Livre blanc sur la sécurité

Enterprise Security Overview - AI Interview Analyzer

Fournisseur:	AI Interview Analyzer Sp. z o.o.
Adresse:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Classification:	PUBLIC
Date:	24.06.2026

Contents

Livre blanc sur la sécurité

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

Public : Équipes de sécurité d'entreprise, IT et achats

Classification : Public

1. Résumé exécutif

AI Interview Analyzer est une plateforme de recrutement d'entreprise qui enregistre les entretiens avec le consentement explicite du candidat, les transcrit et les structure, puis produit une aide à l'évaluation fondée sur des preuves pour les recruteurs. Étant donné que la plateforme traite des données personnelles de candidats et prend en charge des processus de recrutement, la sécurité et la confidentialité sont considérées comme des contraintes de conception primaires, et non comme des fonctionnalités ajoutées ultérieurement.

Ce livre blanc décrit, en termes concrets et vérifiables, comment nous protégeons les données des clients et des candidats. Il est rédigé pour les personnes qui évaluent les fournisseurs : ingénieurs sécurité, administrateurs IT, délégués à la protection des données et équipes achats. Chaque chiffre de ce document est directement issu de nos propres systèmes d'ingénierie plutôt que de supports marketing.

Le message central est simple : **nous ne nous contentons pas d'affirmer que la plateforme est sécurisée, nous vérifions en continu qu'elle l'est.** Notre base de code contient **3,171 tests automatisés**, dont une suite dédiée à la sécurité qui met à l'épreuve l'authentification, l'autorisation, l'isolation inter-organisation, les défenses contre les injections et la suppression des données. En complément, nous exécutons un dispositif reproductible de tests de pénétration sur des déploiements en production et produisons des rapports d'audit écrits. Au cours de sept audits de sécurité internes en mars et avril 2026, nous avons enregistré **zero critical findings**, notre audit le plus récent s'étant conclu par un verdict de **PASS**. (La certification formelle par un tiers de ces contrôles figure sur notre feuille de route ; voir la section 18.)

Caractéristique de sécurité	Résumé
Hébergement	Microsoft Azure, régions de l'UE uniquement
Modèle réseau	Private endpoints, segmentation réseau par refus par défaut, aucune base de données publique
Chiffrement	AES-256 au repos, TLS 1.2 ou supérieur en transit
Identité	Tokens signés à courte durée de vie, hachage des mots de passe avec bcrypt, prise en charge du SSO
Contrôle d'accès	Contrôle d'accès basé sur les rôles avec isolation stricte par organisation
Secrets	Coffre-fort centralisé de secrets avec accès par managed identity
Confidentialité	Consentement explicite, rétention configurable, effacement par unité unique
IA responsable	Aide à la décision uniquement, humain systématiquement dans la boucle
Assurance	3,171 tests automatisés plus tests de pénétration et audits récurrents

1.1 Comment lire ce document

Les sections 3 à 11 décrivent les contrôles qui protègent les données : architecture, réseau, identité, application, protection des données, confidentialité et cycle de développement sécurisé. Les sections 12 et 13 couvrent notre programme distinctif de tests continus et l'historique de nos audits. Les sections 14 à 17 traitent des opérations, de la modélisation des menaces, de la gestion des vulnérabilités et de la cartographie de conformité. Les annexes fournissent un catalogue de contrôles, une FAQ pour les

évaluateurs et un glossaire qu’une équipe de sécurité peut utiliser directement pendant une évaluation.

2. Périmètre et approche du document

2.1 Ce que couvre ce document

Ce livre blanc couvre l'architecture de sécurité et les pratiques du service AI Interview Analyzer : l'environnement d'hébergement, la conception réseau, la gestion des identités et des accès, les contrôles au niveau applicatif, la protection des données, la confidentialité et l'alignement réglementaire, le cycle de développement sécurisé et notre programme continu de tests de sécurité.

2.2 Ce qui le rend vérifiable

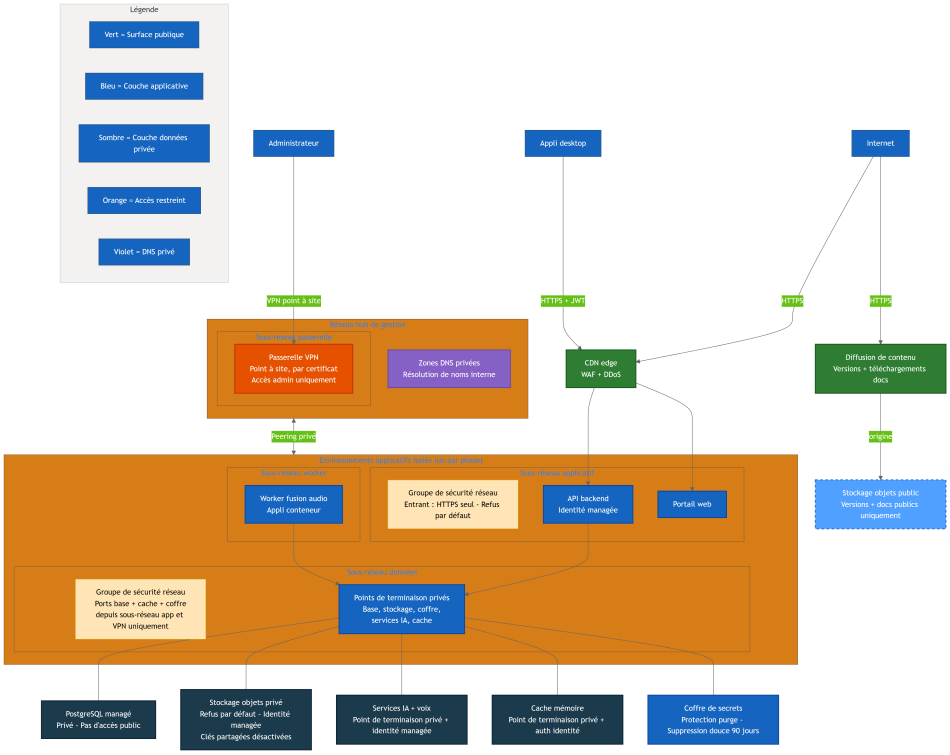
Les affirmations de sécurité des fournisseurs sont faciles à écrire et difficiles à croire. Nous avons donc rattaché chaque affirmation majeure de ce document à un élément concret et quantifiable au sein de nos systèmes d'ingénierie : un contrôle implémenté dans le code, un test qui prouve le bon fonctionnement du contrôle, une définition d'infrastructure qui l'impose, ou un rapport d'audit qui consigne une vérification documentée. Lorsqu'un contrôle fait partie de notre feuille de route future plutôt que d'être livré aujourd'hui, nous l'indiquons explicitement. Nous préférons minimiser nos affirmations et être dignes de confiance plutôt que d'en faire trop et être pris en défaut.

2.3 Responsabilité partagée

La plateforme est fournie sous forme de software as a service. Nous exploitons l'infrastructure, l'application, la chaîne IA et la gestion des données. Le client est responsable de la gestion de ses propres comptes utilisateurs et rôles, de la configuration des durées de rétention des données selon sa politique interne et de la garantie que le consentement du candidat est obtenu via le flux de consentement fourni par la plateforme. La section 14 décrit plus en détail cette répartition.

3. Vue d’ensemble de l’architecture de sécurité

La plateforme est construite comme un petit nombre de services coopérants plutôt qu’un monolithe unique. Une application desktop et un portail web agissent comme clients. Une API backend centrale gère toute la persistance, l’authentification, la facturation, la chaîne IA, le consentement, les e-mails, la gestion des fichiers et les tableaux de bord. Un worker de fusion audio traite les enregistrements de manière asynchrone. Tout état sensible réside derrière l’API backend ; les clients ne communiquent jamais directement avec la base de données, le stockage ou les services IA.



Le schéma ci-dessus montre la topologie de production avec des noms de ressources volontairement généralisés. Trois principes y sont visibles :

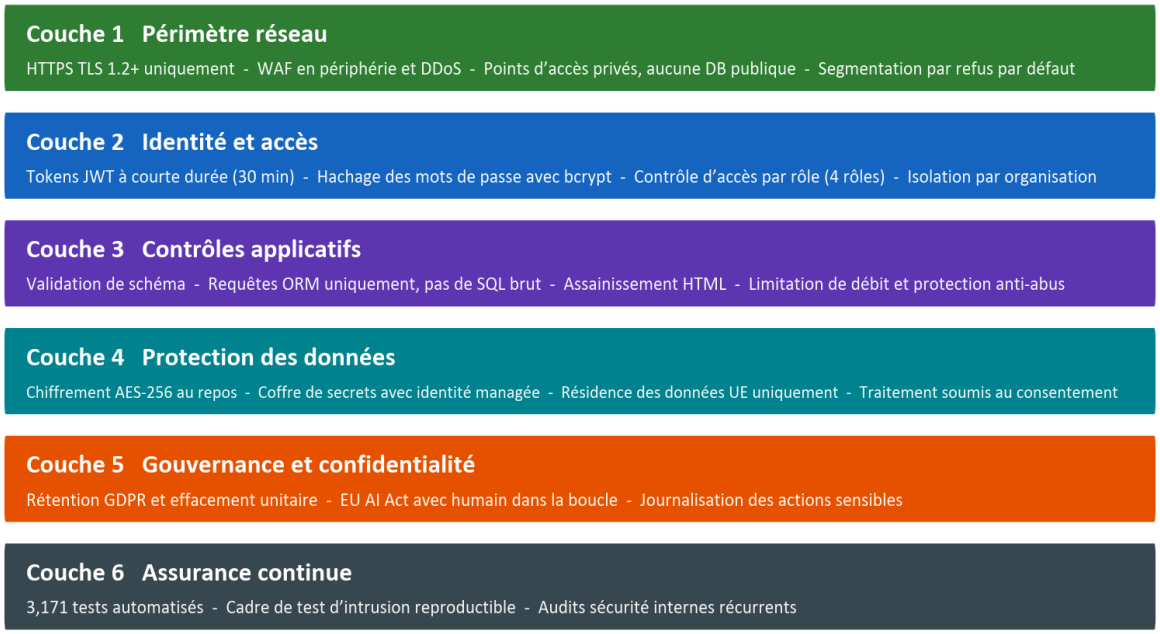
- **Aucune exposition directe des services de données.** La base de données, le stockage privé d’objets, les services IA et le cache ont l’accès réseau public désactivé et ne sont accessibles que via des private endpoints au sein d’un réseau virtuel isolé. Le coffre-fort de secrets est atteint par l’application via un private endpoint et est en outre protégé par une authentification d’identité de la plateforme et des politiques d’accès au moindre privilège, de sorte que tout accès nécessite une identité valide et autorisée, indépendamment du chemin réseau.
- **Une surface publique séparée.** Le seul stockage public d’objets contient les téléchargements de versions et les documents publics. Il ne contient jamais de données de candidats. Le trafic applicatif orienté client passe par une couche en périphérie qui fournit un web application firewall, une protection contre les distributed-denial-of-service et la diffusion de contenu.
- **L’accès administratif est contrôlé.** Les opérateurs accèdent aux ressources internes uniquement via un VPN point à site basé sur certificat vers un réseau hub de gestion, et non via l’internet public.

Chaque étape de déploiement (développement et production) est un environnement totalement isolé avec son propre réseau, ses comptes de stockage, sa base de données et ses secrets. Les données de production des clients ne sont jamais présentes dans les environnements inférieurs. Un hub de gestion partagé ne contient que la passerelle VPN et le DNS privé, appairés de manière privée à chaque environnement.

4. Défense en profondeur

Aucun contrôle unique n'est considéré comme suffisant pour arrêter toutes les attaques. La plateforme superpose des contrôles indépendants de sorte que l'échec d'une couche n'expose pas les données. Les couches ci-dessous sont chacune implémentées et, comme décrit dans la section 12, testées individuellement.

Modèle de sécurité en couches : contrôles indépendants à chaque niveau



Couche	Contrôles représentatifs
Périphérie réseau	Transport TLS uniquement, WAF en périphérie et protection DDoS, private endpoints, segmentation par refus par défaut
Identité et accès	Tokens signés à courte durée de vie, hachage bcrypt, contrôle d'accès basé sur les rôles, isolation par organisation
Application	Validation de schéma sur toutes les entrées, accès aux données via ORM uniquement, encodage des sorties, limitation de débit
Protection des données	Chiffrement au repos, coffre-fort de secrets avec managed identity, résidence des données dans l'UE, traitement soumis au consentement
Gouvernance et confidentialité	Rétention configurable, effacement par unité unique, IA avec humain dans la boucle, journalisation d'audit
Assurance continue	Suite de tests automatisés, tests de pénétration reproductibles, audits de sécurité internes récurrents

La suite de ce document passe en revue chacune de ces couches, puis décrit comment nous démontrons en continu qu'elles tiennent.

5. Sécurité réseau

5.1 Privé par défaut

Le niveau de données est privé par construction. La base de données managée PostgreSQL a l'accès réseau public désactivé et n'est accessible que via un private endpoint. Le stockage privé d'objets est configuré pour refuser l'accès réseau par défaut, désactive entièrement les shared access keys et n'est accessible que via managed identity depuis le sous-réseau applicatif. Le cache, les services IA et le coffre-fort de secrets sont également atteints via des private endpoints avec résolution DNS privée.

En pratique, cela signifie qu'il n'existe aucune chaîne de connexion exposée sur internet vers la base de données et aucune URL de stockage publique pour l'audio des candidats : l'accès réseau public à la base de données et au stockage privé est purement et simplement désactivé. Le coffre-fort de secrets est atteint par l'application via un private endpoint et protégé par l'authentification d'identité de la plateforme et des politiques d'accès au moindre privilège, les identités applicatives ne disposant que d'un accès en lecture aux seuls secrets dont elles ont besoin ; les secrets ne peuvent donc pas être récupérés sans identité valide et autorisée. La surface d'attaque qu'un adversaire externe peut simplement toucher est limitée aux endpoints HTTPS de l'application derrière la couche en périphérie.

5.2 Segmentation réseau

Chaque environnement est divisé en sous-réseaux distincts pour la couche applicative, la couche de données et le worker asynchrone. Chaque sous-réseau est régi par un network security group dont la règle finale refuse tout trafic entrant. Le sous-réseau applicatif n'accepte que le HTTPS entrant. Le sous-réseau de données n'accepte que les ports spécifiques de base de données, de cache et de coffre-fort, et uniquement depuis le sous-réseau applicatif ou le VPN administratif. Cela signifie que même un attaquant qui parviendrait d'une manière ou d'une autre à atteindre la couche applicative ne pourrait pas pivoter librement vers la couche de données ; les seuls chemins autorisés sont ceux que l'application utilise légitimement.

5.3 La périphérie

Le trafic applicatif public est placé derrière une couche en périphérie fournissant un web application firewall, une protection DDoS et un CDN. Les téléchargements de versions et de documents sont servis depuis un compte de stockage public dédié via une front door de diffusion de contenu, totalement séparée du stockage privé qui contient les données des candidats. Les deux plans de stockage ne se mélangent jamais : une mauvaise configuration du plan public ne peut pas exposer les données privées des candidats, car il s'agit de comptes distincts avec des règles réseau distinctes.

5.4 Accès administratif

Il n'existe aucun endpoint administratif public vers le réseau privé. Les opérateurs se connectent via une passerelle VPN point à site utilisant une authentification basée sur certificat. L'accès administratif à la base de données et au cache n'est possible qu'à l'intérieur de ce tunnel, puisque ces services ont l'accès réseau public désactivé. Cela maintient les opérations quotidiennes entièrement hors de l'internet public.

6. Gestion des identités et des accès

6.1 Authentification

Les sessions utilisateur sont établies avec un token d'accès signé valable trente minutes, associé à un token de rafraîchissement distinct, opaque et côté serveur. Les tokens d'accès sont vérifiés à chaque requête, et l'utilisateur est revalidé par rapport à la base de données (y compris une vérification de compte actif) plutôt que d'accorder sa confiance au seul contenu du token. La déconnexion révoque immédiatement la session de rafraîchissement côté serveur, de sorte qu'un token de rafraîchissement volé ne peut pas survivre à une déconnexion.

Les mots de passe ne sont jamais stockés en clair. Ils sont hachés avec bcrypt en utilisant un sel unique par mot de passe. Pour les organisations qui préfèrent le single sign-on, la plateforme prend en charge la connexion OAuth avec Microsoft et Google, auquel cas aucun mot de passe n'est conservé.

La propriété de l'adresse e-mail est vérifiée au moyen d'un lien de vérification à usage unique et à durée limitée avant qu'un compte auto-enregistré ne soit considéré comme vérifié, et les renvois d'e-mails de vérification sont soumis à limitation de débit pour empêcher les abus.

6.2 Contrôle d'accès basé sur les rôles

L'autorisation est appliquée via un modèle à quatre rôles de privilèges croissants : interviewer, hiring manager, recruiter et administrator. L'accès aux opérations privilégiées est imposé par des dépendances côté serveur qui vérifient à la fois le rôle et le statut de vérification de l'appelant. Ces vérifications de rôle protègent bien plus d'une centaine d'opérations API distinctes.

Rôle	Capacités typiques
Interviewer	Mène les entretiens qui lui sont attribués ; ne voit que les entretiens qui lui sont attribués
Hiring manager	Gère les recrutements qu'il possède ou dont il est membre
Recruiter	Gestion complète des recrutements et des candidats au sein de l'organisation
Administrator	Paramètres de l'organisation, facturation, administration des utilisateurs et des API keys

Au-delà des vérifications grossières de rôle, la plateforme applique des règles de visibilité au niveau des données. Les hiring managers ne voient que les recrutements qu'ils ont créés ou dont ils sont membres ; les interviewers ne voient que les entretiens qui leur sont attribués. Le privilège est donc imposé à la fois au niveau de « quelle action » et au niveau de « quels enregistrements ».

6.3 Isolation par organisation

La plateforme est multi-tenant, et l'isolation des tenants est traitée comme un contrôle de sécurité de premier ordre. Chaque identité authentifiée porte un identifiant d'organisation, et les requêtes de données sont limitées à cette organisation. Lorsqu'un utilisateur demande un enregistrement appartenant à une autre organisation, la plateforme renvoie une réponse « not found » plutôt que de révéler que l'enregistrement existe. Les identifiants internes de la base de données ne sont jamais exposés sur le réseau ; l'API présente des identifiants d'affichage et les remappe à chaque requête, ce qui élimine une classe courante d'attaques d'énumération inter-tenant.

Il ne s'agit pas seulement d'une intention de conception. Comme décrit dans la section 12, notre suite automatisée exécute une large matrice inter-organisation qui tente d'atteindre les données d'une organisation à l'aide des identifiants d'une autre et vérifie que chacune de ces tentatives échoue.

6.4 Accès programmatique

Pour les intégrations, les organisations disposant des offres éligibles peuvent émettre des API keys. Les clés utilisent un préfixe reconnaissable, portent 128 bits d'entropie et ne sont stockées que sous forme de hachage ; la clé brute n'est affichée qu'une

seule fois lors de sa création et jamais plus ensuite. Chaque clé porte un périmètre d'autorisation explicite (lecture, écriture ou intégration ATS), peut être restreinte à des réseaux sources spécifiques, peut être révoquée instantanément et est soumise à des limites de débit par clé dérivées du niveau d'abonnement de l'organisation. La vérification des clés utilise une comparaison sûre vis-à-vis du temps afin d'éviter les fuites d'information par le temps de réponse.

7. Sécurité applicative

L’application est écrite de manière à éliminer des catégories entières de vulnérabilités plutôt qu’à les corriger au cas par cas.

• **Injection.** Tout accès à la base de données passe par un object-relational mapper avec des requêtes paramétrées. La base de code ne contient aucun SQL brut formaté par chaînes de caractères. Cela élimine structurellement l’injection SQL.

• **Validation des entrées.** Chaque corps de requête est validé par rapport à un schéma strict avant d’atteindre la logique métier. Les charges utiles surdimensionnées sont rejetées et les endpoints de liste sont paginés pour borner l’utilisation des ressources.

• **Encodage des sorties et cross-site scripting.** Le texte fourni par l’utilisateur et généré par l’IA est traité comme non fiable. Lorsque le contenu doit être rendu en HTML, il passe par un assainisseur à liste d’autorisation au moment de l’écriture, et une suite de tests dédiée confirme que les balises script, les gestionnaires d’événements et les URLs javascript sont supprimés.

• **Mass assignment.** Les opérations de mise à jour utilisent des schémas explicites excluant les champs privilégiés tels que le rôle, l’organisation et le solde de crédits, de sorte qu’un client ne peut pas élever ses privilèges en publiant des champs supplémentaires.

• **Limitation de débit.** Les endpoints d’authentification et exposés aux abus sont soumis à une limitation de débit à l’aide d’un limiteur durable, adossé à la base de données, qui survit aux redémarrages et fonctionne correctement sur plusieurs instances applicatives. La connexion, l’inscription, la réinitialisation de mot de passe et le renvoi des vérifications ont chacun leurs propres limites. La résolution de l’IP client est renforcée contre l’usurpation des headers de transfert.

• **Webhooks.** Les webhooks entrants des fournisseurs de paiement et d’e-mail sont vérifiés par rapport aux signatures du fournisseur sur le corps brut de la requête avant d’être traités.

• **Téléversements de fichiers.** Les téléversements sont plafonnés en taille, validés, stockés sous des identifiants générés plutôt que sous des noms fournis par l’utilisateur, et contraints par requête et par organisation.

• **Headers de sécurité.** En production, les réponses portent des headers strict transport security, des options de type de contenu et de frame, une politique de referrer et une permissions policy restrictive, et suppriment les bannières du serveur et du framework.

8. Protection des données

8.1 Chiffrement

Toutes les données sont chiffrées au repos à l'aide d'AES-256 via les couches de chiffrement de stockage et de base de données de la plateforme Azure. Tout le trafic réseau est servi exclusivement sur HTTPS avec TLS 1.2 ou supérieur ; le HTTP en clair est redirigé vers HTTPS à tous les niveaux. En production, l'API et le portail web émettent des headers strict transport security ainsi qu'un ensemble de headers de durcissement, et suppriment les bannières de version du serveur et du framework.

8.2 Gestion des secrets

Les secrets applicatifs sont conservés dans un coffre-fort centralisé de secrets avec purge protection activée et une fenêtre de soft-delete de quatre-vingt-dix jours. Les applications s'authentifient aux ressources Azure à l'aide de managed identities attribuées par le système plutôt qu'au moyen de clés de longue durée de vie ; par exemple, le stockage privé a les shared access keys entièrement désactivées, de sorte que l'accès n'est possible qu'au moyen d'attributions de rôles fondées sur l'identité et limitées à la ressource individuelle. Les politiques d'accès au coffre-fort accordent aux principaux applicatifs un accès en lecture seule aux secrets spécifiques dont ils ont besoin, selon le principe du moindre privilège.

8.3 Résidence des données

Toutes les données des clients et des candidats sont stockées et traitées au sein de l'Union européenne. L'hébergement de l'application, la base de données, le stockage, le cache et les secrets résident en Europe de l'Ouest, et le traitement IA s'exécute dans des régions de l'UE. Le fournisseur d'IA n'utilise pas les données client pour entraîner ses modèles.

8.4 Le cycle de vie d'un entretien unique

La manière la plus claire de comprendre les contrôles de protection des données est de suivre un entretien de bout en bout. Le consentement est capturé et enregistré avant tout traitement. Le téléversement est chiffré en transit. La transcription et l'analyse s'exécutent dans des centres de données situés dans l'UE. Les résultats sont écrits dans un stockage chiffré. Chaque enregistrement est ensuite régi par une horloge de rétention unique qui se termine par une suppression en cascade journalisée. À tout moment, les droits du candidat tels que le retrait du consentement, la suppression, l'accès ou la portabilité peuvent interrompre ce flux.

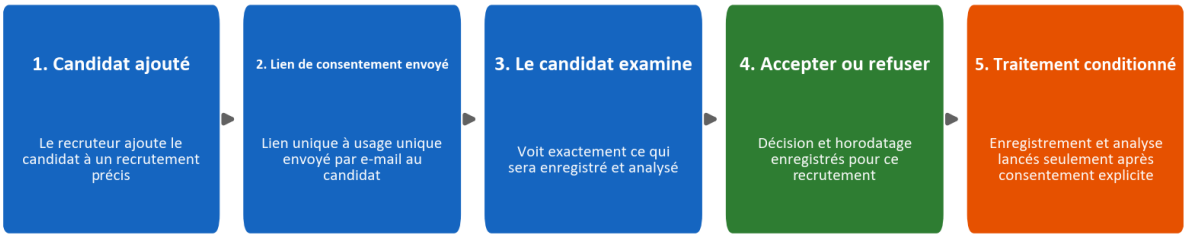
9. Protection de la vie privée dès la conception et GDPR

La confidentialité est intégrée au modèle de données et au workflow, et non ajoutée uniquement par la politique.

9.1 Consentement

Aucun entretien n'est enregistré ni analysé sans le consentement explicite du candidat. Lorsqu'un candidat est ajouté à un recrutement, la plateforme émet par e-mail un lien de consentement unique et à usage unique. Le candidat examine ce qui va se passer puis accepte ou refuse. L'état du consentement, y compris l'heure de réponse, est enregistré pour ce recrutement spécifique, de sorte que le consentement est toujours limité à un processus de recrutement concret plutôt qu'accordé globalement.

Consentement candidat : explicite et enregistré avant tout traitement

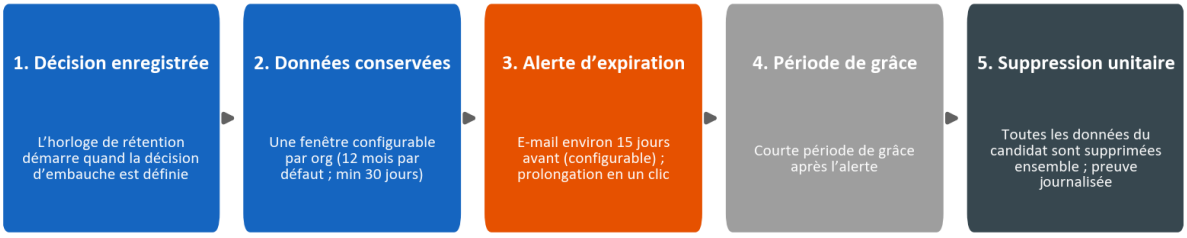


9.2 Rétention et effacement

La rétention des données est configurable par organisation, avec une valeur par défaut de douze mois et un minimum configurable de trente jours, et peut être surchargée pour chaque candidat. Il existe une seule horloge de rétention pour les données d'un candidat, et non un minuteur distinct par artefact. L'horloge démarre lorsqu'une décision de recrutement est enregistrée. Avant l'expiration des données, la plateforme envoie un avertissement (par défaut environ quinze jours à l'avance) et propose une extension en un clic. Lorsque les données sont supprimées, elles le sont comme une unité unique : l'enregistrement du candidat, les entretiens, les transcriptions, les enregistrements audio, les documents et les comparaisons sont tous supprimés ensemble, et la suppression est consignée dans un journal d'audit. Il n'existe aucun résidu partiel ou orphelin.

Le cycle de vie ci-dessous montre cette horloge unique et la manière dont elle converge vers une suppression en cascade unique avec une preuve journalisée d'effacement.

Rétention des données : une horloge par candidat, suppression unitaire



9.3 Droits des personnes concernées et sous-traitants

La plateforme prend en charge les droits des personnes concernées requis au titre du GDPR, notamment l'accès, la suppression, la portabilité, l'opposition et l'explication. Le traitement est réalisé dans le cadre d'un DPA que les clients acceptent lors de l'inscription et qui est versionné par organisation. Nos sous-traitants et leurs rôles, tous situés dans l'UE ou couverts par des garanties appropriées, sont divulgués dans cet accord, et les clients reçoivent un préavis de toute modification. La section 17 contient le registre des sous-traitants et la cartographie de conformité article par article.

10. IA responsable et EU AI Act

La plateforme relève de la catégorie à haut risque du EU AI Act parce qu'elle soutient des décisions d'emploi, et nous traitons cette classification avec sérieux.

La règle déterminante du produit est la suivante : **l'IA est une aide à la décision, pas un décideur.** Le système n'accepte ni ne rejette jamais automatiquement un candidat. Il transcrit la parole, structure les questions et les réponses, note les réponses par rapport à des critères définis par le recruteur et rédige un retour, puis un humain examine chaque résultat avant son utilisation. Cela maintient fermement un humain dans la boucle.

Il est tout aussi important de préciser ce que l'IA ne fait pas. Elle n'évalue pas la personnalité, le « fit culturel », l'état émotionnel, le ton de la voix, l'accent, le genre, l'âge, l'origine ethnique, l'apparence ou le langage corporel. La notation est ancrée dans des preuves issues de la transcription et dans des critères définis par le recruteur, et les noms des candidats sont exclus des entrées d'évaluation afin de réduire les biais. Nous publions une fiche de transparence, une documentation utilisateur et une déclaration de conformité décrivant le système, ses limites et ses garde-fous.

Contrôle d'IA responsable	Fonctionnement
Humain dans la boucle	Chaque score et chaque retour sont examinés par un recruteur avant utilisation
Aucune décision automatisée	Le système n'accepte ni ne rejette jamais automatiquement un candidat
Notation fondée sur des preuves	Les scores font référence à des preuves issues de la transcription
Conception anti-biais	Noms exclus de l'évaluation ; le fond est noté plutôt que le style
Limites de périmètre	La personnalité, l'émotion, l'accent et les caractéristiques protégées ne sont jamais évalués
Sécurité du retour candidat	Le retour privé au candidat passe par un garde-fou de génération et de validation

Ces contraintes ne sont pas seulement énoncées dans la documentation ; elles sont encodées dans la couche de prompts IA et mises à l'épreuve par un programme de tests dédié à la sécurité de l'IA décrit dans la section 12.3.

11. Cycle de développement sécurisé

La sécurité est imposée dans la façon dont nous construisons et livrons les logiciels, pas seulement dans le système en fonctionnement.

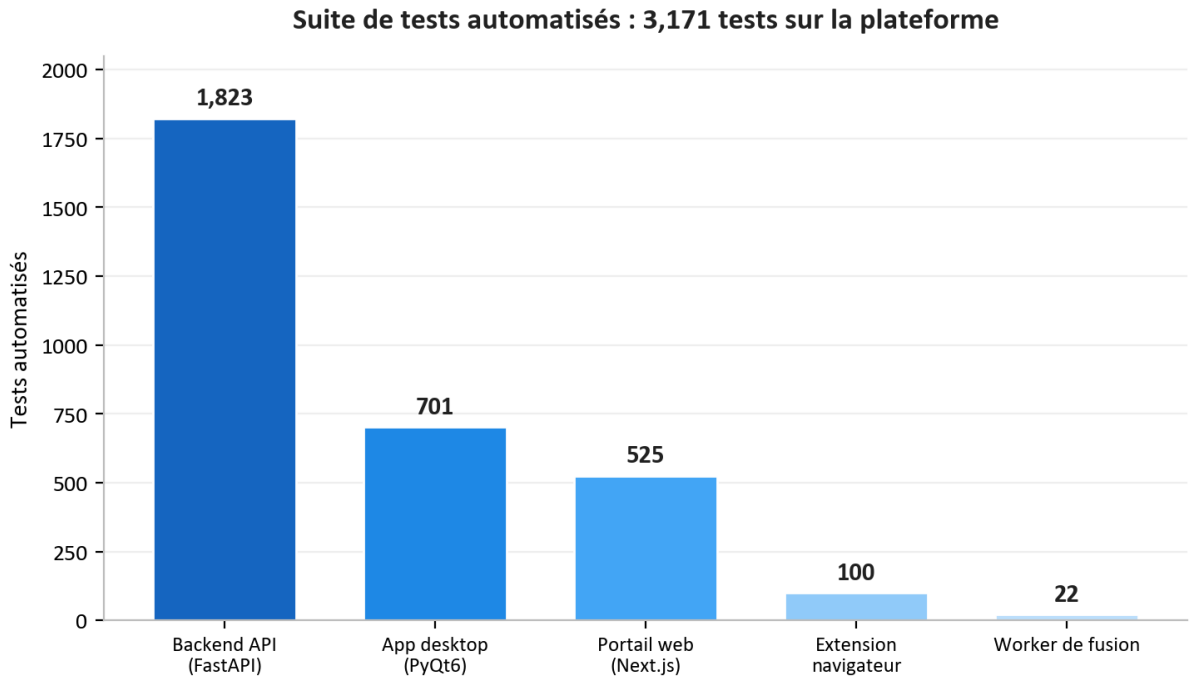
- **Séparation des environnements.** Le développement et la production sont totalement séparés, chacun avec sa propre infrastructure, ses comptes de stockage, sa base de données, ses secrets et ses sous-domaines. Il n'existe aucun état partagé.
- **Infrastructure as code.** L'ensemble de l'environnement cloud est défini comme du code et revu comme du code, ce qui rend la posture de sécurité auditable et reproductible. Un évaluateur peut lire exactement quels ports sont ouverts, quelles ressources sont privées et quelles identités possèdent quelles autorisations.
- **Déploiements épinglés et contrôlés.** Chaque étape du pipeline de continuous integration est épinglée à une version exacte et immuable. Les déploiements de production sont fondés sur des tags, s'exécutent uniquement via le pipeline de production protégé et sont soumis à une approbation obligatoire. La suite de tests automatisés sert de garde de mise en production : un déploiement ne peut pas être livré si les tests échouent.
- **Hygiène des dépendances.** Un suivi automatisé des dépendances propose des mises à jour chaque semaine sur le backend, le desktop, le web, l'infrastructure et les définitions de pipeline, et les audits de dépendances font partie de notre revue périodique de sécurité.
- **Artefacts signés.** Les installateurs desktop sont signés numériquement, afin que les clients puissent vérifier que le logiciel qu'ils installent provient réellement de nous.
- **Discipline des secrets.** Les secrets résident dans le coffre-fort et dans les secrets protégés du pipeline, jamais dans le code source.

12. Tests de sécurité continus

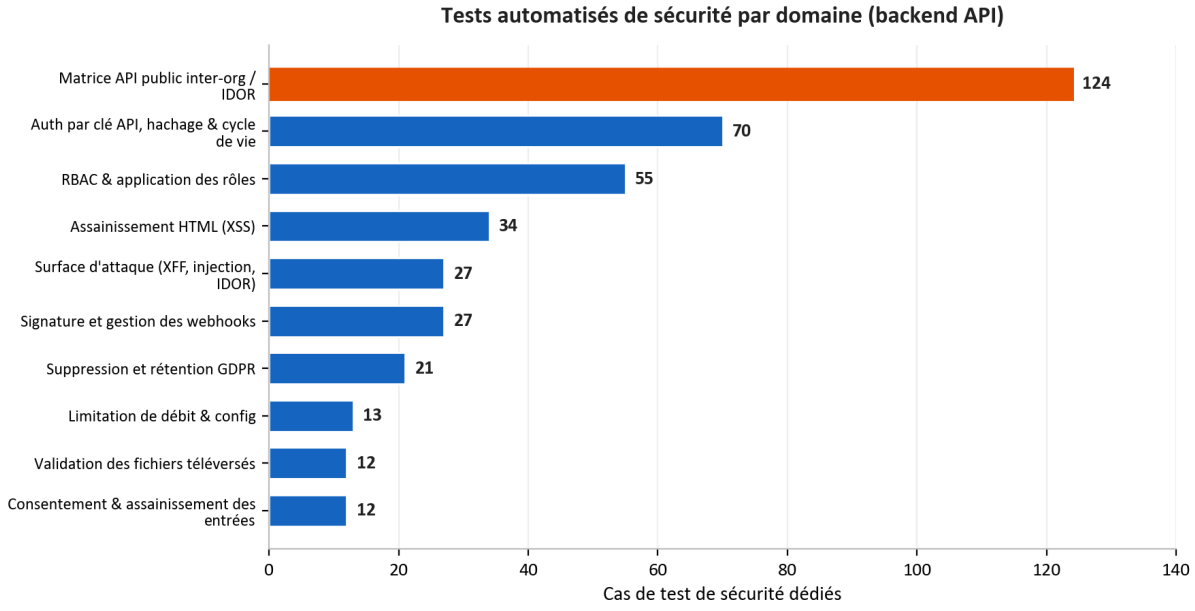
Il s'agit du cœur de notre dispositif d'assurance et de la partie que la plupart des fournisseurs ne peuvent pas montrer. Nous considérons la sécurité comme quelque chose qui doit être mesuré en continu, au moyen de vérifications exécutables, plutôt qu'affirmé une seule fois.

12.1 La suite de tests automatisés

La plateforme est couverte par **3,171 tests automatisés** couvrant l'API backend, l'application desktop, le portail web, l'extension navigateur et le worker de fusion audio.



Il ne s'agit pas seulement de tests fonctionnels. Une suite de sécurité substantielle et dédiée met à l'épreuve les contrôles décrits précédemment dans ce document. Le graphique ci-dessous détaille les tests spécifiques à la sécurité dans l'API backend par domaine.



Parmi beaucoup d'autres, cette suite inclut une large matrice d'API publiques qui exécute chaque endpoint en tant qu'utilisateur légitime, en tant qu'API key propre à l'organisation et en tant qu'API key d'une organisation rivale, en vérifiant que chaque tentative inter-organisation est bloquée. Elle comprend des dizaines de tests adversariaux de surface d'attaque pour l'usurpation de forwarding headers, l'injection de headers et la fuite d'identifiants, une suite ciblée d'assainissement HTML pour le cross-site scripting, des tests d'application des rôles pour l'ensemble du modèle de rôles, et des tests qui prouvent que les données des candidats sont réellement supprimées en tant qu'unité. Comme ces tests s'exécutent comme garde de mise en production, une régression affaiblissant l'un quelconque de ces contrôles bloquerait la livraison au lieu d'atteindre les clients.

12.2 Tests de pénétration en environnement réel

Les tests unitaires automatisés prouvent que les contrôles se comportent correctement en isolation. Pour prouver qu'ils tiennent ensemble dans un déploiement réel, nous maintenons une méthodologie reproductible de tests de pénétration qui exécute de véritables scripts d'attaque contre un environnement en fonctionnement. Elle est organisée en six phases :

Phase	Domaine	Exemples de ce qui est testé
1. Analyse statique	Code source	Secrets, modèles d'injection, fonctions dangereuses, authentification manquante, HTML non sûr
2. Revue d'architecture	Infrastructure	Private endpoints, segmentation, TLS, configuration des secrets
3. Analyse des vecteurs d'attaque	Contrôle de source et cloud	Protection des branches, périmètre des identités, exposition publique
4. Tests de pénétration en direct	Environnement en fonctionnement	Sondage non authentifié, accès inter-organisation, injection, altération de tokens, SSRF, rafales de rate limiting
5. Scoring entreprise	Maturité	Seize catégories de sécurité notées par rapport à une base de référence entreprise
6. Dépendances et supply chain	Risque tiers	Audit de CVE des dépendances, actions de pipeline épinglées, intégrité des lock files

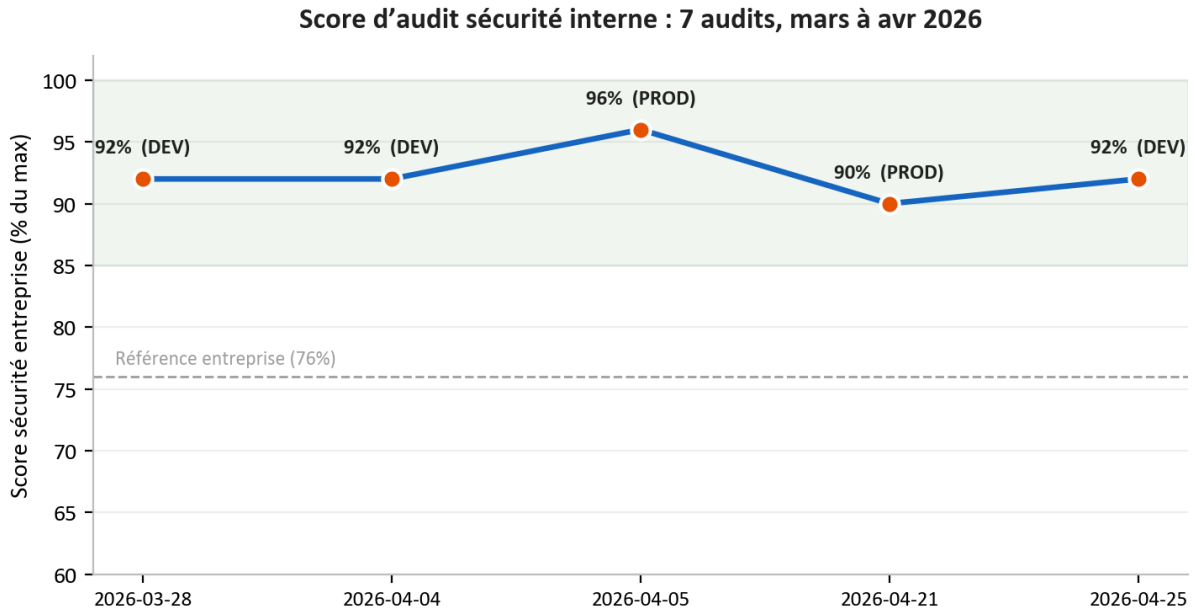
La phase 4 correspond à un véritable test adversarial contre un système déployé, et non à une checklist. Elle sonde les endpoints protégés sans identifiants et confirme qu'ils refusent l'accès ; elle enregistre deux organisations et tente d'atteindre les enregistrements de l'une avec le compte de l'autre ; elle injecte des charges utiles de cross-site-scripting et de server-side-template et confirme qu'elles sont neutralisées ; elle altère des tokens d'authentification et confirme qu'ils sont rejetés ; elle tente des server-side request forgery contre des endpoints de métadonnées cloud ; et elle provoque des rafales sur les endpoints d'authentification pour confirmer que la limitation de débit se déclenche réellement dans l'environnement en direct, et pas seulement en théorie.

12.3 Tests de sécurité du retour candidat

Parce que la plateforme peut générer un retour de développement privé pour les candidats, nous exécutons un programme de sécurité adversariale distinct sur cette fonctionnalité. Il alimente délibérément le système avec des notes de recruteurs dures et hostiles et confirme que la sortie orientée candidat ne contient jamais de vulgarité, ne révèle ni n'attribue jamais l'identité d'un recruteur ou une opinion privée, et n'applique jamais d'étiquettes de personnalité péjoratives. Cela protège à la fois le candidat, qui doit recevoir un retour constructif et respectueux, et le client, qui ne doit jamais voir une opinion interne fuiter vers l'extérieur.

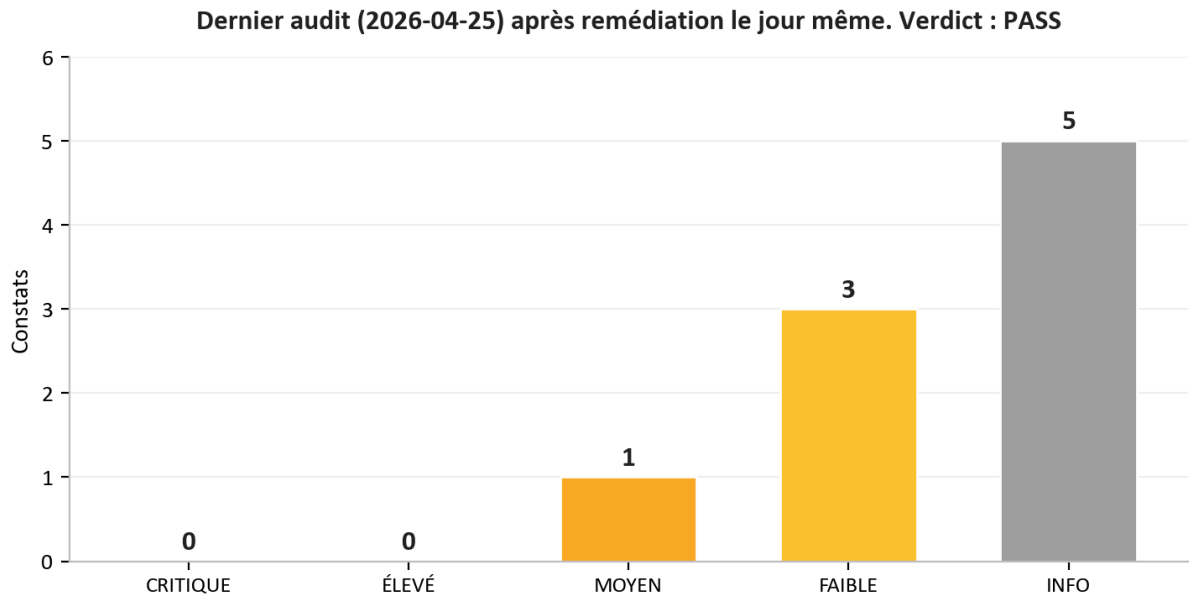
13. Résultats des audits de sécurité

Nous menons des audits de sécurité récurrents à l'aide d'une méthodologie structurée et reproductible de tests de pénétration, et chacun donne lieu à un rapport daté avec constats classés par gravité, preuves et remédiation. Il s'agit d'audits internes exécutés par notre propre processus de sécurité ; la certification formelle par un tiers des mêmes contrôles figure sur notre feuille de route. Entre la fin mars et la fin avril 2026, nous avons réalisé **seven such audits** sur les environnements de développement et de production.



Le résultat qui importe le plus pour un client potentiel est la constance : **across all seven audits there were zero critical findings.** Dans les rares cas où un problème de gravité supérieure apparaissait, il était corrigé rapidement, souvent le jour même, puis revérifié. La grille de notation a été délibérément durcie au cours de cette période (le score maximal possible a été relevé à mesure que nous ajoutions davantage de catégories à évaluer), raison pour laquelle la courbe de score normalisé reste élevée même si le niveau d'exigence a augmenté.

Notre audit le plus récent, le 25 April 2026, illustre la manière dont le processus fonctionne en pratique. Deux problèmes de gravité supérieure ont été identifiés, tous deux ont été corrigés et revérifiés le jour même, et l'audit s'est clôturé avec un verdict de **PASS** sans aucun problème exploitable restant dans le modèle de menace actuel.



Audit	Environnement	Critical	Verdict
2026-03-28	Développement	0	Prêt pour la production
2026-04-04	Développement	0	Prêt pour l’entreprise
2026-04-05	Production	0	Prêt pour l’entreprise
2026-04-20	Développement	0	Prêt pour la production, remarques
2026-04-20	Développement	0	Réussite avec remarques
2026-04-21	Production	0	Sûr, aucun constat exploitable
2026-04-25	Développement	0	Réussite

Le schéma observé sur ces audits constitue la preuve la plus honnête que nous puissions offrir : des problèmes sont trouvés, parce que nous les recherchons activement, et ils sont clos rapidement, parce que le processus est conçu pour les clore. Un fournisseur qui ne signale jamais de constat est généralement un fournisseur qui ne cherche pas.

---

14. Résilience opérationnelle et responsabilité partagée

14.1 Supervision et journalisation

La télémétrie applicative et de plateforme alimente un espace de travail centralisé d'analyse des journaux et un service de supervision applicative, nous donnant de la visibilité sur la disponibilité et le comportement. Les actions sensibles telles que la suppression de données, l'acceptation d'accords juridiques et les invocations d'IA sont enregistrées dans des tables d'audit dédiées, de sorte qu'il existe une trace durable de qui a fait quoi sur des données importantes.

14.2 Sauvegarde et reprise

La base de données managée conserve des sauvegardes automatisées, et le stockage privé est protégé par une rétention soft-delete à la fois sur les blobs et les conteneurs, de sorte qu'une suppression accidentelle ou malveillante peut être restaurée dans la fenêtre de rétention. L'infrastructure critique est protégée par des verrous de suppression afin d'empêcher le démontage accidentel des ressources de production.

14.3 Résumé de la responsabilité partagée

Domaine	AI Interview Analyzer	Client
Infrastructure, réseau, correctifs	Oui	-
Sécurité applicative et chaîne IA	Oui	-
Chiffrement, secrets, résidence des données	Oui	-
Administration des utilisateurs et des rôles	Fournit les contrôles	Gère les utilisateurs et les rôles
Configuration de la politique de rétention	Fournit les contrôles	Définit la fenêtre de rétention
Consentement du candidat	Fournit le workflow	Veille à son utilisation
Identifiants robustes pour les utilisateurs finaux et SSO	Prend en charge le SSO et la politique	Applique la politique interne

15. Modèle de menace et cartographie OWASP

Nous concevons la sécurité face à un ensemble concret d'adversaires : un attaquant externe sans identifiants, un utilisateur authentifié curieux ou malveillant d'une organisation tentant d'accéder aux données d'une autre organisation, une dépendance compromise et une erreur interne. Le tableau ci-dessous cartographie les catégories de risques largement utilisées de l'OWASP Top 10 aux contrôles spécifiques qui les traitent dans cette plateforme, chacun étant mis à l'épreuve par les tests décrits dans la section 12.

Risque OWASP	Comment la plateforme l'atténue
Broken access control	Contrôle d'accès basé sur les rôles sur chaque endpoint privilégié ; limitation par organisation ; « not found » sur l'accès inter-organisation ; remappage des identifiants ; matrice de tests inter-organisation
Cryptographic failures	TLS 1.2+ en transit ; AES-256 au repos ; hachage des mots de passe avec bcrypt ; secrets dans un coffre-fort managé
Injection	Requêtes paramétrées via ORM uniquement ; validation stricte des schémas ; assainissement HTML au moment de l'écriture
Insecure design	Défense en profondeur par couches ; modélisation des menaces et revue d'architecture à chaque audit
Security misconfiguration	Infrastructure as code ; groupes réseau par refus par défaut ; headers de sécurité ; shared storage keys désactivées ; schéma API non exposé en production
Vulnerable components	Suivi automatisé hebdomadaire des dépendances ; audits de CVE des dépendances lors des revues périodiques
Identification and authentication failures	Tokens à courte durée de vie ; connexion avec limitation de débit ; vérification e-mail ; prise en charge du SSO ; aucun mot de passe en clair
Software and data integrity failures	Étapes de pipeline épinglées et immuables ; installateurs desktop signés ; vérification de signature des webhooks ; déploiements de production contrôlés par tags
Security logging and monitoring failures	Télémétrie centralisée ; tables d'audit dédiées pour les actions sensibles
Server-side request forgery	Appels sortants limités à des endpoints de confiance ; sondes SSRF dans le dispositif de tests de pénétration

Cette cartographie constitue l'ossature de notre argumentaire d'assurance : pour chaque classe d'attaque bien connue, il existe un contrôle nommé, et pour chaque contrôle nommé, il existe un test.

16. Gestion des vulnérabilités et divulgation responsable

La sécurité n’est jamais achevée ; nous exécutons donc une boucle continue de découverte et de remédiation.

• **Découverte.** Les vulnérabilités sont détectées à partir de quatre sources : la suite de tests automatisés, les audits récurrents de tests de pénétration, le suivi automatisé des dépendances et les signalements des clients ou des chercheurs.

• **Triage.** Chaque constat se voit attribuer un niveau de gravité (critical, high, medium, low ou informational), avec preuves et responsable de remédiation, exactement comme consigné dans nos rapports d’audit.

• **Objectifs de remédiation.** Les constats critical et high sont priorisés pour une remédiation immédiate ; dans notre historique d’audit, les constats de gravité supérieure ont généralement été résolus et revérifiés le jour même. Les constats medium et inférieurs sont planifiés dans le cycle normal de maintenance.

• **Vérification.** Les correctifs sont retestés et, lorsque c’est pertinent, une vérification en direct est exécutée sur l’environnement déployé pour confirmer que le problème est réellement clos, et pas seulement clos dans le code.

• **Divulgation.** Les préoccupations de sécurité peuvent nous être signalées directement. Nous accusons réception des signalements, enquêtons et tenons l’auteur informé jusqu’à la résolution.

17. Cartographie de conformité

17.1 GDPR

Domaine GDPR	Implémentation dans la plateforme
Base juridique (Art. 6)	Consentement explicite du candidat capturé avant traitement
Minimisation des données et limitation de conservation (Art. 5)	Seules les données pertinentes pour l'entretien sont traitées ; rétention configurable avec suppression automatique
Droit à l'effacement (Art. 17)	Suppression par unité unique de toutes les données du candidat, avec preuve journalisée d'effacement
Droits de la personne concernée (Art. 15 to 20)	Accès, suppression, portabilité et opposition sont pris en charge
Obligations du sous-traitant (Art. 28)	DPA accepté lors de l'inscription et versionné par organisation
Sécurité du traitement (Art. 32)	Chiffrement, contrôle d'accès, isolation et tests continus comme décrit dans ce document
Transparence des sous-traitants	Divulguée dans le DPA avec préavis en cas de modification

17.2 EU AI Act

La plateforme est traitée comme un système d'IA à haut risque soutenant les décisions d'emploi, et nous maintenons une documentation alignée sur le règlement, comprenant une fiche de transparence, une documentation utilisateur et une déclaration de conformité. Les principaux garde-fous, la supervision humaine, la transparence, la notation fondée sur des preuves et les limites strictes du périmètre de ce que l'IA évalue sont décrits dans la section 10. Nous continuons à faire mûrir notre documentation formelle de conformité à mesure que le calendrier de mise en œuvre du règlement progresse.

17.3 Certifications d'hébergement

La plateforme s'exécute entièrement sur Microsoft Azure, dont les centres de données disposent de certifications indépendantes, notamment ISO 27001 et SOC 2. Ces certifications couvrent les couches physiques et de plateforme sous-jacentes à notre application ; les contrôles de la couche applicative sont ceux décrits tout au long de ce document.

17.4 Registre des sous-traitants

Sous-traitant	Finalité	Région
Microsoft Azure	Hébergement, traitement IA et vocal, stockage, e-mail transactionnel	UE (West Europe, Sweden Central)
Stripe	Traitement des abonnements et des paiements	UE (Ireland)
Fakturownia	Facturation	UE (Poland)
Connecteur ATS (optionnel)	Intégration applicant-tracking, activée uniquement sur demande	UE

18. Feuille de route sécurité

Nous traitons la sécurité comme un programme d’amélioration continue. Les initiatives actuellement sur notre feuille de route comprennent le renforcement des options d’authentification multifacteur pour les comptes administratifs, l’extension de la journalisation d’audit centralisée des accès aux données, la poursuite du durcissement régulier de l’actualité des dépendances et l’avancement de la certification formelle par un tiers des contrôles décrits dans ce document. Aucun de ces points ne constitue une lacune exposant les données client aujourd’hui ; chacun est une amélioration d’une posture déjà multicouche.

19. Résumé

AI Interview Analyzer protège les données des candidats et des clients grâce à une architecture multicouche : un réseau privé par défaut sans services de données publics, une identité forte et une isolation par organisation, un code applicatif qui élimine des classes entières de vulnérabilités, le chiffrement et la résidence des données dans l'UE, ainsi que des contrôles de confidentialité intégrés au modèle de données. Ce qui distingue la plateforme est la preuve derrière ces affirmations. Avec 3,171 tests automatisés, une méthodologie reproductible de tests de pénétration en environnement réel, un programme dédié à la sécurité de l'IA et un historique de sept audits de sécurité internes avec zero critical findings, nous pouvons montrer, et non seulement dire, que la plateforme est sécurisée.

Annexe A : Catalogue des contrôles de sécurité

Une référence condensée des contrôles primaires et des preuves qui étayent chacun d'eux.

Contrôle	Mécanisme	Preuve
Chiffrement du transport	HTTPS uniquement, TLS 1.2+, HTTP redirigé	Infrastructure as code ; audit d'architecture
Chiffrement au repos	Chiffrement de plateforme AES-256 sur le stockage et la base de données	Configuration de la plateforme ; audit d'architecture
Protection des mots de passe	bcrypt avec sel par mot de passe	Contrôle de source ; tests d'authentification
Gestion des sessions	Tokens signés de 30 minutes, rafraîchissement côté serveur révocable	Contrôle de source ; tests d'authentification
Autorisation	Contrôle d'accès à quatre rôles sur les endpoints privilégiés	Suite de tests d'application des rôles
Isolation des tenants	Limitation des requêtes par organisation ; 404 en cas d'accès inter-organisation	Matrice de tests inter-organisation
Sécurité des API keys	Stockage haché, autorisations limitées, limites de débit par clé	Suite de tests des API keys
Défense contre les injections	Requêtes paramétrées via ORM uniquement	Analyse statique ; tests d'injection
Défense contre le cross-site scripting	Assainissement HTML au moment de l'écriture	Suite de tests d'assainissement HTML
Limitation de débit	Limiteur durable adossé à la base de données sur les endpoints d'authentification	Tests de rate limiting ; vérifications de rafales en direct
Intégrité des webhooks	Vérification de signature du fournisseur sur le corps brut	Suite de tests des webhooks
Gestion des secrets	Coffre-fort managé, purge protection, managed identity	Infrastructure as code ; audit d'architecture
Isolation réseau	Private endpoints ; segmentation par refus par défaut	Infrastructure as code ; audit d'architecture
Suppression des données	Suppression en cascade par unité unique avec journal d'audit	Suite de tests de suppression GDPR
Supply chain	Étapes de pipeline épinglées ; suivi hebdomadaire des dépendances	Configuration du pipeline ; audit des dépendances

Annexe B : Questions fréquentes pour les évaluateurs sécurité

Où nos données sont-elles stockées ? Entièrement au sein de l'Union européenne, sur Microsoft Azure, en West Europe avec traitement IA dans des régions de l'UE. Les données des candidats ne quittent jamais l'UE.

Nos données sont-elles utilisées pour entraîner des modèles d'IA ? Non. Le fournisseur d'IA n'utilise pas les données client pour l'entraînement.

La base de données est-elle accessible depuis internet ? Non. L'accès réseau public est désactivé et la base de données n'est accessible que via un private endpoint à l'intérieur du réseau virtuel.

Un client peut-il voir les données d'un autre client ? Non. Chaque requête est limitée à l'organisation de l'appelant, les accès inter-organisation renvoient « not found », et une matrice automatisée teste en continu cette isolation.

Comment les mots de passe sont-ils stockés ? Hachés avec bcrypt et un sel unique par mot de passe. Le single sign-on avec Microsoft et Google est pris en charge, auquel cas aucun mot de passe n'est stocké.

Prenez-vous en charge le single sign-on ? Oui, via Microsoft et Google OAuth.

Quelle est la durée de validité des tokens d'accès ? Trente minutes, associés à une session de rafraîchissement côté serveur révocable qui est invalidée lors de la déconnexion.

Comment le consentement du candidat est-il géré ? Chaque candidat reçoit un lien de consentement unique et à usage unique et doit accepter avant tout enregistrement ou analyse. Le consentement est enregistré pour le processus de recrutement spécifique.

Comment les données sont-elles supprimées ? Comme une unité unique couvrant l'enregistrement du candidat, les entretiens, les transcriptions, l'audio, les documents et les comparaisons, selon une planification de rétention configurable, avec une preuve journalisée d'effacement. Les candidats peuvent également demander directement la suppression.

Avez-vous un DPA ? Oui, accepté lors de l'inscription et versionné par organisation, y compris le registre des sous-traitants.

L'IA prend-elle des décisions de recrutement ? Non. Elle fournit uniquement une aide à la décision ; un humain examine chaque résultat et prend toutes les décisions.

Comment prouvez-vous vos affirmations de sécurité ? Au moyen de 3,171 tests automatisés comprenant une suite de sécurité dédiée, une méthodologie reproductible de tests de pénétration en six phases exécutée sur des environnements en direct, un programme de tests de sécurité de l'IA et des rapports d'audit écrits récurrents.

Que se passe-t-il lorsque vous trouvez une vulnérabilité ? Un niveau de gravité lui est attribué avec preuves et responsable, elle est corrigée selon un calendrier priorisé, revérifiée y compris au moyen de vérifications en direct lorsque pertinent, puis consignée dans un rapport d'audit.

Pouvons-nous mener notre propre test de pénétration ? Des évaluations de sécurité peuvent être organisées via votre représentant de compte selon un périmètre et un calendrier appropriés.

Annexe C : Glossaire

Terme	Signification
AES-256	Norme robuste de chiffrement symétrique utilisée pour protéger les données au repos
bcrypt	Fonction de hachage de mots de passe conçue à cet effet avec salage par mot de passe
Managed identity	Identité émise par la plateforme permettant à un service de s'authentifier sans clés stockées
Private endpoint	Adresse de réseau privé qui maintient un service cloud hors de l'internet public
Network security group	Ensemble de règles d'autorisation et de refus qui filtrent le trafic réseau vers un sous-réseau
RBAC	Contrôle d'accès basé sur les rôles, accordant des autorisations selon le rôle d'un utilisateur
IDOR	Insecure direct object reference, faille de contrôle d'accès contre laquelle la plateforme se défend
SSRF	Server-side request forgery, classe d'attaque sondée dans nos tests de pénétration
Web application firewall	Contrôle en périphérie qui filtre le trafic web malveillant
Data processing agreement	Contrat régissant la manière dont un sous-traitant traite des données personnelles pour le compte d'un responsable de traitement

Annexe D : Contact et contrôle du document

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Pour une évaluation de sécurité, une copie de notre DPA ou notre documentation de conformité au EU AI Act, veuillez contacter votre représentant de compte.

Ce document décrit la posture de sécurité du service AI Interview Analyzer à la date de génération indiquée dans le pied de page. Il est fourni à des fins d'évaluation et ne fait partie d'aucun contrat. Les engagements contractuels de sécurité spécifiques sont définis dans l'accord applicable et le DPA.