Säkerhetsvitbok

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Säkerhetsvitbok

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

Målgrupp: Företagsteam för säkerhet, IT och inköp

Klassificering: Offentlig

1. Sammanfattning

AI Interview Analyzer är en företagsplattform för rekrytering som spelar in intervjuer med kandidatens uttryckliga samtycke, transkriberar och strukturerar dem samt tar fram evidensbaserat stöd för utvärdering till rekryterare. Eftersom plattformen hanterar kandidaters personuppgifter och stödjer rekryteringsprocesser behandlas säkerhet och integritet som primära designbegränsningar, inte som funktioner som lagts till i efterhand.

Denna vitbok beskriver i konkreta och verifierbara termer hur vi skyddar kund- och kandidatdata. Den är skriven för dem som granskar leverantörer: säkerhetsingenjörer, IT-administratörer, dataskyddsombud och inköp. Varje siffra i detta dokument hämtas direkt från våra egna tekniska system snarare än från marknadsföringsmaterial.

Det centrala budskapet är enkelt: **vi hävdar inte bara att plattformen är säker, vi testar kontinuerligt att den är det.** Vår kodbas innehåller **3,171 automatiserade tester**, inklusive en särskild säkerhetssvit som testar autentisering, auktorisering, isolering mellan organisationer, skydd mot injektioner och dataradering. Utöver detta kör vi ett repeterbart ramverk för penetrationstestning mot live-driftsättningar och tar fram skriftliga granskningsrapporter. Under sju interna säkerhetsrevisioner i mars och april 2026 registrerade vi **zero critical findings**, och vår senaste revision avslutades med bedömningen **PASS**. (Formell tredjepartscertifiering av dessa kontroller finns på vår roadmap; se avsnitt 18.)

Säkerhetsegenskap	Sammanfattning
Hosting	Microsoft Azure, endast EU-regioner
Nätverksmodell	Private endpoints, default-deny nätverkssegmentering, ingen publik databas
Kryptering	AES-256 i vila, TLS 1.2 eller högre under överföring
Identitet	Kortlivade signerade tokens, bcrypt-lösenordshashning, stöd för SSO
Åtkomstkontroll	Rollbaserad åtkomstkontroll med strikt isolering per organisation
Hemligheter	Centraliserat valv för hemligheter med åtkomst via managed identity
Integritet	Uttryckligt samtycke, konfigurerbar lagringstid, radering som en sammanhållen enhet
Ansvarsfull AI	Endast beslutsstöd, människa alltid i loopen
Säkerställande	3,171 automatiserade tester plus återkommande penetrationstester och revisioner

1.1 Så läser du detta dokument

Avsnitt 3 till 11 beskriver de kontroller som skyddar data: arkitektur, nätverk, identitet, applikation, dataskydd, integritet och den säkra utvecklingslivscykeln. Avsnitt 12 och 13 behandlar vårt utmärkande program för kontinuerlig testning och vår revisionshistorik. Avsnitt 14 till 17 täcker drift, hotmodellering, sårbarhetshantering och compliance-mappning. Bilagorna innehåller en kontrollkatalog, en FAQ för granskare och en ordlista som ett säkerhetsteam kan använda direkt under en bedömning.

2. Dokumentets omfattning och metod

2.1 Vad detta dokument omfattar

Denna vitbok omfattar säkerhetsarkitekturen och säkerhetspraxisen för tjänsten AI Interview Analyzer: hostingmiljön, nätverksdesignen, identitets- och åtkomsthanteringen, kontroller på applikationsnivå, dataskydd, integritet och regulatorisk anpassning, den säkra utvecklingslivscykeln samt vårt program för kontinuerlig säkerhetstestning.

2.2 Vad som gör det verifierbart

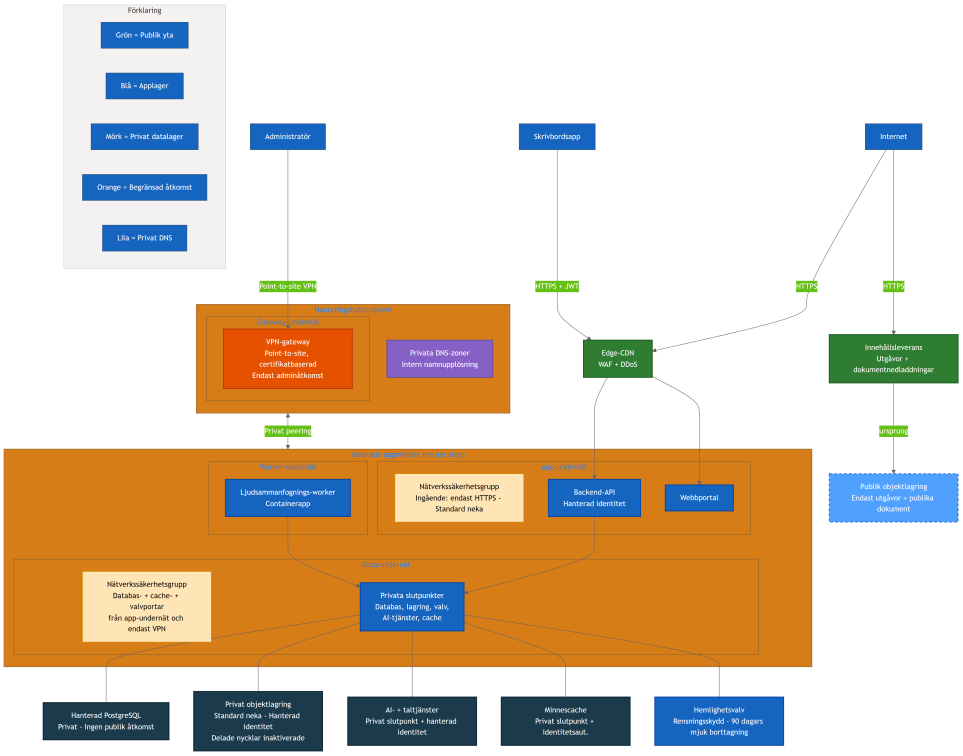
Det är enkelt att skriva leverantörers säkerhetspåståenden och svårt att lita på dem. Vi har därför kopplat varje större påstående i detta dokument till något konkret och mätbart i våra tekniska system: en kontroll som implementerats i kod, ett test som bevisar att kontrollen fungerar, en infrastrukturdefinition som upprätthåller den eller en revisionsrapport som dokumenterar en verifierad kontroll. När en kontroll är en del av vår framtida roadmap snarare än levererad idag säger vi det uttryckligen. Vi gör hellre underdrivna påståenden och blir betrodda än överdriver och blir påkomna.

2.3 Delat ansvar

Plattformen levereras som software as a service. Vi driver infrastrukturen, applikationen, AI-pipelinen och datahanteringen. Kunden ansvarar för att hantera sina egna användarkonton och roller, konfigurera lagringsperioder för data så att de matchar den interna policyn samt säkerställa att kandidatens samtycke inhämtas genom det samtyckesflöde som plattformen tillhandahåller. Avsnitt 14 beskriver denna ansvarsfördelning mer i detalj.

3. Översikt över säkerhetsarkitekturen

Plattformen är byggd som ett litet antal samverkande tjänster snarare än en enda monolit. En desktopapplikation och en webbportal fungerar som klienter. Ett centralt backend API äger all persistens, autentisering, fakturering, AI-pipelinen, samtycke, e-post, filhantering och dashboards. En worker för ljudsammanfogning bearbetar inspelningar asynkront. Allt känsligt tillstånd ligger bakom backend API; klienter kommunicerar aldrig direkt med databasen, lagringen eller AI-tjänsterna.



Diagrammet ovan visar produktionstopologin med resursnamn avsiktligt generaliserade. Tre principer är synliga i det:

- **Ingen direkt exponering av datatjänster.** Databasen, privat objektlagring, AI-tjänster och cache har publik nätverksåtkomst inaktiverad och är endast nåbara via private endpoints inom ett isolerat virtuellt nätverk. Valvet för hemligheter nås av applikationen via en private endpoint och skyddas dessutom av autentisering med plattformsidentitet och åtkomstpolicyer med minsta privilegium, så all åtkomst kräver en giltig, auktoriserad identitet oavsett nätverkssökväg.
- **En separerad publik yta.** Den enda publika objektlagringen innehåller versionsnedladdningar och offentliga dokument. Den innehåller aldrig kandidatdata. Kundvänd applikationstrafik passerar genom ett edge-lager som tillhandahåller web application firewall, skydd mot distributed-denial-of-service och innehållsleverans.
- **Administrativ åtkomst är styrd.** Operatörer når interna resurser endast genom en certifikatbaserad point-to-site VPN till ett administrationshubnätverk, inte via det publika internet.

Varje driftsättningssteg (utveckling och produktion) är en fullt isolerad miljö med eget nätverk, egna lagringskonton, egen databas och egna hemligheter. Kunders produktionsdata finns aldrig i lägre miljöer. En delad administrationshub innehåller endast VPN-gatewayen och privat DNS, privat peered till varje miljö.

4. Defense in Depth

Ingen enskild kontroll anses kunna stoppa varje attack. Plattformen använder lager av oberoende kontroller så att fel i ett lager inte exponerar data. Lagren nedan är vart och ett implementerade och, som beskrivs i avsnitt 12, individuellt testade.

Lager	Representativa kontroller
Nätverkskant	Endast TLS-transport, edge WAF och DDoS-skydd, private endpoints, default-deny-segmentering
Identitet och åtkomst	Kortlivade signerade tokens, bcrypt-hashning, rollbaserad åtkomstkontroll, isolering per organisation
Applikation	Schemavalidering på all indata, endast ORM-baserad dataåtkomst, output-kodning, rate limiting
Dataskydd	Kryptering i vila, valv för hemligheter med managed identity, EU-datalokalisering, behandling styrd av samtycke
Styrning och integritet	Konfigurerbar lagringstid, radering som en sammanhållen enhet, human-in-the-loop AI, audit-loggning
Kontinuerligt säkerställande	Automatiserad testsvit, repeterbara penetrationstester, återkommande interna säkerhetsrevisioner

Resten av detta dokument går igenom varje lager i tur och ordning och beskriver därefter hur vi kontinuerligt bevisar att lagren håller.

5. Nätverkssäkerhet

5.1 Privat som standard

Dataskiktet är privat genom konstruktion. Den hanterade PostgreSQL-databasen har publik nätverksåtkomst inaktiverad och är endast nåbar via en private endpoint. Privat objektlagring är konfigurerad för att neka nätverksåtkomst som standard, har shared access keys helt inaktiverade och är endast åtkomlig via managed identity från applikationssubnätet. Cache, AI-tjänster och valvet för hemligheter nås på motsvarande sätt via private endpoints med privat DNS-upplösning.

I praktiken innebär detta att det inte finns någon internetexponerad anslutningssträng till databasen och ingen publik lagrings-URL för kandidatljud: databasen och den privata lagringen har publik nätverksåtkomst direkt avstängd. Valvet för hemligheter nås av applikationen via en private endpoint och skyddas av autentisering med plattformsidentitet och åtkomstpolicyer med minsta privilegium, där applikationsidentiteter endast får läsåtkomst till de hemligheter de behöver, så hemligheter kan inte hämtas utan en giltig, auktoriserad identitet. Angreppsytan som en extern angripare överhuvudtaget kan nå är begränsad till applikationens HTTPS-endpoints bakom edge-lagret.

5.2 Nätverkssegmentering

Varje miljö är uppdelad i separata subnät för applikationsskiktet, dataskiktet och den asynkrona workern. Varje subnät styrs av en network security group vars sista regel nekar all inkommande trafik. Applikationssubnätet accepterar endast inkommande HTTPS. Datasubnätet accepterar endast de specifika portar som används för databas, cache och vault, och endast från applikationssubnätet eller den administrativa VPN. Detta innebär att även en angripare som på något sätt nådde applikationsskiktet inte fritt kan pivotera till dataskiktet; de enda tillåtna vägarna är de som applikationen legitimt använder.

5.3 Edge-lagret

Publik applikationstrafik frontas av ett edge-lager som tillhandahåller web application firewall, DDoS-skydd och ett content delivery network. Nedladdningar av versioner och dokument levereras från ett dedikerat publikt lagringskonto genom en front door för innehållsleverans, helt separat från den privata lagring som innehåller kandidatdata. De två lagringsplanen blandas aldrig: en felkonfiguration i den publika planen kan inte exponera privata kandidatdata, eftersom det är olika konton med olika nätverksregler.

5.4 Administrativ åtkomst

Det finns ingen publik administrativ endpoint in i det privata nätverket. Operatörer ansluter via en point-to-site VPN-gateway som använder certifikatbaserad autentisering. Administrativ åtkomst till databas och cache är endast möjlig inifrån den tunneln, eftersom dessa tjänster har publik nätverksåtkomst inaktiverad. Detta håller den dagliga driften helt borta från det publika internet.

6. Identitets- och åtkomsthantering

6.1 Autentisering

Användarsessioner etableras med en signerad access token som är giltig i trettio minuter, tillsammans med en separat, opak refresh token på serversidan. Access tokens verifieras vid varje förfrågan, och användaren valideras på nytt mot databasen (inklusive kontroll av aktivt konto) i stället för att litas på enbart utifrån tokeninnehållet. Utloggning återkallar omedelbart refresh-sessionen på serversidan, så en stulen refresh token kan inte överleva en utloggning.

Lösenord lagras aldrig i klartext. De hashas med bcrypt med ett unikt salt per lösenord. För organisationer som föredrar single sign-on stöder plattformen OAuth-inloggning med Microsoft och Google, i vilket fall inget lösenord alls lagras.

Ägandeskap till e-postadresser verifieras genom en engångslänk för verifiering med begränsad giltighetstid innan ett självregistrerat konto behandlas som verifierat, och omsändningar av verifieringsmejl är rate limited för att förhindra missbruk.

6.2 Rollbaserad åtkomstkontroll

Auktorisering upprätthålls genom en rollmodell med fyra roller med ökande privilegier: intervjuare, rekryterande chef, rekryterare och administratör. Åtkomst till privilegierade operationer upprätthålls av beroenden på serversidan som kontrollerar både rollen och den anropandes verifieringsstatus. Dessa rollkontroller skyddar långt över hundra olika API-operationer.

Roll	Typiska behörigheter
Intervjuare	Genomför tilldelade intervjuer; ser endast intervjuer som är tilldelade dem
Rekryterande chef	Hanterar rekryteringar som de äger eller är medlem i
Rekryterare	Full hantering av rekrytering och kandidater inom organisationen
Administratör	Organisationsinställningar, fakturering, administration av användare och API-nycklar

Utöver grova rollkontroller tillämpar plattformen regler för synlighet på datanivå. Rekryterande chefer ser endast de rekryteringar som de skapat eller är medlem i; intervjuare ser endast de intervjuer som tilldelats dem. Privilegier upprätthålls därför både på nivån ”vilken åtgärd” och på nivån ”vilka poster”.

6.3 Isolering per organisation

Plattformen är multi-tenant, och tenant-isolering behandlas som en säkerhetskontroll av första klass. Varje autentiserad identitet bär ett organisations-ID, och datafrågor avgränsas till den organisationen. När en användare begär en post som tillhör en annan organisation returnerar plattformen svaret ”not found” i stället för att avslöja att posten existerar. Interna databasidentifierare exponeras aldrig över nätet; API:et presenterar visningsidentifierare och mappar om dem per förfrågan, vilket eliminerar en vanlig klass av uppräkningattacker mellan tenants.

Detta är inte bara en designavsikt. Som beskrivs i avsnitt 12 kör vår automatiserade svit en stor matris mellan organisationer som försöker nå en organisations data med en annan organisations inloggningsuppgifter och verifierar att varje sådant försök misslyckas.

6.4 Programmatisk åtkomst

För integrationer kan organisationer på berättigade planer utfärda API-nycklar. Nycklar använder ett igenkännbart prefix, innehåller 128 bits entropi och lagras endast som en hash; den råa nyckeln visas en gång vid skapandet och aldrig igen. Varje nyckel har ett uttryckligt behörighetsomfång (read, write eller ATS integration), kan begränsas till specifika källnätverk, kan återkallas omedelbart och omfattas av rate limits per nyckel som härleds från organisationens plannivå. Nyckelverifiering använder en timing-safe-jämförelse för att undvika informationsläckage genom svarstider.

7. Applikationssäkerhet

Applikationen är skriven för att eliminera hela kategorier av sårbarheter snarare än att åtgärda dem från fall till fall.

- **Injektion.** All databasåtkomst går via en object-relational mapper med parameteriserade frågor. Kodbasen innehåller ingen rå strängformatterad SQL. Detta eliminerar strukturellt SQL injection.
- **Indatavalidering.** Varje request body valideras mot ett strikt schema innan den når affärslogik. Överdimensionerade payloads avvisas, och list-endpoints är paginerade för att begränsa resursanvändningen.
- **Output-kodning och cross-site scripting.** Text som tillhandahålls av användare och genereras av AI behandlas som opålitlig. Där innehåll måste renderas som HTML passerar det genom en sanitizer baserad på allow-list vid skrivning, och en dedikerad testsvit bekräftar att script-taggar, event handlers och javascript URLs tas bort.
- **Mass assignment.** Uppdateringsoperationer använder explicita scheman som utesluter privilegierade fält såsom roll, organisation och kreditbalans, så att en klient inte kan eskalera privilegier genom att posta extra fält.
- **Rate limiting.** Endpoints för autentisering och sådana som är känsliga för missbruk är rate limited med en robust limiter som backas av databasen, överlever omstarter och fungerar korrekt över flera applikationsinstanser. Inloggning, registrering, lösenordsåterställning och omsändning av verifiering har var och en sina egna gränser. Upplösning av klient-IP är härdad mot spoofing av vidarebefordringsheaders.
- **Webhooks.** Inkommande webhooks från betalnings- och e-postleverantörer verifieras mot leverantörssignaturer på den råa request body innan de behandlas.
- **Filuppladdningar.** Uppladdningar är storleksbegränsade, valideras, lagras under genererade identifierare i stället för användartillhandahållna namn och begränsas per request och per organisation.
- **Säkerhetsheaders.** I produktion innehåller svar strict transport security, content-type- och frame-alternativ, en referrer policy och en restriktiv permissions policy, och undertrycker server- och ramverksbanners.

8. Dataskydd

8.1 Kryptering

All data är krypterad i vila med AES-256 via Azure-plattformens krypteringslager för lagring och databaser. All nätverkstrafik levereras uteslutande över HTTPS med TLS 1.2 eller högre; klartext-HTTP omdirigeras till HTTPS i varje lager. I produktion skickar API:et och webbportalen strict transport security headers tillsammans med en uppsättning härdningsheaders och undertrycker server- och ramverksversionsbanners.

8.2 Hantering av hemligheter

Applikationshemligheter lagras i ett centraliserat valv för hemligheter med purge protection aktiverat och ett soft-delete-fönster på nittio dagar. Applikationer autentiserar till Azure-resurser med system-assigned managed identities i stället för långlivade nycklar; privat lagring har till exempel shared access keys helt inaktiverade, så åtkomst är endast möjlig genom identitetsbaserade rolltilldelningar avgränsade till den enskilda resursen. Vault access policies ger applikationsprincipaler läsåtkomst enbart till de specifika hemligheter de behöver, i enlighet med principen om minsta privilegium.

8.3 Datalokalisering

All kund- och kandidatdata lagras och behandlas inom Europeiska unionen. Applikationshosting, databasen, lagring, cache och hemligheter finns i West Europe, och AI-bearbetning körs i EU-regioner. AI-leverantören använder inte kunddata för att träna sina modeller.

8.4 Livscykeln för en enskild intervju

Det tydligaste sättet att förstå dataskyddskontrollerna är att följa en intervju från början till slut. Samtycke inhämtas och registreras innan något behandlas. Uppladdningen krypteras under överföring. Transkribering och analys körs inom EU-datacenter. Resultat skrivs till krypterad lagring. Varje post styrs därefter av en gemensam lagringsklocka som avslutas med en loggad, kaskaderande radering. När som helst kan kandidaträttigheter såsom återkallelse, radering, åtkomst eller portabilitet avbryta detta flöde.

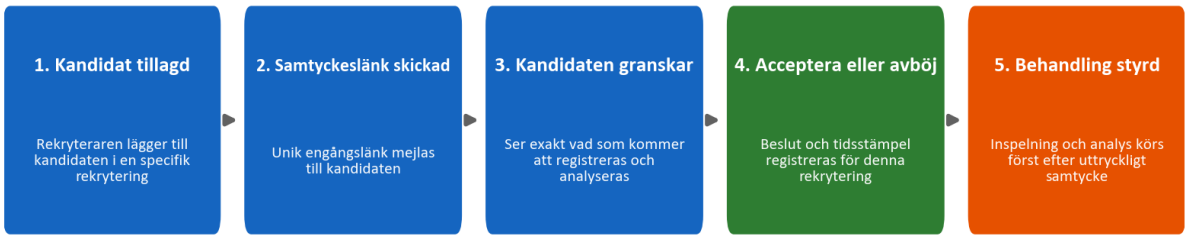
9. Integritet genom design och GDPR

Integritet är inbyggd i datamodellen och arbetsflödet, inte påklistrad enbart genom policy.

9.1 Samtycke

Ingen intervju spelas in eller analyseras utan kandidatens uttryckliga samtycke. När en kandidat läggs till i en rekrytering skickar plattformen en unik samtyckeslänk för engångsanvändning via e-post. Kandidaten granskar vad som kommer att hända och accepterar eller avböjer. Samtyckesstatus, inklusive tidpunkten för svaret, registreras mot just den rekryteringen, så samtycke är alltid avgränsat till en konkret rekryteringsprocess i stället för att ges globalt.

Kandidatsamtycke: uttryckligt och registrerat före all behandling



9.2 Lagringstid och radering

Lagringstiden för data är konfigurerbar per organisation, med en standard på tolv månader och ett konfigurerbart minimum på trettio dagar, och kan åsidosättas per kandidat. Det finns en enda lagringsklocka för en kandidats data, inte en separat timer per artefakt. Klockan startar när ett rekryteringsbeslut registreras. Innan data löper ut skickar plattformen en varning (som standard cirka femton dagar i förväg) och erbjuder en förlängning med ett klick. När data raderas raderas de som en sammanhållen enhet: kandidatposten, intervjuer, transkriptioner, ljudinspelningar, dokument och jämförelser tas bort tillsammans, och raderingen registreras i en audit-logg. Det finns inga partiella eller föräldralösa rester.

Livscykeln nedan visar denna enda klocka och hur den leder till en kaskaderande radering med ett loggat bevis på radering.

Datalagringstid: en klocka per kandidat, radering per enhet

9.3 Rättigheter för registrerade och underbiträden

Plattformen stödjer de rättigheter för registrerade som krävs enligt GDPR, inklusive åtkomst, radering, portabilitet, invändning och förklaring. Behandlingen utförs enligt ett personuppgiftsbiträdesavtal som kunder accepterar vid registrering och som versionshanteras per organisation. Våra underbiträden och deras roller, alla inom EU eller under lämpliga skyddsåtgärder, redovisas i det avtalet, och kunder får förhandsbesked om varje förändring. Avsnitt 17 innehåller registret över underbiträden

och compliance-mappningen artikel för artikel.

10. Ansvarsfull AI och EU AI Act

Plattformen faller inom högriskkategorin enligt EU AI Act eftersom den stödjer anställningsbeslut, och vi tar denna klassificering på stort allvar.

Den definierande regeln för produkten är att **AI:n är beslutsstöd, inte en beslutsfattare.** Systemet accepterar eller avvisar aldrig automatiskt en kandidat. Det transkriberar tal, strukturerar frågor och svar, poängsätter svar mot kriterier som rekryteraren har definierat och utarbetar återkoppling, och en människa granskar varje output innan den används. Detta håller en människa fast i loopen.

Lika viktigt är vad AI:n inte gör. Den utvärderar inte personlighet, ”kulturell passform”, känslotillstånd, tonfall, accent, kön, ålder, etnicitet, utseende eller kroppsspråk. Poängsättning förankras i evidens från transkriptet och i kriterier definierade av rekryteraren, och kandidatnamn utesluts från utvärderingsindatan för att minska bias. Vi publicerar ett transparenskort, användardokumentation och en försäkran om överensstämmelse som beskriver systemet, dess begränsningar och dess skyddsåtgärder.

Kontroll för ansvarsfull AI	Hur den fungerar
Människa i loopen	Varje poäng och varje återkopplingsdel granskas av en rekryterare innan användning
Inga automatiserade beslut	Systemet accepterar eller avvisar aldrig automatiskt en kandidat
Evidensbaserad poängsättning	Poäng hänvisar till stödjande evidens från transkriptet
Design mot bias	Namn utesluts från utvärdering; innehåll poängsätts före stil
Omfångsbegränsningar	Personlighet, känslor, accent och skyddade egenskaper bedöms aldrig
Säkerhet för kandidatåterkoppling	Privat kandidatåterkoppling passerar ett säkerhetsräcke för generering och validering

Dessa begränsningar anges inte bara i dokumentation; de är kodade i AI-promptlagret och testas av ett dedikerat AI-säkerhetsprogram som beskrivs i avsnitt 12.3.

11. Säker utvecklingslivscykel

Säkerhet upprätthålls i hur vi bygger och levererar programvara, inte bara i det körande systemet.

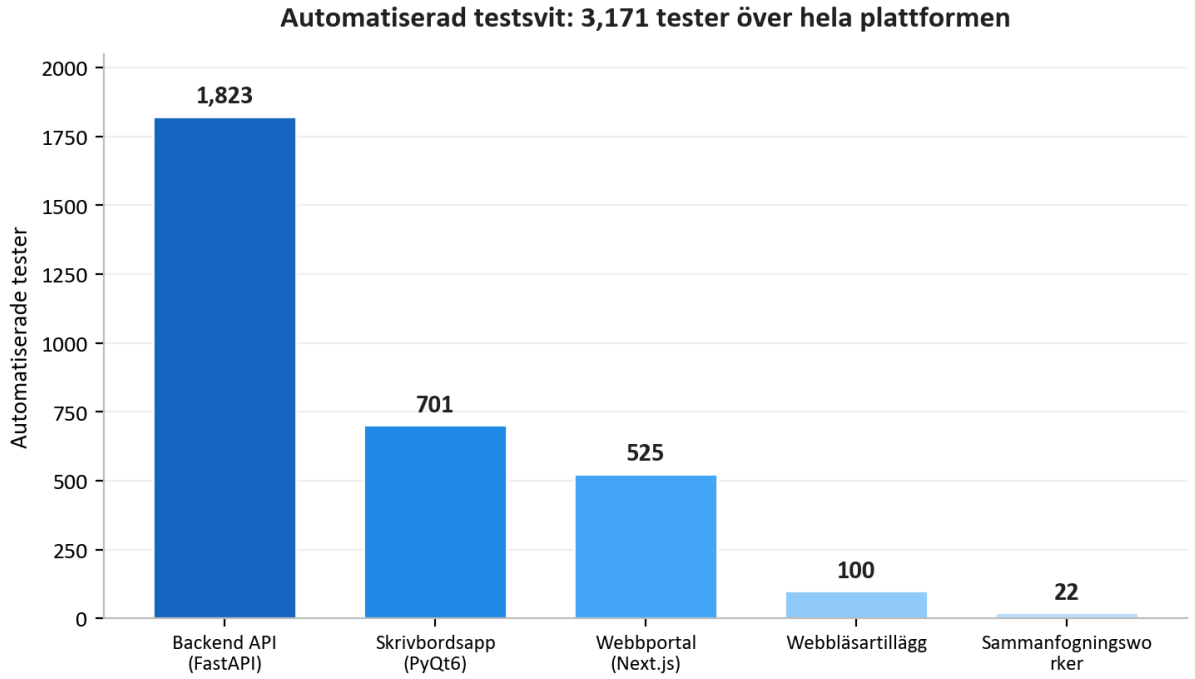
- **Miljöseparering.** Utveckling och produktion är fullt separerade, var och en med egen infrastruktur, egna lagringskonton, egen databas, egna hemligheter och egna subdomäner. Det finns inget delat tillstånd.
- **Infrastruktur som kod.** Hela molnmiljön definieras som kod och granskas som kod, vilket gör säkerhetshållningen granskningsbar och reproducerbar. En granskare kan läsa exakt vilka portar som är öppna, vilka resurser som är privata och vilka identiteter som har vilka behörigheter.
- **Pinnade, styrda driftsättningar.** Varje steg i continuous-integration-pipelinen är pinnat till en exakt, oföränderlig version. Produktionsdriftsättningar är tag-baserade, körs endast genom den skyddade produktionspipelinen och är styrda av obligatoriskt godkännande. Den automatiserade testsviten körs som en release gate: en driftsättning kan inte levereras om tester misslyckas.
- **Beroendehygien.** Automatiserad övervakning av beroenden föreslår uppdateringar veckovis över backend, desktop, webb, infrastruktur och pipelinedefinitioner, och revisioner av beroenden ingår i vår periodiska säkerhetsgranskning.
- **Signerade artefakter.** Desktopinstallationsprogram är kodsignerade, så kunder kan verifiera att programvaran de installerar faktiskt kommer från oss.
- **Disciplin för hemligheter.** Hemligheter finns i vault och i skyddade pipeline-hemligheter, aldrig i källkod.

12. Kontinuerlig säkerhetstestning

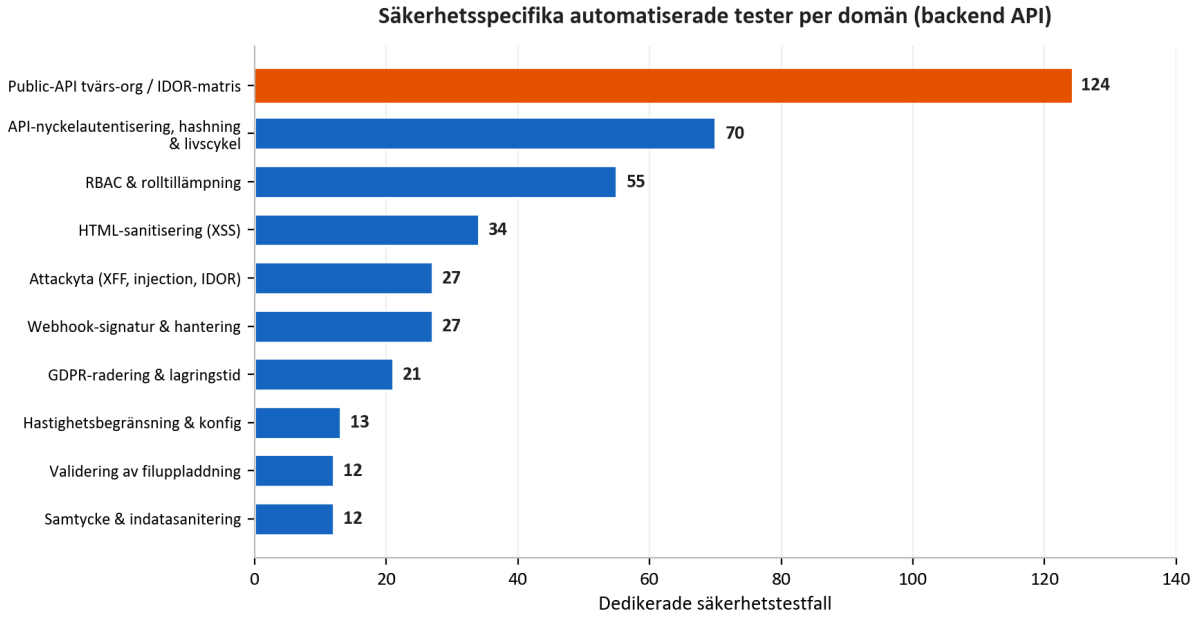
Detta är kärnan i vår säkerhetsförsäkran och den del som de flesta leverantörer inte kan visa. Vi behandlar säkerhet som något som ska mätas kontinuerligt, med körbara kontroller, snarare än något som påstås en gång.

12.1 Den automatiserade testsviten

Plattformen täcks av **3,171 automatiserade tester** som omfattar backend API, desktopapplikationen, webbportalen, browser extension och workern för ljudsammanfogning.



Detta är inte bara funktionella tester. En omfattande, dedikerad säkerhetssvit testar de kontroller som beskrivits tidigare i detta dokument. Diagrammet nedan bryter ned de säkerhetsspecifika testerna i backend API efter domän.



Bland mycket annat innehåller denna svit en stor matris för publika API:er som kör varje endpoint som en legitim användare, som organisationens egen API-nyckel och som en rivaliserande organisations API-nyckel, och verifierar att varje försök mellan organisationer blockeras. Den innehåller dussintals adversariella tester av angreppsytan för spoofing av forwarding headers, header injection och läckage av identifierare, en fokuserad HTML-sanitiseringssvit för cross-site scripting, tester av rolltillämpning för hela rollmodellen och tester som bevisar att kandidatdata verkligen raderas som en sammanhållen enhet. Eftersom dessa tester körs som en release gate skulle en regression som försvagade någon av dessa kontroller stoppa releasen i stället för att nå kunder.

12.2 Live-penetrationstestning

Automatiserade enhetstester bevisar att kontroller beter sig korrekt isolerat. För att bevisa att de håller ihop i en verklig driftsättning upprätthåller vi en repeterbar metod för penetrationstestning som kör verkliga attackskript mot en live-miljö. Den är organiserad i sex faser:

Fas	Fokus	Exempel på vad som testas
1. Statisk analys	Källkod	Hemligheter, injektionsmönster, farliga funktioner, saknad auth, osäker HTML
2. Arkitekturgranskning	Infrastruktur	Private endpoints, segmentering, TLS, konfiguration av hemligheter
3. Analys av attackvektorer	Källkodshantering och moln	Branch protection, identitetsomfång, publik exponering
4. Live-penetrationstestning	Körande miljö	Probing utan autentisering, åtkomst mellan organisationer, injektion, token manipulation, SSRF, bursts mot rate limits
5. Företagspoängsättning	Mognad	Sexton säkerhetskategorier poängsatta mot en företagsbaslinje
6. Beroenden och försörjningskedja	Risk från tredje part	Dependency CVE audit, pinnade pipeline actions, lock-file-integritet

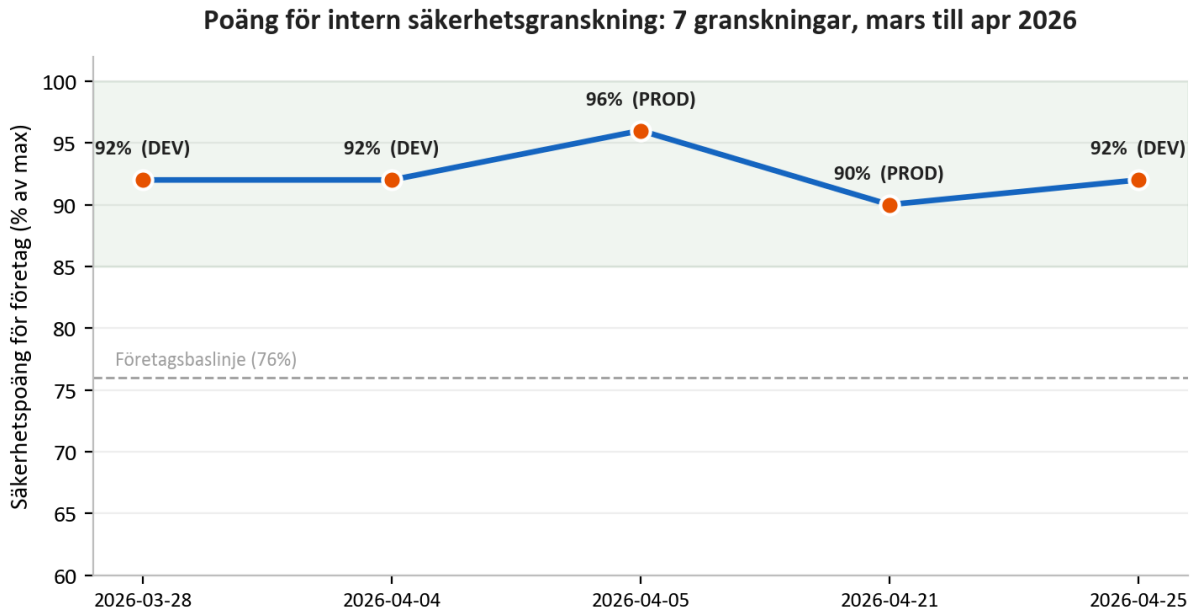
Fas 4 är verklig adversariell testning mot ett driftsatt system, inte en checklista. Den sonderar skyddade endpoints utan autentiseringsuppgifter och bekräftar att de nekar åtkomst; den registrerar två organisationer och försöker nå den ena organisationens poster med den andras konto; den injicerar payloads för cross-site scripting och server-side-template och bekräftar att de neutraliseras; den manipulerar autentiseringstokens och bekräftar att de avvisas; den försöker server-side request forgery mot molnmetadata-endpoints; och den överbelastar autentiseringsendpoints för att bekräfta att rate limiting faktiskt triggas i live-miljön, inte bara i teorin.

12.3 Säkerhetstestning av kandidatåterkoppling

Eftersom plattformen kan generera privat utvecklingsinriktad återkoppling till kandidater kör vi ett separat adversariellt säkerhetsprogram mot den funktionen. Det matar medvetet systemet med hårda och fientliga rekryterarnoteringar och bekräftar att output riktad till kandidaten aldrig innehåller vulgaritet, aldrig avslöjar eller tillskriver en rekryterares identitet eller privata åsikt och aldrig använder dömande personlighetsetiketter. Detta skyddar både kandidaten, som bör få konstruktiv och respektfull återkoppling, och kunden, vars interna uppfattning aldrig bör läcka utåt.

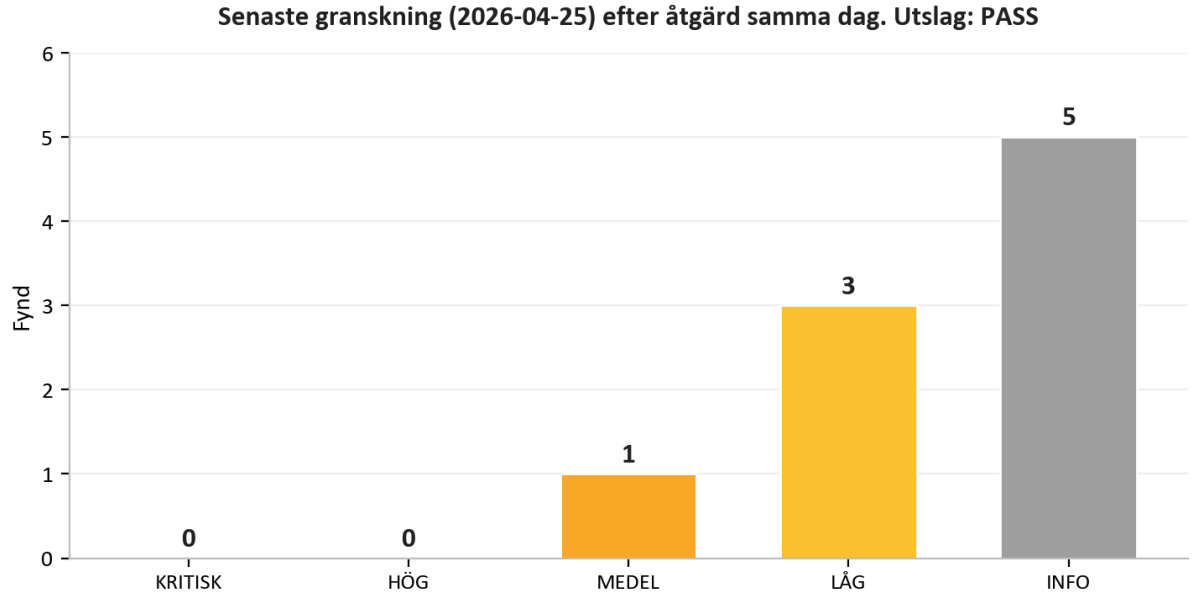
13. Resultat från säkerhetsrevisioner

Vi genomför återkommande säkerhetsrevisioner med hjälp av en strukturerad, repeterbar metod för penetrationstestning och dokumenterar var och en som en daterad rapport med fynd graderade efter allvarlighetsgrad, evidens och åtgärder. Dessa är interna revisioner som drivs av vår egen säkerhetsprocess; formell tredjepartscertifiering av samma kontroller finns på vår roadmap. Mellan slutet av mars och slutet av april 2026 genomförde vi **seven such audits** i utveckling och produktion.



Det resultat som betyder mest för en potentiell kund är konsekvensen: **across all seven audits there were zero critical findings.** Vid de sällsynta tillfällen då en fråga med högre allvarlighetsgrad uppstod åtgärdades den snabbt, ofta samma dag, och verifierades på nytt. Poängsättningsrubriken skärptes medvetet under denna period (högsta möjliga poäng höjdes när vi lade till fler kategorier att bedöma), vilket är anledningen till att den normaliserade poänglinjen förblir hög även när ribban flyttades upp.

Vår senaste revision, den 25 April 2026, illustrerar hur processen fungerar i praktiken. Två frågor med högre allvarlighetsgrad identifierades, båda åtgärdades och verifierades på nytt samma dag, och revisionen avslutades med bedömningen **PASS** utan några exploateringsbara problem kvar i den aktuella hotmodellen.



Revision	Miljö	Kritisk	Bedömning
2026-03-28	Utveckling	0	Redo för produktion
2026-04-04	Utveckling	0	Enterprise-ready
2026-04-05	Produktion	0	Enterprise-ready
2026-04-20	Utveckling	0	Production-ready, notes
2026-04-20	Utveckling	0	Pass with notes
2026-04-21	Produktion	0	Safe, no exploitable findings
2026-04-25	Utveckling	0	Pass

Mönstret i dessa revisioner är den mest ärliga evidens vi kan erbjuda: problem hittas, eftersom vi aktivt letar efter dem, och de stängs snabbt, eftersom processen är byggd för att stänga dem. En leverantör som aldrig rapporterar ett fynd är vanligtvis en leverantör som inte letar.

14. Operativ motståndskraft och delat ansvar

14.1 Övervakning och loggning

Telemetri från applikation och plattform flödar in i en centraliserad arbetsyta för logganalys och en tjänst för applikationsövervakning, vilket ger oss synlighet i tillgänglighet och beteende. Känsliga åtgärder såsom dataradering, godkännande av rättsliga avtal och AI-anrop registreras i dedikerade audittabeller, så att det finns ett varaktigt register över vem som gjorde vad med viktig data.

14.2 Säkerhetskopiering och återställning

Den hanterade databasen behåller automatiserade säkerhetskopior, och privat lagring skyddas av soft-delete-lagring på både blobs och containrar, så oavsiktlig eller skadlig radering kan återställas inom lagringsfönstret. Kritisk infrastruktur har deletion locks för att förhindra oavsiktlig nedmontering av produktionsresurser.

14.3 Sammanfattning av delat ansvar

Område	AI Interview Analyzer	Kund
Infrastruktur, nätverk, patchning	Ja	-
Applikationssäkerhet och AI-pipeline	Ja	-
Kryptering, hemligheter, datalokalisering	Ja	-
Administration av användare och roller	Tillhandahåller kontrollerna	Hanterar användare och roller
Konfiguration av lagringspolicy	Tillhandahåller kontrollerna	Anger lagringsfönstret
Kandidatsamtycke	Tillhandahåller arbetsflödet	Säkerställer att det används
Starka slutanvändaruppgifter och SSO	Stödjer SSO och policy	Upprätthåller intern policy

15. Hotmodell och OWASP-mappning

Vi designar mot en konkret uppsättning angripare: en extern angripare utan autentiseringsuppgifter, en nyfiken eller illvillig autentiserad användare i en organisation som försöker nå en annan organisations data, ett komprometterat beroende och ett internt misstag. Tabellen nedan mappar de allmänt använda riskkategorierna i OWASP Top 10 till de specifika kontroller som hanterar dem i denna plattform, och var och en av dessa testas genom den testning som beskrivs i avsnitt 12.

OWASP-risk	Hur plattformen begränsar den
Bruten åtkomstkontroll	Rollbaserad åtkomstkontroll på varje privilegierad endpoint; avgränsning per organisation; ”not found” vid åtkomst mellan organisationer; ommappning av identifierare; testmatris mellan organisationer
Kryptografiska fel	TLS 1.2+ under överföring; AES-256 i vila; bcrypt-lösenordshashning; hemligheter i ett hanterat vault
Injektion	Endast ORM-baserade parameteriserade frågor; strikt schemavalidering; HTML-sanitisering vid skrivning
Osäker design	Lagerbaserad defense in depth; hotmodellering och arkitekturgranskning i varje revision
Säkerhetsfelkonfiguration	Infrastruktur som kod; default-deny network groups; säkerhetsheaders; inaktiverade delade lagringsnycklar; API-schema exponeras inte i produktion
Sårbara komponenter	Veckovis automatiserad övervakning av beroenden; dependency CVE audits i periodisk granskning
Fel i identifiering och autentisering	Kortlivade tokens; inloggning med rate limiting; e-postverifiering; stöd för SSO; inga lösenord i klartext
Fel i programvaru- och dataintegritet	Pinnade, oföränderliga pipelinesteg; signerade desktopinstallationsprogram; verifiering av webhook-signaturer; tag-styrda produktionsdriftsättningar
Fel i säkerhetsloggning och övervakning	Centraliserad telemetri; dedikerade audittabeller för känsliga åtgärder
Server-side request forgery	Utgående anrop begränsade till betrodda endpoints; SSRF-sonder i ramverket för penetrationstestning

Denna mappning är ryggraden i vårt säkerhetsargument: för varje välkänd angreppsklass finns en namngiven kontroll, och för varje namngiven kontroll finns ett test.

16. Sårbarhetshantering och ansvarsfull rapportering

Säkerhet blir aldrig färdig, så vi driver en kontinuerlig loop av upptäckt och åtgärd.

- **Upptäckt.** Sårbarheter identifieras från fyra källor: den automatiserade testsviten, de återkommande revisionsbaserade penetrationstesterna, automatiserad övervakning av beroenden samt rapporter från kunder eller forskare.
- **Triage.** Varje fynd tilldelas en allvarlighetsgrad (critical, high, medium, low eller informational) med evidens och en ansvarig för åtgärd, exakt såsom det registreras i våra revisionsrapporter.
- **Mål för åtgärder.** Fynd av typen critical och high prioriteras för omedelbar åtgärd; i vår revisionshistorik har fynd med högre allvarlighetsgrad vanligtvis lösts och verifierats på nytt samma dag. Fynd av typen medium och lägre planeras in i den ordinarie underhållscykeln.
- **Verifiering.** Fixar testas på nytt, och där det är relevant körs en live-kontroll mot den driftsatta miljön för att bekräfta att problemet verkligen är stängt, inte bara stängt i kod.
- **Rapportering.** Säkerhetsfrågor kan rapporteras direkt till oss. Vi bekräftar rapporter, utreder dem och håller rapportören informerad fram till lösning.

17. Compliance-mappning

17.1 GDPR

GDPR-område	Plattformens implementering
Laglig grund (Art. 6)	Kandidatens uttryckliga samtycke inhämtas före behandling
Dataminimering och lagringsbegränsning (Art. 5)	Endast intervjurelevant data behandlas; konfigurerbar lagringstid med automatisk radering
Rätt till radering (Art. 17)	Radering som en sammanhållen enhet av all kandidatdata, med loggat bevis på radering
Rättigheter för registrerade (Art. 15 to 20)	Åtkomst, radering, portabilitet och invändning stöds
Personuppgiftsbiträdets skyldigheter (Art. 28)	Personuppgiftsbiträdesavtal accepteras vid registrering och versionshanteras per organisation
Säkerhet i behandlingen (Art. 32)	Kryptering, åtkomstkontroll, isolering och kontinuerlig testning enligt detta dokument
Transparens kring underbiträden	Redovisas i personuppgiftsbiträdesavtalet med förhandsbesked om förändringar

17.2 EU AI Act

Plattformen behandlas som ett högrisk-AI-system som stödjer anställningsbeslut, och vi upprätthåller dokumentation som är anpassad till regleringen, inklusive ett transparenskort, användardokumentation och en försäkran om överensstämmelse. De centrala skyddsåtgärderna, mänsklig översyn, transparens, evidensbaserad poängsättning och strikta omfångsbegränsningar för vad AI:n utvärderar, beskrivs i avsnitt 10. Vi fortsätter att utveckla vår formella dokumentation om överensstämmelse i takt med att regleringens tidslinje för implementering fortskrider.

17.3 Hostingcertifieringar

Plattformen körs helt på Microsoft Azure, vars datacenter har oberoende certifieringar inklusive ISO 27001 och SOC 2. Dessa certifieringar täcker de fysiska lagren och plattformslagren under vår applikation; kontrollerna på applikationsnivå är de som beskrivs genom hela detta dokument.

17.4 Register över underbiträden

Underbiträde	Syfte	Region
Microsoft Azure	Hosting, AI- och talbearbetning, lagring, transaktionell e-post	EU (West Europe, Sweden Central)
Stripe	Hantering av abonnemang och betalningar	EU (Ireland)
Fakturownia	Fakturering	EU (Poland)
ATS connector (optional)	Integration för applicant-tracking, aktiveras endast på begäran	EU

18. Säkerhetsroadmap

Vi behandlar säkerhet som ett program för kontinuerlig förbättring. Pågående initiativ på vår roadmap inkluderar att stärka alternativen för multifaktorautentisering för administrativa konton, utöka centraliserad audit-loggning av dataåtkomst, fortsätta att regelbundet skärpa aktualiteten i beroenden samt driva fram formell tredjepartscertifiering av de kontroller som beskrivs i detta dokument. Inget av detta utgör en lucka som exponerar kunddata idag; varje punkt är en förbättring av en redan lagerbaserad säkerhetshållning.

19. Sammanfattning

AI Interview Analyzer skyddar kandidat- och kunddata genom en lagerbaserad arkitektur: ett privat-som-standard-nätverk utan publika datatjänster, stark identitet och isolering per organisation, applikationskod som designar bort hela sårbarhetsklasser, kryptering och datalagring inom EU samt integritetskontroller inbyggda i datamodellen. Det som skiljer plattformen åt är evidensen bakom dessa påståenden. Med 3,171 automatiserade tester, en repeterbar metod för live-penetrationstestning, ett dedikerat AI-säkerhetsprogram och en historik av sju interna säkerhetsrevisioner med zero critical findings kan vi visa, inte bara säga, att plattformen är säker.

Bilaga A: Katalog över säkerhetskontroller

En kondenserad referens över primära kontroller och den evidens som stöder var och en.

Kontroll	Mekanism	Evidens
Kryptering under överföring	Endast HTTPS, TLS 1.2+, HTTP omdirigerat	Infrastruktur som kod; arkitekturrevision
Kryptering i vila	AES-256-plattformskryptering på lagring och databas	Plattforms-konfiguration; arkitekturrevision
Lösenordsskydd	bcrypt med salt per lösenord	Källkodshantering; autentiseringstester
Sessionshantering	30-minuters signerade tokens, återkallningsbar refresh på serversidan	Källkodshantering; autentiseringstester
Auktorisering	Åtkomstkontroll med fyra roller på privilegierade endpoints	Testsvit för rolltillämpning
Tenant-isolering	Frågeavgränsning per organisation; 404 mellan organisationer	Testmatris mellan organisationer
Säkerhet för API-nycklar	Hashad lagring, avgränsade behörigheter, rate limits per nyckel	Testsvit för API-nycklar
Skydd mot injektion	Endast ORM-baserade parameteriserade frågor	Statisk analys; injektionstester
Skydd mot cross-site scripting	HTML-sanitisering vid skrivning	Testsvit för HTML-sanitisering
Rate limiting	Robust limiter för auth-endpoints backad av databas	Rate-limit-tester; live burst-kontroller
Integritet för webhooks	Verifiering av leverantörssignaturer på rå body	Testsvit för webhooks
Hantering av hemligheter	Hanterat vault, purge protection, managed identity	Infrastruktur som kod; arkitekturrevision
Nätverksisolering	Private endpoints; default-deny-segmentering	Infrastruktur som kod; arkitekturrevision
Dataradering	Kaskaderande radering som en sammanhållen enhet med audit-logg	GDPR-testsvit för radering
Försörjningskedja	Pinnade pipelinesteg; veckovis övervakning av beroenden	Pipeline-konfiguration; beroenderevision

Bilaga B: Vanliga frågor för säkerhetsgranskare

Var lagras våra data? Helt inom Europeiska unionen, på Microsoft Azure, i West Europe med AI-bearbetning i EU-regioner. Kandidatdata lämnar aldrig EU.

Används våra data för att träna AI-modeller? Nej. AI-leverantören använder inte kunddata för träning.

Är databasen nåbar från internet? Nej. Publik nätverksåtkomst är inaktiverad och databasen är endast nåbar via en private endpoint i det virtuella nätverket.

Kan en kund se en annan kunds data? Nej. Varje fråga avgränsas till den anropande organisationen, åtkomst mellan organisationer returnerar ”not found”, och en automatiserad matris testar kontinuerligt denna isolering.

Hur lagras lösenord? Hashade med bcrypt och ett unikt salt per lösenord. Single sign-on med Microsoft och Google stöds, i vilket fall inget lösenord lagras.

Stöder ni single sign-on? Ja, via Microsoft och Google OAuth.

Hur länge är access tokens giltiga? Trettio minuter, tillsammans med en återkallningsbar refresh-session på serversidan som ogiltigförklaras vid utloggning.

Hur hanteras kandidatsamtycke? Varje kandidat får en unik samtyckeslänk för engångsanvändning och måste acceptera innan någon inspelning eller analys sker. Samtycke registreras mot den specifika rekryteringsprocessen.

Hur raderas data? Som en sammanhållen enhet som omfattar kandidatposten, intervjuer, transkript, ljud, dokument och jämförelser, enligt ett konfigurerbart lagringsschema, med ett loggat bevis på radering. Kandidater kan också begära radering direkt.

Har ni ett personuppgiftsbiträdesavtal? Ja, det accepteras vid registrering och versionshanteras per organisation, inklusive registret över underbiträden.

Fattar AI:n rekryteringsbeslut? Nej. Den tillhandahåller endast beslutsstöd; en människa granskar varje output och fattar alla beslut.

Hur bevisar ni era säkerhetspåståenden? Genom 3,171 automatiserade tester inklusive en dedikerad säkerhetssvit, en repeterbar metod för penetrationstestning i sex faser som körs mot live-miljöer, ett AI-säkerhetsprogram och återkommande skriftliga revisionsrapporter.

Vad händer när ni hittar en sårbarhet? Den tilldelas en allvarlighetsgrad med evidens och en ansvarig, åtgärdas enligt en prioriterad tidsplan, verifieras på nytt inklusive live-kontroller där det är relevant och registreras i en revisionsrapport.

Kan vi genomföra vårt eget penetrationstest? Säkerhetsbedömningar kan arrangeras genom er kontaktperson under lämplig omfattning och schemaläggning.

Bilaga C: Ordlista

Term	Betydelse
AES-256	En stark symmetrisk krypteringsstandard som används för att skydda data i vila
bcrypt	En specialbyggd funktion för lösenordshashning med salt per lösenord
Managed identity	En plattformsutfärdad identitet som låter en tjänst autentisera utan lagrade nycklar
Private endpoint	En privat nätverksadress som håller en molntjänst borta från det publika internet
Network security group	En uppsättning tillåt- och neka-regler som filtrerar nätverkstrafik till ett subnät
RBAC	Rollbaserad åtkomstkontroll som beviljar behörigheter enligt en användares roll
IDOR	Insecure direct object reference, en åtkomstkontrollbrist som plattformen skyddar mot
SSRF	Server-side request forgery, en angreppsklass som sonderas i våra penetrationstester
Web application firewall	En edge-kontroll som filtrerar skadlig webbtrafik
Data processing agreement	Avtalet som reglerar hur ett personuppgiftsbiträde hanterar personuppgifter för en personuppgiftsansvarigs räkning

Bilaga D: Kontakt och dokumentstyrning

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

För en säkerhetsgranskning, en kopia av vårt personuppgiftsbiträdesavtal eller vår dokumentation om överensstämmelse med EU AI Act, vänligen kontakta er kontaktperson.

Detta dokument beskriver säkerhetshållningen för tjänsten AI Interview Analyzer per det genereringsdatum som visas i sidfoten. Det tillhandahålls för utvärderingsändamål och utgör inte en del av något avtal. Specifika avtalsmässiga säkerhetsåtaganden anges i tillämpligt avtal och personuppgiftsbiträdesavtal.