Whitepaper tas-Sigurtà

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Whitepaper tas-Sigurtà

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

Udjenza: Timijiet tas-sigurtà tal-intrapriża, IT, u akkwist

Klassifikazzjoni: Pubbliku

1. Sommarju Eżekuttiv

AI Interview Analyzer hija pjattaforma ta' reklutaġġ għall-intrapriżi li tirreġistra intervisti bil-kunsens espliċitu tal-kandidat, tittraskrivihom u tistrutturahom, u tipproduċi appoġġ għall-evalwazzjoni bbażat fuq evidenza għar-reklutaturi. Minħabba li l-pjattaforma timmaniġġja data personali tal-kandidati u tappoġġja proċessi ta' reklutaġġ, is-sigurtà u l-privatezza huma trattati bħala restrizzjonijiet ewlenin tad-disinn, mhux bħala karatteristiċi miżjuda aktar tard.

Dan il-whitepaper jiddeskrivi, f'termini konkreti u verifikabbli, kif nipproteġu d-data tal-klijenti u tal-kandidati. Huwa miktub għall-persuni li jirrevedu l-forniturі: inġiniera tas-sigurtà, amministraturi tal-IT, uffiċjali tal-protezzjoni tad-data, u timijiet tal-akkwist. Kull ċifra f'dan id-dokument hija meħuda direttament mis-sistemi tagħna stess tal-inġinerija aktar milli minn materjal ta' marketing.

Il-messaġġ ċentrali huwa sempliċi: **aħna mhux sempliċement niddikjaraw li l-pjattaforma hija sigura, aħna nittestjaw kontinwament li hija hekk.** Il-codebase tagħna fih **3,171 test awtomatizzati**, inkluża suite dedikata tas-sigurtà li teżerċita l-awtentikazzjoni, l-awtorizzazzjoni, l-iżolament bejn organizzazzjonijiet differenti, id-difiżi kontra injection, u t-tħassir tad-data. Barra minn hekk, inħaddmu harness ripetibbli ta' penetration-testing kontra deployments live u nipproduċu rapporti ta' awditjar bil-miktub. F'seba' awditi interni tas-sigurtà matul March u April 2026, irreġistrajna **zero critical findings**, bl-aktar awditu reċenti tagħna jagħlaq b'verdett ta' **PASS**. (Ċertifikazzjoni formali minn parti terza ta' dawn il-kontrolli tinsab fil-pjan direzzjonali tagħna; ara Taqsima 18.)

Karatteristika tas-sigurtà	Sommarju
Hosting	Microsoft Azure, reġjuni tal-UE biss
Mudell tan-network	Endpoints privati, segmentazzjoni tan-network default-deny, l-ebda database pubblika
Encryption	AES-256 at rest, TLS 1.2 jew ogħla in transit
Identità	Tokens iffirmati ta' ħajja qasira, hashing tal-passwords b'bcrypt, appoġġ għal SSO
Kontroll tal-aċċess	Kontroll tal-aċċess ibbażat fuq ir-rwoli b'iżolament strett għal kull organizzazzjoni
Secrets	Vault ċentralizzat tas-secrets b'aċċess managed-identity
Privatezza	Kunsens espliċitu, retention konfigurabbli, erasure ta' unità waħda
AI responsabbli	Appoġġ għad-deċiżjonijiet biss, bniedem dejjem fil-loop
Assigurazzjoni	3,171 test awtomatizzati flimkien ma' penetration tests u awditi rikorrenti

1.1 Kif Taqra Dan id-Dokument

It-Taqsimiet 3 sa 11 jiddeskrivu l-kontrolli li jipproteġu d-data: l-arkitettura, in-network, l-identità, l-applikazzjoni, il-protezzjoni tad-data, il-privatezza, u ċ-ċiklu ta' ħajja tal-iżvilupp sigur. It-Taqsimiet 12 u 13 ikopru l-programm distintiv tagħna ta' ttestjar kontinwu u l-istorja tal-awditi tagħna. It-Taqsimiet 14 sa 17 ikopru l-operazzjonijiet, l-immudellar tat-theddid, il-ġestjoni tal-vulnerabbiltajiet, u l-allinjament tal-konformità. L-appendiċijiet jipprovdu katalogu tal-kontrolli, FAQ għal reviżuri, u glossarju li tim tas-sigurtà jista' juża direttament waqt valutazzjoni.

2. Ambitu u Approċċ tad-Dokument

2.1 X'Jikopri Dan id-Dokument

Dan il-whitepaper ikopri l-arkitettura tas-sigurtà u l-prattiki tas-servizz AI Interview Analyzer: l-ambjent tal-hosting, id-disinn tan-network, il-ġestjoni tal-identità u l-aċċess, il-kontrolli fil-livell tal-applikazzjoni, il-protezzjoni tad-data, il-privatezza u l-allinjament regolatorju, iċ-ċiklu ta' ħajja tal-iżvilupp sigur, u l-programm tagħna ta' ttestjar kontinwu tas-sigurtà.

2.2 X'Jagħmlu Verifikabbli

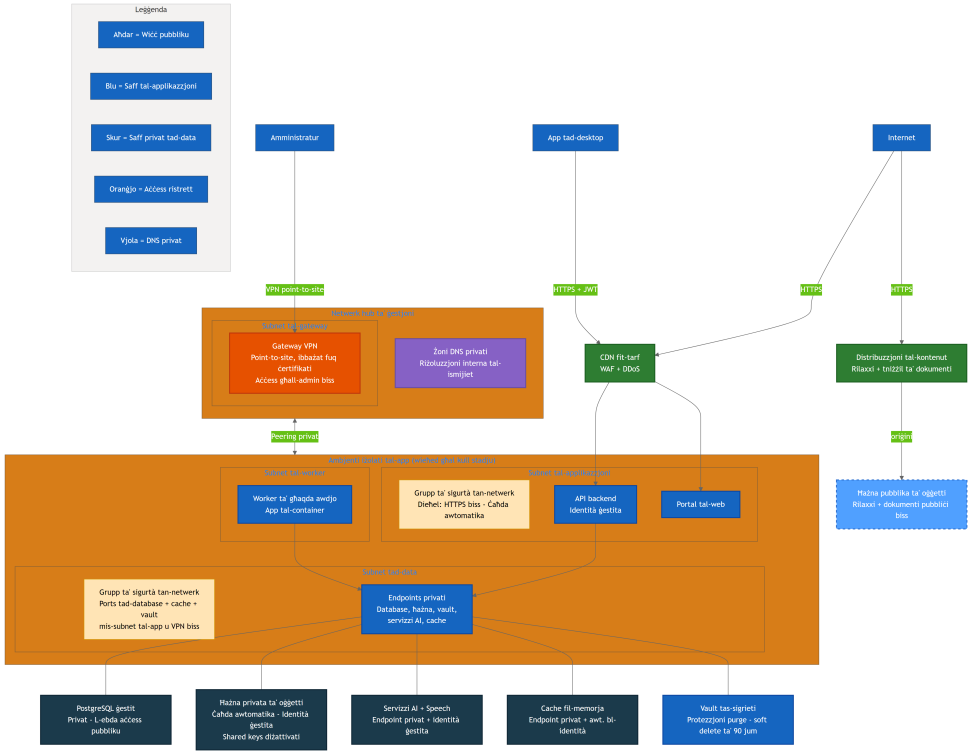
Dikjarazzjonijiet tas-sigurtà minn fornitur huma faċli biex jinkitbu u diffiċli biex jiġu fdati. Għaldaqstant rabatna kull dikjarazzjoni ewlenija f'dan id-dokument ma' xi ħaġa konkreta u li tista' tingħadd fis-sistemi tagħna tal-inġinerija: kontroll implimentat fil-kodiċi, test li jipprova li l-kontroll jaħdem, definizzjoni tal-infrastruttura li tinfurzah, jew rapport ta' awditjar li jirreġistra verifika dokumentata. Fejn kontroll huwa parti mill-pjan direzzjonali futur tagħna aktar milli diġà rilaxxat illum, ngħidu dan b'mod espliċitu. Nippreferu niddikjaraw inqas u nkunu fdati milli niddikjaraw wisq u ninqabdu.

2.3 Responsabbiltà Kondiviża

Il-pjattaforma tingħata bħala software as a service. Aħna noperaw l-infrastruttura, l-applikazzjoni, il-pipeline tal-AI, u l-immaniġġjar tad-data. Il-klijent huwa responsabbli għall-ġestjoni tal-kontijiet u r-rwoli tal-utenti tiegħu stess, għall-konfigurazzjoni tal-perjodi ta' data-retention biex jaqblu mal-politika interna tiegħu, u biex jiżgura li l-kunsens tal-kandidat jinkiseb permezz tal-workflow tal-kunsens li tipprovdi l-pjattaforma. It-Taqsima 14 tiddeskrivi din il-qasma b'aktar dettall.

3. Ħarsa Ġenerali lejn l-Arkitettura tas-Sigurtà

Il-pjattaforma hija mibnija bħala numru żgħir ta' servizzi li jikkooperaw aktar milli monolit wieħed. Applikazzjoni desktop u portal web jaġixxu bħala clients. API backend ċentrali tippossjedi l-persistence kollu, l-awtentikazzjoni, il-billing, il-pipeline tal-AI, il-kunsens, l-email, l-immaniġġjar tal-fajls, u d-dashboards. Worker tal-audio merge jipproċessa r-reġistrazzjonijiet b'mod asinkroniku. Kull stat sensittiv jgħix wara l-API backend; il-clients qatt ma jitkellmu direttament mad-database, mal-ħażna, jew mas-servizzi tal-AI.



Id-dijagramma ta' hawn fuq turi t-topoloġija tal-produzzjoni bl-ismijiet tar-riżorsi intenzjonalment ġeneralizzati. Fiha huma viżibbli tliet prinċipji:

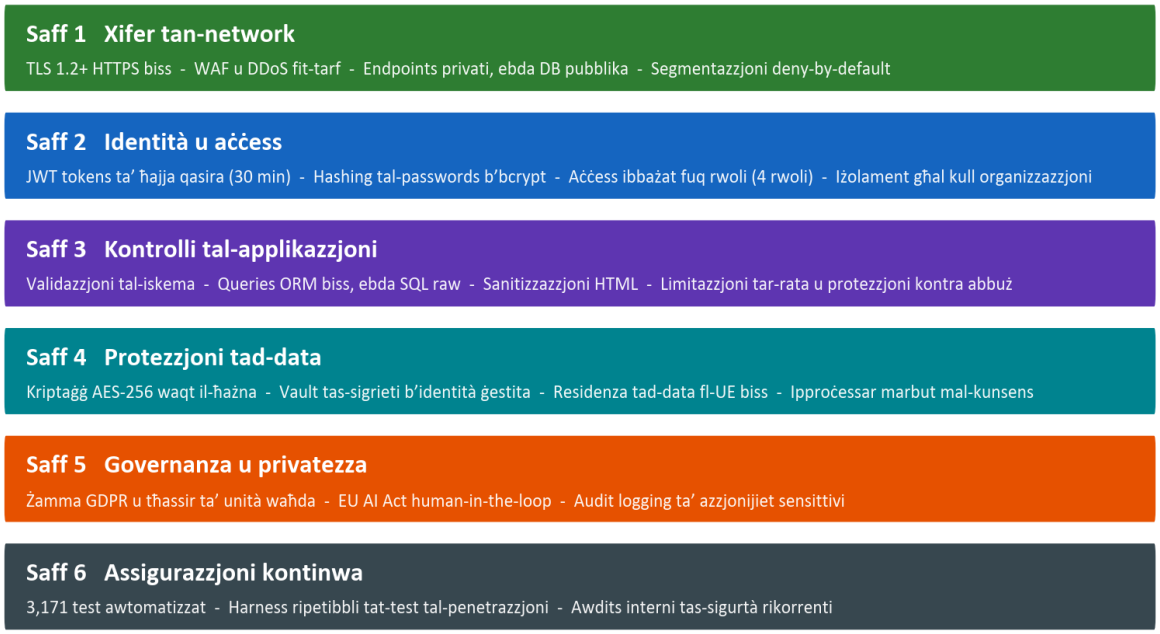
- **L-ebda espożizzjoni diretta tas-servizzi tad-data.** Id-database, il-ħażna privata tal-oġġetti, is-servizzi tal-AI, u l-cache għandhom l-aċċess pubbliku tan-network diżattivat u jistgħu jintlaħqu biss permezz ta' endpoints privati ġewwa network virtwali iżolat. Il-vault tas-secrets jintlaħaq mill-applikazzjoni fuq endpoint privat u huwa protett addizzjonalment b'awtentikazzjoni tal-identità tal-pjattaforma u politiki ta' aċċess least-privilege, b'tali mod li kull aċċess jeħtieġ identità valida u awtorizzata irrispettivament mill-passaġġ tan-network.
- **Wiċċ pubbliku separat.** L-unika ħażna pubblika tal-oġġetti żżomm downloads ta' rilaxxi u dokumenti pubbliċi. Qatt ma fiha data tal-kandidati. It-traffiku tal-applikazzjoni li jħares lejn il-klijent jgħaddi minn edge layer li jipprovdi web application firewall, protezzjoni DDoS, u content delivery.
- **L-aċċess amministrattiv huwa rregolat.** L-operaturi jilħqu r-riżorsi interni biss permezz ta' VPN point-to-site ibbażat fuq ċertifikati f'network ta' management hub, mhux fuq l-internet pubbliku.

Kull stadju ta' deployment (żvilupp u produzzjoni) huwa ambjent kompletament iżolat bin-network, storage accounts, database, u secrets tiegħu stess. Id-data tal-produzzjoni tal-klijenti qatt ma tkun preżenti f'ambjenti inferjuri. Management hub maqsum iżomm biss il-VPN gateway u private DNS, imqabbad privatament ma' kull ambjent.

4. Defense in Depth

L-ebda kontroll wieħed ma huwa fdat biex iwaqqaf kull attakk. Il-pjattaforma tpoġġi f'saffi kontrolli indipendenti sabiex il-falliment ta' kwalunkwe saff wieħed ma jesponix id-data. Is-saffi hawn taħt huma kull wieħed implimentati u, kif deskritt fit-Taqsima 12, ittestjati individwalment.

Mudell ta' sigurtà b'saffi: kontrolli indipendenti f'kull livell



Saff	Kontrolli rappreżentattivi
Xifer tan-network	Trasport TLS biss, edge WAF u protezzjoni DDoS, endpoints privati, segmentazzjoni default-deny
Identità u aċċess	Tokens iffirmati ta' ħajja qasira, hashing b'bcrypt, kontroll tal-aċċess ibbażat fuq ir-rwoli, iżolament għal kull organizzazzjoni
Applikazzjoni	Validazzjoni tal-iskema fuq kull input, aċċess għad-data b'ORM biss, output encoding, rate limiting
Protezzjoni tad-data	Encryption at rest, vault tas-secrets b'managed identity, residenza tad-data fl-UE, ipproċessar ikkundizzjonat mill-kunsens
Governanza u privatezza	Retention konfigurabbli, erasure ta' unità waħda, AI human-in-the-loop, audit logging
Assigurazzjoni kontinwa	Suite ta' test awtomatizzati, penetration tests ripetibbli, awditi interni rikorrenti tas-sigurtà

Il-bqija ta' dan id-dokument jgħaddi minn kull saff wieħed wieħed u mbagħad jiddeskrivi kif nippruvaw, kontinwament, li s-saffi jibqgħu sodi.

5. Sigurtà tan-Network

5.1 Privat b'Default

It-tier tad-data huwa privat mill-kostruzzjoni. Id-database managed PostgreSQL għandha l-aċċess pubbliku tan-network diżattivat u tista' tintlaħaq biss permezz ta' endpoint privat. Il-ħażna privata tal-oġġetti hija kkonfigurata biex tiċħad l-aċċess tan-network b'default, tiddiżattiva kompletament shared access keys, u hija aċċessibbli biss permezz ta' managed identity mis-subnet tal-applikazzjoni. Il-cache, is-servizzi tal-AI, u l-vault tas-secrets bl-istess mod jintlaħqu permezz ta' endpoints privati b'private DNS resolution.

Fil-prattika dan ifisser li ma hemm l-ebda connection string li tħares lejn l-internet għad-database u l-ebda URL pubbliku tal-ħażna għall-awdjo tal-kandidati: id-database u l-ħażna privata għandhom l-aċċess pubbliku tan-network diżattivat kompletament. Il-vault tas-secrets jintlaħaq mill-applikazzjoni fuq endpoint privat u huwa protett b'awtentikazzjoni tal-identità tal-pjattaforma u politiki ta' aċċess least-privilege, b'identitajiet tal-applikazzjoni mogħtija aċċess read-only biss għas-secrets li għandhom bżonn, sabiex is-secrets ma jistgħux jinkisbu mingħajr identità valida u awtorizzata. Il-wiċċ ta' attakk li avversarju estern jista' saħansitra jmiss huwa limitat għall-endpoints HTTPS tal-applikazzjoni wara l-edge layer.

5.2 Segmentazzjoni tan-Network

Kull ambjent huwa maqsum f'subnets separati għat-tier tal-applikazzjoni, it-tier tad-data, u l-worker asinkroniku. Kull subnet hija rregolata minn network security group li r-regola finali tiegħu tiċħad kull traffiku inbound. Is-subnet tal-applikazzjoni taċċetta biss HTTPS inbound. Is-subnet tad-data taċċetta biss il-ports speċifiċi tad-database, cache, u vault, u biss mis-subnet tal-applikazzjoni jew mill-VPN amministrattiv. Dan ifisser li anki attakkant li b'xi mod jilħaq it-tier tal-applikazzjoni ma jistax idur liberament lejn it-tier tad-data; l-uniċi passaġġi permessi huma dawk li l-applikazzjoni tuża b'mod leġittimu.

5.3 Ix-Xifer

It-traffiku pubbliku tal-applikazzjoni huwa quddiem edge layer li jipprovdi web application firewall, protezzjoni DDoS, u content delivery network. Downloads ta' rilaxxi u dokumenti jingħataw minn public storage account dedikat permezz ta' front door ta' content-delivery, kompletament separat mill-ħażna privata li żżomm id-data tal-kandidati. Iż-żewġ pjani tal-ħażna qatt ma jitħalltu: misconfiguration fuq il-pjan pubbliku ma tistax tesponi data privata tal-kandidati, minħabba li huma kontijiet differenti b'regoli differenti tan-network.

5.4 Aċċess Amministrattiv

Ma hemm l-ebda endpoint amministrattiv pubbliku fin-network privat. L-operaturi jikkonnettjaw permezz ta' VPN gateway point-to-site li juża awtentikazzjoni bbażata fuq ċertifikati. L-aċċess amministrattiv għad-database u l-cache huwa possibbli biss minn ġewwa dak it-tunnel, peress li dawn is-servizzi għandhom l-aċċess pubbliku tan-network diżattivat. Dan iżomm l-operazzjonijiet ta' kuljum kompletament barra mill-internet pubbliku.

6. Ġestjoni tal-Identità u l-Aċċess

6.1 Awtentikazzjoni

Is-sessjonijiet tal-utenti jiġu stabbiliti b'access token iffirmat li huwa validu għal tletin minuta, imqabbad ma' refresh token separat, opak, min-naħa tas-server. L-access tokens jiġu vverifikati fuq kull talba, u l-utent jiġi rivalidat kontra d-database (inkluż verifika ta' kont attiv) aktar milli jkun fdat biss fuq il-kontenut tat-token. Il-logout jirrevoka s-sessjoni refresh min-naħa tas-server immedjatament, sabiex refresh token misruq ma jistax jgħix aktar mill-logout.

Il-passwords qatt ma jinħażnu f'test sempliċi. Huma jiġu hashed b'bcrypt billi jintuża salt uniku għal kull password. Għal organizzazzjonijiet li jippreferu single sign-on, il-pjattaforma tappoġġja login OAuth ma' Microsoft u Google, f'liema każ ma tinżamm l-ebda password.

Is-sjieda tal-email tiġi vverifikata permezz ta' verification link ta' użu wieħed u limitata fiż-żmien qabel ma kont irreġistrat minnu nnifsu jitqies bħala verifikat, u r-rigenerazzjoni ta' verification-email hija rate limited biex tipprevjeni abbuż.

6.2 Kontroll tal-Aċċess Ibbażat fuq ir-Rwoli

L-awtorizzazzjoni hija infurzata permezz ta' mudell ta' rwoli b'erba' rwoli ta' privileġġ dejjem jiżdied: interviewer, hiring manager, recruiter, u administrator. L-aċċess għal operazzjonijiet privileġġjati huwa infurzat minn dipendenzi min-naħa tas-server li jivverifikaw kemm ir-rwol kif ukoll l-istatus ta' verifika ta' min qed isejjaħ. Dawn il-verifiki tar-rwoli jipproteġu ferm aktar minn mitt operazzjoni API distinta.

Rwol	Kapaċitajiet tipiċi
Interviewer	Jagħmel intervisti assenjati; jara biss intervisti assenjati lilu
Hiring manager	Jimmaniġġja reklutaġġi li jippossjedi jew li tagħhom huwa membru
Recruiter	Ġestjoni sħiħa tar-reklutaġġ u tal-kandidati fi ħdan l-organizzazzjoni
Administrator	Settings tal-organizzazzjoni, billing, amministrazzjoni tal-utenti u tal-API keys

Lil hinn minn verifiki ġenerali tar-rwoli, il-pjattaforma tapplika regoli ta' viżibbiltà fil-livell tad-data. Il-hiring managers jaraw biss ir-reklutaġġi li huma ħolqu jew li tagħhom huma membri; l-interviewers jaraw biss l-intervisti assenjati lilhom. Għalhekk il-privileġġ jiġi infurzat kemm fil-livell ta' "liema azzjoni" kif ukoll fil-livell ta' "liema rekords."

6.3 Iżolament għal Kull Organizzazzjoni

Il-pjattaforma hija multi-tenant, u l-iżolament bejn tenants huwa trattat bħala kontroll tas-sigurtà ta' klassi ewlenija. Kull identità awtentikata ġġorr identifikatur ta' organizzazzjoni, u l-queries tad-data huma scoped għal dik l-organizzazzjoni. Meta utent jitlob rekord li jappartjeni lil organizzazzjoni oħra, il-pjattaforma tirritorna tweġiba ta' "not found" aktar milli tiżvela li r-rekord jeżisti. Identifikaturi interni tad-database qatt ma jiġu esposti fuq il-wire; l-API tippreżenta display identifiers u terġa' timmappjahom għal kull talba, li jneħħi klassi komuni ta' attakk ta' enumerazzjoni bejn tenants.

Dan mhux biss intenzjoni ta' disinn. Kif deskritt fit-Taqsima 12, is-suite awtomatizzata tagħna tħaddem matrix kbira bejn organizzazzjonijiet li tipprova tilħaq id-data ta' organizzazzjoni waħda billi tuża kredenzjali ta' organizzazzjoni oħra u tasserixxi li kull tentattiv bħal dan ifalli.

6.4 Aċċess Programmatiku

Għall-integrazzjonijiet, organizzazzjonijiet fuq pjani eliġibbli jistgħu joħorġu API keys. Iċ-ċwievet jużaw prefiss rikonoxxibbli, iġorru 128 bits ta' entropy, u jinħażnu biss bħala hash; iċ-ċavetta mhux maħduma tintwera darba fil-ħolqien u qatt aktar. Kull ċavetta ġġorr permission scope espliċitu (read, write, jew integrazzjoni ATS), tista' tiġi ristretta għal networks sors speċifiċi, tista' tiġi revokata istantanjament, u hija suġġetta għal limiti ta' rata għal kull ċavetta derivati mil-livell tal-pjan tal-organizzazzjoni. Il-verifika taċ-ċwievet tuża timing-safe comparison biex tevita tnixxija ta' informazzjoni permezz tal-ħin tar-rispons.

7. Sigurtà tal-Applikazzjoni

L-applikazzjoni hija miktuba biex tneħħi kategoriji sħaħ ta' vulnerabbiltà aktar milli tagħmel patch għalihom każ b'każ.

• **Injection.** L-aċċess kollu għad-database jgħaddi minn object-relational mapper b'parameterized queries. Il-codebase ma fih l-ebda SQL mhux maħdum ifformattat bħala string. Dan jelimina b'mod strutturali SQL injection.

• **Validazzjoni tal-input.** Kull request body tiġi vvalidata kontra skema stretta qabel ma tilħaq il-business logic. Payloads kbar wisq jiġu miċħuda, u list endpoints huma paginated biex jillimitaw l-użu tar-riżorsi.

• **Output encoding u cross-site scripting.** Test fornuta mill-utent u ġġenerata mill-AI hija trattata bħala mhux fdata. Fejn il-kontenut irid jiġi rrendut bħala HTML, jgħaddi minn sanitizer allow-list fil-ħin tal-kitba, u suite dedikata ta' testijiet tikkonferma li script tags, event handlers, u URLs javascript jitneħħew.

• **Mass assignment.** Operazzjonijiet ta' update jużaw skemi espliċiti li jeskludu oqsma privileġġjati bħal role, organization, u credit balance, sabiex client ma jistax iżid il-privileġġ billi jippubblika oqsma żejda.

• **Rate limiting.** Endpoints tal-awtentikazzjoni u dawk suxxettibbli għall-abbuż huma rate limited bl-użu ta' limiter durabbli, appoġġjat mid-database, li jibqa' jgħix wara restarts u jaħdem korrettament fuq istanzi multipli tal-applikazzjoni. Login, reġistrazzjoni, password reset, u verification resends kull wieħed għandhom il-limiti tagħhom. Ir-riżoluzzjoni tal-IP tal-client hija mwebbsa kontra spoofing tal-forwarding headers.

• **Webhooks.** Webhooks inbound minn fornituri ta' pagamenti u email jiġu vverifikati kontra firem tal-fornitur fuq ir-request body mhux maħdum qabel ma jiġu pproċessati.

• **File uploads.** Uploads għandhom limitu ta' daqs, jiġu vvalidati, jinħażnu taħt identifikaturi ġġenerati aktar milli ismijiet mogħtija mill-utent, u jiġu limitati għal kull talba u għal kull organizzazzjoni.

• **Security headers.** Fil-produzzjoni, ir-risposti jġorru strict transport security, content-type u frame options, referrer policy, u permissions policy restrittiva, u jrażżnu server u framework banners.

8. Protezzjoni tad-Data

8.1 Encryption

Id-data kollha hija encrypted at rest bl-użu ta' AES-256 permezz tas-saffi tal-encryption tal-ħażna u tad-database tal-pjattaforma Azure. It-traffiku kollu tan-network jingħata esklussivament fuq HTTPS bl-użu ta' TLS 1.2 jew ogħla; HTTP plaintext jiġi redirected għal HTTPS f'kull tier. Fil-produzzjoni, l-API u l-portal web joħorġu strict transport security headers flimkien ma' sett ta' hardening headers, u jrażżnu banners tal-verżjoni tas-server u tal-framework.

8.2 Ġestjoni tas-Secrets

Secrets tal-applikazzjoni jinżammu f'vault ċentralizzat tas-secrets b'purge protection attivat u soft-delete window ta' disgħin jum. L-applikazzjonijiet jawtentikaw mar-riżorsi ta' Azure bl-użu ta' system-assigned managed identities aktar milli ċwievet ta' ħajja twila; pereżempju, il-ħażna privata għandha shared access keys diżattivati kompletament, għalhekk l-aċċess huwa possibbli biss permezz ta' identity-based role assignments scoped għar-riżorsa individwali. Il-politiki ta' aċċess għall-vault jagħtu lill-principals tal-applikazzjoni aċċess read-only biss għas-secrets speċifiċi li għandhom bżonn, skont il-prinċipju tal-least privilege.

8.3 Residenza tad-Data

Id-data kollha tal-klijenti u tal-kandidati tinħażen u tiġi pproċessata fi ħdan l-Unjoni Ewropea. Il-hosting tal-applikazzjoni, id-database, il-ħażna, il-cache, u s-secrets jinsabu f'West Europe, u l-ipproċessar tal-AI jaħdem f'reġjuni tal-UE. Il-fornitur tal-AI ma jużax id-data tal-klijenti biex iħarreġ il-mudelli tiegħu.

8.4 Il-Ħajja ta' Intervista Waħda

L-aktar mod ċar biex tifhem il-kontrolli tal-protezzjoni tad-data huwa li ssegwi intervista waħda mill-bidu sat-tmiem. Il-kunsens jinqabad u jiġi rreġistrat qabel ma jiġi pproċessat xejn. L-upload jiġi encrypted in transit. It-traskrizzjoni u l-analiżi jsiru ġewwa data centers tal-UE. Ir-riżultati jinkitbu f'ħażna encrypted. Kull rekord imbagħad jiġi rregolat minn arloġġ wieħed ta' retention li jispiċċa f'tħassir cascading irreġistrat. Fi kwalunkwe mument, drittijiet tal-kandidat bħall-irtirar, it-tħassir, l-aċċess, jew il-portabbiltà jistgħu jinterrompu dan il-fluss.

9. Privatezza by Design u GDPR

Il-privatezza hija mibnija fil-mudell tad-data u fil-workflow, mhux miżjuda biss permezz ta' politika.

9.1 Kunsens

L-ebda intervista ma tiġi rreġistrata jew analizzata mingħajr il-kunsens espliċitu tal-kandidat. Meta kandidat jiġi miżjud ma' reklutaġġ, il-pjattaforma toħroġ link tal-kunsens uniku ta' użu wieħed bl-email. Il-kandidat jirrevedi x'se jiġri u jew jaċċetta jew jirrifjuta. L-istat tal-kunsens, inkluż il-ħin tar-rispons, jiġi rreġistrat kontra dak ir-reklutaġġ speċifiku, sabiex il-kunsens dejjem ikun scoped għal proċess konkret ta' reklutaġġ aktar milli mogħti globalment.

Kunsens tal-kandidat: espliċitu u rreġistrat qabel kull ipproċessar

9.2 Retention u Erasure

Id-data retention hija konfigurabbli għal kull organizzazzjoni, b'default ta' tnax-il xahar u minimum konfigurabbli ta' tletin jum, u tista' tiġi override għal kull kandidat. Hemm arloġġ wieħed ta' retention għad-data ta' kandidat, mhux timer separat għal kull artifact. L-arloġġ jibda meta tiġi rreġistrata deċiżjoni ta' reklutaġġ. Qabel ma d-data tiskadi, il-pjattaforma tibgħat twissija (b'default madwar ħmistax-il jum qabel) u toffri estensjoni b'klik waħda. Meta d-data titħassar, titħassar bħala unità waħda: ir-rekord tal-kandidat, l-intervisti, it-traskrizzjonijiet, ir-reġistrazzjonijiet awdjo, id-dokumenti, u l-komparazzjonijiet jitneħħew kollha flimkien, u t-tħassir jiġi rreġistrat f'audit log. Ma hemm l-ebda residwu parzjali jew orphaned.

Iċ-ċiklu ta' ħajja hawn taħt juri dan l-arloġġ wieħed u kif jikkonverġi fuq tħassir cascading wieħed bi prova rreġistrata ta' erasure.

Żamma tad-data: arloġġ wieħed għal kull kandidat, tħassir ta' unità waħda

9.3 Drittijiet tas-Subject tad-Data u Sub-processors

Il-pjattaforma tappoġġja d-drittijiet tas-subject tad-data meħtieġa taħt il-GDPR, inklużi aċċess, tħassir, portabbiltà, oġġezzjoni, u spjegazzjoni. L-ipproċessar jitwettaq taħt data processing agreement li l-klijenti jaċċettaw fir-reġistrazzjoni u li huwa versioned għal kull organizzazzjoni. Is-sub-processors tagħna u r-rwoli tagħhom, kollha fi ħdan l-UE jew taħt safeguards xierqa, huma żvelati f'dak il-ftehim, u l-klijenti jirċievu avviż minn qabel ta' kwalunkwe bidla. It-Taqsima 17 fiha r-reġistru tas-sub-processors u

l-mappatura tal-konformità article-by-article.

10. AI Responsabbli u l-EU AI Act

Il-pjattaforma taqa' fil-kategorija high-risk tal-EU AI Act minħabba li tappoġġja deċiżjonijiet ta' impjieg, u aħna nittrattaw dik il-klassifikazzjoni bis-serjetà.

Ir-regola definittiva tal-prodott hija li **l-AI hija appoġġ għad-deċiżjonijiet, mhux min jieħu d-deċiżjoni.** Is-sistema qatt ma taċċetta jew tirrifjuta kandidat awtomatikament. Hija tittraskrivi d-diskors, tistruttura l-mistoqsijiet u t-tweġibiet, tagħti punteġġ lit-tweġibiet kontra kriterji li r-reklutatur iddefinixxa, u tabbozza feedback, u bniedem jirrevedi kull output qabel ma jintuża. Dan iżomm bniedem b'mod sod fil-loop.

Bl-istess importanza hemm dak li l-AI ma tagħmilx. Hija ma tevalwax il-personalità, "cultural fit," stat emozzjonali, ton tal-vuċi, aċċent, ġeneru, età, etniċità, dehra, jew body language. Il-punteġġar huwa ankrat mal-evidenza mit-traskrizzjoni u mal-kriterji definiti mir-reklutatur, u l-ismijiet tal-kandidati huma esklużi mill-input tal-evalwazzjoni biex jitnaqqas il-bias. Aħna nippubblikaw karta ta' trasparenza, dokumentazzjoni għall-utent, u dikjarazzjoni ta' konformità li tiddeskrivi s-sistema, il-limitazzjonijiet tagħha, u s-safeguards tagħha.

Kontroll ta' AI responsabbli	Kif jaħdem
Human in the loop	Kull punteġġ u kull biċċa feedback tiġi riveduta minn reklutatur qabel l-użu
L-ebda deċiżjoni awtomatizzata	Is-sistema qatt ma taċċetta jew tirrifjuta kandidat awtomatikament
Punteġġar ibbażat fuq evidenza	Il-punteġġi jirreferu għal evidenza ta' appoġġ mit-traskrizzjoni
Disinn anti-bias	L-ismijiet huma esklużi mill-evalwazzjoni; is-sustanza tiġi ppeżata aktar mill-istil
Limiti tal-ambitu	Il-personalità, l-emozzjoni, l-aċċent, u karatteristiċi protetti qatt ma jiġu evalwati
Sigurtà tal-feedback għall-kandidati	Feedback privat għall-kandidati jgħaddi minn guardrail ta' sigurtà ta' generation-and-validation

Dawn ir-restrizzjonijiet mhux biss huma ddikjarati fid-dokumentazzjoni; huma encoded fis-saff tal-prompts tal-AI u eżerċitati minn programm dedikat ta' testijiet ta' AI-safety deskritt fit-Taqsima 12.3.

11. Ċiklu ta’ Ħajja tal-Iżvilupp Sigur

Is-sigurtà hija infurzata fil-mod kif nibnu u nibgħatu s-software, mhux biss fis-sistema li tkun qed taħdem.

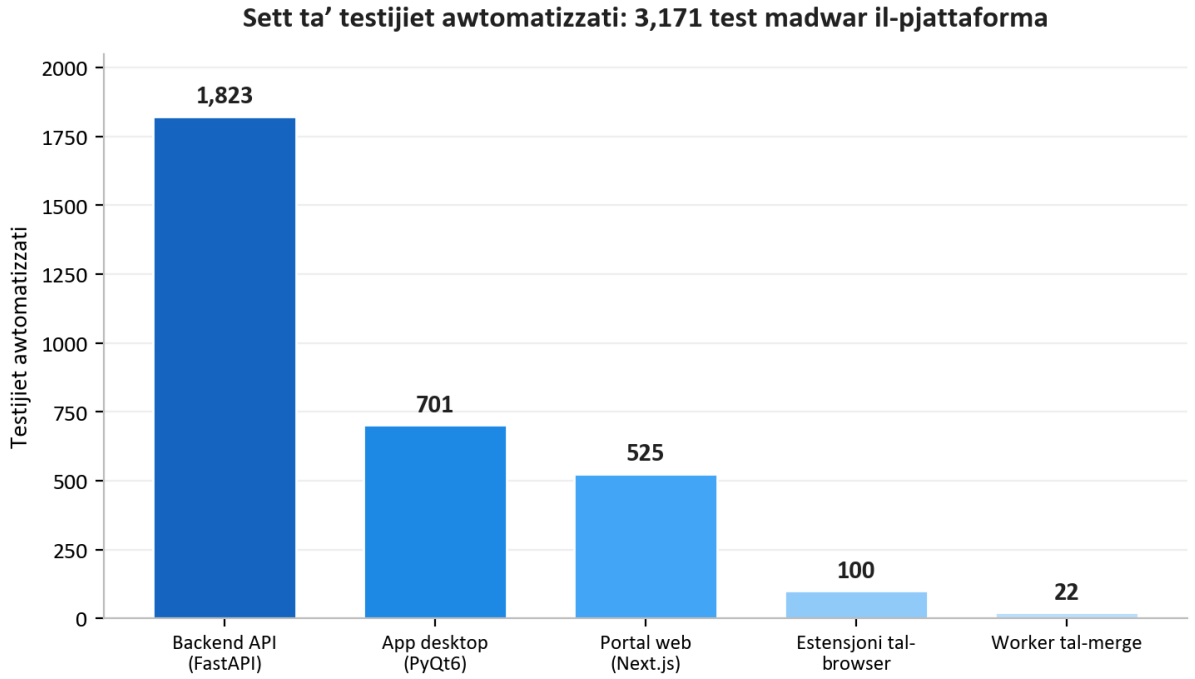
- **Separazzjoni tal-ambjenti.** L-iżvilupp u l-produzzjoni huma kompletament separati, kull wieħed bl-infrastruttura, storage accounts, database, secrets, u subdomains tiegħu stess. Ma hemm l-ebda stat maqsum.
- **Infrastructure as code.** L-ambjent kollu tal-cloud huwa definit bħala kodiċi u rivedut bħala kodiċi, u dan jagħmel il-pożizzjoni tas-sigurtà awditabbli u riproduċibbli. Reviżur jista’ jaqra eżattament liema ports huma miftuħa, liema riżorsi huma privati, u liema identitajiet għandhom liema permessi.
- **Deployments pinned u gated.** Kull pass fil-pipeline ta’ continuous integration huwa pinned għal verżjoni eżatta u immutabbli. Deployments tal-produzzjoni huma bbażati fuq tags, jitħaddmu biss permezz tal-pipeline protett tal-produzzjoni, u huma gated wara approvazzjoni meħtieġa. Is-suite ta’ test awtomatizzati taħdem bħala release gate: deployment ma jistax jintbagħat jekk it-testijiet ifallu.
- **Iġjene tad-dipendenzi.** Monitoraġġ awtomatizzat tad-dipendenzi jipproponi aġġornamenti kull ġimgħa madwar il-backend, desktop, web, infrastruttura, u d-definizzjonijiet tal-pipeline, u awditi tad-dipendenzi huma parti mir-reviżjoni perjodika tagħna tas-sigurtà.
- **Artifacts iffirmati.** Installers desktop huma code-signed, sabiex il-klijenti jkunu jistgħu jivverifikaw li s-software li jinstallaw ġej ġenwinament mingħandna.
- **Dixxiplina tas-secrets.** Is-secrets jgħixu fil-vault u f’pipeline secrets protetti, qatt fil-source code.

12. Ittestjar Kontinwu tas-Sigurtà

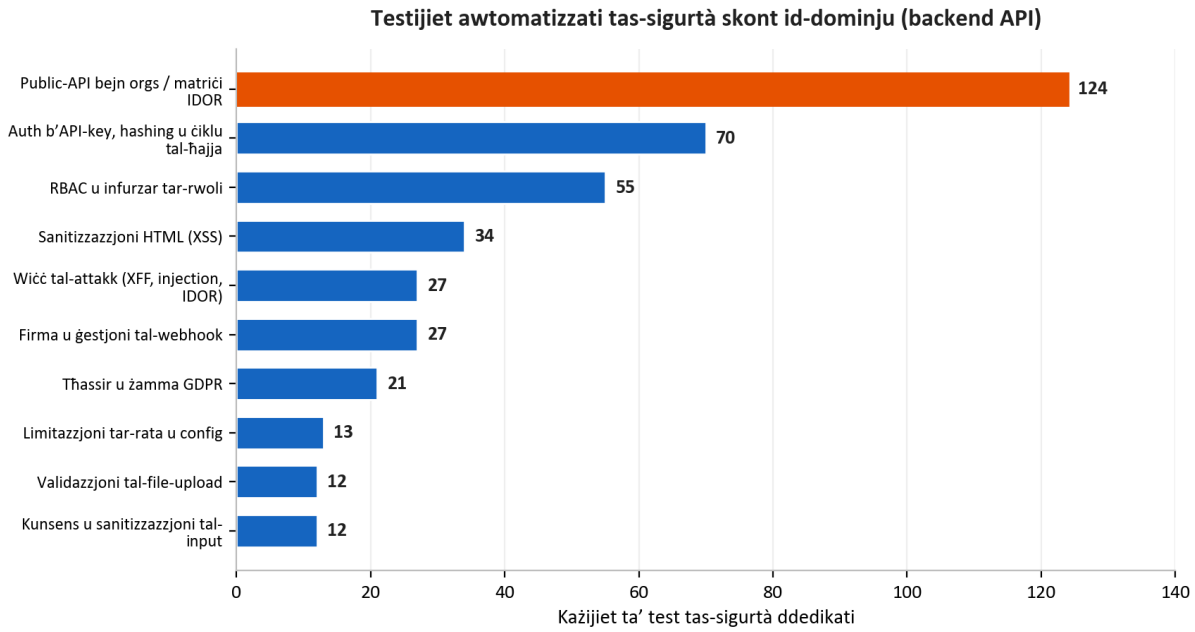
Dan huwa l-qalba tal-istorja tagħna tal-assigurazzjoni u l-parti li ħafna fornituri ma jistgħux juru. Aħna nittrattaw is-sigurtà bħala xi ħaġa li trid titkejjel kontinwament, b'checks eżegwibbli, aktar milli ddikjarata darba.

12.1 Is-Suite ta' Test Awtomatizzati

Il-pjattaforma hija koperta minn **3,171 test awtomatizzati** li jkopru l-API backend, l-applikazzjoni desktop, il-portal web, l-estensjoni tal-browser, u l-audio merge worker.



Dawn mhumiex biss testijiet funzjonali. Suite sostanzjali u dedikata tas-sigurtà teżerċita l-kontrolli deskritti aktar kmieni f'dan id-dokument. Il-grafika ta' hawn taħt taqsam it-testijiet speċifiċi tas-sigurtà fil-backend API skont id-dominju.



Fost ħafna oħrajn, din is-suite tinkludi matrix kbira tal-public-API li tħaddem kull endpoint bħala utent leġittimu, bħala l-API key proprja tal-organizzazzjoni, u bħala l-API key ta' organizzazzjoni rivali, billi tasserixxi li kull tentattiv bejn organizzazzjonijiet jiġi mblukkat. Tinkludi għexieren ta' testijiet avversarji tal-wiċċ ta' attakk għal forwarding-header spoofing, header injection, u tnixxija ta' identifikaturi, suite ffukata ta' HTML-sanitization għal cross-site scripting, testijiet ta' infurzar tar-rwoli għall-mudell sħiħ tar-rwoli, u testijiet li jippruvaw li d-data tal-kandidat titħassar ġenwinament bħala unità. Minħabba li dawn it-testijiet jaħdmu bħala release gate, regressjoni li ddgħajjef kwalunkwe wieħed minn dawn il-kontrolli twaqqaf ir-rilaxx aktar milli tasal għand il-klijenti.

12.2 Live Penetration Testing

Testijiet awtomatizzati tal-unità jippruvaw li l-kontrolli jġibu ruħhom b'mod korrett f'iżolament. Biex nippruvaw li jżommu flimkien f'deployment reali, aħna nżommu metodoloġija ripetibbli ta' penetration-testing li tħaddem scripts ta' attakk reali kontra ambjent live. Hija organizzata f'sitt fażijiet:

Fażi	Fokus	Eżempji ta' x'jiġi eżerċitat
1. Analiżi statika	Source code	Secrets, patterns ta' injection, funzjonijiet perikoluż, auth nieqsa, HTML mhux sigur
2. Reviżjoni tal-arkitettura	Infrastruttura	Endpoints privati, segmentazzjoni, TLS, konfigurazzjoni tas-secrets
3. Analiżi tal-vetturi ta' attakk	Source control u cloud	Protezzjoni tal-branch, ambitu tal-identità, espożizzjoni pubblika
4. Live penetration testing	Ambjent li qed jaħdem	Probing mhux awtentikat, aċċess cross-org, injection, token tampering, SSRF, bursts tar-rate-limit
5. Enterprise scoring	Maturità	Sittax-il kategorija ta' sigurtà skurjati kontra baseline tal-intrapriża
6. Dipendenzi u supply chain	Riskju ta' partijiet terzi	Awditjar ta' CVE tad-dipendenzi, pipeline actions pinned, integrità tal-lock-file

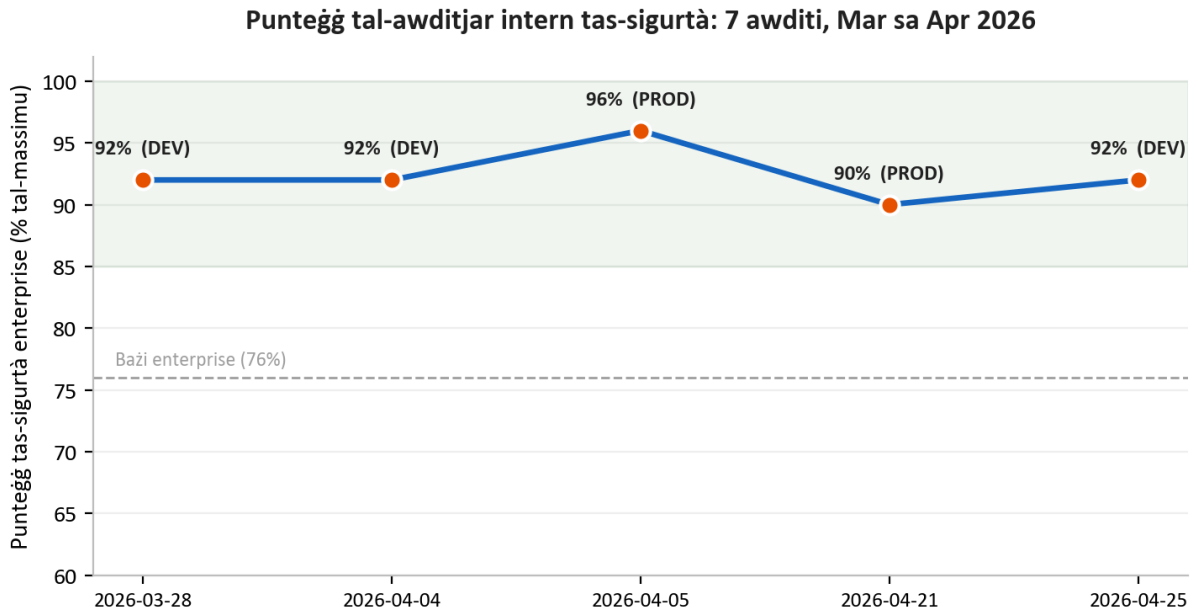
Il-Fażi 4 hija ttestjar avversarju ġenwin kontra sistema deployed, mhux checklist. Tittestja endpoints protetti mingħajr kredenzjali u tikkonferma li jirrifjutaw l-aċċess; tirreġistra żewġ organizzazzjonijiet u tipprova tilħaq ir-rekords ta' organizzazzjoni waħda bil-kont tal-oħra; tinjetta payloads ta' cross-site-scripting u server-side-template u tikkonferma li jiġu newtralizzati; timmodifika tokens tal-awtentikazzjoni u tikkonferma li jiġu miċħuda; tipprova server-side request forgery kontra cloud metadata endpoints; u tagħmel bursts fuq endpoints tal-awtentikazzjoni biex tikkonferma li r-rate limiting verament jattiva fl-ambjent live, mhux biss fit-teorija.

12.3 Ittestjar tas-Sigurtà tal-Feedback għall-Kandidati

Minħabba li l-pjattaforma tista' tiġġenera feedback privat ta' żvilupp għall-kandidati, inħaddmu programm separat ta' sigurtà avversarja kontra dik il-karatteristika. Huwa intenzjonalment jagħti lis-sistema noti ta' reklutaturi ħorox u ostili u jikkonferma li l-output li jħares lejn il-kandidat qatt ma fih vulgarità, qatt ma jiżvela jew jattribwixxi l-identità ta' reklutatur jew opinjoni privata tiegħu, u qatt ma japplika tikketti ta' personalità ġudikanti. Dan jipproteġi kemm lill-kandidat, li għandu jirċievi feedback kostruttiv u rispettabbli, kif ukoll lill-klijent, li qatt m'għandu jkollu opinjoni interna toħroġ 'il barra.

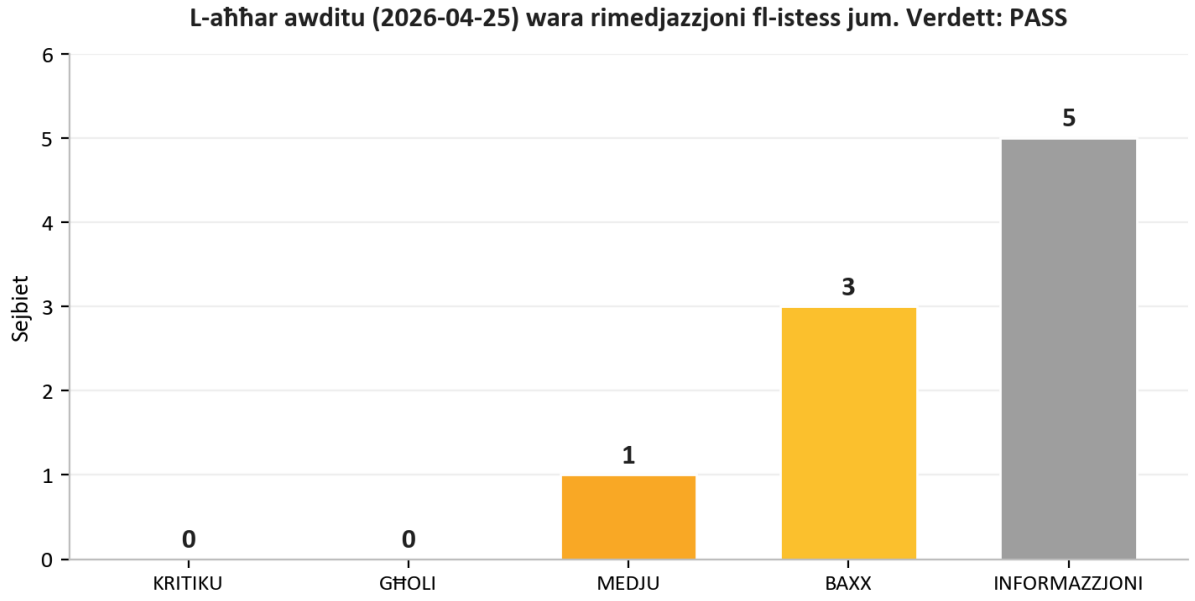
13. Riżultati tal-Awditi tas-Sigurtà

Aħna nwettqu awditi rikorrenti tas-sigurtà billi nużaw metodoloġija strutturata u ripetibbli ta' penetration-testing, u niktbu kull wieħed bħala rapport datat b'findings b'severità klassifikata, evidenza, u remediation. Dawn huma awditi interni mmexxija mill-proċess tagħna stess tas-sigurtà; ċertifikazzjoni formali minn parti terza tal-istess kontrolli tinsab fil-pjan direzzjonali tagħna. Bejn l-aħħar ta' March u l-aħħar ta' April 2026 lestejna **seven such audits** fuq l-iżvilupp u l-produzzjoni.



Ir-riżultat li jimpurta l-aktar għal klijent prospettiv huwa l-konsistenza: **madwar is-seba' awditi kollha kien hemm zero critical findings.** Fl-okkażjonijiet rari fejn feġġet kwistjoni b'severità ogħla, ġiet rimedjata malajr, ħafna drabi fl-istess ġurnata, u ġiet ivverifikata mill-ġdid. Ir-rubrika tal-iskoring ġiet intenzjonalment issikkata matul dan il-perjodu (il-punteġġ massimu possibbli ġie mgħolli hekk kif żidna aktar kategoriji biex nivvalutaw), u għalhekk il-linja tal-punteġġ normalizzat tibqa' għolja anki meta l-livell meħtieġ tela'.

L-aktar awditu reċenti tagħna, fil-25 April 2026, juri kif il-proċess jaħdem fil-prattika. Ġew identifikati żewġ kwistjonijiet b'severità ogħla, it-tnejn ġew iffissati u vverifikati mill-ġdid fl-istess ġurnata, u l-awditu ngħalaq b'verdett ta' **PASS** mingħajr issues exploit-ready li fadal fil-threat model attwali.



Awditu	Ambjent	Critical	Verdett
2026-03-28	Żvilupp	0	Lest għall-produzzjoni
2026-04-04	Żvilupp	0	Lest għall-intrapriża
2026-04-05	Produzzjoni	0	Lest għall-intrapriża
2026-04-20	Żvilupp	0	Lest għall-produzzjoni, noti
2026-04-20	Żvilupp	0	Pass b’noti
2026-04-21	Produzzjoni	0	Sikur, l-ebda finding sfruttabbli
2026-04-25	Żvilupp	0	Pass

Il-mudell tul dawn l-awditi huwa l-aktar evidenza onesta li nistgħu noffru: issues jinstabu, għax infittxuhom bis-serjetà, u jingħalqu malajr, għax il-proċess huwa mibni biex jagħlaqhom. Fornitur li qatt ma jirrapporta finding ġeneralment huwa fornitur li mhux qed ifittex.

14. Reżiljenza Operattiva u Responsabbiltà Kondiviża

14.1 Monitoraġġ u Logging

It-telemetrija tal-applikazzjoni u tal-pjattaforma tgħaddi għal workspace ċentralizzat ta' log analytics u servizz ta' application monitoring, li jagħtina viżibbiltà fuq id-disponibbiltà u l-imġiba. Azzjonijiet sensittivi bħat-tħassir tad-data, l-aċċettazzjoni ta' ftehimiet legali, u l-invokazzjonijiet tal-AI jiġu rreġistrati f'tabelli dedikati tal-awditjar, sabiex ikun hemm rekord durabbli ta' min għamel xiex lil data importanti.

14.2 Backup u Recovery

Id-database managed iżżomm backups awtomatizzati, u l-ħażna privata hija protetta b'soft-delete retention kemm fuq blobs kif ukoll fuq containers, sabiex tħassir aċċidentali jew malizzjuż ikun jista' jiġi rkuprat fi ħdan it-tieqa ta' retention. Infrastruttura kritika ġġorr deletion locks biex tipprevjeni teardown aċċidentali tar-riżorsi tal-produzzjoni.

14.3 Sommarju tar-Responsabbiltà Kondiviża

Qasam	AI Interview Analyzer	Klijent
Infrastruttura, network, patching	Iva	-
Sigurtà tal-applikazzjoni u pipeline tal-AI	Iva	-
Encryption, secrets, residenza tad-data	Iva	-
Amministrazzjoni tal-utenti u tar-rwoli	Tipprovdi l-kontrolli	Jimmaniġġja l-utenti u r-rwoli
Konfigurazzjoni tal-politika ta' retention	Tipprovdi l-kontrolli	Jissettja t-tieqa ta' retention
Kunsens tal-kandidat	Tipprovdi l-workflow	Tiżgura li jintuża
Kredenzjali b'saħħithom għall-utenti finali u SSO	Tappoġġja SSO u politika	Tinforza l-politika interna

15. Threat Model u Mappatura OWASP

Aħna niddisinjaw kontra sett konkret ta' avversarji: attakkant estern mingħajr kredenzjali, utent awtentikat kurjuż jew malizzjuż ta' organizzazzjoni waħda li jipprova jilħaq id-data ta' organizzazzjoni oħra, dipendenza kompromessa, u żball minn insider. It-tabella hawn taħt tgħaqqad il-kategoriji ta' riskju OWASP Top 10 użati b'mod wiesa' mal-kontrolli speċifiċi li jindirizzawhom f'din il-pjattaforma, li kull wieħed minnhom jiġi eżerċitat mit-testijiet deskritti fit-Taqsima 12.

Riskju OWASP	Kif il-pjattaforma timmitigah
Broken access control	Kontroll tal-aċċess ibbażat fuq ir-rwoli fuq kull endpoint privileġġjat; scoping għal kull organizzazzjoni; "not found" fuq aċċess cross-org; remapping tal-identifikaturi; matrix ta' testijiet cross-org
Cryptographic failures	TLS 1.2+ in transit; AES-256 at rest; hashing tal-passwords b'bcrypt; secrets f'vault managed
Injection	ORM-only parameterized queries; validazzjoni stretta tal-iskema; HTML sanitization fil-ħin tal-kitba
Insecure design	Defense in depth f'saffi; threat modeling u reviżjoni tal-arkitettura f'kull awditu
Security misconfiguration	Infrastructure as code; network groups default-deny; security headers; shared storage keys diżattivati; API schema mhux esposta fil-produzzjoni
Vulnerable components	Monitoraġġ awtomatizzat tad-dipendenzi kull ġimgħa; awditi ta' CVE tad-dipendenzi fir-reviżjoni perjodika
Identification and authentication failures	Tokens ta' ħajja qasira; login rate-limited; verifika tal-email; appoġġ għal SSO; l-ebda passwords f'plaintext
Software and data integrity failures	Passi tal-pipeline pinned u immutabbli; installers desktop iffirmati; verifika tal-firem tal-webhooks; deploys tal-produzzjoni gated bit-tags
Security logging and monitoring failures	Telemetrija ċentralizzata; tabelli dedikati tal-awditjar għal azzjonijiet sensittivi
Server-side request forgery	Sejħiet outbound ristretti għal endpoints fdati; probes ta' SSRF fil-harness ta' penetration-test

Din il-mappatura hija l-qafas ċentrali tal-argument tagħna tal-assigurazzjoni: għal kull klassi magħrufa ta' attakk hemm kontroll imsemmi, u għal kull kontroll imsemmi hemm test.

16. Ġestjoni tal-Vulnerabbiltajiet u Responsible Disclosure

Is-sigurtà qatt ma tkun lesta, għalhekk inħaddmu ċiklu kontinwu ta' skoperta u remediation.

- **Skoperta.** Il-vulnerabbiltajiet jidhru minn erba' sorsi: is-suite ta' test awtomatizzati, l-awditi rikorrenti ta' penetration-test, il-monitoraġġ awtomatizzat tad-dipendenzi, u rapporti minn klijenti jew riċerkaturi.
- **Triage.** Kull finding jingħata severità (critical, high, medium, low, jew informational) b'evidenza u sid ta' remediation, eżatt kif irreġistrat fir-rapporti tal-awditjar tagħna.
- **Miri tar-remediation.** Findings critical u high jiġu prijoritizzati għal remediation immedjata; fl-istorja tal-awditi tagħna, findings ta' severità ogħla tipikament ġew riżolti u vverifikati mill-ġdid fl-istess ġurnata. Findings medium u aktar baxxi jiġu skedati fil-kadenza regolari tal-manutenzjoni.
- **Verifika.** Il-fixes jerġgħu jiġu ttestjati, u fejn rilevanti ssir verifika live kontra l-ambjent deployed biex jiġi kkonfermat li l-issue hija ġenwinament magħluqa, mhux biss magħluqa fil-kodiċi.
- **Disclosure.** Tħassib dwar is-sigurtà jista' jiġi rrappurtat lilna direttament. Aħna nirrikonoxxu r-rapporti, ninvestigaw, u nżommu lir-rappurtatur informat sal-ħin tar-riżoluzzjoni.

17. Mappatura tal-Konformità

17.1 GDPR

Qasam GDPR	Implimentazzjoni tal-pjattaforma
Bażi legali (Art. 6)	Kunsens espliċitu tal-kandidat maqbud qabel l-ipproċessar
Minimizzazzjoni tad-data u limitazzjoni tal-ħażna (Art. 5)	Tiġi pproċessata biss data rilevanti għall-intervista; retention konfigurabbli b'tħassir awtomatiku
Dritt għall-erasure (Art. 17)	Tħassir ta' unità waħda tad-data kollha tal-kandidat, bi prova rreġistrata ta' erasure
Drittijiet tas-subject tad-data (Art. 15 sa 20)	Aċċess, tħassir, portabbiltà, u oġġezzjoni huma appoġġjati
Obbligi tal-processor (Art. 28)	Data processing agreement aċċettat fir-reġistrazzjoni u versioned għal kull organizzazzjoni
Sigurtà tal-ipproċessar (Art. 32)	Encryption, kontroll tal-aċċess, iżolament, u ttestjar kontinwu kif deskritt f'dan id-dokument
Trasparenza tas-sub-processor	Żvelata fid-data processing agreement b'avviż bil-quddiem dwar bidla

17.2 EU AI Act

Il-pjattaforma hija trattata bħala sistema AI high-risk li tappoġġja deċiżjonijiet ta' impjieg, u aħna nżommu dokumentazzjoni allinjata mar-regolament, inkluż karta ta' trasparenza, dokumentazzjoni għall-utent, u dikjarazzjoni ta' konformità. Is-safeguards ewlenin, is-sorveljanza umana, it-trasparenza, il-punteġġar ibbażat fuq l-evidenza, u l-limiti stretti tal-ambitu fuq dak li l-AI tevalwa, huma deskritti fit-Taqsima 10. Aħna nkomplu nimmaturaw id-dokumentazzjoni formali tagħna ta' konformità hekk kif it-timeline tal-implimentazzjoni tar-regolament tavvanza.

17.3 Ċertifikazzjonijiet tal-Hosting

Il-pjattaforma taħdem kompletament fuq Microsoft Azure, li d-data centers tiegħu għandhom ċertifikazzjonijiet indipendenti inklużi ISO 27001 u SOC 2. Dawn iċ-ċertifikazzjonijiet ikopru s-saffi fiżiċi u tal-pjattaforma taħt l-applikazzjoni tagħna; il-kontrolli fil-livell tal-applikazzjoni huma dawk deskritti tul dan id-dokument.

17.4 Reġistru tas-Sub-processor

Sub-processor	Għan	Reġjun
Microsoft Azure	Hosting, ipproċessar tal-AI u speech, ħażna, transactional email	EU (West Europe, Sweden Central)
Stripe	Abbonament u pproċessar tal-pagamenti	EU (Ireland)
Fakturownia	Fatturazzjoni	EU (Poland)
ATS connector (optional)	Integrazzjoni ta' applicant-tracking, attivata biss fuq talba	EU

18. Pjan Direzzjonali tas-Sigurtà

Aħna nittrattaw is-sigurtà bħala programm li qed jitjieb kontinwament. Inizjattivi attwali fil-pjan direzzjonali tagħna jinkludu t-tisħiħ tal-għażliet ta' multi-factor authentication għal kontijiet amministrattivi, l-espansjoni tal-audit logging ċentralizzat tal-aċċess għad-data, il-kontinwazzjoni tal-issikkar tar-reċenza tad-dipendenzi b'kadenza regolari, u l-progress taċ-ċertifikazzjoni formali minn parti terza tal-kontrolli deskritti f'dan id-dokument. L-ebda waħda minn dawn mhija lakuna li tesponi d-data tal-klijenti llum; kull waħda hija titjib għal pożizzjoni diġà f'saffi.

19. Sommarju

AI Interview Analyzer tipproteġi d-data tal-kandidati u tal-klijenti permezz ta' arkitettura f'saffi: network privat b'default mingħajr servizzi pubbliċi tad-data, identità b'saħħitha u iżolament għal kull organizzazzjoni, kodiċi tal-applikazzjoni li jelimina klassijiet sħaħ ta' vulnerabbiltà bid-disinn, encryption u residenza tad-data fl-UE, u kontrolli tal-privatezza mibnija fil-mudell tad-data. Dak li jiddistingwi l-pjattaforma huwa l-evidenza wara dawn id-dikjarazzjonijiet. Bi 3,171 test awtomatizzati, metodoloġija ripetibbli ta' live penetration-testing, programm dedikat ta' AI-safety, u rekord ta' seven internal security audits with zero critical findings, nistgħu nuru, mhux biss ngħidu, li l-pjattaforma hija sigura.

Appendiċi A: Katalogu tal-Kontrolli tas-Sigurtà

Referenza kkondensata tal-kontrolli primarji u l-evidenza li tappoġġja kull wieħed minnhom.

Kontroll	Mekkaniżmu	Evidenza
Encryption tat-trasport	HTTPS biss, TLS 1.2+, HTTP redirected	Infrastructure as code; awditu tal-arkitettura
Encryption at rest	AES-256 platform encryption fuq il-ħażna u d-database	Konfigurazzjoni tal-pjattaforma; awditu tal-arkitettura
Protezzjoni tal-password	bcrypt b'salt għal kull password	Source control; testijiet tal-awtentikazzjoni
Ġestjoni tas-sessjoni	Tokens iffirmati ta' 30 minuta, refresh revokabbli min-naħa tas-server	Source control; testijiet tal-awtentikazzjoni
Awtorizzazzjoni	Kontroll tal-aċċess b'erba' rwoli fuq endpoints privileġġjati	Suite ta' testijiet tal-infurzar tar-rwoli
Iżolament tat-tenant	Query scoping għal kull organizzazzjoni; 404 fuq cross-org	Matrix ta' testijiet bejn organizzazzjonijiet
Sigurtà tal-API key	Ħażna hashed, permessi scoped, limiti ta' rata għal kull ċavetta	Suite ta' testijiet tal-API key
Difiża kontra injection	ORM-only parameterized queries	Analiżi statika; testijiet ta' injection
Difiża kontra cross-site scripting	HTML sanitization fil-ħin tal-kitba	Suite ta' testijiet ta' HTML-sanitization
Rate limiting	Limiter durabbli appoġġjat mid-database fuq endpoints tal-auth	Testijiet tar-rate-limit; live burst checks
Integrità tal-webhook	Verifika tal-firma tal-fornitur fuq raw body	Suite ta' testijiet tal-webhook
Ġestjoni tas-secrets	Vault managed, purge protection, managed identity	Infrastructure as code; awditu tal-arkitettura
Iżolament tan-network	Endpoints privati; segmentazzjoni default-deny	Infrastructure as code; awditu tal-arkitettura
Tħassir tad-data	Tħassir cascading ta' unità waħda b'audit log	Suite ta' testijiet GDPR deletion
Supply chain	Passi tal-pipeline pinned; monitoraġġ tad-dipendenzi kull ġimgħa	Konfigurazzjoni tal-pipeline; awditu tad-dipendenzi

Appendiċi B: Mistoqsijiet Frekwenti għar-Reviżuri tas-Sigurtà

Fejn tinħażen id-data tagħna? Kompletament fi ħdan l-Unjoni Ewropea, fuq Microsoft Azure, f'West Europe bl-ipproċessar tal-AI f'reġjuni tal-UE. Id-data tal-kandidati qatt ma titlaq mill-UE.

Id-data tagħna tintuża biex tħarreġ mudelli tal-AI? Le. Il-fornitur tal-AI ma jużax id-data tal-klijenti għat-taħriġ.

Id-database tista' tintlaħaq mill-internet? Le. L-aċċess pubbliku tan-network huwa diżattivat u d-database tista' tintlaħaq biss permezz ta' endpoint privat ġewwa n-network virtwali.

Klijent wieħed jista' jara d-data ta' klijent ieħor? Le. Kull query hija scoped għall-organizzazzjoni ta' min qed isejjaħ, aċċess bejn organizzazzjonijiet jirritorna "not found," u matrix awtomatizzata tittestja kontinwament dan l-iżolament.

Kif jinħażnu l-passwords? Hashed b'bcrypt u salt uniku għal kull password. Single sign-on ma' Microsoft u Google huwa appoġġjat, f'liema każ ma tinħażen l-ebda password.

Tappoġġjaw single sign-on? Iva, permezz ta' Microsoft u Google OAuth.

Għal kemm żmien huma validi l-access tokens? Tletin minuta, imqabbda ma' sessjoni refresh revokabbli min-naħa tas-server li tiġi invalidata fil-logout.

Kif jiġi mmaniġġjat il-kunsens tal-kandidat? Kull kandidat jirċievi link tal-kunsens uniku ta' użu wieħed u għandu jaċċetta qabel kwalunkwe reġistrazzjoni jew analiżi. Il-kunsens jiġi rreġistrat kontra l-proċess speċifiku ta' reklutaġġ.

Kif titħassar id-data? Bħala unità waħda li tkopri r-rekord tal-kandidat, l-intervisti, it-traskrizzjonijiet, l-awdjo, id-dokumenti, u l-komparazzjonijiet, fuq skeda ta' retention konfigurabbli, bi prova rreġistrata ta' erasure. Il-kandidati jistgħu wkoll jitolbu tħassir direttament.

Għandkom data processing agreement? Iva, aċċettat fir-reġistrazzjoni u versioned għal kull organizzazzjoni, inkluż ir-reġistru tas-sub-processors.

L-AI tieħu deċiżjonijiet ta' reklutaġġ? Le. Hija tipprovdi appoġġ għad-deċiżjonijiet biss; bniedem jirrevedi kull output u jieħu d-deċiżjonijiet kollha.

Kif tippruvaw id-dikjarazzjonijiet tas-sigurtà tagħkom? Permezz ta' 3,171 test awtomatizzati inkluża suite dedikata tas-sigurtà, metodoloġija ripetibbli ta' penetration-testing f'sitt fażijiet imħaddma kontra ambjenti live, programm ta' testijiet ta' AI-safety, u rapporti rikorrenti ta' awditjar bil-miktub.

X'jiġri meta ssibu vulnerabbiltà? Tingħata severità b'evidenza u sid, tiġi rimedjata skont skeda ta' prijorità, tiġi vverifikata mill-ġdid inklużi verifiki live fejn rilevanti, u tiġi rreġistrata f'rapport ta' awditjar.

Nistgħu nwettqu penetration test tagħna stess? Valutazzjonijiet tas-sigurtà jistgħu jiġu organizzati permezz tar-rappreżentant tal-kont tiegħek taħt ambitu u skedar xierqa.

Appendiċi C: Glossarju

Terminu	Tifsira
AES-256	Standard qawwi ta' encryption simetriku użat biex jipproteġi data at rest
bcrypt	Funzjoni ta' password-hashing mibnija għal dak l-iskop b'salting għal kull password
Managed identity	Identità maħruġa mill-pjattaforma li tippermetti lil servizz jawtentika mingħajr ċwievet maħżuna
Private endpoint	Indirizz ta' network privat li jżomm servizz cloud barra mill-internet pubbliku
Network security group	Sett ta' regoli ta' allow u deny li jiffiltraw it-traffiku tan-network lejn subnet
RBAC	Kontroll tal-aċċess ibbażat fuq ir-rwoli, li jagħti permessi skont ir-rwol tal-utent
IDOR	Insecure direct object reference, difett ta' kontroll tal-aċċess li l-pjattaforma tiddefendi kontra
SSRF	Server-side request forgery, klassi ta' attakk ittestjata fil-penetration tests tagħna
Web application firewall	Kontroll fuq ix-xifer li jiffiltra traffiku web malizzjuż
Data processing agreement	Il-kuntratt li jirregola kif processor jimmaniġġja data personali f'isem controller

Appendiċi D: Kuntatt u Kontroll tad-Dokument

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Għal reviżjoni tas-sigurtà, kopja tad-data processing agreement tagħna, jew id-dokumentazzjoni tagħna ta' konformità mal-EU AI Act, jekk jogħġbok ikkuntattja lir-rappreżentant tal-kont tiegħek.

Dan id-dokument jiddeskrivi l-pożizzjoni tas-sigurtà tas-servizz AI Interview Analyzer fid-data tal-ġenerazzjoni murija fil-footer. Huwa pprovdut għal skopijiet ta' evalwazzjoni u ma jifformax parti minn ebda kuntratt. Impenji kuntrattwali speċifiċi dwar is-sigurtà huma stabbiliti fil-ftehim applikabbli u fid-data processing agreement.