Tietoturvan whitepaper

Enterprise Security Overview - AI Interview Analyzer

Tarjoaja:	AI Interview Analyzer Sp. z o.o.
Osoite:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Luokitus:	PUBLIC
Päivämäärä:	24.06.2026

Contents

Tietoturvan whitepaper

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

Kohdeyleisö: Yritysturvallisuuden, IT:n ja hankinnan tiimit

Luokitus: Julkinen

1. Tiivistelmä

AI Interview Analyzer on yrityskäyttöön tarkoitettu rekrytointialusta, joka tallentaa haastattelut ehdokkaan nimenomaisella suostumuksella, litteroi ja jäsentää ne sekä tuottaa näyttöön perustuvaa arviointitukea rekrytoijille. Koska alusta käsittelee ehdokkaiden henkilötietoja ja tukee rekrytointiprosesseja, tietoturvaa ja yksityisyyttä käsitellään ensisijaisina suunnittelurajoitteina, ei myöhemmin lisättävinä ominaisuuksina.

Tässä whitepaperissa kuvataan konkreettisesti ja todennettavasti, miten suojaamme asiakkaiden ja ehdokkaiden tietoja. Se on kirjoitettu niille, jotka arvioivat toimittajia: tietoturvainsinööreille, IT-ylläpitäjille, tietosuojavastaaville ja hankinnalle. Jokainen tässä asiakirjassa esitetty luku perustuu suoraan omiin teknisiin järjestelmiimme eikä markkinointimateriaaliin.

Keskeinen viesti on yksinkertainen: **emme ainoastaan väitä alustan olevan turvallinen, vaan testaamme sitä jatkuvasti.** Koodipohjamme sisältää **3,171 automatisoitua testiä**, mukaan lukien erillinen tietoturvatestipaketti, joka harjoittaa todennusta, valtuutusta, organisaatioiden välistä eristystä, suojausta injektioita vastaan ja tietojen poistamista. Tämän lisäksi ajamme toistettavaa penetraatiotestauskehikkoa tuotantokäytössä olevia ympäristöjä vastaan ja tuotamme kirjallisia auditointiraportteja. Seitsemässä sisäisessä tietoturva-auditoinnissa maaliskuussa ja huhtikuussa 2026 kirjasimme **zero critical findings**, ja viimeisin auditointimme päättyi lopputulokseen **PASS**. (Näiden kontrollien muodollinen kolmannen osapuolen sertifiointi on tiekartallamme; katso kohta 18.)

Tietoturvaominaisuus	Yhteenveto
Hosting	Microsoft Azure, vain EU-alueet
Verkkototeutus	Yksityiset päätepisteet, oletuksena estävä verkon segmentointi, ei julkista tietokantaa
Salaus	AES-256 levossa, TLS 1.2 tai uudempi siirrossa
Identiteetti	Lyhytikäiset allekirjoitetut tokenit, bcrypt-salasanojen hajautus, SSO-tuki
Pääsynhallinta	Roolipohjainen pääsynhallinta tiukalla organisaatiokohtaisella eristyksellä
Salaisuudet	Keskitetty salaisuuksien holvi managed identity -pääsyllä
Yksityisyys	Nimenomainen suostumus, määritettävä säilytys, yhden kokonaisuuden poisto
Vastuullinen AI	Vain päätöksenteon tuki, ihminen aina mukana
Varmennus	3,171 automatisoitua testiä sekä toistuvat penetraatiotestit ja auditoinnit

1.1 Miten tämä asiakirja luetaan

Kohdissa 3–11 kuvataan kontrollit, jotka suojaavat tietoja: arkkitehtuuri, verkko, identiteetti, sovellus, tietosuoja, yksityisyys ja turvallinen ohjelmistokehityksen elinkaari. Kohdat 12 ja 13 käsittelevät erottuvaa jatkuvan testauksen ohjelmaamme ja auditointihistoriaamme. Kohdat 14–17 kattavat operatiivisen toiminnan, uhkamallinnuksen, haavoittuvuuksien hallinnan ja vaatimustenmukaisuuskartoituksen. Liitteet tarjoavat kontrolliluettelon, arvioijien FAQ-osion ja sanaston, joita tietoturvatiimi voi käyttää suoraan arvioinnin aikana.

2. Asiakirjan laajuus ja lähestymistapa

2.1 Mitä tämä asiakirja kattaa

Tämä whitepaper kattaa AI Interview Analyzer -palvelun tietoturva-arkkitehtuurin ja käytännöt: hosting-ympäristön, verkkosuunnittelun, identiteetin- ja pääsynhallinnan, sovellustason kontrollit, tietosuojan, yksityisyyden ja sääntelyn mukaisuuden, turvallisen ohjelmistokehityksen elinkaaren sekä jatkuvan tietoturvatestauksen ohjelmamme.

2.2 Mikä tekee tästä todennettavan

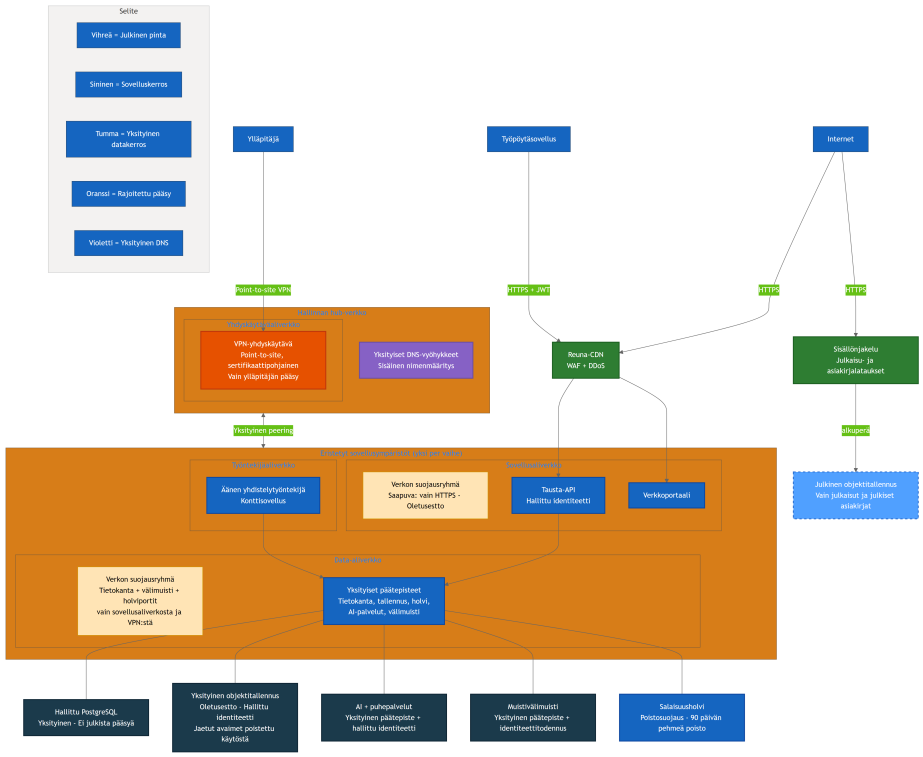
Toimittajien tietoturvaväitteet on helppo kirjoittaa ja vaikea luottaa. Siksi olemme sitoneet jokaisen tässä asiakirjassa esitetyn pääväitteen johonkin konkreettiseen ja laskettavaan omissa teknisissä järjestelmissämme: koodissa toteutettuun kontrolliin, testiin joka osoittaa kontrollin toimivan, infrastruktuurimäärittelyyn joka pakottaa sen voimaan tai auditointiraporttiin joka kirjaa dokumentoidun tarkastuksen. Kun jokin kontrolli on osa tulevaa tiekarttaamme eikä vielä nykyinen tuotantoominaisuus, sanomme sen nimenomaisesti. Mieluummin aliväitämme ja olemme luotettuja kuin yliväitämme ja jäämme kiinni.

2.3 Jaettu vastuu

Alusta toimitetaan ohjelmistona palveluna. Me operoimme infrastruktuuria, sovellusta, AI-putkea ja tietojen käsittelyä. Asiakas vastaa omien käyttäjätiliensä ja rooliensa hallinnasta, tietojen säilytysaikojen määrittämisestä sisäisen politiikkansa mukaisiksi sekä siitä, että ehdokkaan suostumus hankitaan alustan tarjoaman suostumustyönkulun kautta. Kohta 14 kuvaa tätä vastuunjakoa tarkemmin.

3. Tietoturva-arkkitehtuurin yleiskuva

Alusta on rakennettu pienenä joukkona yhteistyössä toimivia palveluja yhden monoliitin sijaan. Työpöytäsovellus ja web-portaali toimivat asiakasohjelmina. Keskitetty backend API hallitsee kaikkea pysyvää tallennusta, todennusta, laskutusta, AI-putkea, suostumusta, sähköpostia, tiedostojen käsittelyä ja koontinäyttöjä. Äänen yhdistämisestä vastaava worker käsittelee tallenteita asynkronisesti. Kaikki arkaluonteinen tila sijaitsee backend API:n takana; asiakasohjelmat eivät koskaan keskustele suoraan tietokannan, tallennuksen tai AI-palveluiden kanssa.



Yllä oleva kaavio näyttää tuotantotopologian, jossa resurssien nimet on tarkoituksellisesti yleistetty. Siinä näkyy kolme periaatetta:

- **Ei suoraa altistusta tietopalveluille.** Tietokannalta, yksityiseltä objektitallennukselta, AI-palveluilta ja välimuistilta on poistettu julkinen verkko-oikeus, ja ne ovat saavutettavissa vain eristetyn virtuaaliverkon sisäisten yksityisten päätepisteiden kautta. Sovellus tavoittaa salaisuuksien holvin yksityisen päätepisteen kautta, ja sitä suojaavat lisäksi alustan identiteettitodennus ja vähimmän oikeuden pääsykäytännöt, joten kaikki pääsy edellyttää kelvollista, valtuutettua identiteettiä verkkopolusta riippumatta.
- **Erotettu julkinen pinta.** Ainoa julkinen objektitallennus sisältää julkaisuversioiden latauksia ja julkisia asiakirjoja. Se ei koskaan sisällä ehdokastietoja. Asiakkaille näkyvä sovelluslikenne kulkee reunakerroksen kautta, joka tarjoaa web application firewall -, distributed-denial-of-service -suojauksen sekä sisällönjakelun.
- **Ylläpitäjien pääsy on vartioitu.** Operoijat tavoittavat sisäiset resurssit vain sertifikaattipohjaisen point-to-site VPN -yhteyden kautta hallintakeskusverkkoon, eivät julkisen internetin kautta.

Jokainen käyttöönoton vaihe (kehitys ja tuotanto) on täysin eristetty ympäristö, jolla on oma verkko, tallennustilit, tietokanta ja salaisuudet. Asiakkaiden tuotantodataa ei koskaan esiinny alemmissa ympäristöissä. Yhteinen hallintakeskus sisältää vain VPN-yhdyskäytävän ja yksityisen DNS:n, jotka on liitetty yksityisesti kuhunkin ympäristöön.

4. Defense in Depth

Yhteen ainoaan kontrolliin ei luoteta kaikkien hyökkäysten pysäyttämisessä. Alusta kerrostaa toisistaan riippumattomia kontrolleja niin, että minkä tahansa yksittäisen kerroksen epäonnistuminen ei paljasta tietoja. Alla olevat kerrokset on kukin toteutettu ja, kuten kohdassa 12 kuvataan, testattu erikseen.

Kerrostettu tietoturvamalli: riippumattomat kontrollit joka tasolla

Kerros	Edustavat kontrollit
Verkon reuna	Vain TLS-siirto, reunan WAF- ja DDoS-suojaus, yksityiset päätepisteet, oletuksena estävä segmentointi
Identiteetti ja pääsy	Lyhytikäiset allekirjoitetut tokenit, bcrypt-hajautus, roolipohjainen pääsynhallinta, organisaatiokohtainen eristys
Sovellus	Skeemavalidointi kaikelle syötteelle, vain ORM-pohjainen tiedonkäyttö, tulosteen koodaus, nopeusrajoitus
Tietosuoja	Salaus levossa, salaisuuksien holvi managed identity -toiminnolla, EU-datan sijainti, suostumukseen sidottu käsittely
Hallintamalli ja yksityisyys	Määritettävä säilytys, yhden kokonaisuuden poisto, human-in-the-loop AI, auditointiloki
Jatkuva varmistus	Automatisoitu testipaketti, toistettavat penetraatiotestit, toistuvat sisäiset tietoturva-auditoinnit

Tämän asiakirjan loppuosa käy läpi jokaisen kerroksen vuorollaan ja kuvaa sitten, miten todistamme jatkuvasti, että kerrokset pitävät.

5. Verkkoturvallisuus

5.1 Oletuksena yksityinen

Tietokerros on rakenteellisesti yksityinen. Hallitulta PostgreSQL-tietokannalta on poistettu julkinen verkko-oikeus, ja se on saavutettavissa vain yksityisen päätepisteen kautta. Yksityinen objektitallennus on määritetty estämään verkkopääsy oletuksena, poistaa jaetut käyttöavaimet kokonaan käytöstä ja on saavutettavissa vain managed identityn kautta sovellusaliverkosta. Välimuisti, AI-palvelut ja salaisuuksien holvi tavoitetaan samoin yksityisten päätepisteiden ja yksityisen DNS-resoluution kautta.

Käytännössä tämä tarkoittaa, ettei tietokantaan ole internetiin näkyvää yhteysmerkkijonoa eikä ehdokkaan äänelle julkista tallennus-URL-osoitetta: tietokannalta ja yksityiseltä tallennukselta on julkinen verkkopääsy poistettu suoraan käytöstä. Sovellus tavoittaa salaisuuksien holvin yksityisen päätepisteen kautta, ja sitä suojaavat alustan identiteettitodennus sekä vähimmän oikeuden pääsykäytännöt; sovellusidentiteeteille annetaan vain lukuoikeus vain niihin salaisuuksiin, joita ne tarvitsevat, joten salaisuuksia ei voida hakea ilman kelvollista, valtuutettua identiteettiä. Hyökkäyspinta, johon ulkoinen vastustaja voi ylipäätään koskea, rajoittuu sovelluksen HTTPS-päätepisteisiin reunakerroksen takana.

5.2 Verkon segmentointi

Jokainen ympäristö on jaettu erillisiin aliverkkoihin sovelluskerrosta, tietokerrosta ja asynkronista workeria varten. Jokaista aliverkkoa hallitsee network security group, jonka viimeinen sääntö estää kaiken saapuvan liikenteen. Sovellusaliverkko hyväksyy vain saapuvan HTTPS-liikenteen. Data-aliverkko hyväksyy vain tietyt tietokannan, välimuistin ja holvin portit, ja vain sovellusaliverkosta tai hallinnollisen VPN-yhteyden kautta. Tämä tarkoittaa, että vaikka hyökkääjä jotenkin pääsisi sovelluskerrokseen, hän ei voi vapaasti liikkua tietokerrokseen; vain ne reitit ovat sallittuja, joita sovellus käyttää laillisesti.

5.3 Reunakerros

Julkinen sovellusliikenne on reunakerroksen edessä, joka tarjoaa web application firewall -, DDoS-suojauksen ja content delivery network -toiminnallisuuden. Julkaisu- ja asiakirjalataukset toimitetaan erilliseltä julkiselta tallennustililtä content-delivery front doorin kautta täysin erillään yksityisestä tallennuksesta, jossa ehdokastiedot sijaitsevat. Nämä kaksi tallennustasoa eivät koskaan sekoitu: väärä konfiguraatio julkisella puolella ei voi paljastaa yksityisiä ehdokastietoja, koska kyse on eri tileistä, joilla on eri verkkosäännöt.

5.4 Hallinnollinen pääsy

Yksityiseen verkkoon ei ole julkista hallinnollista päätepistettä. Operoijat muodostavat yhteyden point-to-site VPN -yhdyskäytävän kautta, joka käyttää sertifikaattipohjaista todennusta. Hallinnollinen pääsy tietokantaan ja välimuistiin on mahdollista vain tämän tunnelin sisältä, koska näiltä palveluilta on poistettu julkinen verkkopääsy. Tämä pitää päivittäisen operoinnin kokonaan poissa julkisesta internetistä.

6. Identiteetin- ja pääsynhallinta

6.1 Todennus

Käyttäjäistunnot muodostetaan allekirjoitetulla access tokenilla, joka on voimassa kolmekymmentä minuuttia, ja paritetaan erilliseen, läpinäkymättömään, palvelinpuoliseen refresh tokeniin. Access tokenit varmennetaan jokaisessa pyynnössä, ja käyttäjä validoidaan uudelleen tietokantaa vasten (mukaan lukien aktiivisen tilin tarkistus) sen sijaan, että luotettaisiin pelkästään tokenin sisältöön. Uloskirjautuminen mitätöi palvelinpuolisen refresh-istunnon välittömästi, joten varastettu refresh token ei voi säilyä voimassa uloskirjautumisen jälkeen.

Salasanoja ei koskaan tallenneta selväkielisinä. Ne hajautetaan bcrypt-algoritmilla käyttäen yksilöllistä per-salasana salt -arvoa. Organisaatioille, jotka suosivat kertakirjautumista, alusta tukee OAuth-kirjautumista Microsoftin ja Googlen kautta, jolloin salasanaa ei säilytetä lainkaan.

Sähköpostin omistajuus varmistetaan kertakäyttöisellä, aikarajoitetulla vahvistuslinkillä ennen kuin itse rekisteröitynyt tiliä käsitellään vahvistettuna, ja vahvistussähköpostin uudelleenlähetyksiä rajoitetaan väärinkäytön estämiseksi.

6.2 Roolipohjainen pääsynhallinta

Valtuutus pannaan täytäntöön roolimallilla, jossa on neljä kasvavan oikeustason roolia: interviewer, hiring manager, recruiter ja administrator. Pääsy etuoikeutettuihin toimintoihin pakotetaan palvelinpuolisilla riippuvuuksilla, jotka tarkistavat sekä kutsujan roolin että vahvistustilan. Nämä roolitarkistukset suojaavat reilusti yli sataa erillistä API-toimintoa.

Rooli	Tyypilliset oikeudet
Interviewer	Toteuttaa sille osoitetut haastattelut; näkee vain itselleen osoitetut haastattelut
Hiring manager	Hallinnoi rekrytointeja, jotka se omistaa tai joiden jäsen se on
Recruiter	Täysi rekrytointi- ja ehdokashallinta organisaation sisällä
Administrator	Organisaatioasetukset, laskutus, käyttäjä- ja API-avainhallinta

Karkeiden roolitarkistusten lisäksi alusta soveltaa tietotason näkyvyyssääntöjä. Hiring managerit näkevät vain rekrytoinnit, jotka he ovat luoneet tai joiden jäseniä he ovat; interviewerit näkevät vain heille osoitetut haastattelut. Oikeudet pannaan siis täytäntöön sekä tasolla "mikä toiminto" että tasolla "mitkä tietueet".

6.3 Organisaatiokohtainen eristys

Alusta on moniasiakasympäristö, ja tenant-eristystä käsitellään ensiluokkaisena tietoturvakontrollina. Jokaisella todennetulla identiteetillä on organisaatiotunniste, ja tietokyselyt rajataan siihen organisaatioon. Kun käyttäjä pyytää tietuetta, joka kuuluu toiselle organisaatiolle, alusta palauttaa "not found" -vastauksen sen sijaan, että paljastaisi tietueen olemassaolon. Sisäisiä tietokanta-ID:itä ei koskaan paljasteta verkon yli; API esittää näyttötunnisteita ja uudelleenkartoit-taa ne jokaisessa pyynnössä, mikä poistaa tavallisen organisaatioiden välisen enumerointihyökkäyksen luokan.

Tämä ei ole vain suunnittelutavoite. Kuten kohdassa 12 kuvataan, automaattinen testipakettimme suorittaa laajan organisaatioiden välisen matriisin, joka yrittää tavoittaa yhden organisaation tietoja toisen organisaation tunnuksilla ja varmistaa, että jokainen tällainen yritys epäonnistuu.

6.4 Ohjelmallinen pääsy

Integraatioita varten tukikelpoisilla tilaustasoilla olevat organisaatiot voivat myöntää API-avaimia. Avaimissa käytetään tunnistettavaa etuliitettä, niissä on 128 bittiä entropiaa ja ne tallennetaan vain hajautteena; raakaa avainta näytetään vain kerran luonnin yhteydessä eikä koskaan uudelleen. Jokaisella avaimella on nimenomainen käyttöoikeusalue (read, write tai ATS integration), se voidaan rajoittaa tiettyihin lähdeverkkoihin, se voidaan mitätöidä välittömästi, ja siihen sovelletaan avainkohtaisia nopeusrajoja, jotka johdetaan organisaation tilaustasosta. Avaimen varmennus käyttää timing-safe -vertailua, jotta tietoa ei vuotaisi vasteaikojen kautta.

7. Sovellustietoturva

Sovellus on kirjoitettu poistamaan kokonaisia haavoittuvuusluokkia sen sijaan, että niitä paikattaisiin tapauskohtaisesti.

- **Injektio.** Kaikki tietokantakäyttö kulkee object-relational mapperin kautta käyttäen parametroitua kyselyä. Koodipohja ei sisällä raakaa merkkijonomuotoiltua SQL:ää. Tämä eliminoi rakenteellisesti SQL-injektion.
- **Syötteen validointi.** Jokainen pyynnön runko validoidaan tiukkaa skeemaa vasten ennen kuin se saavuttaa liiketoimintalogiikan. Ylisuurten hyötykuormien vastaanotto estetään, ja listapäätepisteet on sivutettu resurssien käytön rajaamiseksi.
- **Tulosteen koodaus ja cross-site scripting.** Käyttäjän syöttämää ja AI:n tuottamaa tekstiä käsitellään epäluotettavana. Kun sisältö täytyy renderöidä HTML:nä, se kulkee sallittujen listaan perustuvan puhdistuksen läpi kirjoitushetkellä, ja erillinen testipaketti varmistaa, että script-tagit, tapahtumankäsittelijät ja javascript-URL-osoitteet poistetaan.
- **Mass assignment.** Päivitystoiminnot käyttävät eksplisiittisiä skeemoja, jotka sulkevat pois etuoikeutetut kentät, kuten role, organization ja credit balance, joten asiakas ei voi nostaa oikeuksiaan lähettämällä ylimääräisiä kenttiä.
- **Nopeusrajoitus.** Todennukseen ja väärinkäytöksille alttiisiin päätepisteisiin sovelletaan nopeusrajoituksia käyttäen kestävää, tietokantapohjaista rajoitinta, joka säilyy uudelleenkäynnistysten yli ja toimii oikein useiden sovellusinstanssien kesken. Kirjautumisella, rekisteröitymisellä, salasanan palautuksella ja vahvistuksen uudelleenlähetyksillä on kullakin omat rajansa. Asiakkaan IP-osoitteen resoluutio on kovennettu forwarding header -väärennöksiä vastaan.
- **Webhookit.** Maksu- ja sähköpostipalveluntarjoajien saapuvat webhookit varmennetaan palveluntarjoajan allekirjoituksia vasten pyynnön raakaa runkoa käyttäen ennen käsittelyä.
- **Tiedostojen lataukset.** Latauksille on kokoraja, ne validoidaan, tallennetaan generoituja tunnisteita käyttäen käyttäjän antamien nimien sijaan ja niitä rajoitetaan sekä pyyntöä että organisaatiota kohden.
- **Tietoturvaotsakkeet.** Tuotannossa vastaukset sisältävät strict transport securityn, content-type- ja frame-asetukset, referrer policyn ja rajoittavan permissions policyn sekä piilottavat palvelin- ja framework-bannerit.

8. Tietosuoja

8.1 Salaus

Kaikki tiedot salataan levossa käyttäen AES-256-salausta Azure-alustan tallennus- ja tietokantasalauskerrosten kautta. Kaikki verkkoliikenne palvellaan yksinomaan HTTPS:n yli käyttäen TLS 1.2 tai uudempaa; selväkielinen HTTP ohjataan HTTPS:ään kaikissa kerroksissa. Tuotannossa API ja web-portaali lähettävät strict transport security -otsakkeet yhdessä kovennusotsakkeiden joukon kanssa ja piilottavat palvelin- ja framework-versiobannerit.

8.2 Salaisuuksien hallinta

Sovelluksen salaisuuksia säilytetään keskitetysti salaisuuksien holvissa, jossa purge protection on käytössä ja soft-delete-jakso on yhdeksänkymmentä päivää. Sovellukset todentautuvat Azure-resursseihin käyttäen järjestelmän määrittämiä managed identityjä pitkäikäisten avainten sijaan; esimerkiksi yksityiseltä tallennukselta on jaetut käyttöavaimet poistettu kokonaan käytöstä, joten pääsy on mahdollista vain identiteettipohjaisten roolimääritysten kautta, jotka on rajattu yksittäiseen resurssiin. Holvin pääsykäytännöt myöntävät sovellusprinsipaaleille vain lukuoikeuden niihin nimenomaisiin salaisuuksiin, joita ne tarvitsevat, vähimmän oikeuden periaatteen mukaisesti.

8.3 Datan sijainti

Kaikki asiakkaiden ja ehdokkaiden tiedot tallennetaan ja käsitellään Euroopan unionin sisällä. Sovelluksen hosting, tietokanta, tallennus, välimuisti ja salaisuudet sijaitsevat West Europe -alueella, ja AI-käsittely tapahtuu EU-alueilla. AI-palveluntarjoaja ei käytä asiakasdataa mallien kouluttamiseen.

8.4 Yhden haastattelun elinkaari

Selkein tapa ymmärtää tietosuojakontrollit on seurata yhtä haastattelua alusta loppuun. Suostumus kerätään ja kirjataan ennen minkään käsittelyn aloittamista. Lataus salataan siirron aikana. Litterointi ja analyysi suoritetaan EU:n datakeskuksissa. Tulokset kirjoitetaan salattuun tallennukseen. Sen jälkeen jokaista tietuetta hallitsee yksi säilytyskello, joka päättyy lokitettuun, ketjutettuun poistoon. Missä tahansa vaiheessa ehdokkaan oikeudet, kuten suostumuksen peruuttaminen, poistaminen, pääsy tai siirrettävyys, voivat keskeyttää tämän kulun.

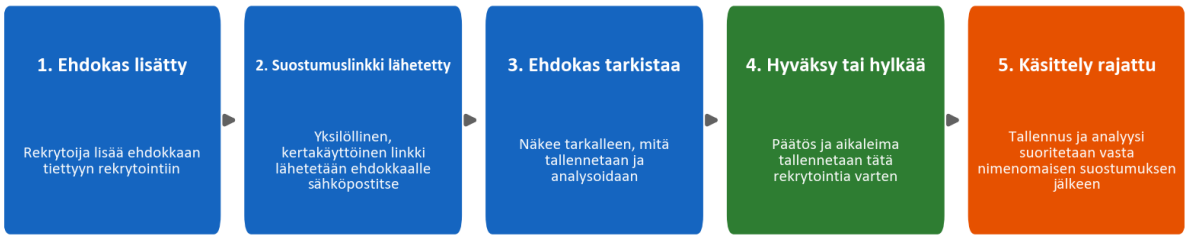
9. Sisäänrakennettu yksityisyys ja GDPR

Yksityisyys on rakennettu tietomalliin ja työnkulkuun, ei liitetty päälle pelkän politiikan kautta.

9.1 Suostumus

Mitään haastattelua ei tallenneta tai analysoida ilman ehdokkaan nimenomaista suostumusta. Kun ehdokas lisätään rekrytointiin, alusta lähettää sähköpostitse yksilöllisen, kertakäyttöisen suostumuslinkin. Ehdokas tarkistaa, mitä tulee tapahtumaan, ja joko hyväksyy tai kieltäytyy. Suostumuksen tila, mukaan lukien vastausajankohta, kirjataan kyseistä rekrytointia vasten, joten suostumus rajautuu aina konkreettiseen rekrytointiprosessiin eikä sitä myönnetä yleisesti.

Ehdokkaan suostumus: nimenomainen ja kirjattu ennen käsittelyä

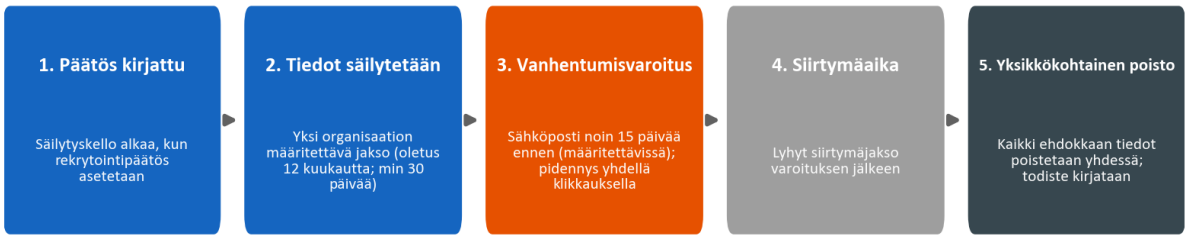


9.2 Säilytys ja poistaminen

Tietojen säilytysaika on määritettävissä organisaatiokohtaisesti, oletuksena kaksitoista kuukautta ja määritettävissä oleva vähimmäisaika kolmekymmentä päivää, ja sitä voidaan ohittaa ehdokaskohtaisesti. Ehdokkaan tiedoille on yksi säilytyskello, ei erillistä ajastinta jokaiselle artefaktille. Kello käynnistyy, kun rekrytointipäätös kirjataan. Ennen tietojen vanhenemista alusta lähettää varoituksen (oletuksena noin viisitoista päivää etukäteen) ja tarjoaa yhden napsautuksen pidennyksen. Kun tiedot poistetaan, ne poistetaan yhtenä kokonaisuutena: ehdokastietue, haastattelut, litteraatit, äänitallenteet, asiakirjat ja vertailut poistetaan kaikki yhdessä, ja poisto kirjataan auditointilokiin. Osittaista tai orvoksi jäävää jäännöstä ei jää.

Alla oleva elinkaari näyttää tämän yhden kellon ja sen, miten se päättyy yhteen ketjutettuun poistoon, josta jää lokitettu todiste poistamisesta.

Tietojen säilytys: yksi kello per ehdokas, yksikkökohtainen poisto



9.3 Rekisteröidyn oikeudet ja alikäsittelijät

Alusta tukee GDPR:n mukaisia rekisteröidyn oikeuksia, mukaan lukien oikeus saada pääsy tietoihin, poisto, siirrettävyys, vastustaminen ja selitys. Käsittely toteutetaan data processing agreement -sopimuksen nojalla, jonka asiakkaat hyväksyvät rekisteröitymisen yhteydessä ja joka versioidaan organisaatiokohtaisesti. Alikäsittelijämme ja niiden roolit, kaikki EU:ssa tai

asianmukaisten suojatoimien piirissä, ilmoitetaan kyseisessä sopimuksessa, ja asiakkaat saavat ennakkoilmoituksen kaikista muutoksista. Kohta 17 sisältää alikäsittelijärekisterin ja artiklakohtaisen vaatimustenmukaisuuskartoituksen.

10. Vastuullinen AI ja EU AI Act

Alusta kuuluu EU AI Actin high-risk -luokkaan, koska se tukee työllistämispäätöksiä, ja suhtaudumme tähän luokitteluun vakavasti.

Tuotteen määrittävä sääntö on, että **AI on päätöksenteon tuki, ei päätöksentekijä.** Järjestelmä ei koskaan automaattisesti hyväksy tai hylkää ehdokasta. Se litteroi puheen, jäsentää kysymykset ja vastaukset, pisteyttää vastaukset rekrytoijan määrittelemien kriteerien mukaan ja laatii palauteluonnoksia, ja ihminen tarkistaa jokaisen tulosteen ennen sen käyttöä. Tämä pitää ihmisen tiukasti mukana prosessissa.

Yhtä tärkeää on se, mitä AI ei tee. Se ei arvioi persoonallisuutta, "cultural fit" -sopivuutta, tunnetilaa, äänen sävyä, aksenttia, sukupuolta, ikää, etnisyyttä, ulkonäköä tai kehonkieltä. Pisteytys ankkuroidaan litteraatista saatavaan näyttöön ja rekrytoijan määrittelemiin kriteereihin, ja ehdokkaiden nimet jätetään arviointisyötteestä pois biasin vähentämiseksi. Julkaisemme läpinäkyvyyskortin, käyttöohjeet ja vaatimustenmukaisuusvakuutuksen, joissa kuvataan järjestelmä, sen rajoitukset ja suojatoimet.

Vastuullisen AI:n kontrolli	Miten se toimii
Ihminen mukana prosessissa	Rekrytoija tarkistaa jokaisen pisteen ja jokaisen palautteen ennen käyttöä
Ei automaattisia päätöksiä	Järjestelmä ei koskaan automaattisesti hyväksy tai hylkää ehdokasta
Näyttöön perustuva pisteytys	Pisteet viittaavat litteraatista saatavaan tukevaan näyttöön
Biasia vähentävä suunnittelu	Nimet suljetaan arvioinnista pois; sisältö pisteytetään tyylin sijaan
Soveltamisalan rajat	Persoonallisuutta, tunnetilaa, aksenttia ja suojattuja ominaisuuksia ei koskaan arvioida
Ehdokaspalautteen turvallisuus	Yksityinen ehdokaspalaute kulkee generointi- ja validointiturvakaiteen läpi

Näitä rajoitteita ei ole ainoastaan kirjattu dokumentaatioon; ne on koodattu AI-prompt-kerrokseen ja niitä harjoitetaan kohdassa 12.3 kuvatulla erillisellä AI-turvallisuuden testiohjelmalla.

11. Turvallinen ohjelmistokehityksen elinkaari

Tietoturva pakotetaan siihen tapaan, jolla rakennamme ja toimitamme ohjelmistoja, ei vain käynnissä olevaan järjestelmään.

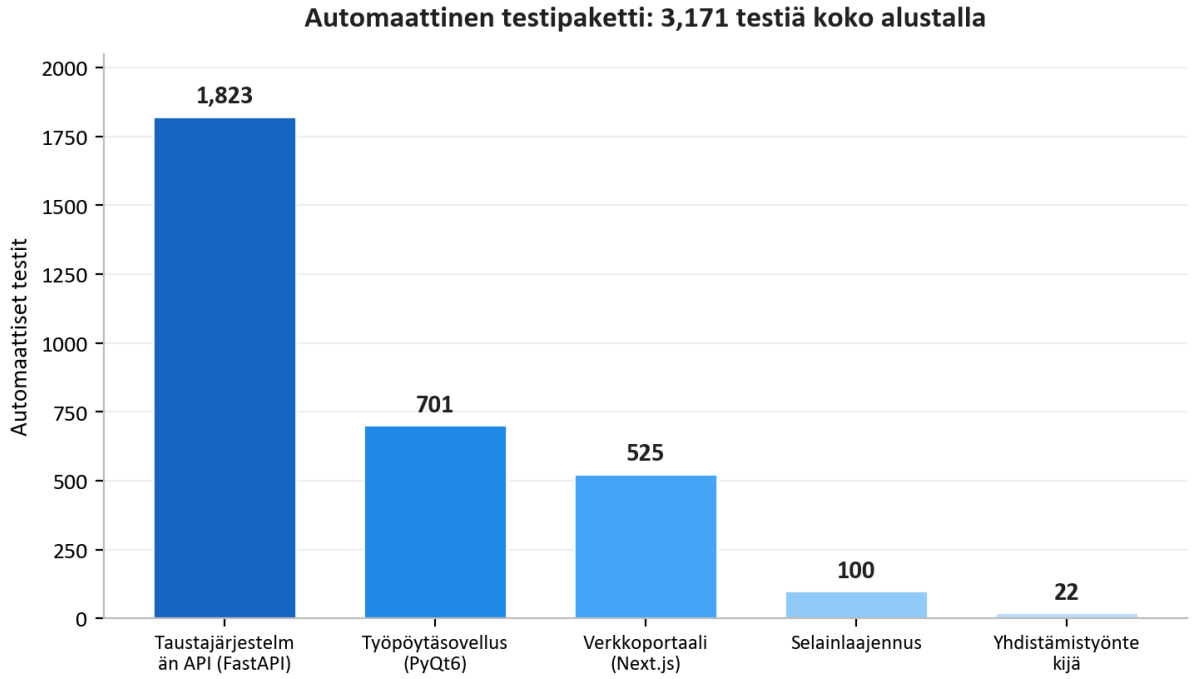
- **Ympäristöjen erottelu.** Kehitys- ja tuotantoympäristöt ovat täysin erillisiä, kummallakin oma infrastruktuurinsa, tallennustilinsä, tietokantansa, salaisuutensa ja aliverkkotunnuksensa. Yhteistä tilaa ei ole.
- **Infrastructure as code.** Koko pilviympäristö määritellään koodina ja katselmoidaan koodina, mikä tekee tietoturva-asemasta auditoitavan ja toistettavan. Arvioija voi lukea tarkalleen, mitkä portit ovat auki, mitkä resurssit ovat yksityisiä ja millä identiteeteillä on mitkäkin oikeudet.
- **Kiinnitetyt, vartioidut käyttöönotot.** Jatkuvan integraation putken jokainen vaihe on kiinnitetty täsmälliseen, muuttumattomaan versioon. Tuotantokäyttöönotot perustuvat tageihin, ne suoritetaan vain suojatun tuotantoputken kautta ja ne ovat pakollisen hyväksynnän takana. Automatisoitu testipaketti toimii julkaisun portinvartijana: käyttöönottoa ei voida toimittaa, jos testit epäonnistuvat.
- **Riippuvuushygienia.** Automatisoitu riippuvuuksien seuranta ehdottaa päivityksiä viikoittain backendiin, työpöytäsovellukseen, web-sovellukseen, infrastruktuuriin ja putkimäärittelyihin, ja riippuvuusauditoinnit ovat osa säännöllistä tietoturvakatselmointiamme.
- **Allekirjoitetut artefaktit.** Työpöytäasennuspaketit on koodiallekirjoitettu, jotta asiakkaat voivat varmistaa asennettavan ohjelmiston aidosti tulevan meiltä.
- **Salaisuuksien kurinalaisuus.** Salaisuudet sijaitsevat holvissa ja suojatuissa putkisalaisuuksissa, eivät koskaan lähdekoodissa.

12. Jatkuva tietoturvatestaus

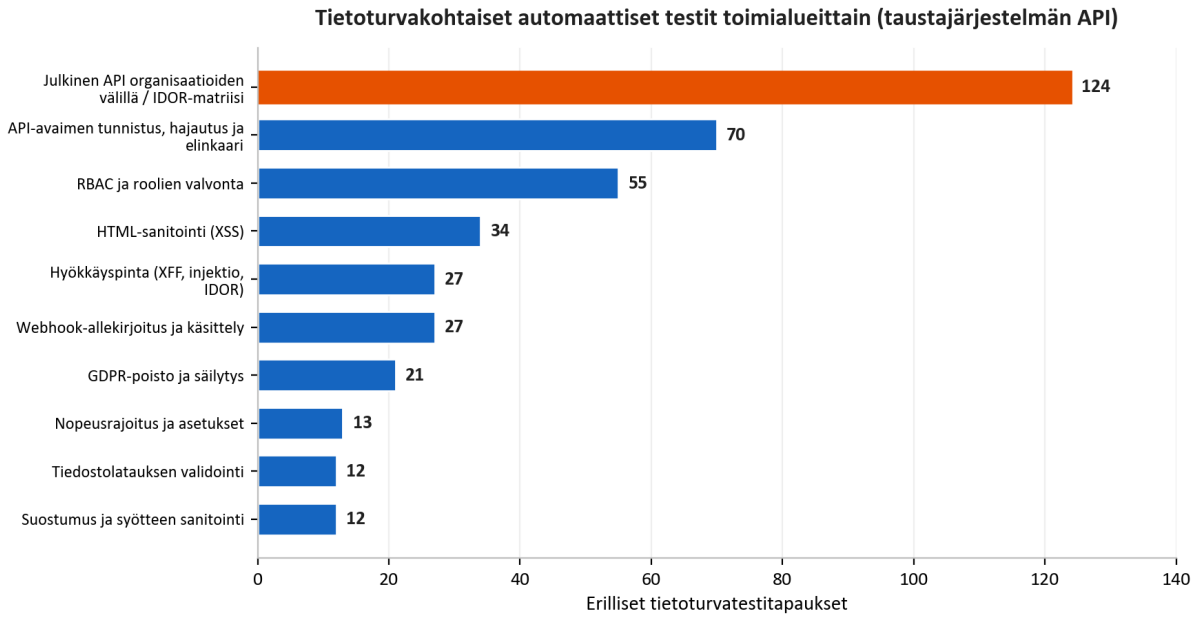
Tämä on varmennustarinamme ydin ja se osa, jota useimmat toimittajat eivät pysty näyttämään. Käsittelemme tietoturvaa jatkuvasti mitattavana asiana, johon kohdistetaan suoritettavia tarkistuksia, emme kertaluonteisesti esitettävänä väitteenä.

12.1 Automatisoitu testipaketti

Alustaa kattaa **3,171 automatisoitua testiä**, jotka ulottuvat backend API:in, työpöytäsovellukseen, web-portaaliin, selainlaajennukseen ja äänen yhdistämisestä vastaavaan workeriin.



Nämä eivät ole vain toiminnallisia testejä. Merkittävä, erillinen tietoturvatestipaketti harjoittaa tässä asiakirjassa aiemmin kuvattuja kontrolleja. Alla oleva kaavio erittelee backend API:n tietoturvakohtaiset testit osa-alueittain.



Monien muiden lisäksi tämä paketti sisältää laajan julkisen API:n matriisin, joka suorittaa jokaisen päätepisteen laillisena käyttäjänä, organisaation omalla API-avaimella ja kilpailevan organisaation API-avaimella ja varmistaa, että jokainen organisaatioiden välinen yritys estetään. Se sisältää kymmeniä hyökkääjämäisiä hyökkäyspintatestejä forwarding header -väärennöksille, header injectionille ja tunnistevuodoille, kohdennetun HTML-puhdistustestipaketin cross-site scripting -tilanteita varten, roolien pakotuksen testit koko roolimallille sekä testit, jotka osoittavat ehdokastietojen todella poistuvan yhtenä kokonaisuutena. Koska nämä testit suoritetaan julkaisun portinvartijana, regressio, joka heikentäisi jotakin näistä kontrolleista, pysäyttäisi julkaisun sen sijaan, että se etenisi asiakkaisiin.

12.2 Tuotantoympäristöä vasten tehtävä penetraatiotestaus

Automatisoidut yksikkötestit todistavat, että kontrollit käyttäytyvät oikein eristyksissä. Todistaaksemme niiden toimivan yhdessä todellisessa käyttöönottossa ylläpidämme toistettavaa penetraatiotestausmenetelmää, joka ajaa todellisia hyökkäysskriptejä käyttöönottua ympäristöä vastaan. Se on järjestetty kuuteen vaiheeseen:

Vaihe	Painopiste	Esimerkkejä siitä, mitä harjoitetaan
1. Staattinen analyysi	Lähdekoodi	Salaisuudet, injektiomallit, vaaralliset funktiot, puuttuva auth, turvaton HTML
2. Arkkitehtuurikatselmointi	Infrastruktuuri	Yksityiset päätepisteet, segmentointi, TLS, salaisuuksien konfiguraatio
3. Hyökkäysvektorianalyysi	Versionhallinta ja pilvi	Haarasuojaukset, identiteetin laajuus, julkinen altistus
4. Tuotantoympäristön penetraatiotestaus	Käynnissä oleva ympäristö	Tunnistautumaton koestus, organisaatioiden välinen pääsy, injektio, token-manipulointi, SSRF, nopeusrajojen purskeet
5. Yritystason pisteytys	Kypsyys	Kuusitoista tietoturvakategoriaa pisteytettynä yritystason vertailupohjaa vasten
6. Riippuvuudet ja toimitusketju	Kolmannen osapuolen riski	Riippuvuuksien CVE-auditointi, kiinnitetyt putkitoiminnot, lock-filen eheys

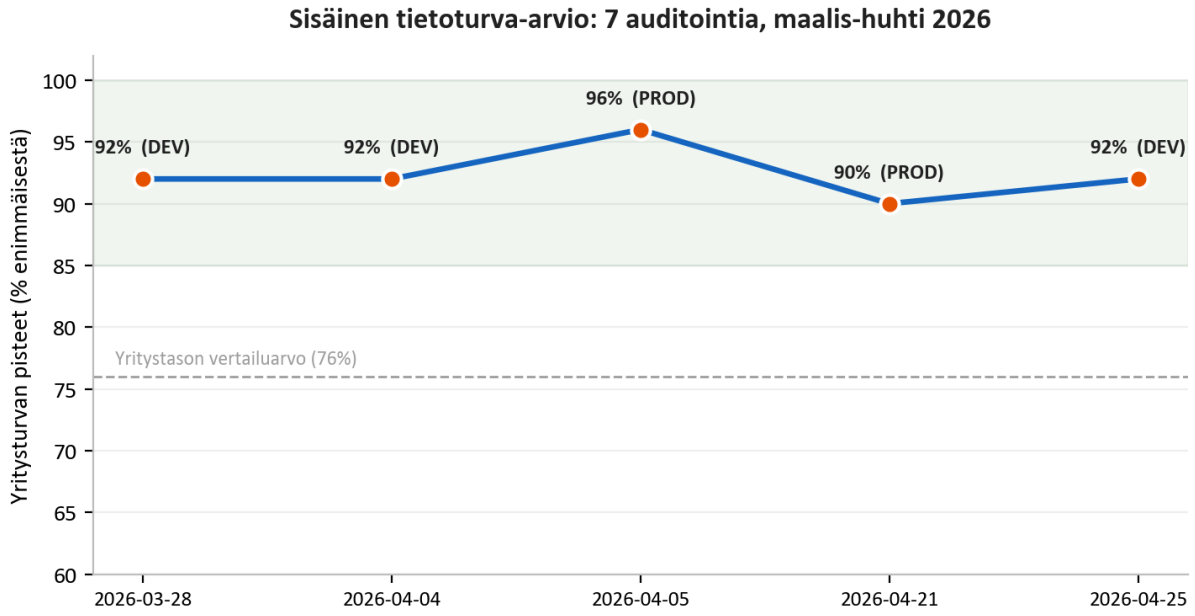
Vaihe 4 on aitoa vastapuolimaista testausta käyttöön otettua järjestelmää vastaan, ei tarkistuslista. Se koestaa suojattuja päätepisteitä ilman tunnuksia ja varmistaa niiden estävän pääsyn; rekisteröi kaksi organisaatiota ja yrittää tavoittaa toisen organisaation tietueita toisen tilillä; injektoi cross-site-scripting- ja server-side-template -hyötykuormia ja varmistaa niiden neutraloituvan; manipuloi todennustokeneita ja varmistaa niiden hylkäämisen; yrittää server-side request forgerya pilven metatietopäätepisteitä vastaan; sekä kuormittaa todennuspäätepisteitä purskeina varmistaakseen, että nopeusrajoitus todella laukeaa tuotantoympäristössä eikä vain teoriassa.

12.3 Ehdokaspalautteen turvallisuustestaus

Koska alusta voi luoda yksityistä kehityspalautetta ehdokkaille, suoritamme kyseistä ominaisuutta vastaan erillistä vastapuolimaisen turvallisuuden ohjelmaa. Se syöttää järjestelmään tarkoituksella kovasanaisia ja vihamielisiä rekrytoijamuistiinpanoja ja varmistaa, ettei ehdokkaalle näkyvä tuloste koskaan sisällä vulgaaria kieltä, ei koskaan paljasta tai liitä rekrytoijan identiteettiä tai yksityistä mielipidettä eikä koskaan käytä tuomitsevia persoonallisuusleimoja. Tämä suojaa sekä ehdokasta, jonka tulee saada rakentavaa ja kunnioittavaa palautetta, että asiakasta, jonka sisäinen mielipide ei saa koskaan vuotaa ulospäin.

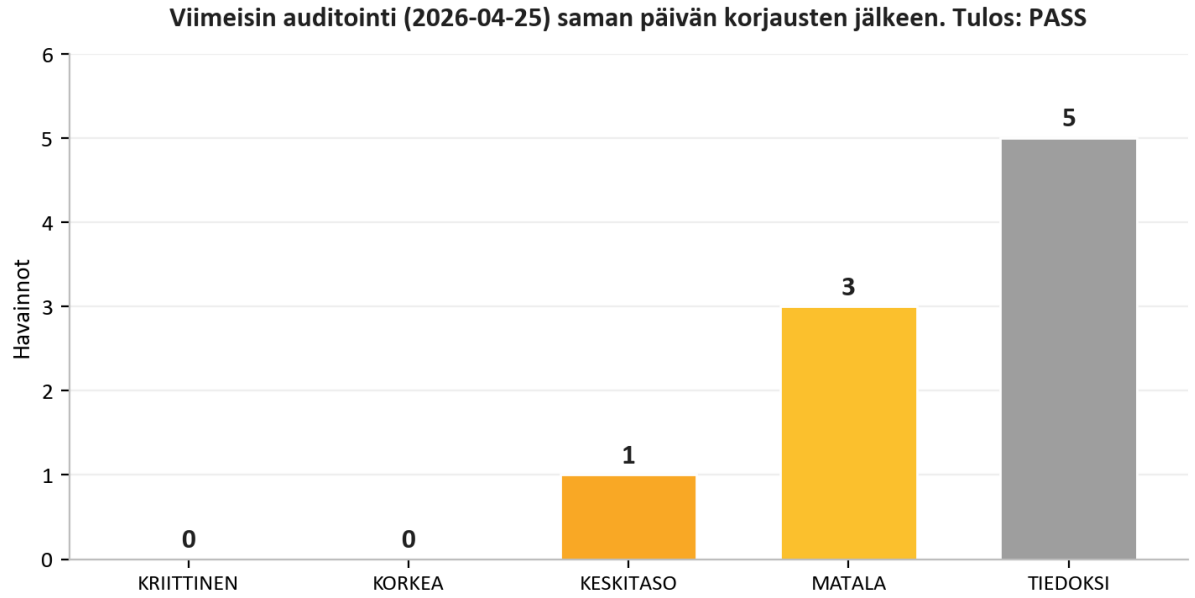
13. Tietoturva-auditointien tulokset

Suoritamme toistuvia tietoturva-auditointeja rakenteellisella, toistettavalla penetraatiotestausmenetelmällä ja laadimme jokaisesta päivätyn raportin, jossa on vakavuusluokitellut havainnot, näyttö ja korjaustoimet. Nämä ovat sisäisiä auditointeja, joita ajetaan oman tietoturvaprosessimme kautta; samojen kontrollien muodollinen kolmannen osapuolen sertifiointi on tiekartallamme. Maaliskuun lopun ja huhtikuun lopun 2026 välillä suoritimme **seven such audits** kehitys- ja tuotantoympäristöissä.



Tulevalle asiakkaalle tärkein tulos on johdonmukaisuus: **kaikissa seitsemässä auditoinnissa critical-havaintoja oli nolla.** Harvinaisissa tilanteissa, joissa esiin nousi vakavampi havainto, se korjattiin nopeasti, usein saman päivän aikana, ja varmistettiin uudelleen. Pisteytysmallia kiristettiin tarkoituksella tämän ajanjakson aikana (mahdollinen maksimipistemäärä nousi, kun lisäsimme arvioitavia kategorioita), minkä vuoksi normalisoitu pistelinja pysyy korkeana, vaikka rimaa nostettiin.

Viimeisin auditointimme, 25 April 2026, havainnollistaa, miten prosessi toimii käytännössä. Kaksi vakavampaa ongelmaa tunnistettiin, molemmat korjattiin ja varmistettiin uudelleen saman päivän aikana, ja auditointi suljettiin lopputuloksella **PASS** ilman nykyisessä uhkamallissa jäljellä olevia suoraan hyödynnettäviä ongelmia.



Auditointi	Ympäristö	Critical	Lopputulos
2026-03-28	Kehitys	0	Ready for production
2026-04-04	Kehitys	0	Enterprise-ready
2026-04-05	Tuotanto	0	Enterprise-ready
2026-04-20	Kehitys	0	Production-ready, notes
2026-04-20	Kehitys	0	Pass with notes
2026-04-21	Tuotanto	0	Safe, no exploitable findings
2026-04-25	Kehitys	0	Pass

Näissä auditoinneissa näkyvä kuvio on rehellisin näyttö, jonka voimme tarjota: ongelmia löydetään, koska etsimme niitä aktiivisesti, ja ne suljetaan nopeasti, koska prosessi on rakennettu sulkemaan ne. Toimittaja, joka ei koskaan raportoi havaintoja, on yleensä toimittaja, joka ei etsi niitä.

---

14. Operatiivinen resilienssi ja jaettu vastuu

14.1 Valvonta ja lokitus

Sovellus- ja alustatelemetria virtaa keskitettyyn log analytics -työtilaan ja sovelluksen valvontapalveluun, mikä antaa meille näkyvyyden saatavuuteen ja toimintaan. Arkaluonteiset toimenpiteet, kuten tietojen poistaminen, oikeudellisten sopimusten hyväksyminen ja AI-kutsut, kirjataan erillisiin auditointitauluihin, joten tärkeisiin tietoihin kohdistuneista toimista säilyy kestävä jälki siitä, kuka teki mitä.

14.2 Varmuuskopiointi ja palautus

Hallittu tietokanta säilyttää automatisoidut varmuuskopiot, ja yksityistä tallennusta suojaavat soft-delete-säilytys sekä blob- että container-tasolla, joten vahingossa tehty tai haitallinen poisto voidaan palauttaa säilytysikkunan sisällä. Kriittisessä infrastruktuurissa on poistolukot, jotka estävät tuotantoresurssien tahattoman purkamisen.

14.3 Jaetun vastuun yhteenveto

Alue	AI Interview Analyzer	Asiakas
Infrastruktuuri, verkko, päivitykset	Kyllä	-
Sovellustietoturva ja AI-putki	Kyllä	-
Salaus, salaisuudet, datan sijainti	Kyllä	-
Käyttäjä- ja roolihallinta	Tarjoaa kontrollit	Hallinnoi käyttäjiä ja rooleja
Säilytyskäytännön konfigurointi	Tarjoaa kontrollit	Asettaa säilytysajan
Ehdokkaan suostumus	Tarjoaa työnkulun	Varmistaa sen käytön
Vahvat loppukäyttäjätunnukset ja SSO	Tukee SSO:ta ja käytäntöjä	Pakottaa sisäisen käytännön

15. Uhkamalli ja OWASP-kartoitus

Suunnittelemme konkreettista joukkoa vastustajia vastaan: ulkoinen hyökkääjä ilman tunnuksia, utelias tai haitallinen yhden organisaation todennettu käyttäjä, joka yrittää päästä toisen organisaation tietoihin, vaarantunut riippuvuus ja sisäinen virhe. Alla oleva taulukko kartoittaa laajalti käytetyt OWASP Top 10 -riskiluokat niihin erityisiin kontrolleihin, joilla niitä tässä alustassa torjutaan; kutakin niistä harjoitetaan kohdassa 12 kuvatulla testauksella.

OWASP-riski	Miten alusta lieventää sitä
Rikkinäinen pääsynhallinta	Roolipohjainen pääsynhallinta kaikissa etuoikeutetuissa päätepisteissä; organisaatiokohtainen rajaus; "not found" organisaatioiden välisessä pääsyssä; tunnisteiden uudelleenkartoitus; organisaatioiden välinen testimatriisi
Kryptografiset epäonnistumiset	TLS 1.2+ siirrossa; AES-256 levossa; bcrypt-salasanojen hajautus; salaisuudet hallitussa holvissa
Injektio	Vain ORM-pohjaiset parametroidut kyselyt; tiukka skeemavalidointi; HTML-puhdistus kirjoitushetkellä
Turvaton suunnittelu	Kerroksellinen defense in depth; uhkamallinnus ja arkkitehtuurikatselmointi jokaisessa auditoinnissa
Tietoturvan virhekonfigurointi	Infrastructure as code; oletuksena estävät verkko-oikeusryhmät; tietoturvaotsakkeet; käytöstä poistetut jaetut tallennusavaimet; API-skeemaa ei paljasteta tuotannossa
Haavoittuvat komponentit	Viikoittainen automatisoitu riippuvuuksien seuranta; riippuvuuksien CVE-auditoinnit säännöllisissä katselmoinneissa
Tunnistamisen ja todennuksen epäonnistumiset	Lyhytikäiset tokenit; nopeusrajoitettu kirjautuminen; sähköpostivahvistus; SSO-tuki; ei selväkielisiä salasanoja
Ohjelmiston ja datan eheyden epäonnistumiset	Kiinnitetyt, muuttumattomat putkivaiheet; allekirjoitetut työpöytäasennuspaketit; webhook-allekirjoitusten varmennus; tageilla vartioidut tuotantokäyttöönotot
Tietoturvalokituksen ja valvonnan epäonnistumiset	Keskitetty telemetria; erilliset auditointitaulut arkaluonteisille toiminnoille
Server-side request forgery	Lähtevät kutsut rajattu luotettuihin päätepisteisiin; SSRF-koestukset penetraatiotestauskehikossa

Tämä kartoitus on varmennusargumenttimme selkäranka: jokaista tunnettua hyökkäysluokkaa kohden on nimetty kontrolli, ja jokaista nimettyä kontrollia kohden on testi.

16. Haavoittuvuuksien hallinta ja vastuullinen ilmoittaminen

Tietoturva ei ole koskaan valmis, joten ylläpidämme jatkuvaa löytämisen ja korjaamisen sykliä.

- **Löytäminen.** Haavoittuvuuksia tulee esiin neljästä lähteestä: automatisoidusta testipaketista, toistuvista penetraatiotestausauditoinneista, automatisoidusta riippuvuuksien seurannasta sekä asiakkaiden tai tutkijoiden raporteista.
- **Luokittelu.** Jokaiselle havainnolle annetaan vakavuusluokka (critical, high, medium, low tai informational) sekä näyttö ja korjauksesta vastaava omistaja, täsmälleen kuten auditointiraporteissamme kirjataan.
- **Korjaustavoitteet.** Critical- ja high-havainnot priorisoidaan välittömään korjaamiseen; auditointihistoriassamme vakavammat havainnot on tyypillisesti ratkaistu ja varmennettu uudelleen saman päivän aikana. Medium- ja sitä alemmat havainnot aikataulutetaan normaaliin ylläpitorytmiin.
- **Varmennus.** Korjaukset testataan uudelleen, ja tarvittaessa käyttöön otettua ympäristöä vasten suoritetaan tuotantotarkistus sen vahvistamiseksi, että ongelma on todella suljettu eikä vain suljettu koodissa.
- **Ilmoittaminen.** Tietoturvahuolista voi ilmoittaa meille suoraan. Kuittaamme raportit, tutkimme ne ja pidämme ilmoittajan ajan tasalla ratkaisuun asti.

17. Vaatimustenmukaisuuskartoitus

17.1 GDPR

GDPR-alue	Alustan toteutus
Oikeusperuste (Art. 6)	Ehdokkaan nimenomainen suostumus kerätään ennen käsittelyä
Tietojen minimointi ja säilytyksen rajoittaminen (Art. 5)	Vain haastatteluun liittyviä tietoja käsitellään; määritettävä säilytys automaattisella poistolla
Oikeus tulla unohdetuksi (Art. 17)	Kaikkien ehdokastietojen poisto yhtenä kokonaisuutena, lokitetulla todisteella poistamisesta
Rekisteröidyn oikeudet (Art. 15 to 20)	Pääsy, poisto, siirrettävyys ja vastustaminen ovat tuettuja
Käsittelijän velvollisuudet (Art. 28)	Data processing agreement hyväksytään rekisteröitymisen yhteydessä ja versioidaan organisaatiokohtaisesti
Käsittelyn turvallisuus (Art. 32)	Salaus, pääsynhallinta, eristys ja jatkuva testaus kuten tässä asiakirjassa kuvataan
Alikäsittelijöiden läpinäkyvyys	Ilmoitetaan data processing agreement -sopimuksessa ennakkoilmoituksella muutoksista

17.2 EU AI Act

Alustaa käsitellään työllistämispäätöksiä tukevana high-risk AI -järjestelmänä, ja ylläpidämme sääntelyn mukaista dokumentaatiota, mukaan lukien läpinäkyvyyskortti, käyttöohjeet ja vaatimustenmukaisuusvakuutus. Keskeiset suojatoimet, ihmisen valvonta, läpinäkyvyys, näyttöön perustuva pisteytys ja tiukat soveltamisalarajat sille, mitä AI arvioi, on kuvattu kohdassa 10. Kehitämme edelleen muodollista vaatimustenmukaisuusdokumentaatiotamme sääntelyn toimeenpanon aikataulun edetessä.

17.3 Hosting-sertifioinnit

Alusta toimii kokonaisuudessaan Microsoft Azure -palvelussa, jonka datakeskuksilla on riippumattomia sertifiointeja, mukaan lukien ISO 27001 ja SOC 2. Nämä sertifioinnit kattavat fyysiset ja alustakerrokset sovelluksemme alapuolella; sovellustason kontrollit ovat niitä, joita on kuvattu kautta tämän asiakirjan.

17.4 Alikäsittelijärekisteri

Alikäsittelijä	Tarkoitus	Alue
Microsoft Azure	Hosting, AI- ja puheenkäsittely, tallennus, transaktionaalinen sähköposti	EU (West Europe, Sweden Central)
Stripe	Tilaus- ja maksunkäsittely	EU (Ireland)
Fakturownia	Laskutus	EU (Poland)
ATS connector (optional)	Hakijaseurantaintegraatio, käytössä vain pyynnöstä	EU

18. Tietoturvan tiekartta

Käsittelemme tietoturvaa jatkuvasti paranevana ohjelmana. Nykyisiä tiekarttamme aloitteita ovat muun muassa monivaiheisen todennuksen vaihtoehtojen vahvistaminen hallinnollisille tileille, tietojen käytön keskitetyn auditointilokituksen laajentaminen, riippuvuuksien ajantasaisuuden jatkuva kiristäminen säännöllisellä rytmillä sekä tässä asiakirjassa kuvattujen kontrollien muodollisen kolmannen osapuolen sertifioinnin edistäminen. Mikään näistä ei ole puute, joka altistaisi asiakasdatan tänään; jokainen niistä on parannus jo valmiiksi kerrokselliseen suojausasemaan.

19. Yhteenveto

AI Interview Analyzer suojaa ehdokkaiden ja asiakkaiden tietoja kerroksellisella arkkitehtuurilla: oletuksena yksityinen verkko ilman julkisia tietopalveluja, vahva identiteetti ja organisaatiokohtainen eristys, sovelluskoodi joka poistaa kokonaisia haavoittuvuusluokkia suunnittelulla, salaus ja EU-datan sijainti sekä tietomalliin rakennetut yksityisyyskontrollit. Alustan erottaa muista näiden väitteiden taustalla oleva näyttö. 3,171 automatisoidun testin, toistettavan tuotantoympäristöä vasten tehtävän penetraatiotestausmenetelmän, erillisen AI-turvallisuusohjelman ja seitsemän nollan critical-havaintoa sisältävän sisäisen tietoturva-auditoinnin historian ansiosta voimme osoittaa, emme vain sanoa, että alusta on turvallinen.

Liite A: Tietoturvakontrollien luettelo

Tiivistetty viite ensisijaisista kontrolleista ja näytöstä, joka tukee kutakin niistä.

Kontrolli	Mekanismi	Näyttö
Siirtosalaus	Vain HTTPS, TLS 1.2+, HTTP uudelleenohjataan	Infrastructure as code; arkkitehtuuriauditointi
Salaus levossa	AES-256-alustasalaus tallennuksessa ja tietokannassa	Alustan konfiguraatio; arkkitehtuuriauditointi
Salasanasuojaus	bcrypt per-salasana salt -arvolla	Versionhallinta; todennustestit
Istunnonhallinta	30 minuutin allekirjoitetut tokenit, mitätöitävä palvelinpuolinen refresh	Versionhallinta; todennustestit
Valtuutus	Neljän roolin pääsynhallinta etuoikeutetuissa päätepisteissä	Roolien pakotuksen testipaketti
Tenant-eristys	Organisaatiokohtainen kyselyrajaus; 404 organisaatioiden välillä	Organisaatioiden välinen testimatriisi
API-avainten turvallisuus	Hajautettu tallennus, rajatut oikeudet, avainkohtaiset nopeusrajat	API-avain-testipaketti
Injektiosuojaus	Vain ORM-pohjaiset parametroidut kyselyt	Staattinen analyysi; injektiotestit
Cross-site scripting -suojaus	HTML-puhdistus kirjoitushetkellä	HTML-puhdistuksen testipaketti
Nopeusrajoitus	Kestävä tietokantapohjainen rajoitin auth-päätepisteissä	Nopeusrajoitustestit; tuotantopursketarkistukset
Webhookien eheys	Palveluntarjoajan allekirjoituksen varmennus raakaa runkoa vasten	Webhook-testipaketti
Salaisuuksien hallinta	Hallittu holvi, purge protection, managed identity	Infrastructure as code; arkkitehtuuriauditointi
Verkkoeristys	Yksityiset päätepisteet; oletuksena estävä segmentointi	Infrastructure as code; arkkitehtuuriauditointi
Tietojen poisto	Yhden kokonaisuuden ketjutettu poisto auditointilokilla	GDPR-poistotestipaketti
Toimitusketju	Kiinnitetyt putkivaiheet; viikoittainen riippuvuuksien seuranta	Putken konfiguraatio; riippuvuusauditointi

Liite B: Usein kysytyt kysymykset tietoturva-arvioijille

Missä tietomme säilytetään? Kokonaan Euroopan unionin sisällä, Microsoft Azure -palvelussa, West Europe -alueella ja AI-käsittely EU-alueilla. Ehdokastiedot eivät koskaan poistu EU:n alueelta.

Käytetäänkö tietojamme AI-mallien kouluttamiseen? Ei. AI-palveluntarjoaja ei käytä asiakasdataa koulutukseen.

Onko tietokanta saavutettavissa internetistä? Ei. Julkinen verkkopääsy on poistettu käytöstä, ja tietokanta on saavutettavissa vain virtuaaliverkon sisäisen yksityisen päätepisteen kautta.

Voiko yksi asiakas nähdä toisen asiakkaan tiedot? Ei. Jokainen kysely rajataan kutsujan organisaatioon, organisaatioiden välinen pääsy palauttaa "not found", ja automatisoitu matriisi testaa tätä eristystä jatkuvasti.

Miten salasanat tallennetaan? Hajautettuina bcrypt-algoritmilla ja yksilöllisellä per-salasana salt -arvolla. Kertakirjautuminen Microsoftin ja Googlen kanssa on tuettu, jolloin salasanaa ei tallenneta.

Tuetteko kertakirjautumista? Kyllä, Microsoftin ja Googlen OAuthin kautta.

Kuinka kauan access tokenit ovat voimassa? Kolmekymmentä minuuttia, paritettuna mitätöitävään palvelinpuoliseen refresh-istuntoon, joka mitätöidään uloskirjautumisessa.

Miten ehdokkaan suostumusta hallitaan? Jokainen ehdokas saa yksilöllisen, kertakäyttöisen suostumuslinkin ja hänen on hyväksyttävä se ennen mitään tallennusta tai analyysiä. Suostumus kirjataan tiettyä rekrytointiprosessia vasten.

Miten tiedot poistetaan? Yhtenä kokonaisuutena, joka kattaa ehdokastietueen, haastattelut, litteraatit, äänen, asiakirjat ja vertailut, määritettävän säilytysaikataulun mukaisesti, lokitetulla todisteella poistamisesta. Ehdokkaat voivat myös pyytää poistoa suoraan.

Onko teillä data processing agreement? Kyllä, se hyväksytään rekisteröitymisen yhteydessä ja versioidaan organisaatiokohtaisesti, mukaan lukien alikäsittelijärekisteri.

Tekeekö AI rekrytointipäätöksiä? Ei. Se tarjoaa vain päätöksenteon tukea; ihminen tarkistaa jokaisen tulosteen ja tekee kaikki päätökset.

Miten todistatte tietoturvaväitteenne? 3,171 automatisoidulla testillä, mukaan lukien erillinen tietoturvatestipaketti, toistettavalla kuusivaiheisella penetraatiotestausmenetelmällä, jota ajetaan tuotantoympäristöjä vastaan, AI-turvallisuuden testiohjelmalla sekä toistuvilla kirjallisilla auditointiraporteilla.

Mitä tapahtuu, kun löydätte haavoittuvuuden? Sille annetaan vakavuusluokka, näyttö ja omistaja, se korjataan prioriteettiaikataulun mukaisesti, varmennetaan uudelleen mukaan lukien tarvittaessa tuotantotarkistukset, ja kirjataan auditointiraporttiin.

Voimmeko suorittaa oman penetraatiotestimme? Tietoturva-arvioinnit voidaan järjestää yhteyshenkilönne kautta asianmukaisen laajuuden ja aikataulutuksen mukaisesti.

Liite C: Sanasto

Termi	Merkitys
AES-256	Vahva symmetrinen salausstandardi, jota käytetään levossa olevien tietojen suojaamiseen
bcrypt	Tarkoitukseen rakennettu salasanan hajautusfunktio per-salasana suolauksella
Managed identity	Alustan myöntämä identiteetti, jonka avulla palvelu voi todentautua ilman tallennettuja avaimia
Private endpoint	Yksityinen verkko-osoite, joka pitää pilvipalvelun poissa julkisesta internetistä
Network security group	Sallivien ja estävien sääntöjen joukko, joka suodattaa aliverkkoon kulkevaa verkkoliikennettä
RBAC	Roolipohjainen pääsynhallinta, jossa oikeudet myönnetään käyttäjän roolin mukaan
IDOR	Insecure direct object reference, pääsynhallinnan virhe, jota vastaan alusta suojautuu
SSRF	Server-side request forgery, hyökkäysluokka, jota koestetaan penetraatiotesteissämme
Web application firewall	Reunakontrolli, joka suodattaa haitallista web-liikennettä
Data processing agreement	Sopimus, joka säätelee, miten käsittelijä käsittelee henkilötietoja rekisterinpitäjän puolesta

Liite D: Yhteystiedot ja asiakirjahallinta

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Tietoturva-arviointia, data processing agreement -sopimuksen kopiota tai EU AI Act -vaatimustenmukaisuusdokumentaatiotamme varten ottakaa yhteyttä omaan yhteyshenkilöönne.

Tämä asiakirja kuvaa AI Interview Analyzer -palvelun tietoturva-asemaa alatunnisteessa ilmoitettuna laatimispäivänä. Se toimitetaan arviointitarkoituksiin eikä muodosta osaa mistään sopimuksesta. Sopimuskohtaiset tietoturvasitoumukset määritellään soveltuvassa sopimuksessa ja data processing agreement -sopimuksessa.