Saugumo techninis dokumentas

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Saugumo techninis dokumentas

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

Auditorija: Įmonių saugumo, IT ir pirkimų komandos

Klasifikacija: Vieša

1. Santrauka vadovybei

AI Interview Analyzer yra įmonėms skirta įdarbinimo platforma, kuri, gavusi aiškų kandidato sutikimą, įrašo darbo pokalbius, juos transkribuoja ir struktūrizuoja bei pateikia įrodymais pagrįstą vertinimo pagalbą atrankų specialistams. Kadangi platforma tvarko kandidatų asmens duomenis ir palaiko įdarbinimo procesus, saugumas ir privatumas laikomi pirminiais projektavimo apribojimais, o ne vėliau pridėtomis funkcijomis.

Šiame techniniame dokumente konkrečiais ir patikrinamais terminais aprašoma, kaip saugome klientų ir kandidatų duomenis. Jis skirtas tiekėjų vertinimą atliekantiems asmenims: saugumo inžinieriams, IT administratoriams, duomenų apsaugos pareigūnams ir pirkimų specialistams. Kiekvienas šiame dokumente pateiktas rodiklis yra tiesiogiai paimtas iš mūsų pačių inžinerinių sistemų, o ne iš rinkodaros medžiagos.

Pagrindinė žinutė paprasta: **mes ne tik teigiame, kad platforma yra saugi, mes nuolat tikriname, kad ji tokia būtų.** Mūsų kodo bazėje yra **3,171 automatizuotų testų**, įskaitant specialią saugumo testų aibę, kuri tikrina autentifikavimą, autorizavimą, izoliaciją tarp organizacijų, apsaugą nuo įterpimo atakų ir duomenų ištrynimą. Be to, vykdome pakartojamą penetration-testing sistemą veikiančiose diegimo aplinkose ir rengiame rašytines audito ataskaitas. Per septynis vidinius saugumo auditus 2026 m. kovo ir balandžio mėn. užfiksavome **zero critical findings**, o naujausias auditas baigtas verdiktu **PASS**. (Formali trečiosios šalies šių kontrolės priemonių sertifikacija yra mūsų veiksmų plane; žr. 18 skyrių.)

Saugumo charakteristika	Santrauka
Talpinimas	Microsoft Azure, tik ES regionai
Tinklo modelis	Privatūs galiniai taškai, default-deny tinklo segmentavimas, nėra viešos duomenų bazės
Šifravimas	AES-256 ramybės būsenoje, TLS 1.2 arba aukštesnė versija perdavimo metu
Tapatybė	Trumpalaikiai pasirašyti žetonai, bcrypt slaptažodžių maišymas, SSO palaikymas
Prieigos kontrolė	RBAC su griežta izoliacija kiekvienai organizacijai
Paslaptys	Centralizuota paslapčių saugykla su managed-identity prieiga
Privatumas	Aiškus sutikimas, konfigūruojamas saugojimo laikotarpis, vienetinės apimties ištrynimas
Atsakingas AI	Tik sprendimų palaikymas, žmogus visada dalyvauja procese
Užtikrinimas	3,171 automatizuotų testų, periodiniai penetration tests ir auditai

1.1 Kaip skaityti šį dokumentą

3–11 skyriai aprašo duomenis saugančias kontrolės priemones: architektūrą, tinklą, tapatybę, taikomąją programą, duomenų apsaugą, privatumą ir saugaus kūrimo gyvavimo ciklą. 12 ir 13 skyriai apima mūsų išskirtinę nuolatinio testavimo programą ir audito istoriją. 14–17 skyriai aprašo operacijas, grėsmių modeliavimą, pažeidžiamumų valdymą ir atitikties susiejimą. Prieduose pateikiamas kontrolės priemonių katalogas, vertintojų DUK ir glosarijus, kuriuos saugumo komanda gali tiesiogiai naudoti vertinimo metu.

2. Dokumento apimtis ir metodas

2.1 Ką apima šis dokumentas

Šis techninis dokumentas apima AI Interview Analyzer paslaugos saugumo architektūrą ir praktikas: talpinimo aplinką, tinklo projektavimą, tapatybės ir prieigos valdymą, taikomojo lygmens kontrolės priemones, duomenų apsaugą, privatumo ir reguliacinę atitiktį, saugaus kūrimo gyvavimo ciklą ir mūsų nuolatinę saugumo testavimo programą.

2.2 Kas daro tai patikrinama

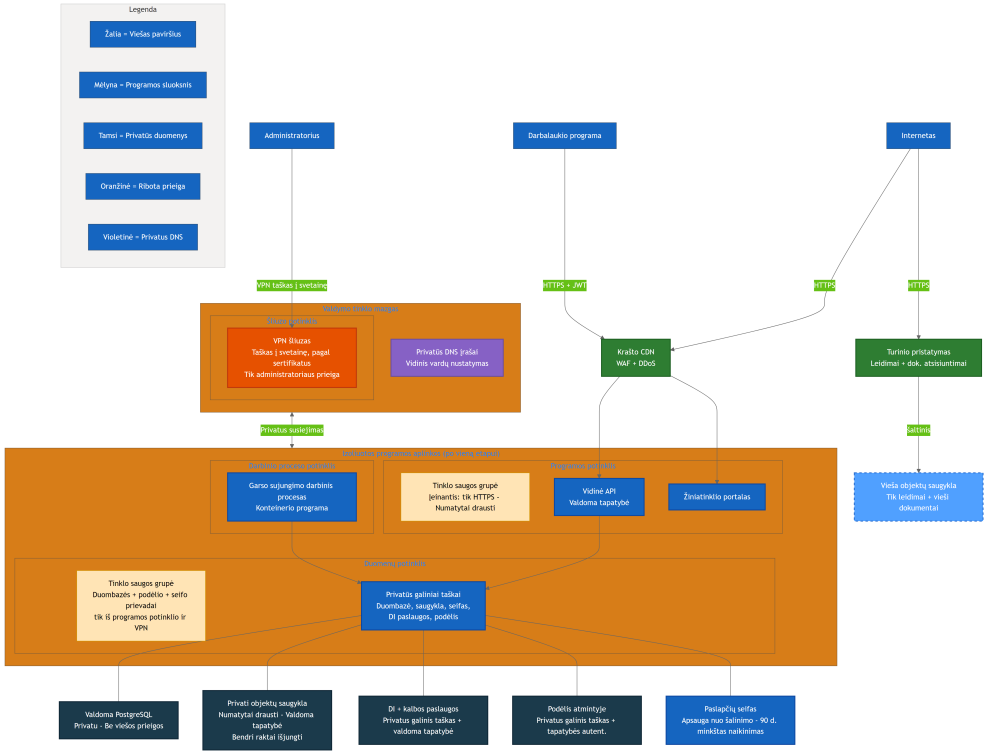
Tiekėjų saugumo teiginius lengva parašyti ir sunku patikėti. Todėl kiekvieną pagrindinį šiame dokumente pateiktą teiginį susiejome su kažkuo konkrečiu ir išmatuojamu mūsų inžinerinėse sistemose: kode įgyvendinta kontrolės priemone, testu, įrodančiu, kad ši kontrolė veikia, infrastruktūros apibrėžimu, kuris ją užtikrina, arba audito ataskaita, kurioje užfiksuotas dokumentuotas patikrinimas. Kai kontrolės priemonė yra mūsų ateities plane, o ne jau įdiegta šiandien, tai aiškiai nurodome. Mums priimtiniau pažadėti mažiau ir būti patikimiems, nei pažadėti per daug ir būti demaskuotiems.

2.3 Bendra atsakomybė

Platforma teikiama kaip programinė įranga kaip paslauga. Mes eksploatuojame infrastruktūrą, taikomąją programą, AI apdorojimo grandinę ir duomenų tvarkymą. Klientas atsako už savo naudotojų paskyrų ir vaidmenų valdymą, duomenų saugojimo laikotarpių konfigūravimą pagal savo vidaus politiką ir užtikrinimą, kad kandidato sutikimas būtų gautas per platformos pateikiamą sutikimo darbo eigą. 14 skyriuje šis atsakomybės pasidalijimas aprašytas išsamiau.

3. Saugumo architektūros apžvalga

Platforma sukurta kaip nedidelis skaičius tarpusavyje bendradarbiaujančių paslaugų, o ne vienas monolitas. Darbalaukio programa ir interneto portalas veikia kaip klientai. Centrinė backend API valdo visą duomenų saugojimą, autentifikavimą, atsiskaitymus, AI apdorojimo grandinę, sutikimus, el. paštą, failų tvarkymą ir valdymo skydus. Garso sujungimo procesas asinchroniškai apdoroja įrašus. Visa jautri būsena egzistuoja už backend API; klientai niekada tiesiogiai nebendrauja su duomenų baze, saugykla ar AI paslaugomis.



Aukščiau pateikta schema rodo produkcinę topologiją, kurioje išteklių pavadinimai sąmoningai apibendrinti. Joje matomi trys principai:

- **Nėra tiesioginio duomenų paslaugų viešinimo.** Duomenų bazė, privati objektų saugykla, AI paslaugos ir spartinančioji atmintis turi išjungtą viešą tinklo prieigą ir yra pasiekiamos tik per privačius galinius taškus izoliuotame virtualiame tinkle. Paslapčių saugykla taikomąja programa pasiekiama per privatų galinį tašką ir papildomai apsaugota platformos tapatybės autentifikavimu bei mažiausių privilegijų prieigos politikomis, todėl bet kokiai prieigai reikalinga galiojanti, autorizuota tapatybė, nepriklausomai nuo tinklo kelio.
- **Atskirta viešoji sritis.** Vienintelė viešoji objektų saugykla laiko leidinių atsisiuntimus ir viešus dokumentus. Joje niekada nėra kandidatų duomenų. Klientams skirti taikomosios programos srautai eina per kraštinį sluoksnį, kuris užtikrina web application firewall, apsaugą nuo distributed-denial-of-service ir turinio pristatymą.
- **Administracinė prieiga yra ribojama.** Operatoriai vidinius išteklius pasiekia tik per sertifikatais pagrįstą point-to-site VPN į valdymo mazgo tinklą, o ne per viešąjį internetą.

Kiekvienas diegimo etapas (kūrimo ir produkcinė aplinka) yra visiškai izoliuota aplinka su savo tinklu, saugyklų paskyromis, duomenų baze ir paslaptimis. Klientų produkciniai duomenys niekada nebūna žemesnėse aplinkose. Bendrame valdymo mazge laikomas tik VPN šliuzas ir privatus DNS, privačiai sujungtas su kiekviena aplinka.

4. Defense in Depth

Nė viena atskira kontrolės priemonė nelaikoma pakankama sustabdyti kiekvieną ataką. Platforma sluoksniuoja nepriklausomas kontrolės priemones taip, kad bet kurio vieno sluoksnio nesėkmė neatskleistų duomenų. Toliau išvardyti sluoksniai yra įgyvendinti ir, kaip aprašyta 12 skyriuje, kiekvienas jų testuojamas atskirai.

Sluoksninis saugumo modelis: nepriklausomos kontrolės kiekviename lygyje

Sluoksnis	Tipinės kontrolės priemonės
Tinklo kraštas	Tik TLS perdavimas, kraštinis WAF ir DDoS apsauga, privatūs galiniai taškai, default-deny segmentavimas
Tapatybė ir prieiga	Trumpalaikiai pasirašyti žetonai, bcrypt maišymas, RBAC, izoliacija kiekvienai organizacijai
Taikomoji programa	Schemos validavimas visiems įvesties duomenims, tik ORM duomenų prieiga, išvesties kodavimas, greičio ribojimas
Duomenų apsauga	Šifravimas ramybės būsenoje, paslapčių saugykla su managed identity, duomenų rezidavimas ES, sutikimu valdomas apdorojimas
Valdymas ir privatumas	Konfigūruojamas saugojimas, vienetinės apimties ištrynimas, žmogus procese AI, audito žurnalai
Nuolatinis užtikrinimas	Automatizuotų testų rinkinys, pakartojami penetration tests, periodiniai vidiniai saugumo auditai

Likusi šio dokumento dalis nuosekliai aptaria kiekvieną sluoksnį, o po to paaiškina, kaip nuolat įrodome, kad šie sluoksniai veikia.

5. Tinklo saugumas

5.1 Privatus pagal numatymą

Duomenų sluoksnis yra privatus pagal savo konstrukciją. Valdoma PostgreSQL duomenų bazė turi išjungtą viešą tinklo prieigą ir yra pasiekiama tik per privatų galinį tašką. Privati objektų saugykla sukonfigūruota pagal numatymą drausti tinklo prieigą, visiškai išjungia shared access keys ir yra pasiekiama tik per managed identity iš taikomosios programos potinklio. Spartinančioji atmintis, AI paslaugos ir paslapčių saugykla taip pat pasiekiamos per privačius galinius taškus su privačiu DNS išsprendimu.

Praktikoje tai reiškia, kad nėra jokios į internetą nukreiptos jungties eilutės į duomenų bazę ir jokio viešo saugyklos URL kandidatų garso įrašams: duomenų bazė ir privati saugykla turi visiškai išjungtą viešą tinklo prieigą. Paslapčių saugykla taikomąja programa pasiekiama per privatų galinį tašką ir yra apsaugota platformos tapatybės autentifikavimu bei mažiausių privilegijų prieigos politikomis; taikomųjų programų tapatybėms suteikta tik skaitymo prieiga tik prie tų paslapčių, kurių joms reikia, todėl paslapčių negalima gauti be galiojančios, autorizuotos tapatybės. Atakos paviršius, kurį išorinis priešininkas apskritai gali pasiekti, apsiriboja taikomosios programos HTTPS galiniais taškais už kraštinio sluoksnio.

5.2 Tinklo segmentavimas

Kiekviena aplinka padalinta į atskirus potinklius taikomosios programos sluoksniui, duomenų sluoksniui ir asinchroniniam procesui. Kiekvieną potinklį valdo network security group, kurios galutinė taisyklė draudžia visą įeinantį srautą. Taikomosios programos potinklis priima tik įeinantį HTTPS. Duomenų potinklis priima tik konkrečius duomenų bazės, spartinančiosios atminties ir saugyklos prievadus, ir tik iš taikomosios programos potinklio arba administracinio VPN. Tai reiškia, kad net užpuolikas, kuris kažkaip pasiektų taikomosios programos sluoksnį, negalėtų laisvai judėti į duomenų sluoksnį; leidžiami tik tie keliai, kuriuos taikomoji programa teisėtai naudoja.

5.3 Kraštinis sluoksnis

Viešasis taikomosios programos srautas pateikiamas per kraštinį sluoksnį, kuris užtikrina web application firewall, DDoS apsaugą ir content delivery network. Leidinių ir dokumentų atsisiuntimai teikiami iš dedikuotos viešos saugyklos paskyros per turinio pristatymo prieigos sluoksnį, visiškai atskirtą nuo privačios saugyklos, kurioje laikomi kandidatų duomenys. Šios dvi saugyklų plokštumos niekada nesimaišo: neteisinga konfigūracija viešojoje plokštumoje negali atskleisti privačių kandidatų duomenų, nes tai skirtingos paskyros su skirtingomis tinklo taisyklėmis.

5.4 Administracinė prieiga

Į privatų tinklą nėra viešo administracinio galinio taško. Operatoriai jungiasi per point-to-site VPN šliuzą, naudojantį sertifikatais pagrįstą autentifikavimą. Administracinė prieiga prie duomenų bazės ir spartinančiosios atminties galima tik iš šio tunelio vidaus, nes šios paslaugos turi išjungtą viešą tinklo prieigą. Tai leidžia kasdienes operacijas visiškai vykdyti be viešojo interneto.

6. Tapatybės ir prieigos valdymas

6.1 Autentifikavimas

Naudotojo sesijos sukuriamos naudojant pasirašytą prieigos žetoną, galiojantį trisdešimt minučių, poroje su atskiru, nepermatomu, serverio pusėje laikomu atnaujinimo žetonu. Prieigos žetonai tikrinami kiekvienos užklausos metu, o naudotojas papildomai iš naujo patvirtinamas pagal duomenų bazę (įskaitant aktyvios paskyros patikrą), o ne pasitikima vien tik žetono turiniu. Atsijungus serverio pusės atnaujinimo sesija nedelsiant panaikinama, todėl pavogtas atnaujinimo žetonas negali išlikti po atsijungimo.

Slaptažodžiai niekada nesaugomi atviru tekstu. Jie maišomi naudojant bcrypt su unikaliu salt kiekvienam slaptažodžiui. Organizacijoms, kurios teikia pirmenybę single sign-on, platforma palaiko OAuth prisijungimą su Microsoft ir Google; tokiu atveju slaptažodžiai apskritai nelaikomi.

El. pašto adreso nuosavybė patvirtinama per vienkartinę, laike ribotą patvirtinimo nuorodą, kol savarankiškai užregistruota paskyra laikoma patvirtinta, o pakartotinis patvirtinimo laiškų siuntimas yra ribojamas, siekiant išvengti piktnaudžiavimo.

6.2 RBAC

Autorizavimas įgyvendintas per vaidmenų modelį su keturiais vis didesnių privilegijų vaidmenimis: pokalbio vedėjas, samdos vadovas, atrankų specialistas ir administratorius. Prieiga prie privilegijuotų operacijų užtikrinama serverio pusės priklausomybėmis, kurios tikrina tiek vaidmenį, tiek kviečiančiojo patvirtinimo būseną. Šios vaidmenų patikros saugo gerokai daugiau nei šimtą skirtingų API operacijų.

Vaidmuo	Tipinės galimybės
Pokalbio vedėjas	Veda jam priskirtus pokalbius; mato tik jam priskirtus pokalbius
Samdos vadovas	Valdo atrankas, kurių savininkas jis yra arba kurių narys yra
Atrankų specialistas	Pilnas atrankų ir kandidatų valdymas organizacijos viduje
Administratorius	Organizacijos nustatymai, atsiskaitymai, naudotojų ir API raktų administravimas

Be bendrų vaidmenų patikrų, platforma taiko duomenų lygmens matomumo taisykles. Samdos vadovai mato tik tas atrankas, kurias sukūrė arba kurių nariai yra; pokalbio vedėjai mato tik jiems priskirtus pokalbius. Taigi privilegijos užtikrinamos tiek „kokį veiksmą“ galima atlikti, tiek „kuriems įrašams“ tai taikoma.

6.3 Izoliacija kiekvienai organizacijai

Platforma yra kelių nuomininkų aplinka, o nuomininkų izoliacija laikoma pirmos klasės saugumo kontrolės priemone. Kiekviena autentifikuota tapatybė turi organizacijos identifikatorių, o duomenų užklausos apribojamos ta organizacija. Kai naudotojas prašo įrašo, priklausančio kitai organizacijai, platforma grąžina atsakymą „not found“, o ne atskleidžia, kad įrašas egzistuoja. Vidiniai duomenų bazės identifikatoriai niekada neatskleidžiami perdavimo metu; API pateikia rodymo identifikatorius ir juos peržemėlapiuoja kiekvienai užklausai, taip pašalindama dažną tarpnuomininkinio enumeravimo atakų klasę.

Tai nėra tik projektavimo intencija. Kaip aprašyta 12 skyriuje, mūsų automatizuotas rinkinys vykdo didelę tarporganizacinę matricą, kuri bando pasiekti vienos organizacijos duomenis naudojant kitos organizacijos kredencialus ir patvirtina, kad kiekvienas toks bandymas nepavyksta.

6.4 Programinė prieiga

Integracijoms organizacijos, turinčios tinkamus planus, gali išduoti API raktus. Raktai turi atpažįstamą prefiksą, turi 128 bits entropijos ir saugomi tik kaip hash; neapdorotas raktas parodomas vieną kartą jo sukūrimo metu ir daugiau niekada. Kiekvienas raktas turi aiškiai apibrėžtą leidimų apimtį (read, write arba ATS integration), gali būti apribotas konkrečiais šaltinio tinklais, gali būti nedelsiant atšauktas ir jam taikomi kiekvienam raktui atskiri greičio limitai, išvesti iš organizacijos plano lygio. Raktų tikrinimas naudoja timing-safe palyginimą, kad būtų išvengta informacijos nutekėjimo per atsako laiką.

7. Taikomosios programos saugumas

Taikomoji programa parašyta taip, kad pašalintų ištisas pažeidžiamumų kategorijas, o ne taisytų jas po vieną.

- **Injection.** Visa prieiga prie duomenų bazės vyksta per object-relational mapper su parametrizuotomis užklausomis. Kodo bazėje nėra neapdoroto, eilutėmis formuojamo SQL. Tai struktūriškai pašalina SQL injection.
- **Įvesties validavimas.** Kiekvieno užklausos kūno duomenys tikrinami pagal griežtą schemą prieš pasiekiant verslo logiką. Per dideli payload atmetami, o sąrašų galiniai taškai naudoja puslapiavimą, kad būtų apribotas išteklių naudojimas.
- **Išvesties kodavimas ir cross-site scripting.** Naudotojų pateiktas ir AI sugeneruotas tekstas laikomas nepatikimu. Kai turinį reikia pateikti kaip HTML, jis įrašymo metu praeina per allow-list sanitizatorių, o specialus testų rinkinys patvirtina, kad script žymos, event handler ir javascript URL yra pašalinami.
- **Mass assignment.** Atnaujinimo operacijos naudoja aiškias schemas, kurios neapima privilegijuotų laukų, tokių kaip vaidmuo, organizacija ir kredito balansas, todėl klientas negali eskaluoti privilegijų pateikdamas papildomus laukus.
- **Greičio ribojimas.** Autentifikavimo ir piktnaudžiavimui jautriems galiniams taškams taikomas greičio ribojimas naudojant patvarią, duomenų baze paremtą ribojimo sistemą, kuri išgyvena perkrovimus ir teisingai veikia per kelias taikomosios programos instancijas. Prisijungimui, registracijai, slaptažodžio atkūrimui ir pakartotiniam patvirtinimo siuntimui taikomi atskiri limitai. Kliento IP nustatymas yra sustiprintas nuo forwarding headers klastojimo.
- **Webhook.** Įeinantys webhook iš mokėjimų ir el. pašto tiekėjų prieš apdorojimą tikrinami pagal tiekėjo parašus neapdorotame užklausos kūne.
- **Failų įkėlimai.** Įkėlimams taikomi dydžio limitai, jie validuojami, saugomi pagal sugeneruotus identifikatorius, o ne naudotojo pateiktus pavadinimus, ir ribojami kiekvienai užklausai bei kiekvienai organizacijai.
- **Saugumo antraštės.** Produkcinėje aplinkoje atsakai pateikia griežto transporto saugumo, content-type ir frame parinktis, referrer politiką ir ribojančią permissions politiką, taip pat slopina serverio ir karkaso reklamines antraštes.

8. Duomenų apsauga

8.1 Šifravimas

Visi duomenys ramybės būsenoje šifruojami naudojant AES-256 per Azure platformos saugyklos ir duomenų bazės šifravimo sluoksnius. Visas tinklo srautas teikiamas išskirtinai per HTTPS naudojant TLS 1.2 arba aukštesnę versiją; nešifruotas HTTP kiekviename sluoksnyje peradresuojamas į HTTPS. Produkcinėje aplinkoje API ir interneto portalas pateikia griežto transporto saugumo antraštes kartu su saugumo stiprinimo antraščių rinkiniu ir slopina serverio bei karkaso versijų reklamines antraštes.

8.2 Paslapčių valdymas

Taikomosios programos paslaptys laikomos centralizuotoje paslapčių saugykloje su įjungta purge protection ir devyniasdešimties dienų soft-delete laikotarpiu. Taikomosios programos autentifikuojasi prie Azure išteklių naudodamos system-assigned managed identities, o ne ilgalaikius raktus; pavyzdžiui, privačioje saugykloje shared access keys yra visiškai išjungti, todėl prieiga įmanoma tik per tapatybe pagrįstus vaidmenų priskyrimus, apribotus iki konkretaus ištekliaus. Saugyklos prieigos politikos suteikia taikomųjų programų subjektams tik skaitymo prieigą prie konkrečių joms reikalingų paslapčių, laikantis mažiausių privilegijų principo.

8.3 Duomenų rezidavimas

Visi klientų ir kandidatų duomenys saugomi ir apdorojami Europos Sąjungoje. Taikomosios programos talpinimas, duomenų bazė, saugykla, spartinančioji atmintis ir paslaptys yra West Europe regione, o AI apdorojimas vykdomas ES regionuose. AI tiekėjas nenaudoja klientų duomenų savo modelių mokymui.

8.4 Vieno pokalbio duomenų gyvavimo ciklas

Aiškiausias būdas suprasti duomenų apsaugos kontrolės priemones yra sekti vieną pokalbį nuo pradžios iki pabaigos. Sutikimas surenkamas ir užfiksuojamas prieš ką nors apdorojant. Įkėlimas šifruojamas perdavimo metu. Transkripcija ir analizė vykdomos ES duomenų centruose. Rezultatai įrašomi į šifruotą saugyklą. Tuomet kiekvienam įrašui taikomas vienas saugojimo laikrodis, kuris baigiasi registruojamu, kaskadiniu ištrynimu. Bet kuriuo momentu kandidato teisės, tokios kaip sutikimo atšaukimas, ištrynimas, prieiga ar duomenų perkeliamumas, gali nutraukti šį srautą.

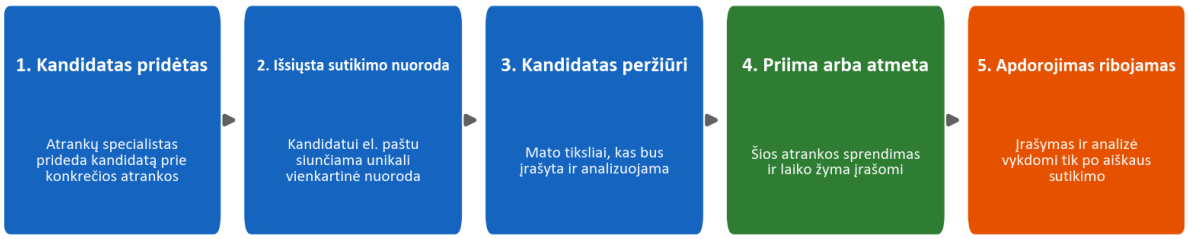
9. Privatumas pagal projektavimą ir GDPR

Privatumas yra įdiegtas į duomenų modelį ir darbo eigą, o ne vien pridėtas politikos lygmeniu.

9.1 Sutikimas

Joks pokalbis nėra įrašomas ar analizuojamas be aiškaus kandidato sutikimo. Kai kandidatas pridedamas prie atrankos, platforma el. paštu išsiunčia unikalią, vienkartinę sutikimo nuorodą. Kandidatas peržiūri, kas vyks, ir sutinka arba atsisako. Sutikimo būsena, įskaitant atsakymo laiką, užfiksuojama būtent prie tos konkrečios atrankos, todėl sutikimas visada apribotas konkrečiu samdos procesu, o ne suteikiamas globaliai.

Kandidato sutikimas: aiškus ir įrašytas prieš bet kokį apdorojimą

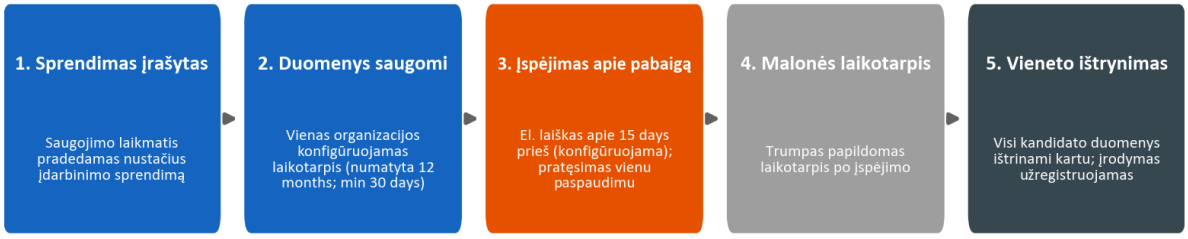


9.2 Saugojimas ir ištrynimas

Duomenų saugojimas konfigūruojamas kiekvienai organizacijai atskirai; numatytoji reikšmė yra dvylika mėnesių, konfigūruojamas minimumas — trisdešimt dienų, ir tai gali būti perrašoma kiekvienam kandidatui. Kandidato duomenims taikomas vienas bendras saugojimo laikrodis, o ne atskiras laikmatis kiekvienam artefaktui. Laikrodis pradedamas, kai užfiksuojamas samdos sprendimas. Prieš duomenų galiojimo pabaigą platforma siunčia įspėjimą (pagal numatymą maždaug prieš penkiolika dienų) ir siūlo pratęsimą vienu paspaudimu. Kai duomenys ištrinami, jie ištrinami kaip vienas vienetas: kandidato įrašas, pokalbiai, transkriptai, garso įrašai, dokumentai ir palyginimai pašalinami kartu, o ištrynimas užfiksuojamas audito žurnale. Nelieka dalinių ar našlaičiais tapusių likučių.

Toliau pateiktas gyvavimo ciklas rodo šį vieną laikrodį ir tai, kaip jis baigiasi vienu kaskadiniu ištrynimu su registruotu ištrynimo įrodymu.

Duomenų saugojimas: vienas laikmatis kandidatui, vieneto ištrynimas



9.3 Duomenų subjekto teisės ir sub-processors

Platforma palaiko GDPR reikalaujamas duomenų subjekto teises, įskaitant prieigą, ištrynimą, perkeliamumą, prieštaravimą ir paaiškinimą. Apdorojimas vykdomas pagal DPA, kurį klientai priima registracijos metu ir kuris yra versijuojamas kiekvienai

organizacijai. Mūsų sub-processors ir jų vaidmenys, visi ES ribose arba pagal tinkamas apsaugos priemones, yra atskleisti toje sutartyje, o klientai iš anksto informuojami apie bet kokį pasikeitimą. 17 skyriuje pateikiamas sub-processors registras ir atitikties susiejimas straipsnis po straipsnio.

10. Atsakingas AI ir EU AI Act

Platforma patenka į aukštos rizikos EU AI Act kategoriją, nes ji palaiko su užimtumu susijusius sprendimus, ir mes į šią klasifikaciją žiūrime rimtai.

Esminė produkto taisyklė yra tokia: **AI yra sprendimų palaikymo priemonė, o ne sprendimų priėmėjas.** Sistema niekada automatiškai nepriima ir neatmeta kandidato. Ji transkribuoja kalbą, struktūrizuoja klausimus ir atsakymus, vertina atsakymus pagal kriterijus, kuriuos apibrėžė atrankų specialistas, ir parengia grįžtamąjį ryšį, o žmogus peržiūri kiekvieną išvestį prieš ją naudojant. Tai užtikrina, kad žmogus tvirtai išlieka procese.

Ne mažiau svarbu ir tai, ko AI nedaro. Jis nevertina asmenybės, „kultūrinio atitikimo“, emocinės būsenos, balso tono, akcento, lyties, amžiaus, etninės kilmės, išvaizdos ar kūno kalbos. Vertinimas grindžiamas transkripto įrodymais ir atrankų specialisto apibrėžtais kriterijais, o kandidatų vardai neįtraukiami į vertinimo įvestį, kad būtų sumažintas šališkumas. Skelbiame skaidrumo kortelę, naudotojo dokumentaciją ir atitikties deklaraciją, aprašančias sistemą, jos ribas ir apsaugos priemones.

Atsakingo AI kontrolės priemonė	Kaip ji veikia
Žmogus procese	Kiekvieną balą ir kiekvieną grįžtamojo ryšio elementą prieš naudojimą peržiūri atrankų specialistas
Nėra automatizuotų sprendimų	Sistema niekada automatiškai nepriima ir neatmeta kandidato
Įrodymais pagrįstas vertinimas	Balai remiasi transkripto patvirtinamais įrodymais
Dizainas prieš šališkumą	Vardai neįtraukiami į vertinimą; vertinama esmė, o ne stilius
Apimties ribos	Asmenybė, emocijos, akcentas ir saugomos charakteristikos niekada nevertinamos
Kandidatų grįžtamojo ryšio sauga	Privatus kandidatų grįžtamasis ryšys pereina generavimo ir validavimo saugos užkardą

Šie apribojimai ne tik nurodyti dokumentacijoje; jie užkoduoti AI prompt sluoksnyje ir tikrinami specialia AI saugos testavimo programa, aprašyta 12.3 skyriuje.

11. Saugaus kūrimo gyvavimo ciklas

Saugumas užtikrinamas tuo, kaip kuriame ir pateikiame programinę įrangą, o ne tik veikiančioje sistemoje.

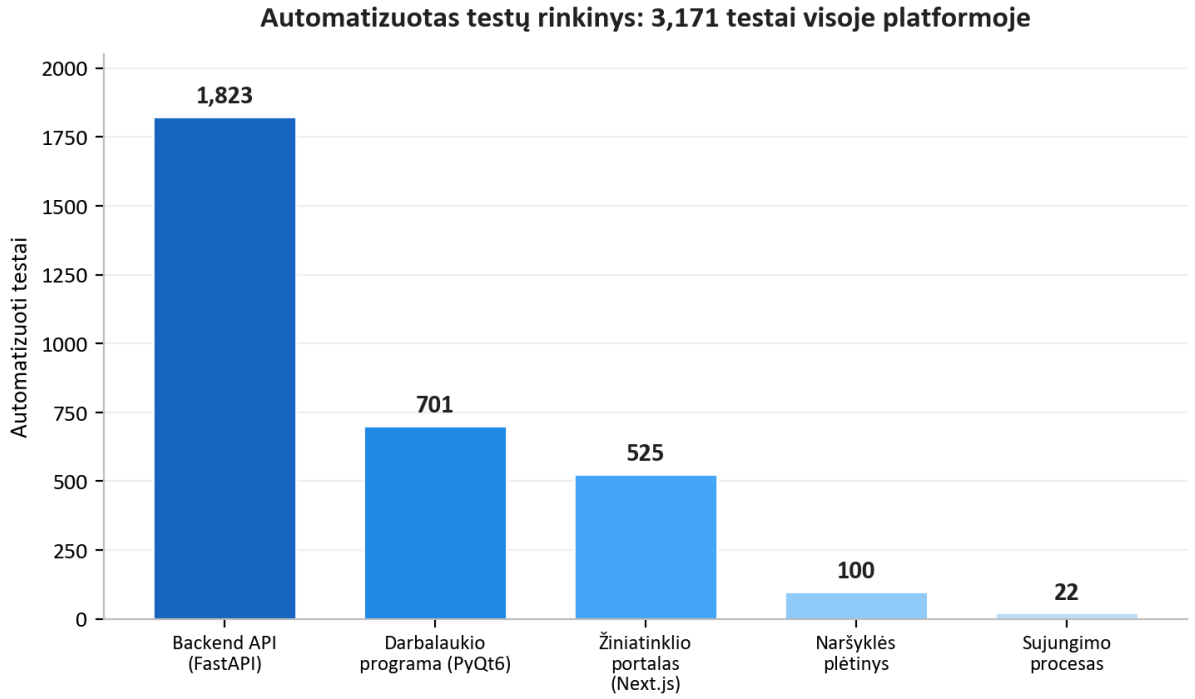
- **Aplinkų atskyrimas.** Kūrimo ir produkcinė aplinkos yra visiškai atskiros, kiekviena turi savo infrastruktūrą, saugyklų paskyras, duomenų bazę, paslaptis ir subdomenus. Nėra jokios bendros būsenos.
- **Infrastruktūra kaip kodas.** Visa debesijos aplinka apibrėžiama kaip kodas ir peržiūrima kaip kodas, todėl saugumo būsena yra audituojama ir atkuriama. Vertintojas gali tiksliai perskaityti, kurie prievadai yra atidaryti, kurie ištekliai yra privatūs ir kurios tapatybės kokias teises turi.
- **Fiksuotos, kontroliuojamos diegimo grandinės.** Kiekvienas continuous-integration grandinės žingsnis yra susietas su tikslia, nekintama versija. Produkciniai diegimai yra grindžiami tag, vykdomi tik per apsaugotą produkcinį pipeline ir reikalauja patvirtinimo. Automatizuotas testų rinkinys veikia kaip leidimo užkarda: diegimas negali būti išleistas, jei testai nepraeina.
- **Priklausomybių higiena.** Automatizuotas priklausomybių stebėjimas kas savaitę siūlo atnaujinimus backend, darbalaukio, interneto, infrastruktūros ir pipeline apibrėžtims, o priklausomybių auditai yra mūsų periodinės saugumo peržiūros dalis.
- **Pasirašyti artefaktai.** Darbalaukio diegikliai yra pasirašyti, todėl klientai gali patikrinti, kad diegiama programinė įranga tikrai gauta iš mūsų.
- **Paslapčių drausmė.** Paslaptys laikomos saugykloje ir apsaugotose pipeline paslaptyse, niekada ne išeities kode.

12. Nuolatinis saugumo testavimas

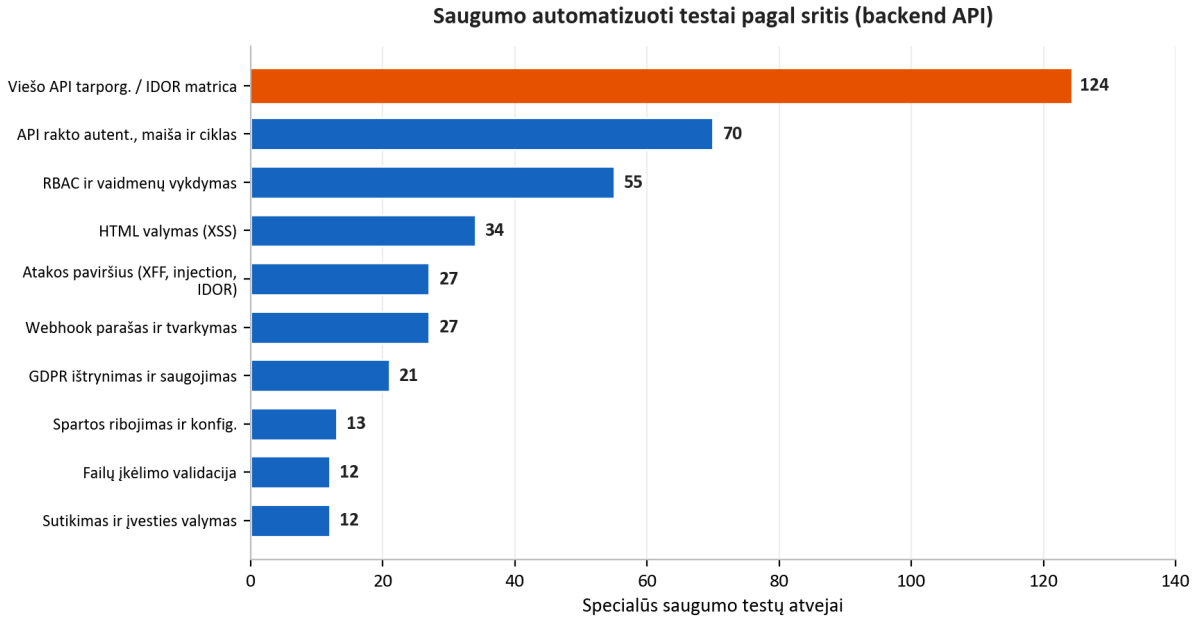
Tai yra mūsų užtikrinimo istorijos šerdis ir ta dalis, kurios dauguma tiekėjų negali parodyti. Saugumą laikome tuo, ką reikia nuolat matuoti vykdomais patikrinimais, o ne vienkartinai deklaruoti.

12.1 Automatizuotų testų rinkinys

Platformą dengia **3,171 automatizuotų testų**, apimančių backend API, darbalaukio programą, interneto portalą, naršyklės plėtinį ir garso sujungimo procesą.



Tai nėra vien funkciniai testai. Reikšminga, specializuota saugumo testų aibė tikrina anksčiau šiame dokumente aprašytas kontrolės priemones. Toliau pateikta diagrama suskaido backend API saugumui skirtus testus pagal sritis.



Be daugelio kitų dalykų, ši aibė apima didelę viešosios API matricą, kuri kiekvieną galinį tašką paleidžia kaip teisėtą naudotoją, kaip organizacijos nuosavą API raktą ir kaip konkuruojančios organizacijos API raktą, patvirtindama, kad kiekvienas bandymas tarp organizacijų yra užblokuojamas. Ji apima dešimtis priešiškų atakos paviršiaus testų dėl forwarding-header spoofing, header injection ir identifikatorių nutekėjimo, koncentruotą HTML sanitizavimo rinkinį dėl cross-site scripting, vaidmenų užtikrinimo testus visam vaidmenų modeliui ir testus, įrodančius, kad kandidato duomenys iš tiesų ištrinami kaip vienas vienetas. Kadangi šie testai veikia kaip leidimo užkarda, regresija, susilpninanti bet kurią iš šių kontrolės priemonių, sustabdytų leidimą, o ne pasiektų klientus.

12.2 Veikiančios aplinkos penetration testing

Automatizuoti vienetiniai testai įrodo, kad kontrolės priemonės atskirai veikia teisingai. Kad įrodytume, jog jos išlieka veiksmingos realioje diegimo aplinkoje, palaikome pakartojamą penetration-testing metodiką, kuri vykdo realius atakų scenarijus prieš veikiančią aplinką. Ji suskirstyta į šešias fazes:

Fazė	Fokusas	Tikrinimo pavyzdžiai
1. Statinė analizė	Išeities kodas	Paslaptys, injection šablonai, pavojingos funkcijos, trūkstamas auth, nesaugus HTML
2. Architektūros peržiūra	Infrastruktūra	Privatūs galiniai taškai, segmentavimas, TLS, paslapčių konfigūracija
3. Atakos vektorių analizė	Išeities kontrolė ir debesija	Šakų apsauga, tapatybės apimtis, viešas pasiekiamumas
4. Veikiantis penetration testing	Veikianti aplinka	Neautentifikuotas zondavimas, tarporganizacinė prieiga, injection, žetonų klastojimas, SSRF, greičio limito pliūpsniai
5. Įmoninis vertinimas	Brandos lygis	Šešiolika saugumo kategorijų vertinamos pagal įmoninį etaloną
6. Priklausomybių ir tiekimo grandinė	Trečiųjų šalių rizika	Priklausomybių CVE auditas, fiksuoti pipeline veiksmai, lock-file vientisumas

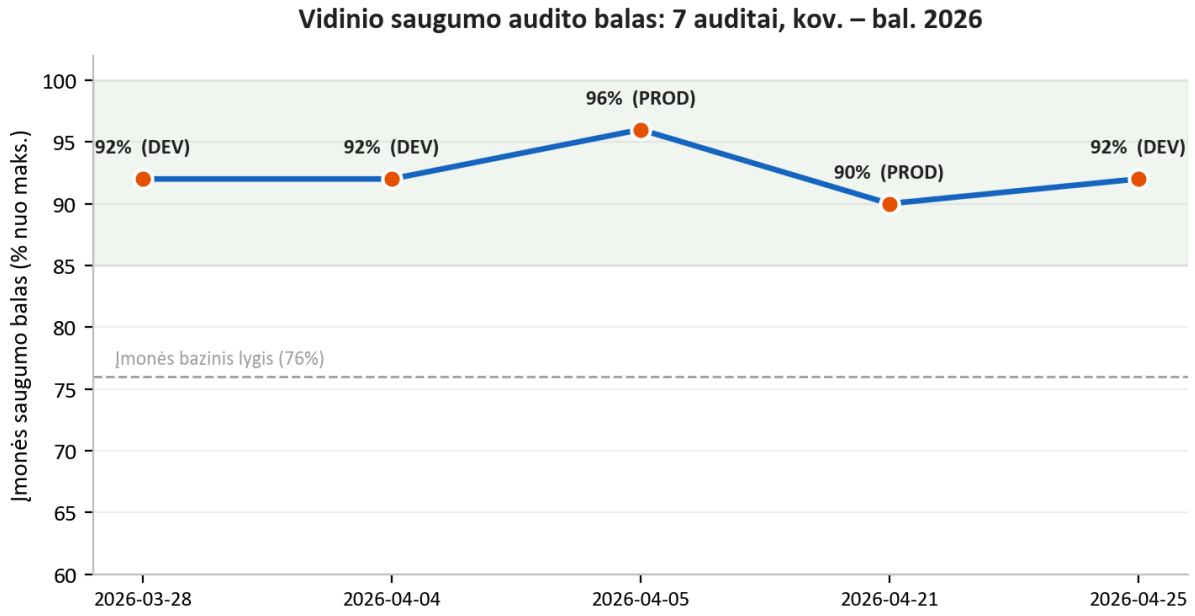
4 fazė yra tikras priešiškas testavimas prieš įdiegtą sistemą, o ne kontrolinis sąrašas. Ji zondais tikrina apsaugotus galinius taškus be kredencialų ir patvirtina, kad jie atsisako suteikti prieigą; užregistruoja dvi organizacijas ir bando pasiekti vienos organizacijos įrašus per kitos paskyrą; įterpia cross-site-scripting ir server-side-template naudmenas ir patvirtina, kad jos neutralizuojamos; klastoja autentifikavimo žetonus ir patvirtina, kad jie atmetami; bando server-side request forgery prieš debesijos metaduomenų galinius taškus; ir užlieja autentifikavimo galinius taškus, kad patvirtintų, jog greičio ribojimas iš tikrųjų įsijungia veikiančioje aplinkoje, o ne tik teoriškai.

12.3 Kandidatų grįžtamojo ryšio saugos testavimas

Kadangi platforma gali generuoti privatų ugdomąjį grįžtamąjį ryšį kandidatams, šiai funkcijai vykdome atskirą priešišką saugos programą. Ji sąmoningai pateikia sistemai griežtas ir priešiškas atrankų specialisto pastabas ir patvirtina, kad kandidatui skirtame rezultate niekada nėra vulgarumo, niekada neatskleidžiama ir nepriskiriama atrankų specialisto tapatybė ar privati nuomonė ir niekada netaikomos vertinančios asmenybės etiketės. Tai saugo ir kandidatą, kuris turi gauti konstruktyvų ir pagarbų grįžtamąjį ryšį, ir klientą, kurio vidinė nuomonė neturi nutekėti į išorę.

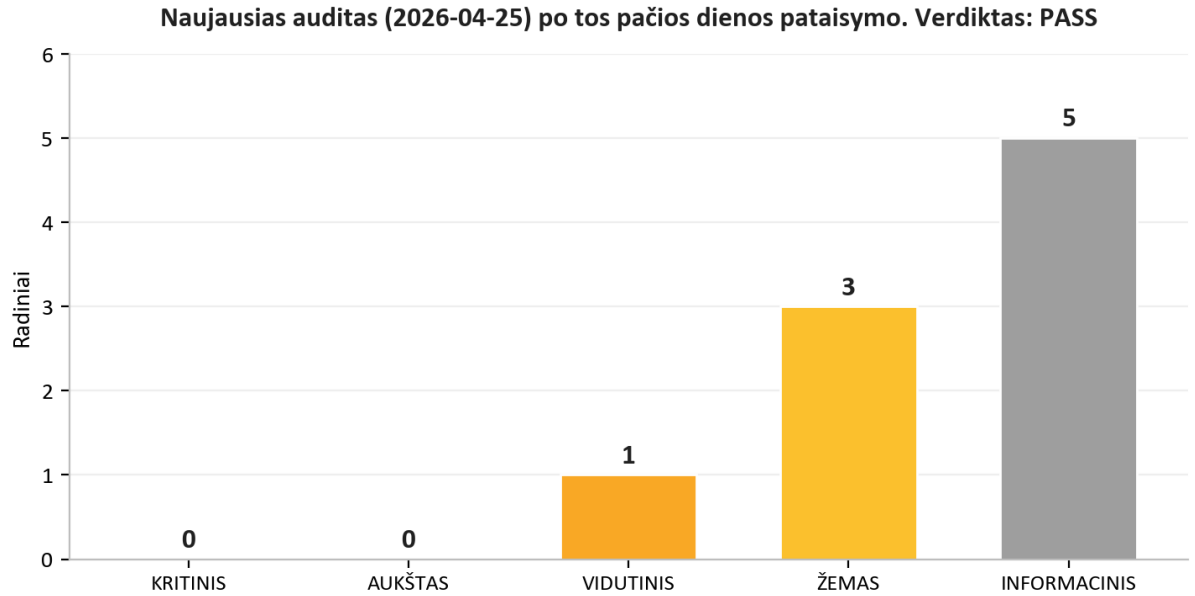
13. Saugumo audito rezultatai

Vykdome periodinius saugumo auditus taikydami struktūruotą, pakartojamą penetration-testing metodiką ir kiekvieną jų dokumentuojame datos žyma pažymėtoje ataskaitoje su pagal rimtumą įvertintais radiniais, įrodymais ir taisomaisiais veiksmais. Tai yra vidiniai auditai, vykdomi pagal mūsų pačių saugumo procesą; formali trečiosios šalies tų pačių kontrolės priemonių sertifikacija yra mūsų veiksmų plane. Tarp 2026 m. kovo pabaigos ir balandžio pabaigos užbaigėme **seven such audits** kūrimo ir produkcinėse aplinkose.



Svarbiausias potencialiam klientui rezultatas yra nuoseklumas: **per visus septynis auditus buvo zero critical findings.** Tais retais atvejais, kai pasirodydavo aukštesnio rimtumo problema, ji būdavo greitai pašalinama, dažnai tą pačią dieną, ir pakartotinai patikrinama. Vertinimo rubrika šiuo laikotarpiu buvo sąmoningai griežtinama (maksimalus galimas balas buvo didinamas, kai pridėdavome daugiau vertinamų kategorijų), todėl normalizuota balų linija išliko aukšta net ir keliant kartelę.

Mūsų naujausias auditas, atliktas 2026 m. balandžio 25 d., gerai iliustruoja, kaip procesas veikia praktikoje. Buvo identifikuotos dvi aukštesnio rimtumo problemos, abi jos buvo ištaisytos ir tą pačią dieną pakartotinai patikrintos, o auditas užbaigtas verdiktu **PASS**, nepaliekant jokių išnaudojimui parengtų problemų esamame grėsmių modelyje.



Auditas	Aplinka	Critical	Verdiktas
2026-03-28	Kūrimo	0	Parengta produkcijai
2026-04-04	Kūrimo	0	Parengta įmonei
2026-04-05	Produkcinė	0	Parengta įmonei
2026-04-20	Kūrimo	0	Parengta produkcijai, su pastabomis
2026-04-20	Kūrimo	0	Praeita su pastabomis
2026-04-21	Produkcinė	0	Saugu, nėra išnaudojamų radinių
2026-04-25	Kūrimo	0	Praeita

Šių auditų tendencija yra sąžiningiausias įrodymas, kurį galime pateikti: problemos randamos, nes jų aktyviai ieškome, ir greitai uždaromos, nes procesas sukurtas joms uždaryti. Tiekėjas, kuris niekada nepraneša apie radinį, dažniausiai yra tiekėjas, kuris neieško.

14. Operacinis atsparumas ir bendra atsakomybė

14.1 Stebėsena ir žurnalai

Taikomosios programos ir platformos telemetrija nukreipiama į centralizuotą log analytics darbo sritį ir taikomosios programos stebėsenos paslaugą, suteikiančią mums matomumą apie pasiekiamumą ir elgseną. Jautrūs veiksmai, tokie kaip duomenų ištrynimas, teisinių sutarčių priėmimas ir AI iškvietimai, registruojami skirtose audito lentelėse, todėl išlieka patvarus įrašas apie tai, kas ką atliko su svarbiais duomenimis.

14.2 Atsarginės kopijos ir atkūrimas

Valdoma duomenų bazė saugo automatines atsargines kopijas, o privati saugykla apsaugota soft-delete saugojimu tiek blob, tiek konteinerių lygmenimis, todėl atsitiktinis ar piktybinis ištrynimas gali būti atkurtas per saugojimo laikotarpį. Kritinei infrastruktūrai taikomi ištrynimo užraktai, kad būtų išvengta atsitiktinio produkcinių išteklių panaikinimo.

14.3 Bendros atsakomybės santrauka

Sritis	AI Interview Analyzer	Klientas
Infrastruktūra, tinklas, pataisų diegimas	Taip	-
Taikomosios programos saugumas ir AI apdorojimo grandinė	Taip	-
Šifravimas, paslaptys, duomenų rezidavimas	Taip	-
Naudotojų ir vaidmenų administravimas	Pateikia kontrolės priemones	Valdo naudotojus ir vaidmenis
Saugojimo politikos konfigūravimas	Pateikia kontrolės priemones	Nustato saugojimo laikotarpį
Kandidatų sutikimas	Pateikia darbo eigą	Užtikrina jos naudojimą
Stiprūs galutinių naudotojų kredencialai ir SSO	Palaiko SSO ir politiką	Užtikrina vidaus politikos vykdymą

15. Grėsmių modelis ir OWASP susiejimas

Projektuojame atsižvelgdami į konkretų priešininkų rinkinį: išorinį užpuoliką be kredencialų, smalsų ar piktybinį vienos organizacijos autentifikuotą naudotoją, bandantį pasiekti kitos organizacijos duomenis, pažeistą priklausomybę ir vidinę klaidą. Toliau pateiktoje lentelėje plačiai naudojamos OWASP Top 10 rizikos kategorijos susiejamos su konkrečiomis kontrolės priemonėmis, kurios šioje platformoje jas mažina ir kurių kiekviena tikrinama 12 skyriuje aprašytu testavimu.

OWASP rizika	Kaip platforma ją mažina
Pažeista prieigos kontrolė	RBAC kiekviename privilegijuotame galiniame taške; apribojimas kiekvienai organizacijai; „not found“ tarporganizacinės prieigos atveju; identifikatorių peržemėlavimas; tarporganizacinių testų matrica
Kriptografiniai trūkumai	TLS 1.2+ perdavimo metu; AES-256 ramybės būsenoje; bcrypt slaptažodžių maišymas; paslaptys valdomoje saugykloje
Injection	Tik ORM parametrizuotos užklausos; griežtas schemos validavimas; HTML sanitizavimas įrašymo metu
Nesaugus dizainas	Sluoksniuota defense in depth; grėsmių modeliavimas ir architektūros peržiūra kiekvieno audito metu
Saugumo neteisinga konfigūracija	Infrastruktūra kaip kodas; default-deny tinklo grupės; saugumo antraštės; išjungti bendri saugyklos raktai; API schema neviešinama produkcinėje aplinkoje
Pažeidžiami komponentai	Savaitinis automatizuotas priklausomybių stebėjimas; priklausomybių CVE auditai periodinių peržiūrų metu
Tapatybės nustatymo ir autentifikavimo trūkumai	Trumpalaikiai žetonai; greičiu ribojamas prisijungimas; el. pašto patvirtinimas; SSO palaikymas; nėra atviru tekstu saugomų slaptažodžių
Programinės įrangos ir duomenų vientisumo trūkumai	Fiksuoti, nekintami pipeline žingsniai; pasirašyti darbalaukio diegikliai; webhook parašų tikrinimas; tag valdomi produkciniai diegimai
Saugumo žurnalavimo ir stebėsenos trūkumai	Centralizuota telemetrija; dedikuotos audito lentelės jautriems veiksmams
Server-side request forgery	Išeinantys kvietimai ribojami patikimais galiniais taškais; SSRF zondai penetration-testing sistemoje

Šis susiejimas yra mūsų užtikrinimo argumento pagrindas: kiekvienai gerai žinomai atakų klasei yra įvardyta kontrolės priemonė, o kiekvienai įvardytai kontrolės priemonei yra testas.

16. Pažeidžiamumų valdymas ir atsakingas atskleidimas

Saugumas niekada nebūna galutinis, todėl vykdome nuolatinį aptikimo ir taisymo ciklą.

- **Aptikimas.** Pažeidžiamumai išryškinami iš keturių šaltinių: automatizuotų testų rinkinio, periodinių penetration-testing auditų, automatizuoto priklausomybių stebėjimo ir klientų ar tyrėjų pranešimų.
- **Triāžas.** Kiekvienam radiniui priskiriamas rimtumo lygis (critical, high, medium, low arba informational) su įrodymais ir taisymo atsakingu asmeniu, tiksliai kaip užfiksuota mūsų audito ataskaitose.
- **Taisymo tikslai.** Critical ir high radiniams teikiamas prioritetas nedelsiam taisymui; mūsų audito istorijoje aukštesnio rimtumo radiniai paprastai buvo ištaisomi ir pakartotinai patikrinami tą pačią dieną. Medium ir žemesnio lygio radiniai planuojami pagal įprastą priežiūros ciklą.
- **Patvirtinimas.** Pataisymai iš naujo testuojami, o kai aktualu, prieš įdiegtą aplinką atliekamas veikiantis patikrinimas, patvirtinantis, kad problema tikrai uždaryta, o ne tik uždaryta kode.
- **Atskleidimas.** Apie saugumo problemas galima pranešti tiesiogiai mums. Mes patvirtiname pranešimus, juos tiriame ir informuojame pranešėją iki pat išsprendimo.

17. Atitikties susiejimas

17.1 GDPR

GDPR sritis	Platformos įgyvendinimas
Teisėtas pagrindas (Art. 6)	Aiškus kandidato sutikimas surenkamas prieš apdorojimą
Duomenų minimizavimas ir saugojimo ribojimas (Art. 5)	Apdorojami tik su pokalbiu susiję duomenys; konfigūruojamas saugojimas su automatiniu ištrynimu
Teisė būti ištrintam (Art. 17)	Visų kandidato duomenų vienetinės apimties ištrynimas su registruotu ištrynimo įrodymu
Duomenų subjekto teisės (Art. 15 to 20)	Palaikoma prieiga, ištrynimas, perkeliamumas ir prieštaravimas
Duomenų tvarkytojo pareigos (Art. 28)	DPA priimamas registracijos metu ir versijuojamas kiekvienai organizacijai
Apdorojimo saugumas (Art. 32)	Šifravimas, prieigos kontrolė, izoliacija ir nuolatinis testavimas, kaip aprašyta šiame dokumente
Sub-processor skaidrumas	Atskleidžiama DPA su išankstiniu pranešimu apie pakeitimus

17.2 EU AI Act

Platforma traktuojama kaip aukštos rizikos AI sistema, palaikanti su užimtumu susijusius sprendimus, ir mes palaikome su reguliavimu suderintą dokumentaciją, įskaitant skaidrumo kortelę, naudotojo dokumentaciją ir atitikties deklaraciją. Pagrindinės apsaugos priemonės — žmogaus priežiūra, skaidrumas, įrodymais pagrįstas vertinimas ir griežtos ribos tam, ką AI vertina — aprašytos 10 skyriuje. Toliau brandiname savo formalią atitikties dokumentaciją, pažengiant reglamento įgyvendinimo terminams.

17.3 Talpinimo sertifikatai

Platforma visa apimtimi veikia Microsoft Azure, kurio duomenų centrai turi nepriklausomas sertifikacijas, įskaitant ISO 27001 ir SOC 2. Šios sertifikacijos apima fizinius ir platformos sluoksnius po mūsų taikomąja programa; taikomojo lygmens kontrolės priemonės yra tos, kurios aprašytos šiame dokumente.

17.4 Sub-processor registras

Sub-processor	Paskirtis	Regionas
Microsoft Azure	Talpinimas, AI ir kalbos apdorojimas, saugykla, transakcinis el. paštas	ES (West Europe, Sweden Central)
Stripe	Prenumeratų ir mokėjimų apdorojimas	ES (Ireland)
Fakturownia	Sąskaitų išrašymas	ES (Poland)
ATS connector (pasirinktinai)	Kandidatų sekimo sistemos integracija, įjungiama tik pagal prašymą	ES

18. Saugumo veiksmų planas

Saugumą laikome nuolat tobulinama programa. Dabartinės mūsų veiksmų plano iniciatyvos apima kelių veiksnių autentifikavimo parinkčių stiprinimą administracinėms paskyroms, centralizuoto duomenų prieigos audito žurnalavimo plėtrą, tolesnį reguliaraus priklausomybių aktualumo griežtinimą ir formalią trečiosios šalies šiame dokumente aprašytų kontrolės priemonių sertifikaciją. Nė viena iš šių iniciatyvų nėra spraga, dėl kurios šiandien būtų atskleisti klientų duomenys; kiekviena yra jau sluoksniuotos saugumo būsenos stiprinimas.

19. Santrauka

AI Interview Analyzer saugo kandidatų ir klientų duomenis naudodama sluoksniuotą architektūrą: pagal numatymą privatų tinklą be viešų duomenų paslaugų, stiprią tapatybę ir izoliaciją kiekvienai organizacijai, taikomosios programos kodą, kuris pašalina ištisas pažeidžiamumų klases, šifravimą ir duomenų rezidavimą ES bei privatumo kontrolės priemones, įdiegtas pačiame duomenų modelyje. Platformą išskiria įrodymai, pagrindžiantys šiuos teiginius. Turėdami 3,171 automatizuotų testų, pakartojamą veikiantį penetration-testing metodiką, specialią AI saugos programą ir septynių vidinių saugumo auditų istoriją be zero critical findings, galime ne tik pasakyti, bet ir parodyti, kad platforma yra saugi.

Priedas A: Saugumo kontrolės priemonių katalogas

Sutrumpinta pirminių kontrolės priemonių ir jas pagrindžiančių įrodymų nuoroda.

Kontrolės priemonė	Mechanizmas	Įrodymai
Perdavimo šifravimas	Tik HTTPS, TLS 1.2+, HTTP peradresuojamas	Infrastruktūra kaip kodas; architektūros auditas
Šifravimas ramybės būsenoje	AES-256 platformos šifravimas saugykloje ir duomenų bazėje	Platformos konfigūracija; architektūros auditas
Slaptažodžių apsauga	bcrypt su salt kiekvienam slaptažodžiui	Išeities kontrolė; autentifikavimo testai
Sesijų valdymas	30 minučių pasirašyti žetonai, atšaukiamas serverio pusės atnaujinimas	Išeities kontrolė; autentifikavimo testai
Autorizavimas	Keturių vaidmenų prieigos kontrolė privilegijuotuose galiniuose taškuose	Vaidmenų užtikrinimo testų rinkinys
Nuomininkų izoliacija	Užklausų apribojimas kiekvienai organizacijai; 404 tarporganizacinės prieigos atveju	Tarporganizacinių testų matrica
API raktų saugumas	Saugojimas hash pavidalu, ribotos teisės, kiekvienam raktui taikomi greičio limitai	API raktų testų rinkinys
Apsauga nuo injection	Tik ORM parametrizuotos užklausos	Statinė analizė; injection testai
Apsauga nuo cross-site scripting	HTML sanitizavimas įrašymo metu	HTML sanitizavimo testų rinkinys
Greičio ribojimas	Patvari, duomenų baze paremta ribojimo sistema auth galiniuose taškuose	Greičio limito testai; veikiantys pliūpsnių patikrinimai
Webhook vientisumas	Tiekėjo parašo tikrinimas neapdorotame kūne	Webhook testų rinkinys
Paslapčių valdymas	Valdoma saugykla, purge protection, managed identity	Infrastruktūra kaip kodas; architektūros auditas
Tinklo izoliacija	Privatūs galiniai taškai; default-deny segmentavimas	Infrastruktūra kaip kodas; architektūros auditas
Duomenų ištrynimas	Vienetinės apimties kaskadinis ištrynimas su audito žurnalu	GDPR ištrynimo testų rinkinys
Tiekimo grandinė	Fiksuoti pipeline žingsniai; savaitinis priklausomybių stebėjimas	Pipeline konfigūracija; priklausomybių auditas

Priedas B: Dažniausiai užduodami klausimai saugumo vertintojams

Kur saugomi mūsų duomenys? Visiškai Europos Sąjungoje, Microsoft Azure, West Europe regione, o AI apdorojimas vyksta ES regionuose. Kandidatų duomenys niekada nepalieka ES.

Ar mūsų duomenys naudojami AI modelių mokymui? Ne. AI tiekėjas nenaudoja klientų duomenų mokymui.

Ar duomenų bazė pasiekiama iš interneto? Ne. Vieša tinklo prieiga yra išjungta, o duomenų bazė pasiekiama tik per privatų galinį tašką virtualiame tinkle.

Ar vienas klientas gali matyti kito kliento duomenis? Ne. Kiekviena užklausa apribojama kviečiančiojo organizacija, tarporganizacinė prieiga grąžina „not found“, o automatizuota matrica nuolat testuoja šią izoliaciją.

Kaip saugomi slaptažodžiai? Maišomi naudojant bcrypt ir unikalų salt kiekvienam slaptažodžiui. Palaikomas single sign-on su Microsoft ir Google, tokiu atveju slaptažodis nesaugomas.

Ar palaikote single sign-on? Taip, per Microsoft ir Google OAuth.

Kiek laiko galioja prieigos žetonai? Trisdešimt minučių, poroje su atšaukiama serverio pusės atnaujinimo sesija, kuri panaikinama atsijungiant.

Kaip tvarkomas kandidato sutikimas? Kiekvienas kandidatas gauna unikalią, vienkartinę sutikimo nuorodą ir turi sutikti prieš bet kokį įrašymą ar analizę. Sutikimas registruojamas prie konkretaus samdos proceso.

Kaip ištrinami duomenys? Kaip vienas vienetas, apimantis kandidato įrašą, pokalbius, transkriptus, garso įrašus, dokumentus ir palyginimus, pagal konfigūruojamą saugojimo grafiką, su registruotu ištrynimo įrodymu. Kandidatai taip pat gali tiesiogiai paprašyti ištrynimo.

Ar turite DPA? Taip, jis priimamas registracijos metu ir versijuojamas kiekvienai organizacijai, įskaitant sub-processor registrą.

Ar AI priima samdos sprendimus? Ne. Jis teikia tik sprendimų palaikymą; žmogus peržiūri kiekvieną išvestį ir priima visus sprendimus.

Kaip įrodote savo saugumo teiginius? Per 3,171 automatizuotų testų, įskaitant specialią saugumo testų aibę, pakartojamą šešių fazių penetration-testing metodiką, vykdomą veikiančiose aplinkose, AI saugos testavimo programą ir periodines rašytines audito ataskaitas.

Kas nutinka radus pažeidžiamumą? Jam priskiriamas rimtumo lygis, įrodymai ir atsakingas asmuo, jis taisomas pagal prioritetinį grafiką, pakartotinai patikrinamas, įskaitant veikiančius patikrinimus, kai reikia, ir užfiksuojamas audito ataskaitoje.

Ar galime atlikti savo penetration test? Saugumo vertinimus galima suderinti per jūsų paskyros atstovą, laikantis tinkamos apimties ir grafiko.

Priedas C: Glosarijus

Terminas	Reikšmė
AES-256	Stiprus simetrinis šifravimo standartas, naudojamas duomenims ramybės būsenoje apsaugoti
bcrypt	Specialiai slaptažodžių maišymui sukurta funkcija su salt kiekvienam slaptažodžiui
Managed identity	Platformos išduota tapatybė, leidžianti paslaugai autentifikuotis be saugomų raktų
Private endpoint	Privatus tinklo adresas, kuris neleidžia debesijos paslaugai būti viešajame internete
Network security group	Leidimo ir draudimo taisyklių rinkinys, filtruojantis tinklo srautą į potinklį
RBAC	Role-based access control, suteikianti teises pagal naudotojo vaidmenį
IDOR	Insecure direct object reference, prieigos kontrolės klaida, nuo kurios platforma ginasi
SSRF	Server-side request forgery, atakų klasė, tikrinama mūsų penetration tests metu
Web application firewall	Kraštinė kontrolės priemonė, filtruojanti piktybinį žiniatinklio srautą
Data processing agreement	Sutartis, reglamentuojanti, kaip duomenų tvarkytojas tvarko asmens duomenis valdytojo vardu

Priedas D: Kontaktai ir dokumento kontrolė

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Dėl saugumo peržiūros, mūsų DPA kopijos arba mūsų EU AI Act atitikties dokumentacijos kreipkitės į savo paskyros atstovą.

Šiame dokumente aprašoma AI Interview Analyzer paslaugos saugumo būsena dokumento paraštėje nurodytos generavimo datos momentu. Jis pateikiamas vertinimo tikslais ir nesudaro jokios sutarties dalies. Konkretūs sutartiniai saugumo įsipareigojimai nustatyti taikytinoje sutartyje ir DPA.