Λευκή Βίβλος Ασφάλειας

Enterprise Security Overview - AI Interview Analyzer

Πάροχος:	AI Interview Analyzer Sp. z o.o.
Διεύθυνση:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Ταξινόμηση:	PUBLIC
Ημερομηνία:	24.06.2026

Contents

Λευκή Βίβλος Ασφάλειας

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

Κοινό: Ομάδες ασφάλειας επιχειρήσεων, IT και προμηθειών

Κατάταξη: Δημόσιο

1. Εκτελεστική Σύνοψη

Το AI Interview Analyzer είναι μια επιχειρησιακή πλατφόρμα προσλήψεων που καταγράφει συνεντεύξεις με ρητή συγκατάθεση του υποψηφίου, τις απομαγνητοφωνεί και τις δομεί, και παράγει υποστήριξη αξιολόγησης βασισμένη σε αποδεικτικά στοιχεία για τους recruiters. Επειδή η πλατφόρμα διαχειρίζεται προσωπικά δεδομένα υποψηφίων και υποστηρίζει διαδικασίες πρόσληψης, η ασφάλεια και η ιδιωτικότητα αντιμετωπίζονται ως πρωταρχικοί σχεδιαστικοί περιορισμοί και όχι ως χαρακτηριστικά που προστίθενται αργότερα.

Αυτή η λευκή βίβλος περιγράφει, με συγκεκριμένους και επαληθεύσιμους όρους, πώς προστατεύουμε τα δεδομένα πελατών και υποψηφίων. Είναι γραμμένη για τα πρόσωπα που αξιολογούν προμηθευτές: μηχανικούς ασφάλειας, διαχειριστές IT, υπευθύνους προστασίας δεδομένων και προμήθειες. Κάθε στοιχείο σε αυτό το έγγραφο προέρχεται απευθείας από τα δικά μας μηχανικά συστήματα και όχι από υλικό marketing.

Το κεντρικό μήνυμα είναι απλό: **δεν απλώς δηλώνουμε ότι η πλατφόρμα είναι ασφαλής, αλλά το δοκιμάζουμε συνεχώς.** Η βάση κώδικά μας περιέχει **3,171 αυτοματοποιημένα tests**, συμπεριλαμβανομένης μιας αποκλειστικής σουίτας ασφάλειας που ελέγχει authentication, authorization, απομόνωση μεταξύ οργανισμών, άμυνες έναντι injection και διαγραφή δεδομένων. Επιπλέον, εκτελούμε μια επαναλήψιμη υποδομή penetration-testing σε ενεργές αναπτύξεις και παράγουμε γραπτές αναφορές ελέγχου. Σε επτά εσωτερικούς ελέγχους ασφάλειας τον Μάρτιο και τον Απρίλιο 2026, καταγράψαμε **zero critical findings**, με τον πιο πρόσφατο έλεγχο να κλείνει με ετυμηγορία **PASS**. (Η επίσημη πιστοποίηση αυτών των ελέγχων από τρίτο μέρος περιλαμβάνεται στον οδικό μας χάρτη· βλ. Ενότητα 18.)

Χαρακτηριστικό ασφάλειας	Σύνοψη
Φιλοξενία	Microsoft Azure, μόνο περιοχές EE
Μοντέλο δικτύου	Private endpoints, δικτυακή τμηματοποίηση default-deny, χωρίς δημόσια βάση δεδομένων
Κρυπτογράφηση	AES-256 σε αδράνεια, TLS 1.2 ή υψηλότερο κατά τη μεταφορά
Ταυτότητα	Υπογεγραμμένα tokens σύντομης διάρκειας, bcrypt κατακερματισμός κωδικών, υποστήριξη SSO
Έλεγχος πρόσβασης	Έλεγχος πρόσβασης βάσει ρόλων με αυστηρή απομόνωση ανά οργανισμό
Secrets	Κεντρικό secrets vault με πρόσβαση μέσω managed identity
Ιδιωτικότητα	Ρητή συγκατάθεση, παραμετροποιήσιμη διατήρηση, διαγραφή ενιαίας μονάδας
Υπεύθυνη AI	Μόνο υποστήριξη αποφάσεων, ο άνθρωπος πάντα στον βρόχο
Διασφάλιση	3,171 αυτοματοποιημένα tests συν επαναλαμβανόμενα penetration tests και έλεγχοι

1.1 Πώς να Διαβάσετε Αυτό το Έγγραφο

Οι Ενότητες 3 έως 11 περιγράφουν τους ελέγχους που προστατεύουν τα δεδομένα: αρχιτεκτονική, δίκτυο, ταυτότητα, εφαρμογή, προστασία δεδομένων, ιδιωτικότητα και τον κύκλο ζωής ασφαλούς ανάπτυξης. Οι Ενότητες 12 και 13 καλύπτουν το διακριτό μας πρόγραμμα συνεχών δοκιμών και το ιστορικό ελέγχων μας. Οι Ενότητες 14 έως 17 καλύπτουν τις λειτουργίες, το threat modeling, τη διαχείριση ευπαθειών και τη χαρτογράφηση συμμόρφωσης. Τα παραρτήματα παρέχουν έναν κατάλογο

ελέγχων, ένα FAQ για αξιολογητές και ένα γλωσσάριο που μια ομάδα ασφάλειας μπορεί να χρησιμοποιήσει απευθείας κατά τη διάρκεια μιας αξιολόγησης.

2. Πεδίο Εφαρμογής και Προσέγγιση του Εγγράφου

2.1 Τι Καλύπτει Αυτό το Έγγραφο

Αυτή η λευκή βίβλος καλύπτει την αρχιτεκτονική ασφάλειας και τις πρακτικές της υπηρεσίας AI Interview Analyzer: το περιβάλλον φιλοξενίας, τον σχεδιασμό του δικτύου, τη διαχείριση ταυτότητας και πρόσβασης, τους ελέγχους σε επίπεδο εφαρμογής, την προστασία δεδομένων, την ιδιωτικότητα και την κανονιστική ευθυγράμμιση, τον κύκλο ζωής ασφαλούς ανάπτυξης και το πρόγραμμά μας συνεχών δοκιμών ασφάλειας.

2.2 Τι την Καθιστά Επαληθεύσιμη

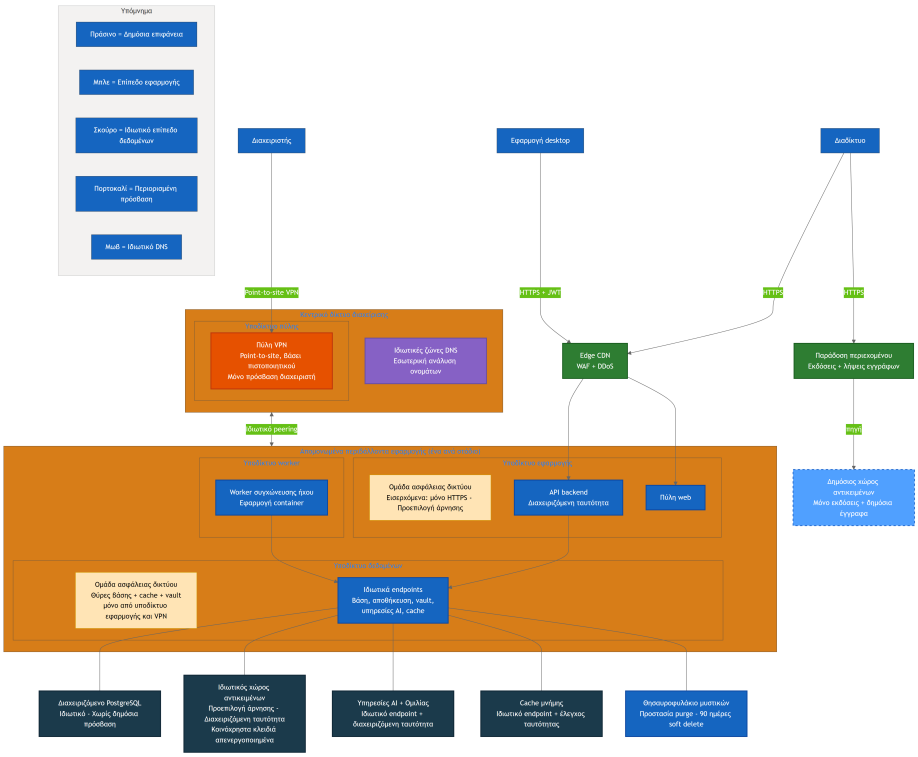
Οι ισχυρισμοί ασφάλειας ενός προμηθευτή είναι εύκολο να γραφτούν και δύσκολο να γίνουν αξιόπιστοι. Επομένως, έχουμε συνδέσει κάθε βασικό ισχυρισμό σε αυτό το έγγραφο με κάτι συγκεκριμένο και μετρήσιμο μέσα στα μηχανικά μας συστήματα: έναν έλεγχο που υλοποιείται σε κώδικα, ένα test που αποδεικνύει ότι ο έλεγχος λειτουργεί, έναν ορισμό υποδομής που τον επιβάλλει ή μια αναφορά ελέγχου που καταγράφει έναν τεκμηριωμένο έλεγχο. Όπου ένας έλεγχος αποτελεί μέρος του μελλοντικού μας οδικού χάρτη και δεν έχει ακόμη διατεθεί σήμερα, το δηλώνουμε ρητά. Προτιμούμε να ισχυριζόμαστε λιγότερα και να μας εμπιστεύονται παρά να ισχυριζόμαστε περισσότερα και να εκτιθέμεθα.

2.3 Κοινή Ευθύνη

Η πλατφόρμα παρέχεται ως λογισμικό ως υπηρεσία. Εμείς λειτουργούμε την υποδομή, την εφαρμογή, τον αγωγό AI και τη διαχείριση δεδομένων. Ο πελάτης είναι υπεύθυνος για τη διαχείριση των δικών του λογαριασμών χρηστών και ρόλων, για τη ρύθμιση των παραθύρων διατήρησης δεδομένων ώστε να αντιστοιχούν στην εσωτερική του πολιτική και για τη διασφάλιση ότι η συγκατάθεση του υποψηφίου λαμβάνεται μέσω της ροής συγκατάθεσης που παρέχει η πλατφόρμα. Η Ενότητα 14 περιγράφει αυτή τη διαίρεση με περισσότερη λεπτομέρεια.

3. Επισκόπηση Αρχιτεκτονικής Ασφάλειας

Η πλατφόρμα είναι δομημένη ως μικρός αριθμός συνεργαζόμενων υπηρεσιών και όχι ως ένα ενιαίο monolith. Μια desktop εφαρμογή και μια διαδικτυακή πύλη λειτουργούν ως clients. Ένα κεντρικό backend API διαχειρίζεται όλη τη μόνιμη αποθήκευση, το authentication, τη χρέωση, τον αγωγό AI, τη συγκατάθεση, το email, τη διαχείριση αρχείων και τα dashboards. Ένας audio merge worker επεξεργάζεται τις εγγραφές ασύγχρονα. Όλη η ευαίσθητη κατάσταση βρίσκεται πίσω από το backend API· οι clients δεν επικοινωνούν ποτέ απευθείας με τη βάση δεδομένων, το storage ή τις υπηρεσίες AI.



Το παραπάνω διάγραμμα δείχνει την τοπολογία παραγωγής με τα ονόματα πόρων σκόπιμα γενικευμένα. Τρεις αρχές είναι ορατές σε αυτό:

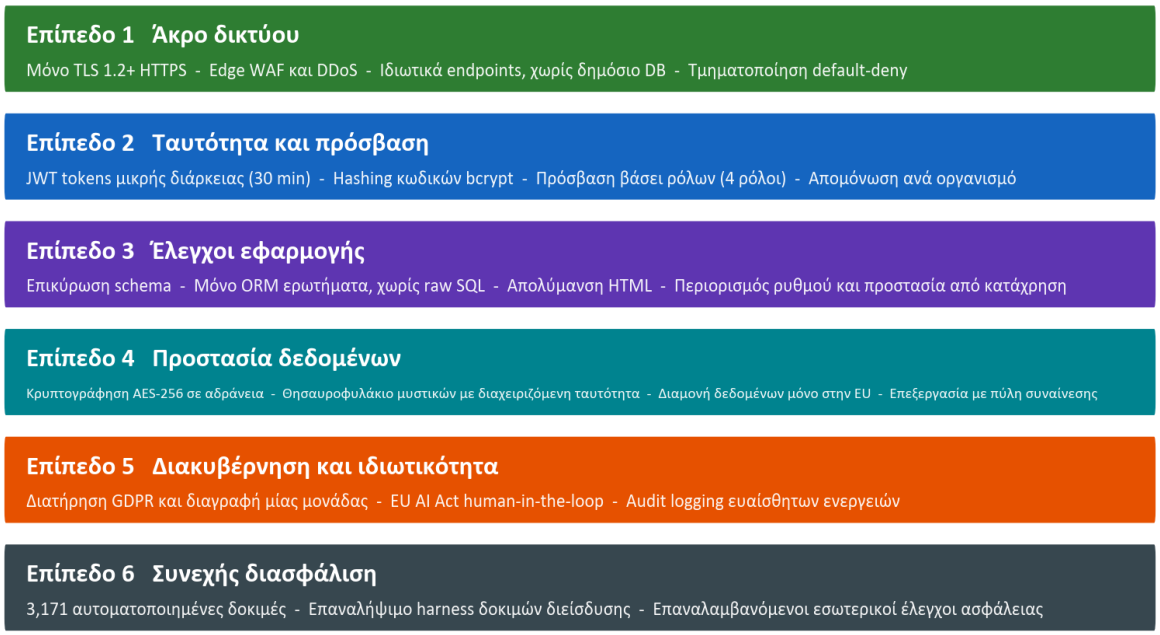
- **Καμία άμεση έκθεση υπηρεσιών δεδομένων.** Η βάση δεδομένων, το private object storage, οι υπηρεσίες AI και η cache έχουν απενεργοποιημένη τη δημόσια δικτυακή πρόσβαση και είναι προσβάσιμα μόνο μέσω private endpoints μέσα σε ένα απομονωμένο virtual network. Το secrets vault προσεγγίζεται από την εφαρμογή μέσω private endpoint και προστατεύεται επιπλέον από authentication ταυτότητας πλατφόρμας και πολιτικές πρόσβασης ελάχιστου προνομίου, ώστε κάθε πρόσβαση να απαιτεί έγκυρη, εξουσιοδοτημένη ταυτότητα ανεξάρτητα από τη δικτυακή διαδρομή.
- **Μια διαχωρισμένη δημόσια επιφάνεια.** Το μόνο δημόσιο object storage διατηρεί λήψεις εκδόσεων και δημόσια έγγραφα. Δεν περιέχει ποτέ δεδομένα υποψηφίων. Η κίνηση της εφαρμογής που απευθύνεται στους πελάτες διέρχεται μέσω ενός edge layer που παρέχει web application firewall, προστασία distributed-denial-of-service και content delivery.
- **Η διαχειριστική πρόσβαση είναι ελεγχόμενη.** Οι operators προσεγγίζουν εσωτερικούς πόρους μόνο μέσω certificate-based point-to-site VPN προς ένα management hub network και όχι μέσω του δημόσιου internet.

Κάθε στάδιο ανάπτυξης (development και production) είναι ένα πλήρως απομονωμένο περιβάλλον με δικό του δίκτυο, storage accounts, βάση δεδομένων και secrets. Τα δεδομένα παραγωγής πελατών δεν υπάρχουν ποτέ σε χαμηλότερα περιβάλλοντα. Ένα κοινό management hub διατηρεί μόνο το VPN gateway και το private DNS, με ιδιωτική peering σύνδεση προς κάθε περιβάλλον.

4. Άμυνα σε Βάθος

Κανένας μεμονωμένος έλεγχος δεν θεωρείται επαρκής για να σταματήσει κάθε επίθεση. Η πλατφόρμα τοποθετεί ανεξάρτητους ελέγχους σε επίπεδα ώστε η αστοχία οποιουδήποτε ενός επιπέδου να μην εκθέτει δεδομένα. Τα παρακάτω επίπεδα υλοποιούνται το καθένα και, όπως περιγράφεται στην Ενότητα 12, δοκιμάζονται ξεχωριστά.

Πολυεπίπεδο μοντέλο ασφάλειας: ανεξάρτητοι έλεγχοι σε κάθε επίπεδο



Επίπεδο	Ενδεικτικοί έλεγχοι
Άκρο δικτύου	Μεταφορά μόνο μέσω TLS, edge WAF και προστασία DDoS, private endpoints, τμηματοποίηση default-deny
Ταυτότητα και πρόσβαση	Υπογεγραμμένα tokens σύντομης διάρκειας, bcrypt hashing, έλεγχος πρόσβασης βάσει ρόλων, απομόνωση ανά οργανισμό
Εφαρμογή	Επικύρωση schema σε όλες τις εισόδους, πρόσβαση σε δεδομένα μόνο μέσω ORM, output encoding, rate limiting
Προστασία δεδομένων	Κρυπτογράφηση σε αδράνεια, secrets vault με managed identity, διαμονή δεδομένων στην ΕΕ, επεξεργασία ελεγχόμενη από συγκατάθεση
Διακυβέρνηση και ιδιωτικότητα	Παραμετροποιήσιμη διατήρηση, διαγραφή ενιαίας μονάδας, human-in-the-loop AI, audit logging
Συνεχής διασφάλιση	Αυτοματοποιημένη σουίτα tests, επαναλήψιμα penetration tests, επαναλαμβανόμενοι εσωτερικοί έλεγχοι ασφάλειας

Το υπόλοιπο αυτού του εγγράφου εξετάζει διαδοχικά κάθε επίπεδο και στη συνέχεια περιγράφει πώς αποδεικνύουμε, συνεχώς, ότι τα επίπεδα αντέχουν.

5. Ασφάλεια Δικτύου

5.1 Ιδιωτικό εξ Ορισμού

Το επίπεδο δεδομένων είναι ιδιωτικό από κατασκευή. Η διαχειριζόμενη βάση δεδομένων PostgreSQL έχει απενεργοποιημένη τη δημόσια δικτυακή πρόσβαση και είναι προσβάσιμη μόνο μέσω private endpoint. Το private object storage είναι ρυθμισμένο να αρνείται τη δικτυακή πρόσβαση εξ ορισμού, απενεργοποιεί πλήρως τα shared access keys και είναι προσβάσιμο μόνο μέσω managed identity από το application subnet. Η cache, οι υπηρεσίες AI και το secrets vault προσεγγίζονται ομοίως μέσω private endpoints με private DNS resolution.

Στην πράξη αυτό σημαίνει ότι δεν υπάρχει connection string προς τη βάση δεδομένων εκτεθειμένο στο internet και δεν υπάρχει δημόσιο storage URL για τον ήχο υποψηφίων: η βάση δεδομένων και το private storage έχουν ευθέως απενεργοποιημένη τη δημόσια δικτυακή πρόσβαση. Το secrets vault προσεγγίζεται από την εφαρμογή μέσω private endpoint και προστατεύεται από authentication ταυτότητας πλατφόρμας και πολιτικές πρόσβασης ελάχιστου προνομίου, με τις ταυτότητες εφαρμογών να έχουν δικαιώματα μόνο ανάγνωσης μόνο στα secrets που χρειάζονται, ώστε τα secrets να μην μπορούν να ανακτηθούν χωρίς έγκυρη, εξουσιοδοτημένη ταυτότητα. Η επιφάνεια επίθεσης που ένας εξωτερικός αντίπαλος μπορεί έστω να αγγίξει περιορίζεται στα HTTPS endpoints της εφαρμογής πίσω από το edge layer.

5.2 Δικτυακή Τμηματοποίηση

Κάθε περιβάλλον διαιρείται σε ξεχωριστά subnets για το επίπεδο εφαρμογής, το επίπεδο δεδομένων και τον ασύγχρονο worker. Κάθε subnet διέπεται από ένα network security group του οποίου ο τελικός κανόνας αρνείται όλη την εισερχόμενη κίνηση. Το application subnet δέχεται μόνο εισερχόμενο HTTPS. Το data subnet δέχεται μόνο τις συγκεκριμένες θύρες βάσης δεδομένων, cache και vault, και μόνο από το application subnet ή το διαχειριστικό VPN. Αυτό σημαίνει ότι ακόμη και ένας επιτιθέμενος που κατά κάποιον τρόπο έφτανε στο επίπεδο εφαρμογής δεν θα μπορούσε να μετακινηθεί ελεύθερα προς το επίπεδο δεδομένων· οι μόνες επιτρεπόμενες διαδρομές είναι εκείνες που χρησιμοποιεί νόμιμα η εφαρμογή.

5.3 Το Edge

Η δημόσια κίνηση της εφαρμογής εξυπηρετείται από ένα edge layer που παρέχει web application firewall, προστασία DDoS και content delivery network. Οι λήψεις εκδόσεων και εγγράφων εξυπηρετούνται από έναν αποκλειστικό δημόσιο storage account μέσω μιας content-delivery front door, πλήρως διαχωρισμένο από το private storage που διατηρεί δεδομένα υποψηφίων. Τα δύο επίπεδα storage δεν αναμειγνύονται ποτέ: μια κακή ρύθμιση στο δημόσιο επίπεδο δεν μπορεί να εκθέσει ιδιωτικά δεδομένα υποψηφίων, επειδή πρόκειται για διαφορετικούς λογαριασμούς με διαφορετικούς κανόνες δικτύου.

5.4 Διαχειριστική Πρόσβαση

Δεν υπάρχει δημόσιο διαχειριστικό endpoint προς το private network. Οι operators συνδέονται μέσω point-to-site VPN gateway που χρησιμοποιεί certificate-based authentication. Η διαχειριστική πρόσβαση σε βάση δεδομένων και cache είναι δυνατή μόνο μέσα από αυτό το tunnel, καθώς αυτές οι υπηρεσίες έχουν απενεργοποιημένη τη δημόσια δικτυακή πρόσβαση. Αυτό διατηρεί τις καθημερινές λειτουργίες εντελώς εκτός του δημόσιου internet.

6. Διαχείριση Ταυτότητας και Πρόσβασης

6.1 Authentication

Οι συνεδρίες χρηστών καθιερώνονται με ένα υπογεγραμμένο access token που ισχύει για τριάντα λεπτά, σε συνδυασμό με ένα ξεχωριστό, opaque, server-side refresh token. Τα access tokens επαληθεύονται σε κάθε αίτημα και ο χρήστης επαναεπικυρώνεται έναντι της βάσης δεδομένων (συμπεριλαμβανομένου ελέγχου ενεργού λογαριασμού) αντί να θεωρείται αξιόπιστος μόνο βάσει του περιεχομένου του token. Η αποσύνδεση ανακαλεί αμέσως τη server-side refresh session, επομένως ένα κλεμμένο refresh token δεν μπορεί να επιβιώσει μετά από logout.

Οι κωδικοί πρόσβασης δεν αποθηκεύονται ποτέ ως απλό κείμενο. Κατακερματίζονται με bcrypt χρησιμοποιώντας μοναδικό salt ανά κωδικό. Για οργανισμούς που προτιμούν single sign-on, η πλατφόρμα υποστηρίζει OAuth login με Microsoft και Google, οπότε δεν διατηρείται καθόλου κωδικός.

Η κυριότητα του email επαληθεύεται μέσω ενός συνδέσμου επαλήθευσης μίας χρήσης, περιορισμένης χρονικής ισχύος, πριν ένας αυτοεγγεγραμμένος λογαριασμός θεωρηθεί επαληθευμένος, και οι επαναποστολές email επαλήθευσης υπόκεινται σε rate limiting για αποτροπή κατάχρησης.

6.2 Έλεγχος Πρόσβασης Βάσει Ρόλων

Το authorization επιβάλλεται μέσω ενός μοντέλου ρόλων με τέσσερις ρόλους αυξανόμενου προνομίου: interviewer, hiring manager, recruiter και administrator. Η πρόσβαση σε προνομιούχες ενέργειες επιβάλλεται από server-side dependencies που ελέγχουν τόσο τον ρόλο όσο και την κατάσταση επαλήθευσης του καλούντος. Αυτοί οι έλεγχοι ρόλων προστατεύουν πολύ περισσότερες από εκατό διακριτές λειτουργίες API.

Ρόλος	Τυπικές δυνατότητες
Interviewer	Διεξάγει ανατεθειμένες συνεντεύξεις· βλέπει μόνο τις συνεντεύξεις που του έχουν ανατεθεί
Hiring manager	Διαχειρίζεται recruitments των οποίων είναι ιδιοκτήτης ή μέλος
Recruiter	Πλήρης διαχείριση recruitments και υποψηφίων εντός του οργανισμού
Administrator	Ρυθμίσεις οργανισμού, χρέωση, διαχείριση χρηστών και API keys

Πέρα από τους γενικούς ελέγχους ρόλων, η πλατφόρμα εφαρμόζει κανόνες ορατότητας σε επίπεδο δεδομένων. Οι hiring managers βλέπουν μόνο τα recruitments που δημιούργησαν ή στα οποία είναι μέλη· οι interviewers βλέπουν μόνο τις συνεντεύξεις που τους έχουν ανατεθεί. Επομένως, το προνόμιο επιβάλλεται τόσο στο επίπεδο του «ποια ενέργεια» όσο και στο επίπεδο του «ποια αρχεία».

6.3 Απομόνωση Ανά Οργανισμό

Η πλατφόρμα είναι multi-tenant και η απομόνωση tenant αντιμετωπίζεται ως έλεγχος ασφάλειας πρώτης γραμμής. Κάθε authenticated ταυτότητα φέρει αναγνωριστικό οργανισμού και τα ερωτήματα δεδομένων περιορίζονται σε αυτόν τον οργανισμό. Όταν ένας χρήστης ζητά ένα αρχείο που ανήκει σε άλλον οργανισμό, η πλατφόρμα επιστρέφει απόκριση "not found" αντί να αποκαλύπτει ότι το αρχείο υπάρχει. Τα εσωτερικά αναγνωριστικά βάσης δεδομένων δεν εκτίθενται ποτέ στη μεταφορά· το API παρουσιάζει display identifiers και τα επαναχαρτογραφεί ανά αίτημα, εξαλείφοντας μια κοινή κατηγορία επιθέσεων cross-tenant enumeration.

Αυτό δεν αποτελεί μόνο σχεδιαστική πρόθεση. Όπως περιγράφεται στην Ενότητα 12, η αυτοματοποιημένη σουίτα μας εκτελεί ένα μεγάλο cross-organization matrix που επιχειρεί να προσπελάσει τα δεδομένα ενός οργανισμού χρησιμοποιώντας credentials άλλου οργανισμού και επιβεβαιώνει ότι κάθε τέτοια προσπάθεια αποτυγχάνει.

6.4 Προγραμματιστική Πρόσβαση

Για integrations, οργανισμοί σε επιλέξιμα πλάνα μπορούν να εκδώσουν API keys. Τα keys χρησιμοποιούν αναγνωρίσιμο πρόθεμα, φέρουν 128 bits entropy και αποθηκεύονται μόνο ως hash· το ακατέργαστο key εμφανίζεται μία φορά κατά τη

δημιουργία και ποτέ ξανά. Κάθε key φέρει ρητό permission scope (read, write ή ATS integration), μπορεί να περιοριστεί σε συγκεκριμένα source networks, μπορεί να ανακληθεί άμεσα και υπόκειται σε per-key rate limits που προκύπτουν από το plan tier του οργανισμού. Η επαλήθευση key χρησιμοποιεί timing-safe comparison για να αποφεύγεται η διαρροή πληροφοριών μέσω του χρόνου απόκρισης.

7. Ασφάλεια Εφαρμογής

Η εφαρμογή είναι γραμμένη ώστε να εξαλείφει ολόκληρες κατηγορίες ευπαθειών αντί να τις επιδιορθώνει κατά περίπτωση.

- **Injection.** Όλη η πρόσβαση στη βάση δεδομένων περνά μέσω object-relational mapper με parameterized queries. Η βάση κώδικα δεν περιέχει raw SQL μορφοποιημένο με strings. Αυτό εξαλείφει δομικά το SQL injection.
- **Επικύρωση εισόδου.** Κάθε request body επικυρώνεται έναντι αυστηρού schema πριν φτάσει στην επιχειρησιακή λογική. Υπερμεγέθη payloads απορρίπτονται και τα list endpoints είναι paginated ώστε να οριοθετείται η χρήση πόρων.
- **Output encoding και cross-site scripting.** Το κείμενο που παρέχεται από χρήστη και παράγεται από AI αντιμετωπίζεται ως μη έμπιστο. Όπου περιεχόμενο πρέπει να αποδοθεί ως HTML, περνά από allow-list sanitizer κατά τον χρόνο εγγραφής και μια αποκλειστική σουίτα tests επιβεβαιώνει ότι script tags, event handlers και javascript URLs αφαιρούνται.
- **Mass assignment.** Οι ενέργειες ενημέρωσης χρησιμοποιούν ρητά schemas που αποκλείουν προνομιούχα πεδία όπως role, organization και credit balance, ώστε ένας client να μην μπορεί να κλιμακώσει προνόμια δημοσιεύοντας επιπλέον πεδία.
- **Rate limiting.** Τα endpoints authentication και όσα είναι επιρρεπή σε κατάχρηση υπόκεινται σε rate limiting με χρήση durable limiter βασισμένου σε βάση δεδομένων που επιβιώνει από επανεκκινήσεις και λειτουργεί σωστά σε πολλαπλά instances εφαρμογής. Login, registration, password reset και verification resends έχουν το καθένα τα δικά του όρια. Το client IP resolution είναι ενισχυμένο έναντι spoofing των forwarding headers.
- **Webhooks.** Τα εισερχόμενα webhooks από παρόχους πληρωμών και email επαληθεύονται έναντι των signatures των παρόχων στο raw request body πριν υποβληθούν σε επεξεργασία.
- **Μεταφορτώσεις αρχείων.** Οι μεταφορτώσεις έχουν όριο μεγέθους, επικυρώνονται, αποθηκεύονται με παραγόμενα αναγνωριστικά και όχι με ονόματα που παρέχονται από χρήστη και περιορίζονται ανά αίτημα και ανά οργανισμό.
- **Security headers.** Στην παραγωγή, οι αποκρίσεις φέρουν strict transport security, επιλογές content-type και frame, πολιτική referrer και περιοριστική πολιτική permissions, και αποκρύπτουν banners server και framework.

8. Προστασία Δεδομένων

8.1 Κρυπτογράφηση

Όλα τα δεδομένα κρυπτογραφούνται σε αδράνεια χρησιμοποιώντας AES-256 μέσω των επιπέδων κρυπτογράφησης storage και βάσης δεδομένων της πλατφόρμας Azure. Όλη η δικτυακή κίνηση εξυπηρετείται αποκλειστικά μέσω HTTPS χρησιμοποιώντας TLS 1.2 ή υψηλότερο· το HTTP σε απλό κείμενο ανακατευθύνεται σε HTTPS σε κάθε επίπεδο. Στην παραγωγή, το API και η διαδικτυακή πύλη εκπέμπουν strict transport security headers μαζί με ένα σύνολο hardening headers και αποκρύπτουν banners έκδοσης server και framework.

8.2 Διαχείριση Secrets

Τα secrets της εφαρμογής διατηρούνται σε κεντρικό secrets vault με ενεργοποιημένη purge protection και soft-delete window ενενήντα ημερών. Οι εφαρμογές αυθεντικοποιούνται σε πόρους Azure χρησιμοποιώντας system-assigned managed identities αντί για μακρόβια keys· για παράδειγμα, το private storage έχει πλήρως απενεργοποιημένα τα shared access keys, επομένως η πρόσβαση είναι δυνατή μόνο μέσω role assignments βάσει ταυτότητας που περιορίζονται στον επιμέρους πόρο. Οι πολιτικές πρόσβασης στο vault χορηγούν στους application principals μόνο πρόσβαση ανάγνωσης στα συγκεκριμένα secrets που χρειάζονται, ακολουθώντας την αρχή του ελάχιστου προνομίου.

8.3 Διαμονή Δεδομένων

Όλα τα δεδομένα πελατών και υποψηφίων αποθηκεύονται και υποβάλλονται σε επεξεργασία εντός της Ευρωπαϊκής Ένωσης. Η φιλοξενία εφαρμογών, η βάση δεδομένων, το storage, η cache και τα secrets βρίσκονται στη West Europe και η επεξεργασία AI εκτελείται σε περιοχές της ΕΕ. Ο πάροχος AI δεν χρησιμοποιεί τα δεδομένα πελατών για εκπαίδευση των μοντέλων του.

8.4 Η Ζωή μιας Μεμονωμένης Συνέντευξης

Ο σαφέστερος τρόπος κατανόησης των ελέγχων προστασίας δεδομένων είναι να ακολουθήσουμε μία συνέντευξη από άκρο σε άκρο. Η συγκατάθεση λαμβάνεται και καταγράφεται πριν υποβληθεί οτιδήποτε σε επεξεργασία. Η μεταφόρτωση κρυπτογραφείται κατά τη μεταφορά. Η απομαγνητοφώνηση και η ανάλυση εκτελούνται εντός κέντρων δεδομένων της ΕΕ. Τα αποτελέσματα εγγράφονται σε κρυπτογραφημένο storage. Κάθε αρχείο στη συνέχεια διέπεται από ένα ενιαίο ρολόι διατήρησης που καταλήγει σε καταγεγραμμένη, διαδοχική διαγραφή. Σε οποιοδήποτε σημείο, δικαιώματα υποψηφίου όπως ανάκληση, διαγραφή, πρόσβαση ή φορητότητα μπορούν να διακόψουν αυτή τη ροή.

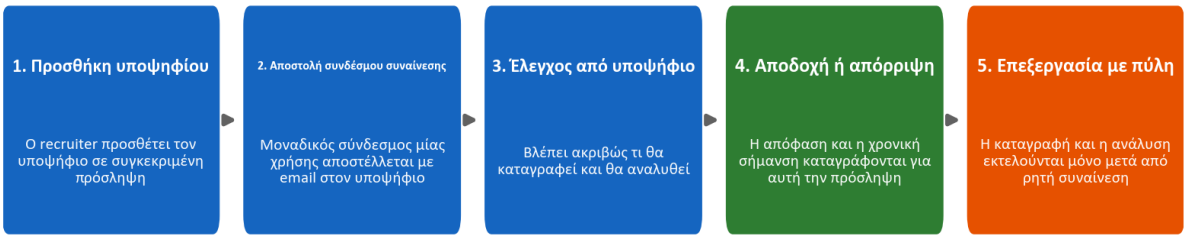
9. Ιδιωτικότητα εξ Ορισμού και GDPR

Η ιδιωτικότητα είναι ενσωματωμένη στο μοντέλο δεδομένων και στη ροή εργασίας, όχι προσαρτημένη μόνο μέσω πολιτικής.

9.1 Συγκατάθεση

Καμία συνέντευξη δεν καταγράφεται ή αναλύεται χωρίς τη ρητή συγκατάθεση του υποψηφίου. Όταν ένας υποψήφιος προστίθεται σε ένα recruitment, η πλατφόρμα εκδίδει μέσω email έναν μοναδικό σύνδεσμο συγκατάθεσης μίας χρήσης. Ο υποψήφιος εξετάζει τι θα συμβεί και είτε αποδέχεται είτε αρνείται. Η κατάσταση συγκατάθεσης, συμπεριλαμβανομένου του χρόνου απόκρισης, καταγράφεται έναντι αυτής της συγκεκριμένης διαδικασίας recruitment, ώστε η συγκατάθεση να περιορίζεται πάντοτε σε μια συγκεκριμένη διαδικασία πρόσληψης αντί να παρέχεται καθολικά.

Συναίνεση υποψηφίου: ρητή και καταγεγραμμένη πριν από κάθε επεξεργασία

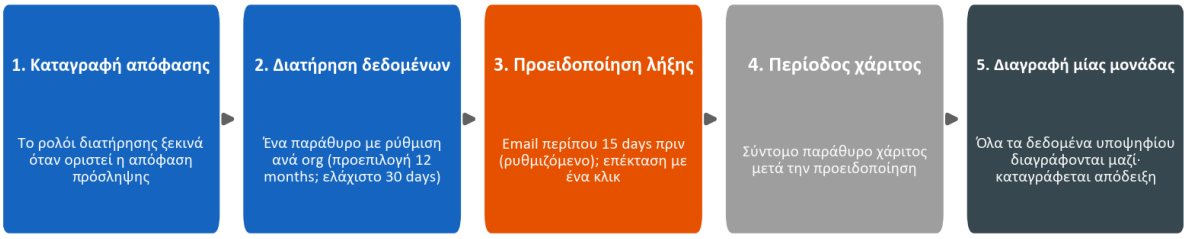


9.2 Διατήρηση και Διαγραφή

Η διατήρηση δεδομένων είναι παραμετροποιήσιμη ανά οργανισμό, με προεπιλογή δώδεκα μήνες και παραμετροποιήσιμο ελάχιστο τριάντα ημερών, και μπορεί να παρακαμφθεί ανά υποψήφιο. Υπάρχει ένα ενιαίο ρολόι διατήρησης για τα δεδομένα ενός υποψηφίου και όχι ξεχωριστός χρονοδιακόπτης για κάθε τεχνούργημα. Το ρολόι ξεκινά όταν καταγραφεί μια απόφαση πρόσληψης. Πριν λήξουν τα δεδομένα, η πλατφόρμα αποστέλλει προειδοποίηση (προεπιλεγμένα περίπου δεκαπέντε ημέρες νωρίτερα) και προσφέρει παράταση με ένα κλικ. Όταν τα δεδομένα διαγράφονται, διαγράφονται ως ενιαία μονάδα: η εγγραφή υποψηφίου, οι συνεντεύξεις, οι απομαγνητοφωνήσεις, οι ηχογραφήσεις, τα έγγραφα και οι συγκρίσεις αφαιρούνται όλα μαζί και η διαγραφή καταγράφεται σε audit log. Δεν υπάρχει μερικό ή ορφανό υπόλειμμα.

Ο παρακάτω κύκλος ζωής δείχνει αυτό το ενιαίο ρολόι και πώς συγκλίνει σε μία διαδοχική διαγραφή με καταγεγραμμένη απόδειξη διαγραφής.

Διατήρηση δεδομένων: ένα ρολόι ανά υποψήφιο, διαγραφή μίας μονάδας



9.3 Δικαιώματα Υποκειμένων Δεδομένων και Sub-processors

Η πλατφόρμα υποστηρίζει τα δικαιώματα υποκειμένων δεδομένων που απαιτούνται βάσει του GDPR, συμπεριλαμβανομένων της πρόσβασης, της διαγραφής, της φορητότητας, της εναντίωσης και της επεξήγησης. Η επεξεργασία διενεργείται βάσει μιας συμφωνίας επεξεργασίας δεδομένων που οι πελάτες αποδέχονται κατά την εγγραφή και η οποία τηρείται σε έκδοση ανά οργανισμό. Οι sub-processors μας και οι ρόλοι τους, όλοι εντός της ΕΕ ή υπό κατάλληλες διασφαλίσεις, γνωστοποιούνται σε αυτή τη συμφωνία και οι πελάτες λαμβάνουν προηγούμενη ειδοποίηση για οποιαδήποτε αλλαγή. Η Ενότητα 17 περιέχει το μητρώο sub-processors και τη χαρτογράφηση συμμόρφωσης άρθρο προς άρθρο.

10. Υπεύθυνη AI και ο EU AI Act

Η πλατφόρμα εμπίπτει στην κατηγορία υψηλού κινδύνου του EU AI Act επειδή υποστηρίζει αποφάσεις απασχόλησης και αντιμετωπίζουμε αυτή την ταξινόμηση με σοβαρότητα.

Ο καθοριστικός κανόνας του προϊόντος είναι ότι **η AI είναι υποστήριξη απόφασης, όχι λήπτης απόφασης.** Το σύστημα δεν αποδέχεται ή απορρίπτει ποτέ αυτόματα έναν υποψήφιο. Απομαγνητοφωνεί ομιλία, δομεί ερωτήσεις και απαντήσεις, βαθμολογεί απαντήσεις έναντι κριτηρίων που έχει ορίσει ο recruiter και συντάσσει πρόχειρο feedback, και ένας άνθρωπος ελέγχει κάθε αποτέλεσμα πριν χρησιμοποιηθεί. Αυτό διατηρεί τον άνθρωπο σταθερά στον βρόχο.

Εξίσου σημαντικό είναι τι δεν κάνει η AI. Δεν αξιολογεί προσωπικότητα, «πολιτισμική προσαρμογή», συναισθηματική κατάσταση, τόνο φωνής, προφορά, φύλο, ηλικία, εθνότητα, εμφάνιση ή γλώσσα σώματος. Η βαθμολόγηση αγκυρώνεται σε αποδεικτικά στοιχεία από την απομαγνητοφώνηση και σε κριτήρια που ορίζει ο recruiter, και τα ονόματα των υποψηφίων εξαιρούνται από την είσοδο αξιολόγησης για μείωση της μεροληψίας. Δημοσιεύουμε transparency card, τεκμηρίωση χρήστη και δήλωση συμμόρφωσης που περιγράφουν το σύστημα, τους περιορισμούς του και τις διασφαλίσεις του.

Έλεγχος υπεύθυνης AI	Πώς λειτουργεί
Άνθρωπος στον βρόχο	Κάθε βαθμολογία και κάθε στοιχείο feedback ελέγχεται από recruiter πριν από τη χρήση
Καμία αυτοματοποιημένη απόφαση	Το σύστημα δεν αποδέχεται ούτε απορρίπτει αυτόματα υποψήφιο
Βαθμολόγηση βάσει αποδεικτικών στοιχείων	Οι βαθμολογίες παραπέμπουν σε υποστηρικτικά στοιχεία από την απομαγνητοφώνηση
Σχεδιασμός κατά της μεροληψίας	Τα ονόματα εξαιρούνται από την αξιολόγηση· αξιολογείται η ουσία αντί του ύφους
Όρια πεδίου εφαρμογής	Προσωπικότητα, συναίσθημα, προφορά και προστατευόμενα χαρακτηριστικά δεν αξιολογούνται ποτέ
Ασφάλεια feedback προς υποψηφίους	Το ιδιωτικό feedback προς υποψηφίους περνά από δικλείδα ασφαλείας generation-and-validation

Αυτοί οι περιορισμοί δεν δηλώνονται μόνο στην τεκμηρίωση· κωδικοποιούνται στο επίπεδο prompt της AI και ασκούνται από ένα αποκλειστικό πρόγραμμα δοκιμών AI-safety που περιγράφεται στην Ενότητα 12.3.

11. Κύκλος Ζωής Ασφαλούς Ανάπτυξης

Η ασφάλεια επιβάλλεται στον τρόπο με τον οποίο κατασκευάζουμε και διαθέτουμε λογισμικό, όχι μόνο στο σύστημα σε λειτουργία.

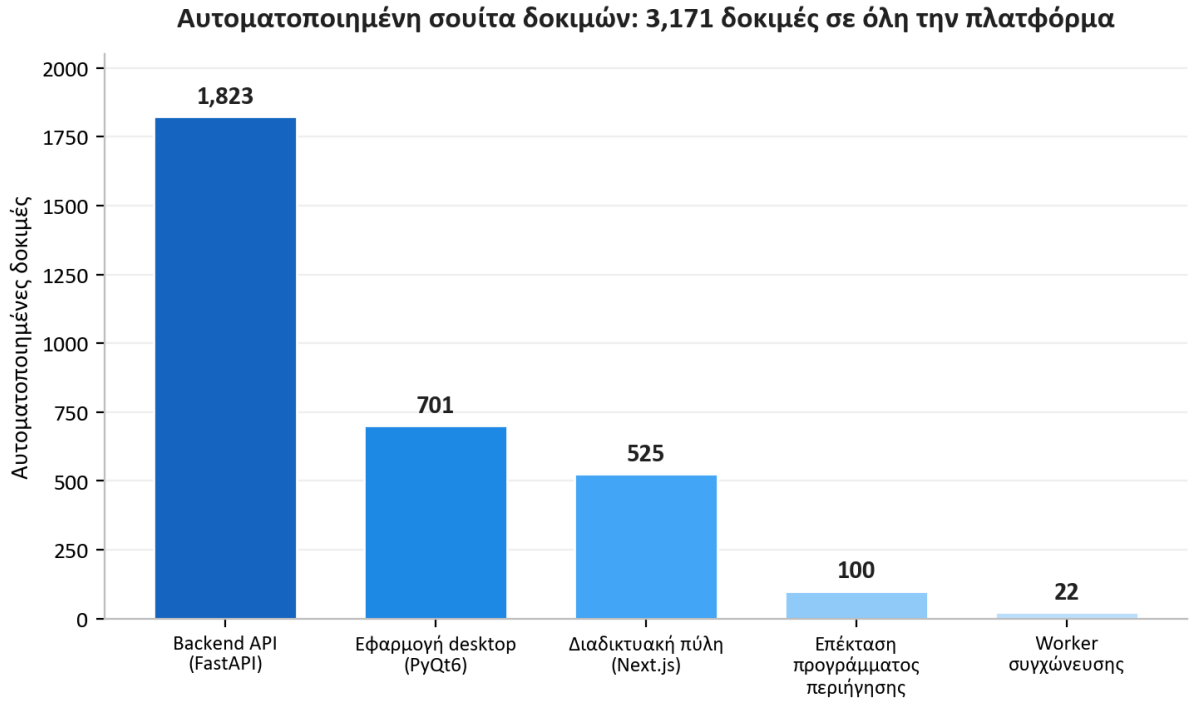
- **Διαχωρισμός περιβαλλόντων.** Τα development και production είναι πλήρως ξεχωριστά, το καθένα με τη δική του υποδομή, storage accounts, βάση δεδομένων, secrets και subdomains. Δεν υπάρχει κοινή κατάσταση.
- **Υποδομή ως κώδικας.** Ολόκληρο το cloud περιβάλλον ορίζεται ως κώδικας και ελέγχεται ως κώδικας, γεγονός που καθιστά τη στάση ασφάλειας ελεγκτέα και αναπαραγώγιμη. Ένας αξιολογητής μπορεί να δει ακριβώς ποιες θύρες είναι ανοιχτές, ποιοι πόροι είναι ιδιωτικοί και ποιες ταυτότητες έχουν ποιες άδειες.
- **Pinned, gated deployments.** Κάθε βήμα στον continuous-integration pipeline είναι pinned σε ακριβή, immutable έκδοση. Τα production deployments βασίζονται σε tags, εκτελούνται μόνο μέσω του προστατευμένου production pipeline και τελούν υπό απαιτούμενη έγκριση. Η αυτοματοποιημένη σουίτα tests λειτουργεί ως release gate: ένα deployment δεν μπορεί να κυκλοφορήσει αν τα tests αποτύχουν.
- **Υγιεινή εξαρτήσεων.** Η αυτοματοποιημένη παρακολούθηση εξαρτήσεων προτείνει εβδομαδιαίες ενημερώσεις σε backend, desktop, web, infrastructure και pipeline definitions, και οι έλεγχοι εξαρτήσεων αποτελούν μέρος της περιοδικής ανασκόπησης ασφάλειας.
- **Υπογεγραμμένα artifacts.** Οι installers desktop υπογράφονται ψηφιακά, ώστε οι πελάτες να μπορούν να επαληθεύουν ότι το λογισμικό που εγκαθιστούν προέρχεται πράγματι από εμάς.
- **Πειθαρχία secrets.** Τα secrets βρίσκονται στο vault και σε προστατευμένα pipeline secrets, ποτέ στον πηγαίο κώδικα.

12. Συνεχής Δοκιμή Ασφάλειας

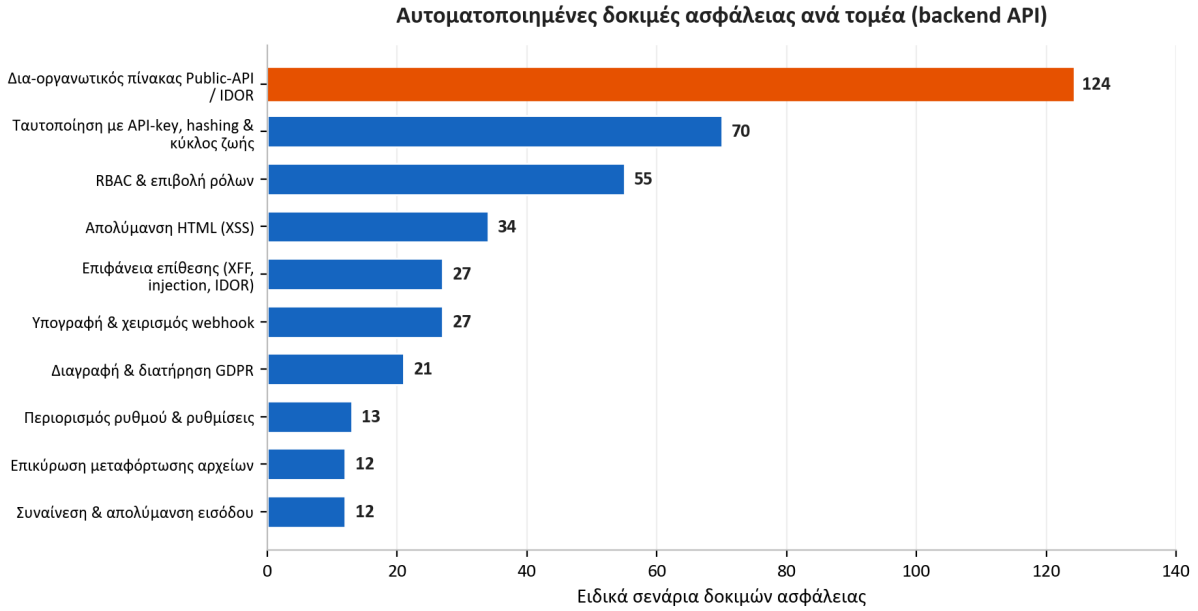
Αυτή είναι η καρδιά της ιστορίας διασφάλισής μας και το μέρος που οι περισσότεροι προμηθευτές δεν μπορούν να επιδείξουν. Αντιμετωπίζουμε την ασφάλεια ως κάτι που πρέπει να μετράται συνεχώς, με εκτελέσιμους ελέγχους, και όχι ως κάτι που δηλώνεται μία φορά.

12.1 Η Αυτοματοποιημένη Σουίτα Tests

Η πλατφόρμα καλύπτεται από **3,171 αυτοματοποιημένα tests** που εκτείνονται στο backend API, την desktop εφαρμογή, τη διαδικτυακή πύλη, το browser extension και τον audio merge worker.



Αυτά δεν είναι μόνο λειτουργικά tests. Μια ουσιαστική, αποκλειστική σουίτα ασφάλειας ελέγχει τους ελέγχους που περιγράφηκαν νωρίτερα σε αυτό το έγγραφο. Το παρακάτω διάγραμμα αναλύει τα ειδικά για την ασφάλεια tests στο backend API ανά τομέα.



Μεταξύ πολλών άλλων, αυτή η σουίτα περιλαμβάνει ένα μεγάλο public-API matrix που εκτελεί κάθε endpoint ως νόμιμος χρήστης, ως το API key του ίδιου του οργανισμού και ως το API key ανταγωνιστικού οργανισμού, επιβεβαιώνοντας ότι κάθε cross-organization προσπάθεια μπλοκάρεται. Περιλαμβάνει δεκάδες adversarial tests επιφάνειας επίθεσης για spoofing forwarding-header, header injection και διαρροή αναγνωριστικών, μια εστιασμένη σουίτα HTML-sanitization για cross-site scripting, tests επιβολής ρόλων για το πλήρες μοντέλο ρόλων και tests που αποδεικνύουν ότι τα δεδομένα υποψηφίων διαγράφονται πράγματι ως ενιαία μονάδα. Επειδή αυτά τα tests εκτελούνται ως release gate, μια παλινδρόμηση που αποδυνάμωνε οποιονδήποτε από αυτούς τους ελέγχους θα σταματούσε την κυκλοφορία αντί να φτάσει στους πελάτες.

12.2 Live Penetration Testing

Τα αυτοματοποιημένα unit tests αποδεικνύουν ότι οι έλεγχοι συμπεριφέρονται σωστά μεμονωμένα. Για να αποδείξουμε ότι διατηρούνται συνδυαστικά σε πραγματική ανάπτυξη, διατηρούμε μια επαναλήψιμη μεθοδολογία penetration-testing που εκτελεί πραγματικά attack scripts σε ενεργό περιβάλλον. Είναι οργανωμένη σε έξι φάσεις:

Φάση	Εστίαση	Παραδείγματα του τι ελέγχεται
1. Static analysis	Πηγαίος κώδικας	Secrets, μοτίβα injection, επικίνδυνες λειτουργίες, ελλείπον auth, μη ασφαλές HTML
2. Architecture review	Υποδομή	Private endpoints, τμηματοποίηση, TLS, ρύθμιση secrets
3. Attack-vector analysis	Source control και cloud	Προστασία branch, εύρος ταυτότητας, δημόσια έκθεση
4. Live penetration testing	Περιβάλλον σε λειτουργία	Διερεύνηση χωρίς credentials, cross-org πρόσβαση, injection, αλλοίωση token, SSRF, bursts rate-limit
5. Enterprise scoring	Ωριμότητα	Δεκαέξι κατηγορίες ασφάλειας βαθμολογημένες έναντι enterprise baseline
6. Dependency and supply chain	Κίνδυνος τρίτων μερών	Έλεγχος dependency CVE, pinned pipeline actions, ακεραιότητα lock-file

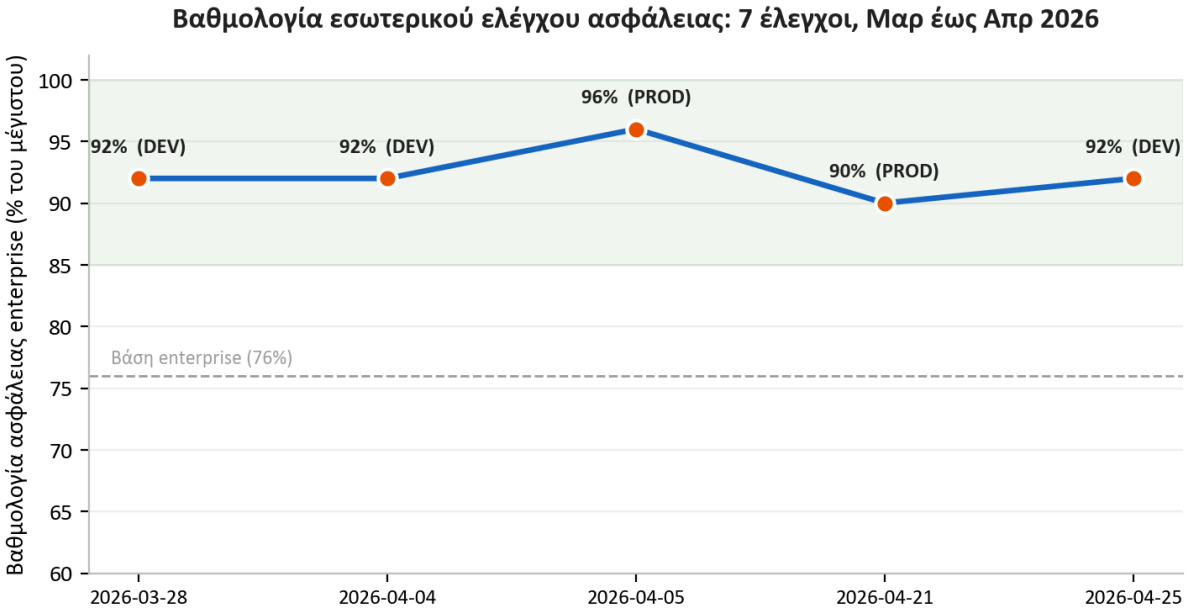
Η Φάση 4 είναι γνήσια adversarial δοκιμή σε αναπτυγμένο σύστημα και όχι checklist. Διερευνά προστατευμένα endpoints χωρίς credentials και επιβεβαιώνει ότι αρνούνται πρόσβαση· καταχωρίζει δύο οργανισμούς και επιχειρεί να προσεγγίσει τα αρχεία του ενός με τον λογαριασμό του άλλου· εισάγει payloads cross-site-scripting και server-side-template και επιβεβαιώνει ότι εξουδετερώνονται· αλλοιώνει authentication tokens και επιβεβαιώνει ότι απορρίπτονται· επιχειρεί server-side request forgery έναντι cloud metadata endpoints· και προκαλεί bursts στα authentication endpoints για να επιβεβαιώσει ότι το rate limiting πράγματι ενεργοποιείται στο ενεργό περιβάλλον και όχι μόνο θεωρητικά.

12.3 Δοκιμή Ασφάλειας Feedback Υποψηφίων

Επειδή η πλατφόρμα μπορεί να παράγει ιδιωτικό feedback ανάπτυξης για υποψηφίους, εκτελούμε ξεχωριστό adversarial πρόγραμμα ασφάλειας για αυτό το χαρακτηριστικό. Τροφοδοτεί σκόπιμα το σύστημα με σκληρές και εχθρικές σημειώσεις recruiters και επιβεβαιώνει ότι το output που απευθύνεται στον υποψήφιο δεν περιέχει ποτέ vulgarity, δεν αποκαλύπτει ή αποδίδει ποτέ ταυτότητα recruiter ή ιδιωτική άποψη και δεν εφαρμόζει ποτέ επικριτικές ετικέτες προσωπικότητας. Αυτό προστατεύει τόσο τον υποψήφιο, που πρέπει να λαμβάνει εποικοδομητικό και σεβαστικό feedback, όσο και τον πελάτη, του οποίου εσωτερική άποψη δεν πρέπει ποτέ να διαρρεύσει προς τα έξω.

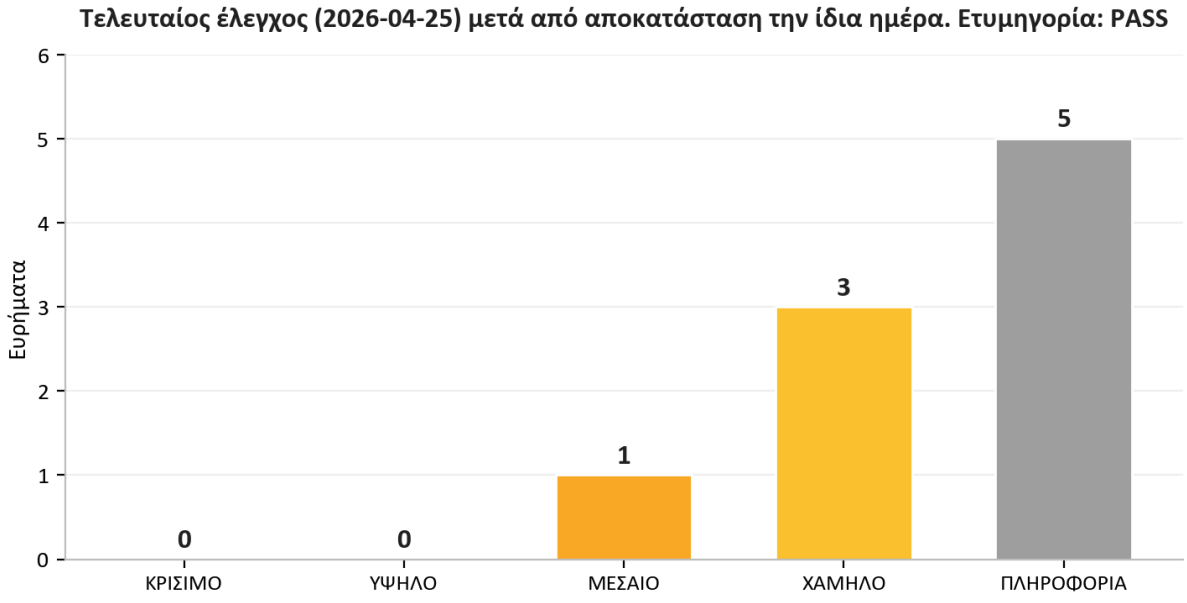
13. Αποτελέσματα Ελέγχων Ασφάλειας

Διενεργούμε επαναλαμβανόμενους ελέγχους ασφάλειας χρησιμοποιώντας δομημένη, επαναλήψιμη μεθοδολογία penetration-testing και συντάσσουμε τον καθένα ως χρονολογημένη αναφορά με ευρήματα αξιολογημένα κατά σοβαρότητα, αποδεικτικά στοιχεία και αποκατάσταση. Πρόκειται για εσωτερικούς ελέγχους που εκτελούνται από τη δική μας διαδικασία ασφάλειας· η επίσημη πιστοποίηση των ίδιων ελέγχων από τρίτο μέρος περιλαμβάνεται στον οδικό μας χάρτη. Μεταξύ τέλους Μαρτίου και τέλους Απριλίου 2026 ολοκληρώσαμε **seven such audits** σε development και production.



Το αποτέλεσμα που έχει τη μεγαλύτερη σημασία για έναν υποψήφιο πελάτη είναι η συνέπεια: **across all seven audits there were zero critical findings.** Στις σπάνιες περιπτώσεις όπου προέκυψε ζήτημα υψηλότερης σοβαρότητας, αποκαταστάθηκε γρήγορα, συχνά την ίδια ημέρα, και επαληθεύτηκε εκ νέου. Η rubric βαθμολόγησης ενισχύθηκε σκόπιμα κατά τη διάρκεια αυτής της περιόδου (η μέγιστη δυνατή βαθμολογία αυξήθηκε καθώς προσθέταμε περισσότερες κατηγορίες προς αξιολόγηση), γι' αυτό η γραμμή κανονικοποιημένης βαθμολογίας παραμένει υψηλή ακόμη και καθώς ο πήχης ανέβαινε.

Ο πιο πρόσφατος έλεγχός μας, στις 25 April 2026, δείχνει πώς λειτουργεί η διαδικασία στην πράξη. Εντοπίστηκαν δύο ζητήματα υψηλότερης σοβαρότητας, και τα δύο διορθώθηκαν και επαληθεύτηκαν εκ νέου την ίδια ημέρα, και ο έλεγχος έκλεισε με ετυμηγορία **PASS** χωρίς να απομένουν ζητήματα έτοιμα για εκμετάλλευση στο τρέχον threat model.



Έλεγχος	Περιβάλλον	Critical	Ετυμηγορία
2026-03-28	Development	0	Έτοιμο για production
2026-04-04	Development	0	Enterprise-ready
2026-04-05	Production	0	Enterprise-ready
2026-04-20	Development	0	Production-ready, σημειώσεις
2026-04-20	Development	0	Pass with notes
2026-04-21	Production	0	Ασφαλές, χωρίς εκμεταλλεύσιμα ευρήματα
2026-04-25	Development	0	Pass

Το μοτίβο σε αυτούς τους ελέγχους είναι η πιο ειλικρινής απόδειξη που μπορούμε να προσφέρουμε: προβλήματα εντοπίζονται, επειδή τα αναζητούμε εντατικά, και κλείνουν γρήγορα, επειδή η διαδικασία είναι σχεδιασμένη να τα κλείνει. Ένας προμηθευτής που δεν αναφέρει ποτέ εύρημα είναι συνήθως προμηθευτής που δεν αναζητά.

14. Επιχειρησιακή Ανθεκτικότητα και Κοινή Ευθύνη

14.1 Παρακολούθηση και Καταγραφή

Η τηλεμετρία εφαρμογής και πλατφόρμας ρέει σε κεντρικό log analytics workspace και υπηρεσία application monitoring, παρέχοντάς μας ορατότητα στη διαθεσιμότητα και τη συμπεριφορά. Ευαίσθητες ενέργειες όπως διαγραφή δεδομένων, αποδοχή νομικής συμφωνίας και κλήσεις AI καταγράφονται σε αποκλειστικούς audit tables, ώστε να υπάρχει διαρκές αρχείο για το ποιος έκανε τι σε σημαντικά δεδομένα.

14.2 Δημιουργία Αντιγράφων Ασφαλείας και Ανάκτηση

Η διαχειριζόμενη βάση δεδομένων διατηρεί αυτοματοποιημένα αντίγραφα ασφαλείας και το private storage προστατεύεται από soft-delete retention τόσο σε blobs όσο και σε containers, ώστε η τυχαία ή κακόβουλη διαγραφή να μπορεί να ανακτηθεί εντός του παραθύρου διατήρησης. Η κρίσιμη υποδομή φέρει deletion locks για αποτροπή τυχαίας κατάργησης πόρων παραγωγής.

14.3 Σύνοψη Κοινής Ευθύνης

Περιοχή	AI Interview Analyzer	Πελάτης
Υποδομή, δίκτυο, patching	Ναι	-
Ασφάλεια εφαρμογής και αγωγός AI	Ναι	-
Κρυπτογράφηση, secrets, διαμονή δεδομένων	Ναι	-
Διαχείριση χρηστών και ρόλων	Παρέχει τους ελέγχους	Διαχειρίζεται χρήστες και ρόλους
Ρύθμιση πολιτικής διατήρησης	Παρέχει τους ελέγχους	Καθορίζει το παράθυρο διατήρησης
Συγκατάθεση υποψηφίου	Παρέχει τη ροή εργασίας	Διασφαλίζει ότι χρησιμοποιείται
Ισχυρά διαπιστευτήρια τελικού χρήστη και SSO	Υποστηρίζει SSO και πολιτική	Επιβάλλει εσωτερική πολιτική

15. Threat Model και Χαρτογράφηση OWASP

Σχεδιάζουμε απέναντι σε ένα συγκεκριμένο σύνολο αντιπάλων: έναν εξωτερικό επιτιθέμενο χωρίς credentials, έναν περίεργο ή κακόβουλο authenticated χρήστη ενός οργανισμού που επιχειρεί να προσεγγίσει δεδομένα άλλου οργανισμού, μια παραβιασμένη dependency και ένα εσωτερικό λάθος. Ο παρακάτω πίνακας χαρτογραφεί τις ευρέως χρησιμοποιούμενες κατηγορίες κινδύνου OWASP Top 10 στους συγκεκριμένους ελέγχους που τις αντιμετωπίζουν σε αυτή την πλατφόρμα, καθένας από τους οποίους ελέγχεται από τις δοκιμές που περιγράφονται στην Ενότητα 12.

Κίνδυνος OWASP	Πώς τον μετριάζει η πλατφόρμα
Broken access control	Έλεγχος πρόσβασης βάσει ρόλων σε κάθε προνομιούχο endpoint· περιορισμός ανά οργανισμό· "not found" σε cross-org πρόσβαση· επαναχαρτογράφηση αναγνωριστικών· cross-org test matrix
Cryptographic failures	TLS 1.2+ κατά τη μεταφορά· AES-256 σε αδράνεια· bcrypt κατακερματισμός κωδικών· secrets σε managed vault
Injection	Parameterized queries μόνο μέσω ORM· αυστηρή επικύρωση schema· HTML sanitization κατά τον χρόνο εγγραφής
Insecure design	Πολυεπίπεδη άμυνα σε βάθος· threat modeling και architecture review σε κάθε έλεγχο
Security misconfiguration	Υποδομή ως κώδικας· network groups default-deny· security headers· απενεργοποιημένα shared storage keys· API schema μη εκτεθειμένο στην παραγωγή
Vulnerable components	Εβδομαδιαία αυτοματοποιημένη παρακολούθηση εξαρτήσεων· έλεγχοι dependency CVE στην περιοδική ανασκόπηση
Identification and authentication failures	Tokens σύντομης διάρκειας· login με rate limiting· email verification· υποστήριξη SSO· χωρίς plaintext κωδικούς
Software and data integrity failures	Pinned, immutable pipeline steps· υπογεγραμμένοι desktop installers· επαλήθευση signature webhook· production deploys ελεγχόμενα από tags
Security logging and monitoring failures	Κεντρικοποιημένη τηλεμετρία· αποκλειστικοί audit tables για ευαίσθητες ενέργειες
Server-side request forgery	Εξερχόμενες κλήσεις περιορισμένες σε αξιόπιστα endpoints· probes SSRF στην υποδομή penetration-test

Αυτή η χαρτογράφηση αποτελεί τη ραχοκοκαλιά του επιχειρήματος διασφάλισής μας: για κάθε γνωστή κατηγορία επίθεσης υπάρχει ένας ονομαστικός έλεγχος, και για κάθε ονομαστικό έλεγχο υπάρχει ένα test.

16. Διαχείριση Ευπαθειών και Υπεύθυνη Γνωστοποίηση

Η ασφάλεια δεν ολοκληρώνεται ποτέ, γι' αυτό λειτουργούμε έναν συνεχή κύκλο εντοπισμού και αποκατάστασης.

- **Εντοπισμός.** Οι ευπάθειες αναδεικνύονται από τέσσερις πηγές: την αυτοματοποιημένη σουίτα tests, τους επαναλαμβανόμενους penetration-test audits, την αυτοματοποιημένη παρακολούθηση εξαρτήσεων και αναφορές από πελάτες ή ερευνητές.
- **Διαλογή.** Σε κάθε εύρημα αποδίδεται σοβαρότητα (critical, high, medium, low ή informational) με αποδεικτικά στοιχεία και υπεύθυνο αποκατάστασης, ακριβώς όπως καταγράφεται στις αναφορές ελέγχου μας.
- **Στόχοι αποκατάστασης.** Τα critical και high ευρήματα ιεραρχούνται για άμεση αποκατάσταση· στο ιστορικό ελέγχων μας, ευρήματα υψηλότερης σοβαρότητας έχουν συνήθως επιλυθεί και επαληθευτεί εκ νέου την ίδια ημέρα. Τα medium και χαμηλότερα ευρήματα εντάσσονται στον κανονικό ρυθμό συντήρησης.
- **Επαλήθευση.** Οι διορθώσεις δοκιμάζονται εκ νέου και, όπου είναι σχετικό, εκτελείται live check στο αναπτυγμένο περιβάλλον για να επιβεβαιωθεί ότι το ζήτημα έχει πράγματι κλείσει, όχι απλώς κλείσει στον κώδικα.
- **Γνωστοποίηση.** Ζητήματα ασφάλειας μπορούν να μας αναφερθούν απευθείας. Αναγνωρίζουμε τις αναφορές, διερευνούμε και κρατούμε τον αναφέροντα ενήμερο έως την επίλυση.

17. Χαρτογράφηση Συμμόρφωσης

17.1 GDPR

Περιοχή GDPR	Υλοποίηση πλατφόρμας
Νόμιμη βάση (Art. 6)	Ρητή συγκατάθεση υποψηφίου που λαμβάνεται πριν από την επεξεργασία
Ελαχιστοποίηση δεδομένων και περιορισμός αποθήκευσης (Art. 5)	Υποβάλλονται σε επεξεργασία μόνο δεδομένα σχετικά με τη συνέντευξη· παραμετροποιήσιμη διατήρηση με αυτόματη διαγραφή
Δικαίωμα διαγραφής (Art. 17)	Διαγραφή ενιαίας μονάδας όλων των δεδομένων υποψηφίου, με καταγεγραμμένη απόδειξη διαγραφής
Δικαιώματα υποκειμένου δεδομένων (Art. 15 to 20)	Υποστηρίζονται πρόσβαση, διαγραφή, φορητότητα και εναντίωση
Υποχρεώσεις εκτελούντος την επεξεργασία (Art. 28)	Συμφωνία επεξεργασίας δεδομένων που αποδέχεται ο πελάτης κατά την εγγραφή και τηρείται σε έκδοση ανά οργανισμό
Ασφάλεια επεξεργασίας (Art. 32)	Κρυπτογράφηση, έλεγχος πρόσβασης, απομόνωση και συνεχείς δοκιμές όπως περιγράφονται σε αυτό το έγγραφο
Διαφάνεια sub-processor	Γνωστοποιείται στη συμφωνία επεξεργασίας δεδομένων με προηγούμενη ειδοποίηση για αλλαγή

17.2 EU AI Act

Η πλατφόρμα αντιμετωπίζεται ως σύστημα AI υψηλού κινδύνου που υποστηρίζει αποφάσεις απασχόλησης και διατηρούμε τεκμηρίωση ευθυγραμμισμένη με τον κανονισμό, συμπεριλαμβανομένων transparency card, τεκμηρίωσης χρήστη και δήλωσης συμμόρφωσης. Οι βασικές διασφαλίσεις, ανθρώπινη εποπτεία, διαφάνεια, βαθμολόγηση βάσει αποδεικτικών στοιχείων και αυστηρά όρια ως προς το τι αξιολογεί η AI, περιγράφονται στην Ενότητα 10. Συνεχίζουμε να ωριμάζουμε την επίσημη τεκμηρίωση συμμόρφωσής μας καθώς προχωρά το χρονοδιάγραμμα εφαρμογής του κανονισμού.

17.3 Πιστοποιήσεις Φιλοξενίας

Η πλατφόρμα λειτουργεί εξ ολοκλήρου στο Microsoft Azure, του οποίου τα data centers διαθέτουν ανεξάρτητες πιστοποιήσεις, συμπεριλαμβανομένων ISO 27001 και SOC 2. Αυτές οι πιστοποιήσεις καλύπτουν τα φυσικά επίπεδα και τα επίπεδα πλατφόρμας κάτω από την εφαρμογή μας· οι έλεγχοι σε επίπεδο εφαρμογής είναι εκείνοι που περιγράφονται σε όλο αυτό το έγγραφο.

17.4 Μητρώο Sub-processor

Sub-processor	Σκοπός	Περιοχή
Microsoft Azure	Φιλοξενία, επεξεργασία AI και ομιλίας, storage, transactional email	EU (West Europe, Sweden Central)
Stripe	Επεξεργασία συνδρομών και πληρωμών	EU (Ireland)
Fakturownia	Τιμολόγηση	EU (Poland)
ATS connector (optional)	Integration με applicant-tracking, ενεργοποιείται μόνο κατόπιν αιτήματος	EU

18. Οδικός Χάρτης Ασφάλειας

Αντιμετωπίζουμε την ασφάλεια ως πρόγραμμα συνεχούς βελτίωσης. Οι τρέχουσες πρωτοβουλίες στον οδικό μας χάρτη περιλαμβάνουν ενίσχυση των επιλογών multi-factor authentication για διαχειριστικούς λογαριασμούς, επέκταση της κεντρικής audit logging της πρόσβασης σε δεδομένα, συνέχιση της αυστηροποίησης της επικαιρότητας εξαρτήσεων σε τακτική βάση και πρόοδο προς επίσημη πιστοποίηση από τρίτο μέρος των ελέγχων που περιγράφονται σε αυτό το έγγραφο. Κανένα από αυτά δεν αποτελεί κενό που εκθέτει τα δεδομένα πελατών σήμερα· το καθένα είναι βελτίωση μιας ήδη πολυεπίπεδης στάσης.

19. Σύνοψη

Το AI Interview Analyzer προστατεύει τα δεδομένα υποψηφίων και πελατών μέσω πολυεπίπεδης αρχιτεκτονικής: δικτύου ιδιωτικού εξ ορισμού χωρίς δημόσιες υπηρεσίες δεδομένων, ισχυρής ταυτότητας και απομόνωσης ανά οργανισμό, κώδικα εφαρμογής που εξαλείφει ολόκληρες κατηγορίες ευπαθειών εκ σχεδιασμού, κρυπτογράφησης και διαμονής δεδομένων στην ΕΕ, και ελέγχων ιδιωτικότητας ενσωματωμένων στο μοντέλο δεδομένων. Αυτό που διακρίνει την πλατφόρμα είναι τα αποδεικτικά στοιχεία πίσω από αυτούς τους ισχυρισμούς. Με 3,171 αυτοματοποιημένα tests, επαναλήψιμη μεθοδολογία live penetration-testing, αποκλειστικό πρόγραμμα AI-safety και ιστορικό επτά εσωτερικών ελέγχων ασφάλειας με zero critical findings, μπορούμε να δείξουμε, όχι απλώς να πούμε, ότι η πλατφόρμα είναι ασφαλής.

Appendix A: Κατάλογος Ελέγχων Ασφάλειας

Συνοπτική αναφορά των κύριων ελέγχων και των αποδεικτικών στοιχείων που υποστηρίζουν τον καθένα.

Έλεγχος	Μηχανισμός	Αποδεικτικά στοιχεία
Κρυπτογράφηση μεταφοράς	Μόνο HTTPS, TLS 1.2+, ανακατεύθυνση HTTP	Υποδομή ως κώδικας· architecture audit
Κρυπτογράφηση σε αδράνεια	Κρυπτογράφηση πλατφόρμας AES-256 σε storage και βάση δεδομένων	Ρύθμιση πλατφόρμας· architecture audit
Προστασία κωδικών	bcrypt με salt ανά κωδικό	Source control· tests authentication
Διαχείριση συνεδρίας	30-minute signed tokens, revocable server-side refresh	Source control· tests authentication
Authorization	Έλεγχος πρόσβασης τεσσάρων ρόλων σε προνομιούχα endpoints	Σουίτα tests επιβολής ρόλων
Απομόνωση tenant	Περιορισμός ερωτημάτων ανά οργανισμό· 404 σε cross-org	Cross-organization test matrix
Ασφάλεια API key	Αποθήκευση ως hash, scoped permissions, per-key rate limits	Σουίτα tests API-key
Άμυνα έναντι injection	Parameterized queries μόνο μέσω ORM	Static analysis· tests injection
Άμυνα έναντι cross-site scripting	HTML sanitization κατά τον χρόνο εγγραφής	Σουίτα tests HTML-sanitization
Rate limiting	Durable limiter βασισμένος σε βάση δεδομένων σε auth endpoints	Tests rate-limit· live burst checks
Ακεραιότητα webhook	Επαλήθευση signature παρόχου στο raw body	Σουίτα tests webhook
Διαχείριση secrets	Managed vault, purge protection, managed identity	Υποδομή ως κώδικας· architecture audit
Απομόνωση δικτύου	Private endpoints· τμηματοποίηση default-deny	Υποδομή ως κώδικας· architecture audit
Διαγραφή δεδομένων	Διαδοχική διαγραφή ενιαίας μονάδας με audit log	Σουίτα tests διαγραφής GDPR
Supply chain	Pinned pipeline steps· εβδομαδιαία παρακολούθηση εξαρτήσεων	Ρύθμιση pipeline· dependency audit

Appendix B: Συχνές Ερωτήσεις για Αξιολογητές Ασφάλειας

Πού αποθηκεύονται τα δεδομένα μας; Εξ ολοκλήρου εντός της Ευρωπαϊκής Ένωσης, στο Microsoft Azure, στη West Europe με επεξεργασία AI σε περιοχές της ΕΕ. Τα δεδομένα υποψηφίων δεν εγκαταλείπουν ποτέ την ΕΕ.

Χρησιμοποιούνται τα δεδομένα μας για εκπαίδευση μοντέλων AI; Όχι. Ο πάροχος AI δεν χρησιμοποιεί δεδομένα πελατών για εκπαίδευση.

Είναι η βάση δεδομένων προσβάσιμη από το internet; Όχι. Η δημόσια δικτυακή πρόσβαση είναι απενεργοποιημένη και η βάση δεδομένων είναι προσβάσιμη μόνο μέσω private endpoint μέσα στο virtual network.

Μπορεί ένας πελάτης να δει τα δεδομένα άλλου πελάτη; Όχι. Κάθε ερώτημα περιορίζεται στον οργανισμό του καλούντος, η cross-organization πρόσβαση επιστρέφει "not found" και ένα αυτοματοποιημένο matrix δοκιμάζει συνεχώς αυτή την απομόνωση.

Πώς αποθηκεύονται οι κωδικοί πρόσβασης; Κατακερματισμένοι με bcrypt και μοναδικό salt ανά κωδικό. Υποστηρίζεται single sign-on με Microsoft και Google, οπότε δεν αποθηκεύεται καθόλου κωδικός.

Υποστηρίζετε single sign-on; Ναι, μέσω Microsoft και Google OAuth.

Για πόσο διάστημα ισχύουν τα access tokens; Τριάντα λεπτά, σε συνδυασμό με revocable server-side refresh session που ακυρώνεται κατά το logout.

Πώς διαχειρίζεστε τη συγκατάθεση υποψηφίων; Κάθε υποψήφιος λαμβάνει έναν μοναδικό σύνδεσμο συγκατάθεσης μίας χρήσης και πρέπει να αποδεχθεί πριν από οποιαδήποτε καταγραφή ή ανάλυση. Η συγκατάθεση καταγράφεται έναντι της συγκεκριμένης διαδικασίας πρόσληψης.

Πώς διαγράφονται τα δεδομένα; Ως ενιαία μονάδα που καλύπτει την εγγραφή υποψηφίου, συνεντεύξεις, απομαγνητοφωνήσεις, ήχο, έγγραφα και συγκρίσεις, βάσει παραμετροποιήσιμου προγράμματος διατήρησης, με καταγεγραμμένη απόδειξη διαγραφής. Οι υποψήφιοι μπορούν επίσης να ζητήσουν διαγραφή απευθείας.

Διαθέτετε συμφωνία επεξεργασίας δεδομένων; Ναι, γίνεται αποδεκτή κατά την εγγραφή και τηρείται σε έκδοση ανά οργανισμό, συμπεριλαμβανομένου του μητρώου sub-processor.

Λαμβάνει η AI αποφάσεις πρόσληψης; Όχι. Παρέχει μόνο υποστήριξη απόφασης· ένας άνθρωπος ελέγχει κάθε output και λαμβάνει όλες τις αποφάσεις.

Πώς αποδεικνύετε τους ισχυρισμούς ασφάλειάς σας; Μέσω 3,171 αυτοματοποιημένων tests, συμπεριλαμβανομένης αποκλειστικής σουίτας ασφάλειας, επαναλήψιμης μεθοδολογίας penetration-testing έξι φάσεων που εκτελείται σε ενεργά περιβάλλοντα, προγράμματος δοκιμών AI-safety και επαναλαμβανόμενων γραπτών αναφορών ελέγχου.

Τι συμβαίνει όταν βρίσκετε μια ευπάθεια; Της αποδίδεται σοβαρότητα με αποδεικτικά στοιχεία και υπεύθυνο, αποκαθίσταται βάσει προτεραιοτήτων, επαληθεύεται εκ νέου συμπεριλαμβανομένων live checks όπου απαιτείται και καταγράφεται σε αναφορά ελέγχου.

Μπορούμε να εκτελέσουμε δικό μας penetration test; Οι αξιολογήσεις ασφάλειας μπορούν να κανονιστούν μέσω του account representative σας υπό κατάλληλο scope και προγραμματισμό.

Appendix C: Γλωσσάριο

Όρος	Σημασία
AES-256	Ισχυρό πρότυπο συμμετρικής κρυπτογράφησης που χρησιμοποιείται για την προστασία δεδομένων σε αδράνεια
bcrypt	Ειδικά σχεδιασμένη συνάρτηση κατακερματισμού κωδικών με salting ανά κωδικό
Managed identity	Ταυτότητα που εκδίδεται από την πλατφόρμα και επιτρέπει σε μια υπηρεσία να αυθεντικοποιείται χωρίς αποθηκευμένα keys
Private endpoint	Ιδιωτική διεύθυνση δικτύου που κρατά μια cloud υπηρεσία εκτός του δημόσιου internet
Network security group	Σύνολο κανόνων allow και deny που φιλτράρουν την κίνηση δικτύου προς ένα subnet
RBAC	Έλεγχος πρόσβασης βάσει ρόλων, που αποδίδει άδειες σύμφωνα με τον ρόλο του χρήστη
IDOR	Insecure direct object reference, flaw ελέγχου πρόσβασης έναντι του οποίου αμύνεται η πλατφόρμα
SSRF	Server-side request forgery, κατηγορία επίθεσης που διερευνάται στα penetration tests μας
Web application firewall	Edge έλεγχος που φιλτράρει κακόβουλη web κίνηση
Data processing agreement	Η σύμβαση που διέπει τον τρόπο με τον οποίο ένας processor χειρίζεται προσωπικά δεδομένα για λογαριασμό controller

Appendix D: Επικοινωνία και Έλεγχος Εγγράφου

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Για αξιολόγηση ασφάλειας, αντίγραφο της συμφωνίας επεξεργασίας δεδομένων μας ή την τεκμηρίωση συμμόρφωσής μας με τον EU AI Act, παρακαλούμε επικοινωνήστε με τον account representative σας.

Αυτό το έγγραφο περιγράφει τη στάση ασφάλειας της υπηρεσίας AI Interview Analyzer κατά την ημερομηνία δημιουργίας που εμφανίζεται στο footer. Παρέχεται για σκοπούς αξιολόγησης και δεν αποτελεί μέρος οποιασδήποτε σύμβασης. Οι συγκεκριμένες συμβατικές δεσμεύσεις ασφάλειας καθορίζονται στην εφαρμοστέα συμφωνία και στη συμφωνία επεξεργασίας δεδομένων.