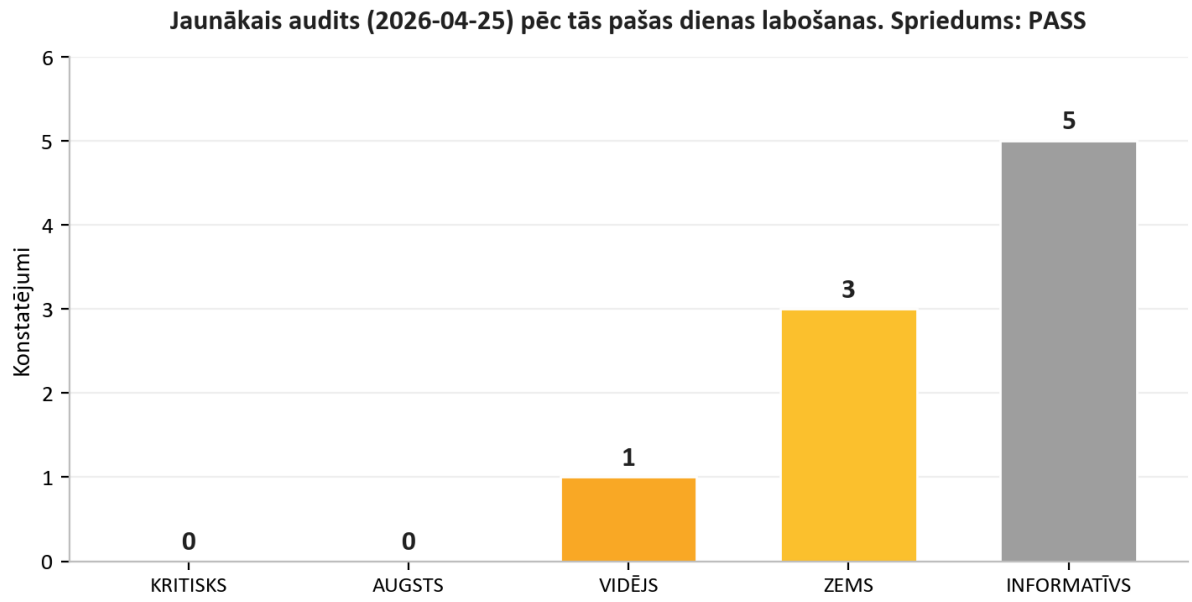
13. Drošības auditu rezultāti

Mēs veicam periodiskus drošības auditus, izmantojot strukturētu, atkārtojamu ielaušanās testēšanas metodoloģiju, un katru no tiem noformējam kā datētu ziņojumu ar smaguma pakāpēs klasificētiem konstatējumiem, pierādījumiem un korekcijas pasākumiem. Tie ir iekšējie auditi, ko veic mūsu pašu drošības process; šo pašu kontroļu formāla trešās puses sertifikācija ir iekļauta mūsu attīstības plānā. Laikā no 2026. gada marta beigām līdz aprīļa beigām mēs pabeidzām **seven such audits** izstrādes un ražošanas vidēs.



Rezultāts, kas potenciālajam klientam ir vissvarīgākais, ir konsekvence: **across all seven audits there were zero critical findings.** Retajos gadījumos, kad parādījās augstākas smaguma pakāpes jautājums, tas tika ātri novērsts, bieži tajā pašā dienā, un atkārtoti pārbaudīts. Vērtēšanas skala šajā periodā tika apzināti padarīta stingrāka (maksimāli iespējamais punktu skaits tika palielināts, jo mēs pievienojām vairāk novērtējamo kategoriju), tāpēc normalizētā rezultātu līnija saglabājas augsta pat tad, kad latiņa tika pacelta.

Mūsu jaunākais audits, 2026-04-25, ilustrē, kā process darbojas praksē. Tika identificēti divi augstākas smaguma pakāpes jautājumi, abi tika novērsti un atkārtoti pārbaudīti tajā pašā dienā, un audits noslēdzās ar verdiktu **PASS**, bez neviena ekspluatācijai gatava jautājuma pašreizējā draudu modelī.



Audits	Vide	Kritiskie	Verdikts
2026-03-28	Izstrāde	0	Gatavs ražošanai
2026-04-04	Izstrāde	0	Gatavs uzņēmuma lietošanai
2026-04-05	Ražošana	0	Gatavs uzņēmuma lietošanai
2026-04-20	Izstrāde	0	Gatavs ražošanai, piezīmes
2026-04-20	Izstrāde	0	PASS ar piezīmēm
2026-04-21	Ražošana	0	Drošs, nav ekspluatējamu konstatējumu
2026-04-25	Izstrāde	0	PASS

Raksts, kas redzams šajos auditos, ir visgodīgākais pierādījums, ko varam piedāvāt: problēmas tiek atrastas, jo mēs tās mērķtiecīgi meklējam, un tās tiek ātri aizvērtas, jo process ir veidots tā, lai tās aizvērtu. Piegādātājs, kurš nekad neziņo par nevienu konstatējumu, parasti ir piegādātājs, kurš nemeklē.

14. Operacionālā noturība un dalītā atbildība

14.1 Uzraudzība un žurnalēšana

Lietojumprogrammas un platformas telemetrija ieplūst centralizētā log analytics workspace un lietojumprogrammu uzraudzības pakalpojumā, nodrošinot mums redzamību par pieejamību un uzvedību. Sensitīvas darbības, piemēram, datu dzēšana, juridisko vienošanos akceptēšana un AI izsaukumi, tiek reģistrētas īpašās audita tabulās, lai pastāvētu noturīgs ieraksts par to, kurš ko darīja ar svarīgiem datiem.

14.2 Rezerves kopijas un atjaunošana

Pārvaldītā datubāze saglabā automatizētas rezerves kopijas, un privātā glabātuve ir aizsargāta ar soft-delete glabāšanu gan blobiem, gan konteineriem, tāpēc nejaušu vai ļaunprātīgu dzēšanu var atjaunot glabāšanas loga ietvaros. Kritiskajai infrastruktūrai ir dzēšanas slēdži, lai novērstu nejaušu ražošanas resursu demontāžu.

14.3 Dalītās atbildības kopsavilkums

Joma	AI Interview Analyzer	Klients
Infrastruktūra, tīkls, ielāpošana	Jā	-
Lietojumprogrammu drošība un AI procesu plūsma	Jā	-
Šifrēšana, noslēpumi, datu rezidence	Jā	-
Lietotāju un lomu administrēšana	Nodrošina kontroles	Pārvalda lietotājus un lomas
Glabāšanas politikas konfigurācija	Nodrošina kontroles	Nosaka glabāšanas termiņu
Kandidāta piekrišana	Nodrošina darbplūsmu	Nodrošina tās izmantošanu
Spēcīgi gala lietotāju akreditācijas dati un SSO	Atbalsta SSO un politiku	Ievieš iekšējo politiku

15. Draudu modelis un OWASP kartējums

Mēs projektējam aizsardzību pret konkrētu pretinieku kopumu: ārēju uzbrucēju bez akreditācijas datiem, ziņkārīgu vai ļaunprātīgu autentificētu vienas organizācijas lietotāju, kurš mēģina piekļūt citas organizācijas datiem, kompromitētu atkarību un iekšēju kļūdu. Tālāk esošajā tabulā plaši izmantotās OWASP Top 10 riska kategorijas ir kartētas pret konkrētajiem kontroles mehānismiem, kas tās risina šajā platformā, un katrs no tiem tiek pārbaudīts ar 12. sadaļā aprakstīto testēšanu.

OWASP risks	Kā platforma to mazina
Bojāta piekļuves kontrole	Lomu balstīta piekļuves kontrole katrā privileģētajā galapunktā; organizācijas tvēruma ierobežošana; “not found” starporganizāciju piekļuvē; identifikatoru pārkartēšana; starporganizāciju testu matrica
Kriptogrāfiskas kļūmes	TLS 1.2+ pārraidē; AES-256 glabāšanā; bcrypt paroļu jaukšana; noslēpumi pārvaldītā glabātuvē
Injekcija	Tikai ORM parametrizēti vaicājumi; stingra shēmas validācija; HTML sanitizācija rakstīšanas brīdī
Nedrošs dizains	Slāņaina aizsardzība vairākos līmeņos; draudu modelēšana un arhitektūras pārskats katrā auditā
Drošības nepareiza konfigurācija	Infrastruktūra kā kods; noklusējuma-liegt tīkla grupas; drošības galvenes; atspējotas koplietotās glabātuves atslēgas; API shēma nav atklāta ražošanā
Ievainojami komponenti	Iknedēļas automatizēta atkarību uzraudzība; atkarību CVE auditi periodiskajā pārskatā
Identifikācijas un autentifikācijas kļūmes	Īslaicīgi tokeni; pieteikšanās ar ātruma ierobežojumu; e-pasta verifikācija; SSO atbalsts; nav paroļu atklātā tekstā
Programmatūras un datu integritātes kļūmes	Piesprausti, nemainīgi procesu soļi; parakstīti darbvirsmas instalatori; webhook parakstu verifikācija; ar tagiem kontrolētas ražošanas izvietošanas
Drošības žurnalēšanas un uzraudzības kļūmes	Centralizēta telemetrija; īpašas audita tabulas sensitīvām darbībām
Server-side request forgery	Izejošie izsaukumi ierobežoti uz uzticamiem galapunktiem; SSRF zondes ielaušanās testēšanas sistēmā

Šis kartējums ir mūsu pārliecības argumentācijas mugurkauls: katrai labi zināmai uzbrukumu klasei ir nosaukta kontrole, un katrai nosauktajai kontrolei ir tests.

16. Ievainojamību pārvaldība un atbildīga atklāšana

Drošība nekad nav pabeigta, tāpēc mēs uzturam nepārtrauktu atklāšanas un novēršanas ciklu.

- **Atklāšana.** Ievainojamības tiek identificētas no četriem avotiem: automatizēto testu kopas, periodiskajiem ielaušanās testu auditiem, automatizētās atkarību uzraudzības un ziņojumiem no klientiem vai pētniekiem.
- **Triāža.** Katram konstatējumam tiek piešķirta smaguma pakāpe (critical, high, medium, low vai informational) ar pierādījumiem un novēršanas atbildīgo, tieši tā, kā tas tiek reģistrēts mūsu audita ziņojumos.
- **Novēršanas mērķi.** Critical un high konstatējumi tiek prioritizēti tūlītējai novēršanai; mūsu auditu vēsturē augstākas smaguma pakāpes konstatējumi parasti ir novērsti un atkārtoti pārbaudīti tajā pašā dienā. Medium un zemākas pakāpes konstatējumi tiek ieplānoti regulārajā uzturēšanas ritmā.
- **Verifikācija.** Labojumi tiek pārtestēti, un attiecīgajos gadījumos tiek veikta aktīva pārbaude pret izvietoto vidi, lai apstiprinātu, ka problēma patiešām ir aizvērta, nevis tikai aizvērta kodā.
- **Atklāšana.** Par drošības jautājumiem mums var ziņot tieši. Mēs apstiprinām ziņojumu saņemšanu, izmeklējam un informējam ziņotāju līdz pat risinājumam.

17. Atbilstības kartējums

17.1 GDPR

GDPR joma	Platformas īstenojums
Likumīgais pamats (Art. 6)	Kandidāta nepārprotama piekrišana tiek iegūta pirms apstrādes
Datu minimizācija un glabāšanas ierobežošana (Art. 5)	Tiek apstrādāti tikai ar interviju saistītie dati; konfigurējama glabāšana ar automātisku dzēšanu
Tiesības uz dzēšanu (Art. 17)	Visu kandidāta datu dzēšana kā vienotai vienībai ar reģistrētu dzēšanas pierādījumu
Datu subjekta tiesības (Art. 15 to 20)	Tiek atbalstīta piekļuve, dzēšana, pārnesamība un iebildumi
Apstrādātāja pienākumi (Art. 28)	Datu apstrādes līgums tiek pieņemts reģistrācijas laikā un ir versēts katrai organizācijai
Apstrādes drošība (Art. 32)	Šifrēšana, piekļuves kontrole, izolācija un nepārtraukta testēšana, kā aprakstīts šajā dokumentā
Apakšapstrādātāju pārredzamība	Atklāta datu apstrādes līgumā ar iepriekšēju paziņojumu par izmaiņām

17.2 EU AI Act

Platforma tiek uzskatīta par augsta riska AI sistēmu, kas atbalsta nodarbinātības lēmumus, un mēs uzturam dokumentāciju, kas ir saskaņota ar regulējumu, tostarp pārredzamības karti, lietotāja dokumentāciju un atbilstības deklarāciju. Galvenie aizsardzības pasākumi, cilvēka uzraudzība, pārredzamība, uz pierādījumiem balstīta vērtēšana un stingri ierobežojumi tam, ko AI vērtē, ir aprakstīti 10. sadaļā. Mēs turpinām pilnveidot formālo atbilstības dokumentāciju, virzoties uz priekšu regulējuma ieviešanas grafikam.

17.3 Mitināšanas sertifikāti

Platforma pilnībā darbojas uz Microsoft Azure, kura datu centriem ir neatkarīgas sertifikācijas, tostarp ISO 27001 un SOC 2. Šīs sertifikācijas aptver fizisko un platformas līmeni zem mūsu lietojumprogrammas; lietojumprogrammas līmeņa kontroles ir tās, kas aprakstītas visā šajā dokumentā.

17.4 Apakšapstrādātāju reģistrs

Apakšapstrādātājs	Mērķis	Reģions
Microsoft Azure	Mitināšana, AI un runas apstrāde, glabāšana, transakciju e-pasts	ES (West Europe, Sweden Central)
Stripe	Abonementu un maksājumu apstrāde	ES (Ireland)
Fakturownia	Rēķinu izrakstīšana	ES (Poland)
ATS connector (optional)	Kandidātu uzskaites integrācija, iespējota tikai pēc pieprasījuma	ES

18. Drošības attīstības plāns

Mēs uztveram drošību kā nepārtraukti pilnveidojamu programmu. Pašreizējās iniciatīvas mūsu attīstības plānā ietver daudzfaktoru autentifikācijas iespēju stiprināšanu administratīvajiem kontiem, centralizētas datu piekļuves audita žurnalēšanas paplašināšanu, regulāru atkarību aktualitātes turpmāku uzlabošanu un šajā dokumentā aprakstīto kontroļu formālās trešās puses sertifikācijas virzīšanu uz priekšu. Neviena no šīm jomām nav trūkums, kas šodien pakļautu riskam klientu datus; katra no tām ir jau slāņainas drošības pozas uzlabojums.

19. Kopsavilkums

AI Interview Analyzer aizsargā kandidātu un klientu datus ar slāņainu arhitektūru: privātu pēc noklusējuma tīklu bez publiskiem datu pakalpojumiem, spēcīgu identitāti un izolāciju katrai organizācijai, lietojumprogrammas kodu, kas novērš veselas ievainojamību klases, šifrēšanu un datu rezidenci ES, kā arī privātuma kontroles, kas iestrādātas datu modelī. Platformu izceļ pierādījumi, kas stāv aiz šiem apgalvojumiem. Ar 3,171 automatizētiem testiem, atkārtojamu aktīvās ielaušanās testēšanas metodoloģiju, īpašu AI drošības programmu un septiņu iekšējo drošības auditu vēsturi ar zero critical findings, mēs varam parādīt, nevis tikai pateikt, ka platforma ir droša.

Pielikums A: Drošības kontroļu katalogs

Saīsināta atsauce uz primārajām kontrolēm un pierādījumiem, kas atbalsta katru no tām.

Kontrole	Mehānisms	Pierādījumi
Pārraides šifrēšana	Tikai HTTPS, TLS 1.2+, HTTP pāradresēts	Infrastruktūra kā kods; arhitektūras audits
Šifrēšana glabāšanā	AES-256 platformas šifrēšana glabātuvē un datubāzē	Platformas konfigurācija; arhitektūras audits
Paroļu aizsardzība	bcrypt ar sāli katrai parolei	Versiju kontrole; autentifikācijas testi
Sesiju pārvaldība	30 minūšu parakstīti tokeni, atsaucama servera puses atjaunošana	Versiju kontrole; autentifikācijas testi
Autorizācija	Četru lomu piekļuves kontrole privileģētajos galapunktos	Lomu ieviešanas testu kopa
Nomnieku izolācija	Organizācijas tvēruma vaicājumi; 404 starporganizāciju piekļuvē	Starporganizāciju testu matrica
API atslēgu drošība	Jaukta glabāšana, tvēruma atļaujas, ātruma ierobežojumi katrai atslēgai	API atslēgu testu kopa
Aizsardzība pret injekcijām	Tikai ORM parametrizēti vaicājumi	Statiskā analīze; injekciju testi
Aizsardzība pret cross-site scripting	HTML sanitizācija rakstīšanas brīdī	HTML sanitizācijas testu kopa
Ātruma ierobežošana	Noturīgs datubāzē balstīts ierobežotājs auth galapunktos	Ātruma ierobežojumu testi; aktīvās pārslogošanas pārbaudes
Webhook integritāte	Pakalpojumu sniedzēja parakstu pārbaude neapstrādātajam saturam	Webhook testu kopa
Noslēpumu pārvaldība	Pārvaldīta glabātuve, purge protection, managed identity	Infrastruktūra kā kods; arhitektūras audits
Tīkla izolācija	Privātie galapunkti; noklusējuma-liegt segmentēšana	Infrastruktūra kā kods; arhitektūras audits
Datu dzēšana	Kaskadējoša dzēšana kā vienotai vienībai ar audita žurnālu	GDPR dzēšanas testu kopa
Piegādes ķēde	Piesprausti procesu soļi; iknedēļas atkarību uzraudzība	Procesu konfigurācija; atkarību audits

Pielikums B: Biežāk uzdotie jautājumi drošības izvērtētājiem

Kur tiek glabāti mūsu dati? Pilnībā Eiropas Savienībā, uz Microsoft Azure, West Europe reģionā, ar AI apstrādi ES reģionos. Kandidātu dati nekad nepamet ES.

Vai mūsu dati tiek izmantoti AI modeļu apmācībai? Nē. AI pakalpojuma sniedzējs neizmanto klientu datus apmācībai.

Vai datubāze ir sasniedzama no interneta? Nē. Publiskā tīkla piekļuve ir atspējota, un datubāze ir sasniedzama tikai caur privātu galapunktu virtuālā tīkla iekšienē.

Vai viens klients var redzēt cita klienta datus? Nē. Katrs vaicājums ir ierobežots pieprasītāja organizācijas ietvaros, starporganizāciju piekļuve atgriež “not found”, un automatizēta matrica nepārtraukti testē šo izolāciju.

Kā tiek glabātas paroles? Jauktā veidā ar bcrypt un unikālu sāli katrai parolei. Tiek atbalstīts single sign-on ar Microsoft un Google, un tādā gadījumā parole netiek glabāta.

Vai jūs atbalstāt single sign-on? Jā, izmantojot Microsoft un Google OAuth.

Cik ilgi ir derīgi piekļuves tokeni? Trīsdesmit minūtes, pārī ar atsaucamu servera puses refresh sesiju, kas tiek anulēta izrakstīšanās brīdī.

Kā tiek apstrādāta kandidāta piekrišana? Katrs kandidāts saņem unikālu, vienreiz lietojamu piekrišanas saiti, un viņam jāpiekrīt pirms jebkādas ierakstīšanas vai analīzes. Piekrišana tiek reģistrēta attiecībā uz konkrēto darbā pieņemšanas procesu.

Kā tiek dzēsti dati? Kā viena vienība, kas aptver kandidāta ierakstu, intervijas, transkriptus, audio, dokumentus un salīdzinājumus, saskaņā ar konfigurējamu glabāšanas grafiku, ar reģistrētu dzēšanas pierādījumu. Kandidāti var arī pieprasīt dzēšanu tieši.

Vai jums ir datu apstrādes līgums? Jā, tas tiek pieņemts reģistrācijas laikā un ir versēts katrai organizācijai, tostarp ietver apakšapstrādātāju reģistru.

Vai AI pieņem lēmumus par darbā pieņemšanu? Nē. Tas nodrošina tikai lēmumu atbalstu; cilvēks pārskata katru rezultātu un pieņem visus lēmumus.

Kā jūs pierādāt savus drošības apgalvojumus? Ar 3,171 automatizētiem testiem, tostarp īpašu drošības testu kopu, atkārtojamu sešu fāžu ielaušanās testēšanas metodoloģiju, kas tiek izpildīta pret aktīvām vidēm, AI drošības testēšanas programmu un periodiskiem rakstiskiem audita ziņojumiem.

Kas notiek, kad jūs atrodat ievainojamību? Tai tiek piešķirta smaguma pakāpe ar pierādījumiem un atbildīgo, tā tiek novērsta atbilstoši prioritātes grafikam, atkārtoti pārbaudīta, vajadzības gadījumā ietverot aktīvās pārbaudes, un reģistrēta audita ziņojumā.

Vai mēs varam veikt savu ielaušanās testu? Drošības novērtējumus var organizēt ar jūsu konta pārstāvi atbilstošā tvēruma un grafika ietvaros.

Pielikums C: Glosārijs

Termins	Nozīme
AES-256	Spēcīgs simetriskās šifrēšanas standarts, ko izmanto datu aizsardzībai glabāšanā
bcrypt	Speciāli parolei paredzēta jaukšanas funkcija ar sāli katrai parolei
Managed identity	Platformas izsniegta identitāte, kas ļauj pakalpojumam autentificēties bez glabātām atslēgām
Private endpoint	Privāta tīkla adrese, kas notur mākoņpakalpojumu ārpus publiskā interneta
Network security group	Atļauju un liegumu noteikumu kopums, kas filtrē tīkla datplūsmu uz apakštīklu
RBAC	Lomu balstīta piekļuves kontrole, piešķirot atļaujas atbilstoši lietotāja lomai
IDOR	Insecure direct object reference, piekļuves kontroles trūkums, pret kuru platforma aizsargājas
SSRF	Server-side request forgery, uzbrukumu klase, kas tiek pārbaudīta mūsu ielaušanās testos
Web application firewall	Malas kontrole, kas filtrē ļaunprātīgu tīmekļa datplūsmu
Data processing agreement	Līgums, kas nosaka, kā apstrādātājs apstrādā personas datus pārziņa vārdā

Pielikums D: Kontakti un dokumenta kontrole

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Lai saņemtu drošības izvērtējumu, mūsu datu apstrādes līguma kopiju vai mūsu EU AI Act atbilstības dokumentāciju, lūdzu, sazinieties ar savu konta pārstāvi.

Šis dokuments apraksta AI Interview Analyzer pakalpojuma drošības stāvokli uz ģenerēšanas datumu, kas norādīts kājenē. Tas ir sniegts izvērtēšanas nolūkiem un neveido neviena līguma daļu. Konkrētas līgumiskās drošības saistības ir noteiktas piemērojamajā līgumā un datu apstrādes līgumā.