# الورقة البيضاء للأمن

نظرة عامة على الأمان المؤسسي - AI Interview Analyzer

| | |
|---|---|
| **المزود:** | AI Interview Analyzer Sp. z o.o. |
| **العنوان:** | ul. Jedrusik 6/53, 01-748 Warszawa, Poland |
| **NIP:** | 5253079974 |
| **REGON:** | 54402118500000 |
| **التصنيف:** | PUBLIC |
| **التاريخ:** | 08.07.2026 |

# المحتويات

# الورقة البيضاء للأمن

**المزود:** AI Interview Analyzer Sp. z o.o.، بولندا وارسو

**الجمهور المستهدف:** المشتريات، وتقنية المعلومات، وفرق أمن المؤسسات

**التصنيف:** عام

## 1. الملخص التنفيذي

AI Interview Analyzer هي منصة توظيف مؤسسية تسجل المقابلات بموافقة صريحة من المرشح، وتحولها إلى نص، وتنظمها، وتنتج دعما للتقييم قائما على الأدلة لصالح مسؤولي التوظيف. ونظرا لأن المنصة تتعامل مع البيانات الشخصية للمرشحين وتدعم عمليات التوظيف، فإن الأمن والخصوصية يعاملان على أنهما قيود تصميم أساسية، وليس ميزات أضيفت لاحقا.

البيانات، وفرق المشتريات. كل رقم في هذا المستند مستمد مباشرة من أنظمتنا الهندسية الداخلية، وليس من مواد تسويقية. بيانات العملاء والمرشحين. وقد كتبت للأشخاص الذين يراجعون الموردين: مهندسو الأمن، ومديرو تقنية المعلومات، ومسؤولو حماية تصف هذه الورقة البيضاء، بعبارات ملموسة وقابلة للتحقق، كيف نحمي

الرسالة المركزية بسيطة: **نحن لا نزعم فقط أن المنصة آمنة، بل نختبر ذلك باستمرار.** **آلي** تحتوي قاعدة الشفرة لدينا على فعليا، وننتج تقارير تدقيق مكتوبة. عبر سبعة تدقيقات أمنية داخلية في مارس وأبريل 2026، سجلنا **أكثر من 3,100 اختبار** ووسائل الحماية من الحقن، وحذف البيانات. وإضافة إلى ذلك، نشغل إطارا قابلا للتكرار لاختبارات الاختراق ضد البيئات المنشورة لدينا بحكم **zero critical findings**، بما في ذلك مجموعة أمنية مخصصة تختبر المصادقة، والتفويض، والعزل بين المؤسسات، على اعتماد رسمي من جهة خارجية لهذه الضوابط مدرج على خارطة طريقنا؛ انظر القسم 18.)**PASS**، وانتهى أحدث تدقيق . (إن الحصول

| الملخص | الخاصية الأمنية |
|---|---|
| ضمن مناطق الاتحاد الأوروبي فقط، Microsoft Azure | الاستضافة |
| شبكي بسياسة الرفض الافتراضي، وعدم وجود قاعدة بيانات عامة نقاط نهاية خاصة، تقسيم | نموذج الشبكة |
| أو أعلى أثناء النقل TLS 1.2 أثناء التخزين، و AES-256 | التشفير |
| قصيرة العمر، وتجزئة كلمات المرور باستخدام bcrypt، ودعم SSO رموز موقعة | الهوية |
| مع عزل صارم لكل مؤسسة RBAC | التحكم في الوصول |
| خزينة أسرار مركزية مع وصول عبر managed identity | الأسرار |
| موافقة صريحة، واحتفاظ قابل للتهيئة، ومحو كوحدة واحدة | الخصوصية |
| دعم للقرار فقط، مع بقاء الإنسان دائما ضمن الحلقة | الذكاء الاصطناعي المسؤول |
| من 3,100 اختبار آلي إضافة إلى اختبارات اختراق وتدقيقات متكررة أكثر | الضمان |

### 1.1 كيفية قراءة هذا المستند

وتوفر الملاحق فهرسا للضوابط، وأسئلة شائعة للمراجعين، ومعجما يمكن لفريق الأمن استخدامه مباشرة أثناء التقييم. الامتثال. للاختبار المستمر وسجل التدقيق لدينا. أما الأقسام من 14 إلى 17 فتغطي العمليات، ونمذجة التهديدات، وإدارة الثغرات، ومواءمة والشبكة، والهوية، والتطبيق، وحماية البيانات، والخصوصية، ودورة حياة التطوير الآمن. ويغطي القسمان 12 و13 برنامجنا المتميز تصف الأقسام من 3 إلى 11 الضوابط التي تحمي البيانات: البنية،

# 2. نطاق المستند والمنهجية

## 2.1 ما الذي يغطيه هذا المستند

التطبيق، وحماية البيانات، ومواءمة الخصوصية والأنظمة التنظيمية، ودورة حياة التطوير الآمن، وبرنامجنا المستمر لاختبارات الأمن.
البنية الأمنية وممارسات خدمة AI Interview Analyzer: بيئة الاستضافة، وتصميم الشبكة، وإدارة الهوية والوصول، وضوابط مستوى
تغطي هذه الورقة البيضاء

## 2.2 ما الذي يجعله قابلا للتحقق

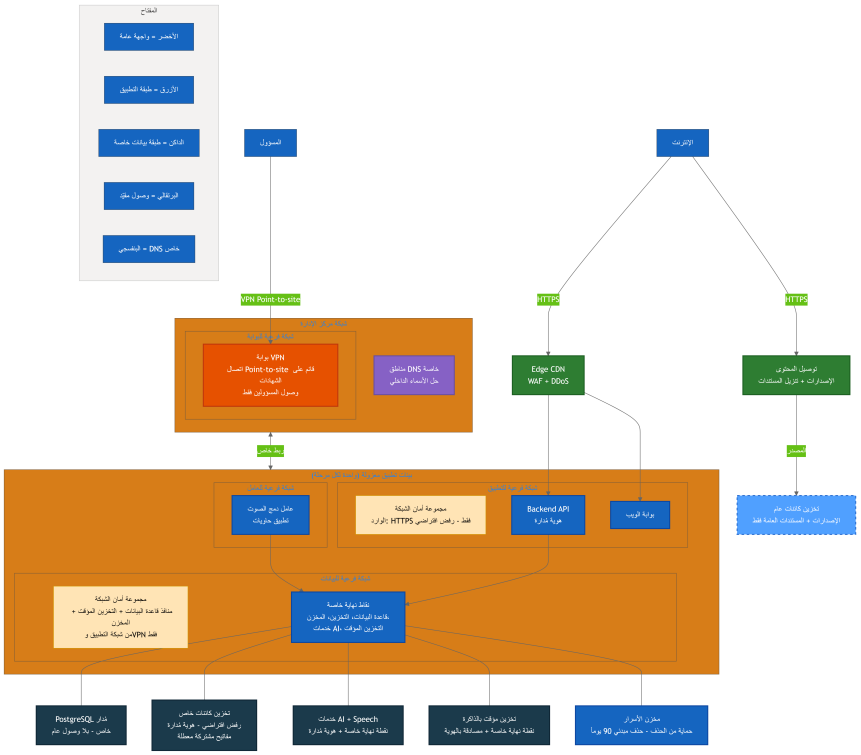
وليس مطروحا اليوم، فإننا نصرح بذلك بوضوح. نحن نفضل التقليل في الادعاء وأن نوثق، على المبالغة فيه وأن يكشف أمرنا.
يعمل، أو تعريف بنية تحتية يفرضه، أو تقرير تدقيق يسجل فحصا موثقا. وحيث يكون أحد الضوابط جزءا من خارطة طريقنا المستقبلية
رئيسي في هذا المستند بشيء ملموس وقابل للعد داخل أنظمتنا الهندسية: ضابط منفذ في الشفرة، أو اختبار يثبت أن الضابط
من السهل كتابة ادعاءات أمن الموردين، ومن الصعب الوثوق بها. لذلك ربطنا كل ادعاء

## 2.3 المسؤولية المشتركة

وضمان الحصول على موافقة المرشح عبر سير عمل الموافقة الذي توفره المنصة. يصف القسم 14 هذا التقسيم بمزيد من التفصيل.
البيانات. ويتحمل العميل مسؤولية إدارة حساباته وأدواره الخاصة، وتهيئة نوافذ الاحتفاظ بالبيانات بما يتوافق مع سياساته الداخلية،
تقدم المنصة كبرنامج كخدمة. نحن نشغل البنية التحتية، والتطبيق، وخط أنابيب الذكاء الاصطناعي، ومعالجة

# 3. نظرة عامة على البنية الأمنية

الحساسة خلف API الخلفية؛ ولا تتحدث التطبيقات العميلة مباشرة إلى قاعدة البيانات أو التخزين أو خدمات الذكاء الاصطناعي. الإلكتروني، ومعالجة الملفات، ولوحات المعلومات. ويعالج عامل دمج الصوت التسجيلات بشكل غير متزامن. وتقع جميع الحالات كعملاء. وتمتلك API خلفية مركزية جميع وظائف الاستمرارية، والمصادقة، والفوترة، وخط أنابيب الذكاء الاصطناعي، والموافقة، والبريد بنيت المنصة باعتبارها عددا صغيرا من الخدمات المتعاونة بدلا من كتلة أحادية واحدة. تعمل بوابة ويب وإضافة متصفح




يوضح المخطط أعلاه الطوبولوجيا الإنتاجية مع تعميم مقصود لأسماء الموارد. وتظهر فيه ثلاثة مبادئ:

بحيث يتطلب أي وصول هوية صالحة ومصرحا بها بغض النظر عن مسار الشبكة.**عدم التعرض المباشر لخدمات البيانات.**
إلى خزينة الأسرار عبر نقطة نهاية خاصة، وهي محمية أيضا بمصادقة هوية المنصة وسياسات وصول بأقل قدر من الامتيازات، وذاكرة التخزين المؤقت، ولا يمكن الوصول إليها إلا عبر نقاط نهاية خاصة داخل شبكة افتراضية معزولة. وتصل التطبيقات
- تم تعطيل الوصول الشبكي العام إلى قاعدة البيانات، وتخزين الكائنات الخاص، وخدمات الذكاء الاصطناعي،

وتمر حركة التطبيق المواجهة للعملاء عبر طبقة طرفية توفر WAF، وحماية DDoS، وتوصيل المحتوى.**سطح عام مفصول.**
- تخزين الكائنات العام الوحيد يحتفظ بتنزيلات الإصدارات والمستندات العامة. وهو لا يحتوي أبدا على بيانات المرشحين.

من نوع point-to-site قائم على الشهادات إلى شبكة محور الإدارة، وليس عبر الإنترنت العام.**الوصول الإداري مضبوط.**
- يصل المشغلون إلى الموارد الداخلية فقط عبر VPN

العملاء الإنتاجية موجودة أبدا في البيئات الأدنى. ويحتفظ محور إدارة مشترك فقط ببوابة VPN وprivate DNS، مع ربط خاص بكل بيئة. والإنتاج) هي بيئة معزولة بالكامل لها شبكتها الخاصة، وحسابات التخزين، وقاعدة البيانات، والأسرار الخاصة بها. ولا تكون بيانات كل مرحلة نشر (التطوير

# 4. الدفاع متعدد الطبقات

أي طبقة واحدة إلى كشف البيانات. وتنفذ كل طبقة من الطبقات أدناه، وكما هو موضح في القسم 12، تختبر كل منها على حدة. لا يعول على ضابط واحد لوقف كل هجوم. تكدس المنصة ضوابط مستقلة بحيث لا يؤدي فشل


| الطبقة | ضوابط تمثيلية |
|---|---|
| حافة الشبكة | DDoS، ونقاط نهاية خاصة، وتقسيم بسياسة الرفض الافتراضي نقل عبر TLS فقط، وWAF طرفي وحماية |
| الهوية والوصول | موقعة قصيرة العمر، وتجزئة bcrypt، وRBAC، وعزل لكل مؤسسة رموز |
| التطبيق | إلى البيانات عبر ORM فقط، وترميز المخرجات، وتحديد المعدل التحقق بالمخطط على جميع المدخلات، ووصول |
| حماية البيانات | وإقامة البيانات في الاتحاد الأوروبي، ومعالجة محكومة بالموافقة تشفير أثناء التخزين، وخزينة أسرار مع managed identity، |
| الحوكمة والخصوصية | واحدة، وذكاء اصطناعي مع إنسان داخل الحلقة، وسجل تدقيق احتفاظ قابل للتهيئة، ومحو كوحدة |
| الضمان المستمر | آلية، واختبارات اختراق قابلة للتكرار، وتدقيقات أمنية داخلية متكررة مجموعة اختبارات |

يمر ما تبقى من هذا المستند على كل طبقة بالتتابع ثم يصف كيف نثبت، باستمرار، أن هذه الطبقات متماسكة.

# 5. أمن الشبكة

## 5.1 الخصوصية افتراضيا

يتم الوصول إلى ذاكرة التخزين المؤقت، وخدمات الذكاء الاصطناعي، وخزينة الأسرار عبر نقاط نهاية خاصة مع تحليل private DNS. ويعطل مفاتيح الوصول المشتركة بالكامل، ولا يمكن الوصول إليه إلا عبر managed identity من الشبكة الفرعية للتطبيق. وبالمثل، المدارة، ولا يمكن الوصول إليها إلا عبر نقطة نهاية خاصة. كما أن تخزين الكائنات الخاص مهيأ لرفض الوصول الشبكي افتراضيا، طبقة البيانات خاصة بحكم التصميم. فقد تم تعطيل الوصول الشبكي العام إلى قاعدة بيانات PostgreSQL

بها. وسطح الهجوم الذي يمكن لخصم خارجي لمسه أصلا يقتصر على نقاط نهاية HTTPS الخاصة بالتطبيق خلف الطبقة الطرفية. مع منح هويات التطبيق صلاحية قراءة فقط للأسرار التي تحتاجها، بحيث لا يمكن استرجاع الأسرار دون هوية صالحة ومصرح التطبيقات إلى خزينة الأسرار عبر نقطة نهاية خاصة، وهي محمية بمصادقة هوية المنصة وسياسات وصول بأقل قدر من الامتيازات، عنوان URL تخزين عام لصوت المرشح: فكل من قاعدة البيانات والتخزين الخاص قد عطل فيهما الوصول الشبكي العام صراحة. وتصل عمليا، يعني ذلك عدم وجود سلسلة اتصال موجهة للإنترنت إلى قاعدة البيانات، وعدم وجود

## 5.2 تقسيم الشبكة

فلن يستطيع الانتقال بحرية إلى طبقة البيانات؛ فالمسارات المسموح بها هي فقط تلك التي يستخدمها التطبيق بشكل مشروع. ومن الشبكة الفرعية للتطبيق أو VPN الإداري فقط. وهذا يعني أنه حتى لو تمكن مهاجم بطريقة ما من الوصول إلى طبقة التطبيق، للتطبيق إلا HTTPS الوارد. أما شبكة البيانات الفرعية فلا تقبل إلا المنافذ المحددة لقاعدة البيانات وذاكرة التخزين المؤقت والخزينة، وتحكم كل شبكة فرعية مجموعة أمان شبكة تكون قاعدتها النهائية رفض جميع حركة المرور الواردة. ولا تقبل الشبكة الفرعية تنقسم كل بيئة إلى شبكات فرعية منفصلة لطبقة التطبيق، وطبقة البيانات، والعامل غير المتزامن.

## 5.3 الحافة

في التهيئة على المستوى العام أن يكشف بيانات المرشحين الخاصة، لأنها موجودة في حسابات مختلفة بقواعد شبكة مختلفة. أمامية، منفصل تماما عن التخزين الخاص الذي يحتفظ ببيانات المرشحين. ولا تختلط مستويات التخزين هذه أبدا: إذ لا يمكن لخطأ WAF، وحماية DDoS، وشبكة CDN. وتقدم تنزيلات الإصدارات والمستندات من حساب تخزين عام مخصص عبر واجهة توصيل محتوى توضع حركة التطبيق العامة أمام طبقة طرفية توفر

## 5.4 الوصول الإداري

داخل هذا النفق، لأن الوصول الشبكي العام إلى تلك الخدمات معطل. وهذا يبقي العمليات اليومية بعيدة تماما عن الإنترنت العام. نوع point-to-site تستخدم مصادقة قائمة على الشهادات. ولا يمكن الوصول إداريا إلى قاعدة البيانات وذاكرة التخزين المؤقت إلا من لا توجد نقطة نهاية إدارية عامة إلى الشبكة الخاصة. يتصل المشغلون عبر بوابة VPN من

# 6. إدارة الهوية والوصول

## 6.1 المصادقة

الخروج إلى إبطال جلسة التحديث على جانب الخادم فورا، بحيث لا يمكن لرمز تحديث مسروق أن يستمر بعد تسجيل الخروج. مصادقة المستخدم مقابل قاعدة البيانات (بما في ذلك فحص الحساب النشط) بدلا من الوثوق فقط بمحتويات الرمز. ويؤدي تسجيل صالح لمدة ثلاثين دقيقة، مقترنا برمز تحديث منفصل ومعتم على جانب الخادم. ويتم التحقق من رموز الوصول عند كل طلب، وتعاد تنشأ جلسات المستخدم باستخدام رمز وصول موقع

التي تفضل SSO، تدعم المنصة تسجيل الدخول عبر OAuth مع Microsoft وGoogle، وفي هذه الحالة لا تحتفظ بأي كلمة مرور أصلا. لا تخزن كلمات المرور مطلقا بنص عادي. بل تجزأ باستخدام bcrypt مع salt فريد لكل كلمة مرور. وبالنسبة للمؤسسات

المدة قبل اعتبار الحساب المسجل ذاتيا حسابا متحققا، كما أن إعادة إرسال رسائل التحقق محددة المعدل لمنع إساءة الاستخدام. ويتحقق من ملكية البريد الإلكتروني عبر رابط تحقق أحادي الاستخدام ومحدد

## 6.2 RBAC

تتحقق من كل من الدور وحالة التحقق للمتصل. وتحرس عمليات التحقق من الأدوار هذه ما يزيد بكثير على مئة عملية API متميزة. وhiring manager، وrecruiter، وadministrator. ويفرض الوصول إلى العمليات المميزة بواسطة تبعيات على جانب الخادم يفرض التفويض من خلال نموذج أدوار بأربعة أدوار متزايدة في الامتياز: interviewer،

| الدور | القدرات النموذجية |
|---|---|
| Interviewer | يجري المقابلات المعينة له؛ ولا يرى إلا المقابلات المسندة إليه |
| Hiring manager | يدير عمليات التوظيف التي يملكها أو يكون عضوا فيها |
| Recruiter | إدارة كاملة لعمليات التوظيف والمرشحين داخل المؤسسة |
| Administrator | إعدادات المؤسسة، والفوترة، وإدارة المستخدمين ومفاتيح API |

يرى interviewers إلا المقابلات المسندة إليهم. ولذلك يفرض الامتياز على مستوى "أي إجراء" وعلى مستوى "أي سجلات" أيضا. المنصة قواعد رؤية على مستوى البيانات. فلا يرى hiring managers إلا عمليات التوظيف التي أنشأوها أو كانوا أعضاء فيها؛ ولا إلى جانب فحوصات الأدوار العامة، تطبق

## 6.3 العزل لكل مؤسسة

على مستوى النقل؛ إذ تقدم API معرفات عرض وتعيد تعيينها لكل طلب، ما يزيل فئة شائعة من هجمات التعداد عبر المستأجرين. أخرى، ترجع المنصة استجابة "not found" بدلا من الكشف عن وجود السجل. ولا تكشف معرفات قاعدة البيانات الداخلية أبدا كل هوية موثقة معرف مؤسسة، وتكون استعلامات البيانات مقيدة بهذه المؤسسة. وعندما يطلب مستخدم سجلا يخص مؤسسة المنصة متعددة المستأجرين، ويعامل عزل المستأجرين كضابط أمني من الدرجة الأولى. تحمل

المؤسسات تحاول الوصول إلى بيانات مؤسسة باستخدام بيانات اعتماد مؤسسة أخرى، وتؤكد أن كل محاولة من هذا النوع تفشل. وهذا ليس مجرد نية تصميمية. فكما هو موضح في القسم 12، تشغل مجموعتنا الآلية مصفوفة كبيرة عبر

## 6.4 الوصول البرمجي

من فئة خطة المؤسسة. ويستخدم التحقق من المفاتيح مقارنة آمنة زمنيا لتجنب تسريب المعلومات عبر توقيت الاستجابة. (قراءة، أو كتابة، أو تكامل ATS)، ويمكن تقييده بشبكات مصدر محددة، ويمكن إبطاله فورا، ويخضع لحدود معدل لكل مفتاح مستمدة تخزن إلا على شكل hash؛ ويعرض المفتاح الخام مرة واحدة عند الإنشاء ولا يعرض مجددا. ويحمل كل مفتاح نطاق صلاحيات صريحا يمكن للمؤسسات في الخطط المؤهلة إصدار مفاتيح API. تستخدم المفاتيح بادئة مميزة، وتحمل 128 bits من entropy، ولا لأغراض التكامل،

# 7. أمن التطبيق

كتب التطبيق بطريقة تهدف إلى إزالة فئات كاملة من الثغرات بدلا من ترقيعها حالة بحالة.

ذات معاملات. ولا تحتوي قاعدة الشفرة على SQL خام منسق كسلاسل نصية. وهذا يزيل SQL injection بنيويا.**الحقن.**
- تتم جميع عمليات الوصول إلى قاعدة البيانات عبر object-relational mapper مع استعلامات

كبيرة الحجم، كما تجزأ نقاط النهاية القائمة على القوائم إلى صفحات للحد من استهلاك الموارد.**التحقق من المدخلات.**
- يتحقق من كل جسم طلب مقابل مخطط صارم قبل أن يصل إلى منطق الأعمال. وترفض الحمولات

وتؤكد مجموعة اختبارات مخصصة إزالة وسوم script، ومعالجات الأحداث، وروابط javascript.**ترميز المخرجات وXSS.**
على أنه غير موثوق. وحيث يلزم عرض المحتوى كـ HTML، فإنه يمر عبر منظف قائم على قائمة سماح عند وقت الكتابة،
- يتعامل مع النص الذي يقدمه المستخدم والنص الذي يولده الذكاء الاصطناعي

الدور، والمؤسسة، ورصيد الاعتمادات، بحيث لا يستطيع العميل تصعيد الامتياز عبر نشر حقول إضافية.**التعيين الجماعي.**
- تستخدم عمليات التحديث مخططات صريحة تستبعد الحقول المميزة مثل

كلمة المرور، وإعادة إرسال التحقق حدوده الخاصة. كما تم تقوية تحليل IP العميل ضد انتحال رؤوس التمرير.**تحديد المعدل.**
أمام إعادة التشغيل ويعمل بشكل صحيح عبر عدة نسخ من التطبيق. ولكل من تسجيل الدخول، والتسجيل، وإعادة تعيين
معدلات نقاط النهاية الخاصة بالمصادقة والمعرضة لإساءة الاستخدام باستخدام محدد متين ومدعوم بقاعدة البيانات يصمد
- تحدد

الواردة من مزودي الدفع والبريد الإلكتروني مقابل توقيعات المزود على جسم الطلب الخام قبل معالجتها..**Webhooks.**
- يتحقق من webhooks

ويتحقق منها، وتخزن تحت معرفات منشأة بدلا من أسماء يزودها المستخدم، وتقيد لكل طلب ولكل مؤسسة.**رفع الملفات.**
- تقيد الرفوعات بالحجم،

نوع المحتوى والإطار، وسياسة المحيل، وسياسة أذونات مقيدة، كما تخفي لافتات الخادم وإطار العمل.**رؤوس الأمان.**
- في الإنتاج، تحمل الاستجابات رؤوس HSTS، وخيارات

# 8. حماية البيانات

## 8.1 التشفير

تصدر API وبوابة الويب رؤوس HSTS الصارمة إلى جانب مجموعة من رؤوس التقوية، وتخفي لافتات إصدارات الخادم وإطار العمل. الشبكة حصريا عبر HTTPS باستخدام TLS 1.2 أو أعلى؛ ويعاد توجيه HTTP النصي الصريح إلى HTTPS في كل طبقة. وفي الإنتاج، جميع البيانات أثناء التخزين باستخدام AES-256 عبر طبقات التشفير الخاصة بالتخزين وقاعدة البيانات في Azure. وتقدم جميع حركة تشفر

## 8.2 إدارة الأسرار

وتمنح سياسات الوصول إلى الخزينة مبادئ التطبيق صلاحية قراءة فقط للأسرار المحددة التي تحتاجها، وفقا لمبدأ أقل الامتيازات. المشتركة للتخزين الخاص بالكامل، بحيث لا يكون الوصول ممكنا إلا عبر تعيينات أدوار قائمة على الهوية ومقيدة بالمورد الفردي. Azure باستخدام system-assigned managed identities بدلا من مفاتيح طويلة العمر؛ فعلى سبيل المثال، عطلت مفاتيح الوصول التطبيق في خزينة أسرار مركزية مع تمكين purge protection ونافذة soft-delete مدتها تسعون يوما. وتصادق التطبيقات على موارد تحتفظ أسرار

## 8.3 إقامة البيانات

وتجري معالجة الذكاء الاصطناعي في مناطق الاتحاد الأوروبي. ولا يستخدم مزود الذكاء الاصطناعي بيانات العملاء لتدريب نماذجه. داخل الاتحاد الأوروبي. وتقع استضافة التطبيق، وقاعدة البيانات، والتخزين، وذاكرة التخزين المؤقت، والأسرار في West Europe، تخزن جميع بيانات العملاء والمرشحين وتعالج

## 8.4 حياة مقابلة واحدة

متسلسل مسجل. وفي أي وقت، يمكن لحقوق المرشح مثل السحب، أو الحذف، أو الوصول، أو قابلية النقل أن تقاطع هذا التدفق. داخل مراكز بيانات في الاتحاد الأوروبي. وتكتب النتائج إلى تخزين مشفر. ثم تحكم كل سجلاتها بساعة احتفاظ واحدة تنتهي بحذف واحدة من البداية إلى النهاية. تلتقط الموافقة وتسجل قبل معالجة أي شيء. ويشفر الرفع أثناء النقل. ويجري النسخ والتحليل أوضح طريقة لفهم ضوابط حماية البيانات هي تتبع مقابلة

# 9. الخصوصية حسب التصميم وGDPR

الخصوصية مدمجة في نموذج البيانات وسير العمل، وليست مجرد شيء يضاف عبر السياسة وحدها.

## 9.1 الموافقة

الاستجابة، مقابل عملية التوظيف المحددة تلك، بحيث تكون الموافقة دائما مقيدة بعملية توظيف ملموسة بدلا من منحها عالميا. أحادي الاستخدام عبر البريد الإلكتروني. يراجع المرشح ما سيحدث ثم يقبل أو يرفض. وتسجل حالة الموافقة، بما في ذلك وقت أي مقابلة ولا تحلل دون موافقة صريحة من المرشح. وعندما يضاف مرشح إلى عملية توظيف، تصدر المنصة رابط موافقة فريدا لا تسجل

**موافقة المرشح: صريحة ومسجلة قبل أي معالجة**


## 9.2 الاحتفاظ والمحو

والنصوص، والتسجيلات الصوتية، والمستندات، والمقارنات كلها معا، ويسجل الحذف في سجل تدقيق. ولا توجد بقايا جزئية أو يتيمة. قبل نحو خمسة عشر يوما) وتوفر تمديدا بنقرة واحدة. وعندما تحذف البيانات، تحذف كوحدة واحدة: يزال سجل المرشح، والمقابلات، وليس مؤقت منفصل لكل عنصر. تبدأ الساعة عند تسجيل قرار التوظيف. وقبل انتهاء صلاحية البيانات، ترسل المنصة تحذيرا (افتراضيا اثنا عشر شهرا وحد أدنى قابل للتهيئة قدره ثلاثون يوما، ويمكن تجاوزه لكل مرشح. وتوجد ساعة احتفاظ واحدة لبيانات المرشح، الاحتفاظ بالبيانات قابل للتهيئة لكل مؤسسة، مع افتراضي قدره

توضح دورة الحياة أدناه هذه الساعة الواحدة وكيف تنتهي إلى حذف متسلسل واحد مع دليل مسجل على المحو.

**الاحتفاظ بالبيانات: ساعة واحدة لكل مرشح، وحذف كوحدة مفردة**


## 9.3 حقوق صاحب البيانات والمعالجون الفرعيون

تلك الاتفاقية، ويتلقى العملاء إشعارا مسبقا بأي تغيير. ويتضمن القسم 17 سجل المعالجين الفرعيين ومواءمة الامتثال مادة بمادة. لكل مؤسسة. ويفصح عن المعالجين الفرعيين لدينا وأدوارهم، وكلهم داخل الاتحاد الأوروبي أو بموجب ضمانات مناسبة، في والحذف، وقابلية النقل، والاعتراض، والشرح. وتنفذ المعالجة بموجب DPA يقبلها العملاء عند التسجيل وتكون مرقمة بالإصدار تدعم المنصة حقوق صاحب البيانات المطلوبة بموجب GDPR، بما في ذلك الوصول،

# 10. الذكاء الاصطناعي المسؤول وEU AI Act

تندرج المنصة ضمن الفئة عالية المخاطر في EU AI Act لأنها تدعم قرارات التوظيف، ونحن نتعامل مع هذا التصنيف بجدية.

وهذا يبقي الإنسان داخل الحلقة بوضوح.**الذكاء الاصطناعي هو دعم للقرار، وليس صانع قرار.**القاعدة الحاكمة للمنتج هي أن والأجوبة، ويقيم الإجابات وفق معايير يحددها مسؤول التوظيف، ويصوغ ملاحظات أولية، ثم يراجع إنسان كل مخرج قبل استخدامه. لا يقبل النظام مرشحا أو يرفضه تلقائيا أبدا. فهو ينسخ الكلام، وينظم الأسئلة

من مدخلات التقييم للحد من التحيز. وننشر بطاقة شفافية، ووثائق مستخدم، وإعلان مطابقة يصف النظام وحدوده وضماناته. أو لغة الجسد. ويرتكز التقييم على أدلة من النص المنسوخ وعلى معايير يحددها مسؤول التوظيف، وتستبعد أسماء المرشحين فهو لا يقيم الشخصية، أو "الملاءمة الثقافية"، أو الحالة العاطفية، أو نبرة الصوت، أو اللكنة، أو الجنس، أو العمر، أو العرق، أو المظهر، ولا تقل أهمية عن ذلك الأمور التي لا يفعلها الذكاء الاصطناعي.

| كيف يعمل | ضابط الذكاء الاصطناعي المسؤول |
|---|---|
| مسؤول توظيف كل درجة وكل جزء من الملاحظات قبل الاستخدام يراجع | الإنسان داخل الحلقة |
| لا يقبل النظام مرشحا تلقائيا ولا يرفضه تلقائيا | عدم وجود قرارات آلية |
| تشير الدرجات إلى الأدلة الداعمة من النص المنسوخ | تقييم قائم على الأدلة |
| تستبعد الأسماء من التقييم؛ ويقيم الجوهر فوق الأسلوب | تصميم مضاد للتحيز |
| لا تقيم الشخصية، أو العاطفة، أو اللكنة، أو الخصائص المحمية مطلقا | حدود النطاق |
| تمر الملاحظات الخاصة بالمرشح عبر حاجز أمان للتوليد والتحقق | سلامة ملاحظات المرشح |

المطالبات الخاصة بالذكاء الاصطناعي وتختبر بواسطة برنامج مخصص لاختبارات سلامة الذكاء الاصطناعي موضح في القسم 12.3. هذه القيود ليست واردة فقط في الوثائق؛ بل هي مشفرة في طبقة

# 11. دورة حياة التطوير الآمن

يفرض الأمن في الطريقة التي نبني بها البرمجيات وننشرها، وليس فقط في النظام أثناء تشغيله.

بنية تحتية، وحسابات تخزين، وقاعدة بيانات، وأسرار، ونطاقات فرعية خاصة بها. ولا توجد حالة مشتركة.**فصل البيئات.**
- بيئتا التطوير والإنتاج منفصلتان بالكامل، ولكل منهما

ويمكن للمراجع أن يقرأ بالضبط أي المنافذ مفتوحة، وأي الموارد خاصة، وأي الهويات تملك أي الأذونات.**البنية التحتية كرمز.**
- تعرف بيئة السحابة بالكامل كرمز وتراجع كرمز، ما يجعل الوضع الأمني قابلا للتدقيق وقابلا لإعادة الإنتاج.

وتعمل مجموعة الاختبارات الآلية كبوابة إصدار: فلا يمكن شحن نشر إذا فشلت الاختبارات.**عمليات نشر مثبتة ومضبوطة.**
وتكون عمليات النشر إلى الإنتاج قائمة على الوسوم، ولا تشغل إلا عبر خط الإنتاج المحمي، وتخضع لموافقة مطلوبة.
- كل خطوة في خط CI/CD مثبتة إلى إصدار دقيق وغير قابل للتغيير.

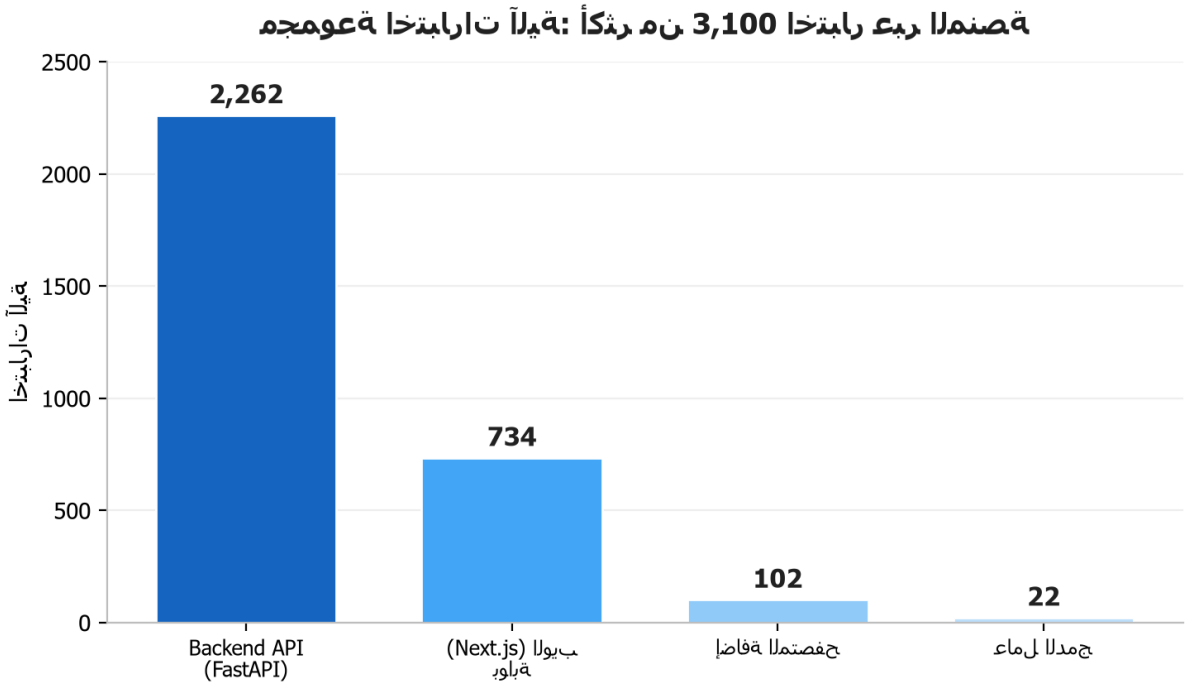
والبنية التحتية، وتعريفات خط الأنابيب، كما تشكل تدقيقات التبعيات جزءا من مراجعتنا الأمنية الدورية.**نظافة التبعيات.**
- تقترح المراقبة الآلية للتبعيات تحديثات أسبوعية عبر الخلفية، والويب،
- تعيش الأسرار في الخزينة وفي أسرار خطوط الأنابيب المحمية، ولا توجد أبدا في الشفرة المصدرية.**انضباط الأسرار.**

# 12. الاختبارات الأمنية المستمرة

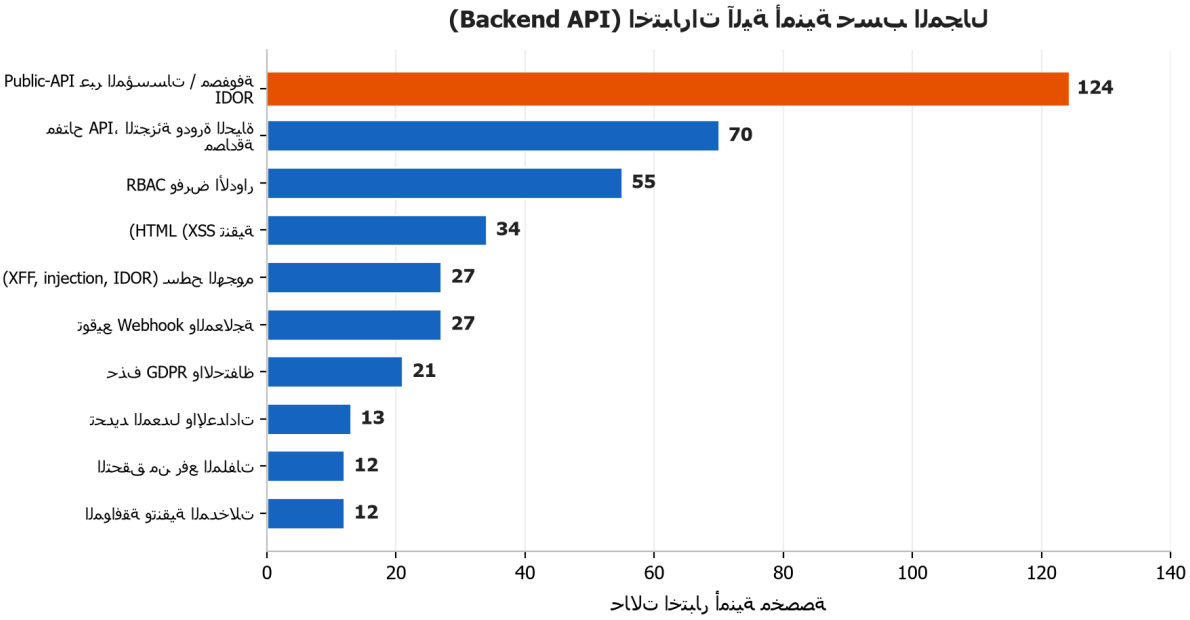
الموردين إظهاره. نحن نتعامل مع الأمن باعتباره شيئا يجب قياسه باستمرار، عبر فحوصات قابلة للتنفيذ، لا شيئا يزعم مرة واحدة. هذا هو قلب قصة الضمان لدينا والجزء الذي لا يستطيع معظم

## 12.1 مجموعة الاختبارات الآلية

تشمل API الخلفية، وبوابة الويب، وإضافة المتصفح، وعامل دمج الصوت.**أكثر من 3,100 اختبار آلي**تغطي المنصة




الضوابط الموصوفة سابقا في هذا المستند. ويعرض المخطط أدناه تفصيل الاختبارات الخاصة بالأمن في API الخلفية حسب المجال. وهذه ليست اختبارات وظيفية فقط. فهناك مجموعة أمنية كبيرة ومخصصة تختبر




ولأن هذه الاختبارات تعمل كبوابة إصدار، فإن أي تراجع يضعف أيا من هذه الضوابط سيوقف الإصدار بدلا من الوصول إلى العملاء. الخاصة بـ XSS، واختبارات فرض الأدوار على نموذج الأدوار الكامل، واختبارات تثبت أن بيانات المرشح تحذف فعليا كوحدة واحدة.

عشرات من اختبارات سطح الهجوم العدائية لانتحال رؤوس التمرير، وحقن الرؤوس، وتسرب المعرفات، ومجموعة مركزة لتنقية HTML API الخاص بالمؤسسة نفسها، ومفتاح API لمؤسسة منافسة، مع التأكيد أن كل محاولة عبر المؤسسات محجوبة. كما تتضمن أمور كثيرة أخرى، تتضمن هذه المجموعة مصفوفة كبيرة للـ API العامة تشغل كل نقطة نهاية باعتبارها مستخدما مشروعا، ومفتاح ومن بين

## 12.2 اختبارات الاختراق الحية

نحافظ على منهجية قابلة للتكرار لاختبارات الاختراق تشغل نصوص هجوم فعلية ضد بيئة حية. وهي منظمة في ست مراحل: تثبت الاختبارات الآلية على مستوى الوحدة أن الضوابط تتصرف بشكل صحيح في العزل. ولإثبات أنها تتماسك في نشر حقيقي،

| المرحلة | التركيز | أمثلة لما يختبر |
|---|---|---|
| 1. التحليل الثابت | الشفرة المصدرية | الخطرة، وغياب المصادقة، وHTML غير الآمن الأسرار، وأنماط الحقن، والوظائف |
| 2. مراجعة البنية | البنية التحتية | الخاصة، والتقسيم، وTLS، وتهيئة الأسرار نقاط النهاية |
| 3. تحليل متجهات الهجوم | التحكم بالمصدر والسحابة | حماية الفروع، ونطاق الهوية، والتعرض العام |
| 4. اختبارات الاختراق الحية | البيئة العاملة | بالرموز، وSSRF، ودفعات حدود المعدل والوصول عبر المؤسسات، والحقن، والتلاعب الفحص دون مصادقة، |
| 5. التقييم المؤسسي | النضج | أمنية مقيمة مقابل خط أساس مؤسسي ست عشرة فئة |
| 6. التبعيات وسلسلة التوريد | مخاطر الأطراف الثالثة | إجراءات خط الأنابيب، وسلامة ملفات القفل تدقيق CVE للتبعيات، وتثبيت |

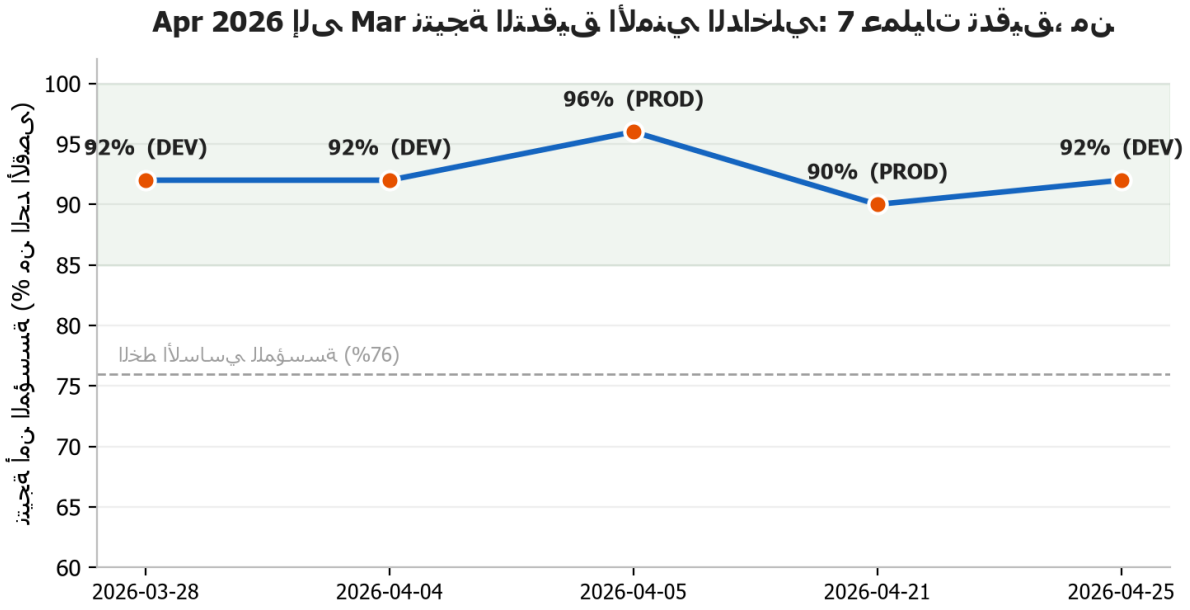
تعريف السحابة؛ وتدفع نقاط نهاية المصادقة بسرعة للتأكد من أن تحديد المعدل يعمل بالفعل في البيئة الحية، وليس نظريا فقط. وتحقن حمولات XSS وقوالب الخادم وتؤكد تحييدها؛ وتتلاعب برموز المصادقة وتؤكد رفضها؛ وتحاول SSRF ضد نقاط نهاية بيانات دون بيانات اعتماد وتؤكد أنها ترفض الوصول؛ وتسجل مؤسستين وتحاول الوصول إلى سجلات إحداهما بواسطة حساب الأخرى؛ المرحلة 4 هي اختبار عدائي حقيقي ضد نظام منشور، وليست قائمة تحقق. فهي تفحص نقاط النهاية المحمية

## 12.3 اختبار سلامة ملاحظات المرشح

كلا من المرشح، الذي ينبغي أن يتلقى ملاحظات بناءة ومحترمة، والعميل، الذي ينبغي ألا يتسرب رأي داخلي منه إلى الخارج. على ألفاظ بذيئة، ولا تكشف أو تنسب هوية مسؤول توظيف أو رأيه الخاص، ولا تطلق تسميات حكمية على الشخصية. وهذا يحمي الميزة. فهو يغذي النظام عمدا بملاحظات قاسية وعدائية من مسؤولي التوظيف ويؤكد أن المخرجات الموجهة للمرشح لا تحتوي أبدا نظرا لأن المنصة يمكنها توليد ملاحظات تطوير خاصة للمرشحين، فإننا نشغل برنامج سلامة عدائيا منفصلا ضد هذه

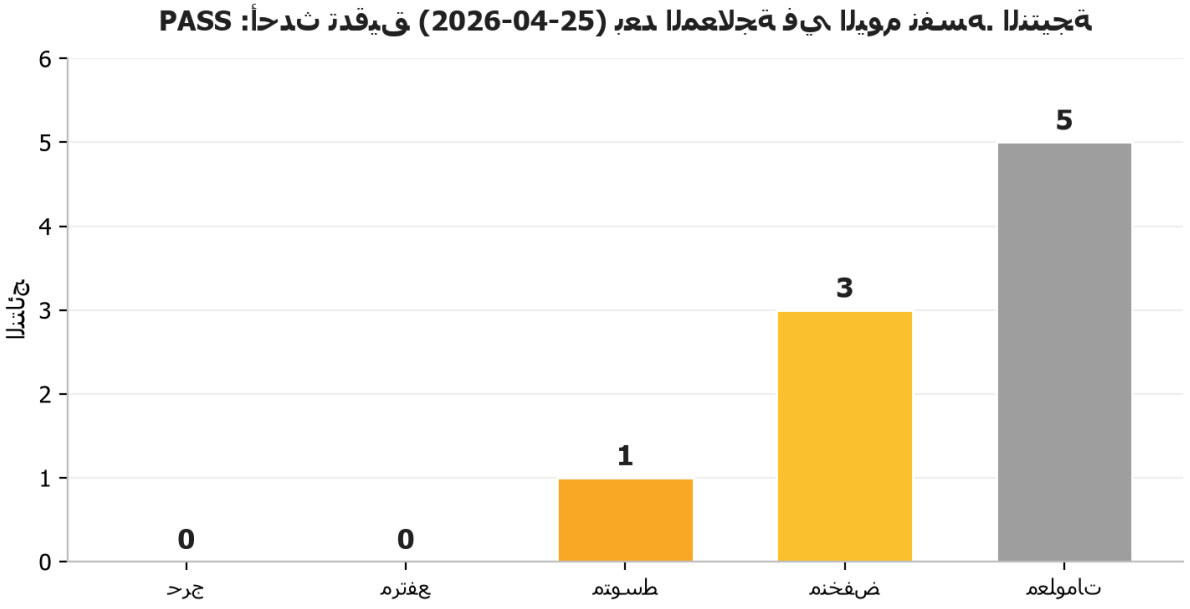
# 13. نتائج التدقيق الأمني

أما الاعتماد الرسمي من جهة خارجية لنفس الضوابط فهو مدرج على خارطة طريقنا. وبين أواخر مارس وأواخر أبريل 2026 أكملنا تقرير مؤرخ يتضمن نتائج مصنفة حسب الشدة، وأدلة، وإجراءات معالجة. وهذه تدقيقات داخلية تجرى عبر عمليتنا الأمنية الخاصة؛ **seven**نجري تدقيقات أمنية متكررة باستخدام منهجية منظمة وقابلة للتكرار لاختبارات الاختراق، ونكتب كل تدقيق على شكل عبر بيئتي التطوير والإنتاج.**such audits**




النتيجة التي تهم العميل المحتمل أكثر من غيرها هي الاتساق: **across all seven audits there were zero critical findings.**. الأقصى الممكن للدرجة مع إضافة فئات أكثر للتقييم)، ولهذا يبقى خط الدرجة المعيارية مرتفعا حتى مع ارتفاع العتبة. تمت معالجتها بسرعة، وغالبا في اليوم نفسه، ثم أعيد التحقق منها. وقد شدد معيار التقييم عمدا خلال هذه الفترة (إذ رفع الحد وفي الحالات النادرة التي ظهرت فيها مشكلة أعلى شدة،

عمليا. فقد جرى تحديد مشكلتين أعلى شدة، وتم إصلاحهما كلتاهما وإعادة التحقق منهما في اليوم نفسه، وأغلق التدقيق بحكم مشكلات جاهزة للاستغلال ضمن نموذج التهديد الحالي.**PASS**ويوضح أحدث تدقيق لدينا، في 25 April 2026، كيف تعمل العملية دون بقاء أي



| الحكم | Critical | البيئة | التدقيق |
|---|---|---|---|
| جاهز للإنتاج | 0 | Development | 2026-03-28 |
| جاهز للمؤسسات | 0 | Development | 2026-04-04 |
| جاهز للمؤسسات | 0 | Production | 2026-04-05 |
| جاهز للإنتاج، مع ملاحظات | 0 | Development | 2026-04-20 |
| نجاح مع ملاحظات | 0 | Development | 2026-04-20 |
| آمن، دون نتائج قابلة للاستغلال | 0 | Production | 2026-04-21 |
| نجاح | 0 | Development | 2026-04-25 |

عنها بجدية، وتغلق بسرعة لأن العملية مصممة لإغلاقها. أما المورد الذي لا يبلغ مطلقا عن أي نتيجة، فعادة ما يكون موردا لا يبحث. إن النمط عبر هذه التدقيقات هو أصدق دليل يمكننا تقديمه: تكتشف المشكلات لأننا نبحث

# 14. المرونة التشغيلية والمسؤولية المشتركة

## 14.1 المراقبة والتسجيل

القانونية، واستدعاءات الذكاء الاصطناعي في جداول تدقيق مخصصة، بحيث يوجد سجل متين يوضح من فعل ماذا بالبيانات المهمة. وخدمة لمراقبة التطبيقات، ما يمنحنا رؤية حول الإتاحة والسلوك. وتسجل الإجراءات الحساسة مثل حذف البيانات، وقبول الاتفاقيات تتدفق القياسات عن التطبيق والمنصة إلى مساحة عمل مركزية لتحليلات السجلات

## 14.2 النسخ الاحتياطي والاستعادة

الحذف العرضي أو الخبيث داخل نافذة الاحتفاظ. كما تحمل البنية التحتية الحرجة أقفال حذف لمنع الإزالة العرضية لموارد الإنتاج. المدارة بنسخ احتياطية آلية، ويحمى التخزين الخاص باحتفاظ soft-delete لكل من blobs وcontainers، بحيث يمكن استعادة تحتفظ قاعدة البيانات

## 14.3 ملخص المسؤولية المشتركة

| العميل | AI Interview Analyzer | المجال |
|---|---|---|
| - | نعم | البنية التحتية، والشبكة، والتصحيح |
| - | نعم | أمن التطبيق وخط أنابيب الذكاء الاصطناعي |
| - | نعم | التشفير، والأسرار، وإقامة البيانات |
| يدير المستخدمين والأدوار | يوفر الضوابط | إدارة المستخدمين والأدوار |
| يحدد نافذة الاحتفاظ | يوفر الضوابط | تهيئة سياسة الاحتفاظ |
| يضمن استخدامه | يوفر سير العمل | موافقة المرشح |
| يفرض السياسة الداخلية | يدعم SSO والسياسة | اعتماد المستخدم النهائي القوية وSSO بيانات |

# 15. نموذج التهديد ومواءمة OWASP

في OWASP Top 10 بالضوابط المحددة التي تعالجها في هذه المنصة، وكل منها يختبر عبر الاختبارات الموصوفة في القسم 12. يحاول الوصول إلى بيانات مؤسسة أخرى، وتبعية مخترقة، وخطأ من الداخل. ويربط الجدول أدناه فئات المخاطر الشائعة الاستخدام نصمم في مواجهة مجموعة ملموسة من الخصوم: مهاجم خارجي بلا بيانات اعتماد، ومستخدم موثق فضولي أو خبيث من مؤسسة نحن

| كيف تخففها المنصة | مخاطر OWASP |
|---|---|
| not"على كل نقطة نهاية مميزة؛ وتقييد لكل مؤسسة؛ و RBAC وإعادة تعيين المعرفات؛ ومصفوفة اختبارات عبر المؤسسات "found عند الوصول عبر المؤسسات؛ | Broken access control |
| وتجزئة كلمات المرور باستخدام AES-256أثناء النقل؛ و TLS 1.2+ ؛ والأسرار في خزينة مدارةbcrypt أثناء التخزين؛ | Cryptographic failures |
| ORM فقط؛ والتحقق الصارم بالمخطط؛ وتنقية HTML عند وقت الكتابة استعلامات ذات معاملات عبر | Injection |
| متعدد الطبقات؛ ونمذجة التهديدات ومراجعة البنية في كل تدقيق دفاع | Insecure design |
| مفاتيح التخزين المشتركة؛ وعدم كشف مخطط API في الإنتاج ومجموعات شبكة بسياسة الرفض الافتراضي؛ ورؤوس أمان؛ وتعطيل البنية التحتية كرمز؛ | Security misconfiguration |
| آلية أسبوعية للتبعيات؛ وتدقيقات CVE للتبعيات في المراجعة الدورية مراقبة | Vulnerable components |
| البريد الإلكتروني؛ ودعم SSO؛ وعدم وجود كلمات مرور بنص عادي رموز قصيرة العمر؛ وتسجيل دخول محدد المعدل؛ والتحقق من | Identification and authentication failures |
| من توقيع webhook؛ وعمليات نشر إنتاجية مضبوطة بالوسوم خطوات خط أنابيب مثبتة وغير قابلة للتغيير؛ والتحقق | Software and data integrity failures |
| قياسات مركزية؛ وجداول تدقيق مخصصة للإجراءات الحساسة | Security logging and monitoring failures |
| إلى نقاط نهاية موثوقة؛ وفحوصات SSRF في إطار اختبار الاختراق تقييد الاتصالات الصادرة | Server-side request forgery |

هذا الربط هو العمود الفقري لحجتنا في الضمان: فلكل فئة معروفة من الهجوم ضابط مسمى، ولكل ضابط مسمى اختبار.

# 16. إدارة الثغرات والإفصاح المسؤول

الأمن لا يكتمل أبدا، لذلك ندير حلقة مستمرة من الاكتشاف والمعالجة.

**الاكتشاف.** الاختبارات الآلية، وتدقيقات اختبارات الاختراق المتكررة، والمراقبة الآلية للتبعيات، وبلاغات العملاء أو الباحثين.
- تكشف الثغرات من أربعة مصادر: مجموعة

**الفرز.** high، أو medium، أو low، أو informational) مع أدلة ومالك للمعالجة، تماما كما هو مسجل في تقارير التدقيق لدينا.
- تسند لكل نتيجة شدة (critical، أو

**أهداف المعالجة.** وإعادة التحقق منها في اليوم نفسه. أما النتائج المتوسطة والأدنى فتدرج في وتيرة الصيانة الاعتيادية.
- تعطى النتائج critical وhigh أولوية للمعالجة الفورية؛ وفي سجل التدقيق لدينا، جرى عادة حل النتائج الأعلى شدة

**التحقق.** وعند الاقتضاء يجرى فحص حي ضد البيئة المنشورة للتأكد من إغلاق المشكلة فعليا، لا إغلاقها في الشفرة فقط.
- تعاد اختبارات الإصلاحات،

**الإفصاح.** الإبلاغ عن المخاوف الأمنية لنا مباشرة. ونحن نقر بالبلاغات، ونحقق فيها، ونبقي المبلغ على اطلاع حتى الحل.
- يمكن

# 17. مواءمة الامتثال

## 17.1 GDPR

| تنفيذ المنصة | مجال GDPR |
|---|---|
| تلتقط موافقة صريحة من المرشح قبل المعالجة | الأساس القانوني (Art. 6) |
| البيانات ذات الصلة بالمقابلة؛ واحتفاظ قابل للتهيئة مع حذف تلقائي لا تعالج إلا | تقليل البيانات وتحديد التخزين (Art. 5) |
| جميع بيانات المرشح كوحدة واحدة، مع دليل مسجل على المحو حذف | الحق في المحو (Art. 17) |
| الوصول، والحذف، وقابلية النقل، والاعتراض مدعومة | حقوق صاحب البيانات (Art. 15 to 20) |
| يقبل عند التسجيل ويرقم بالإصدار لكل مؤسسة DPA | التزامات المعالج (Art. 28) |
| والعزل، والاختبارات المستمرة كما هو موضح في هذا المستند التشفير، والتحكم في الوصول، | أمن المعالجة (Art. 32) |
| يفصح عنها في DPA مع إشعار مسبق بالتغيير | شفافية المعالجين الفرعيين |

## 17.2 EU AI Act

يقيمه الذكاء الاصطناعي، موضحة في القسم 10. ونواصل تطوير وثائق المطابقة الرسمية مع تقدم الجدول الزمني لتطبيق اللائحة. وإعلان مطابقة. والضمانات الأساسية، والإشراف البشري، والشفافية، والتقييم القائم على الأدلة، والحدود الصارمة لنطاق ما اصطناعي عالي المخاطر يدعم قرارات التوظيف، ونحتفظ بوثائق متوائمة مع اللائحة، بما في ذلك بطاقة شفافية، ووثائق المستخدم، تعامل المنصة على أنها نظام ذكاء

## 17.3 شهادات الاستضافة

هذه الشهادات الطبقات المادية وطبقات المنصة الواقعة تحت تطبيقنا؛ أما ضوابط طبقة التطبيق فهي الموصوفة في هذا المستند. تعمل المنصة بالكامل على Microsoft Azure، التي تحمل مراكز بياناتها شهادات مستقلة تشمل ISO 27001 و2 SOC. وتغطي

## 17.4 سجل المعالجين الفرعيين

| المنطقة | الغرض | المعالج الفرعي |
|---|---|---|
| EU (West Europe, Sweden Central) | والتخزين، والبريد الإلكتروني المعاملي ومعالجة الذكاء الاصطناعي والكلام، الاستضافة، | Microsoft Azure |
| EU (Ireland) | معالجة الاشتراكات والمدفوعات | Stripe |
| EU (Poland) | الفوترة | Fakturownia |
| EU | تكامل تتبع المتقدمين، يفعل فقط عند الطلب | ATS connector (optional) |

# 18. خارطة طريق الأمن

في هذا المستند. وليس أي من هذه فجوة تكشف بيانات العملاء اليوم؛ بل كل منها تحسين لوضع قائم أصلا على طبقات متعددة. إلى البيانات، والاستمرار في تشديد حداثة التبعيات بوتيرة منتظمة، والتقدم نحو اعتماد رسمي من جهة خارجية للضوابط الموصوفة الحالية على خارطة طريقنا تعزيز خيارات المصادقة متعددة العوامل للحسابات الإدارية، وتوسيع التسجيل المركزي لتدقيق الوصول نحن نتعامل مع الأمن باعتباره برنامجا في تحسن مستمر. وتشمل المبادرات

# 19. الخلاصة

الاصطناعي، وسجل من سبعة تدقيقات أمنية داخلية دون zero critical findings، يمكننا أن نظهر، لا أن نقول فقط، أن المنصة آمنة. وراء هذه الادعاءات. فمع أكثر من 3,100 اختبار آلي، ومنهجية قابلة للتكرار لاختبارات اختراق حية، وبرنامج مخصص لسلامة الذكاء بالتصميم، وتشفير وإقامة بيانات داخل الاتحاد الأوروبي، وضوابط خصوصية مدمجة في نموذج البيانات. وما يميز المنصة هو الأدلة شبكة خاصة افتراضيا دون خدمات بيانات عامة، وهوية قوية وعزل لكل مؤسسة، وشفرة تطبيق تستبعد فئات كاملة من الثغرات تحمي AI Interview Analyzer بيانات المرشحين والعملاء عبر بنية متعددة الطبقات:

# الملحق A: فهرس ضوابط الأمن

مرجع موجز للضوابط الأساسية والأدلة التي تدعم كل واحد منها.

| الدليل | الآلية | الضابط |
|---|---|---|
| البنية التحتية كرمز؛ وتدقيق البنية | مع إعادة توجيه ،+TLS 1.2فقط، و HTTPS HTTP | تشفير النقل |
| تهيئة المنصة؛ وتدقيق البنية | AES-256 على التخزين وقاعدة البيانات تشفير منصة | التشفير أثناء التخزين |
| التحكم بالمصدر؛ واختبارات المصادقة | لكل كلمة مرور salt مع bcrypt | حماية كلمات المرور |
| التحكم بالمصدر؛ واختبارات المصادقة | وتحديث قابل للإبطال على جانب الخادم رموز موقعة لمدة 30 دقيقة، | إدارة الجلسات |
| مجموعة اختبارات فرض الأدوار | الوصول بأربعة أدوار على نقاط النهاية المميزة تحكم في | التفويض |
| مصفوفة الاختبارات عبر المؤسسات | مؤسسة؛ و404 عند الوصول عبر المؤسسات تقييد الاستعلامات لكل | عزل المستأجرين |
| مجموعة اختبارات مفاتيح API | محددة النطاق، وحدود معدل لكل مفتاح تخزين مجزأ، وصلاحيات | أمن مفاتيح API |
| التحليل الثابت؛ واختبارات الحقن | استعلامات ذات معاملات عبر ORM فقط | الحماية من الحقن |
| مجموعة اختبارات تنقية HTML | تنقية HTML عند وقت الكتابة | الحماية من XSS |
| تحديد المعدل؛ وفحوصات دفعات حية اختبارات | بقاعدة البيانات على نقاط نهاية المصادقة محدد متين ومدعوم | تحديد المعدل |
| مجموعة اختبارات webhook | التحقق من توقيع المزود على الجسم الخام | سلامة Webhook |
| البنية التحتية كرمز؛ وتدقيق البنية | وpurge protection، وmanaged identity خزينة مدارة، | إدارة الأسرار |
| البنية التحتية كرمز؛ وتدقيق البنية | خاصة؛ وتقسيم بسياسة الرفض الافتراضي نقاط نهاية | عزل الشبكة |
| مجموعة اختبارات حذف GDPR | متسلسل كوحدة واحدة مع سجل تدقيق حذف | حذف البيانات |
| تهيئة خط الأنابيب؛ وتدقيق التبعيات | خط أنابيب مثبتة؛ ومراقبة أسبوعية للتبعيات خطوات | سلسلة التوريد |

# الملحق B: الأسئلة الشائعة لمراجعي الأمن

مع معالجة الذكاء الاصطناعي في مناطق الاتحاد الأوروبي. ولا تغادر بيانات المرشحين الاتحاد الأوروبي أبدا.**أين تخزن بياناتنا؟** بالكامل داخل الاتحاد الأوروبي، على Microsoft Azure، في West Europe

لا. لا يستخدم مزود الذكاء الاصطناعي بيانات العملاء في التدريب.**هل تستخدم بياناتنا لتدريب نماذج الذكاء الاصطناعي؟**

إلى قاعدة البيانات إلا عبر نقطة نهاية خاصة داخل الشبكة الافتراضية.**هل يمكن الوصول إلى قاعدة البيانات من الإنترنت؟**
لا. الوصول الشبكي العام معطل ولا يمكن الوصول

الوصول عبر المؤسسات "not found"، وتختبر مصفوفة آلية هذا العزل باستمرار.**هل يمكن لعميل أن يرى بيانات عميل آخر؟**
لا. كل استعلام مقيد بمؤسسة المتصل، ويرجع

فريد لكل كلمة مرور. كما يدعم SSO مع Microsoft وGoogle، وفي هذه الحالة لا تخزن أي كلمة مرور.**كيف تخزن كلمات المرور؟**
تخزن مجزأة باستخدام bcrypt وsalt

نعم، عبر Microsoft وGoogle OAuth.**هل تدعمون SSO؟**

ثلاثون دقيقة، مقترنة بجلسة تحديث قابلة للإبطال على جانب الخادم تبطل عند تسجيل الخروج.**ما مدة صلاحية رموز الوصول؟**

ويجب أن يوافق قبل أي تسجيل أو تحليل. وتسجل الموافقة مقابل عملية التوظيف المحددة.**كيف تعالج موافقة المرشح؟**
يتلقى كل مرشح رابط موافقة فريدا أحادي الاستخدام

وفق جدول احتفاظ قابل للتهيئة، مع دليل مسجل على المحو. ويمكن للمرشحين أيضا طلب الحذف مباشرة.**كيف تحذف البيانات؟**
كوحدة واحدة تشمل سجل المرشح، والمقابلات، والنصوص، والصوت، والمستندات، والمقارنات،

نعم، تقبل عند التسجيل وترقم بالإصدار لكل مؤسسة، بما في ذلك سجل المعالجين الفرعيين.**هل لديكم DPA؟**

لا. إنه يقدم دعما للقرار فقط؛ ويراجع إنسان كل مخرج ويتخذ جميع القرارات.**هل يتخذ الذكاء الاصطناعي قرارات توظيف؟**

ضد بيئات حية، وبرنامج لاختبارات سلامة الذكاء الاصطناعي، وتقارير تدقيق مكتوبة ومتكررة.**كيف تثبتون ادعاءاتكم الأمنية؟**
أكثر من 3,100 اختبار آلي، بما في ذلك مجموعة أمنية مخصصة، ومنهجية من ست مراحل لاختبارات الاختراق قابلة للتكرار وتشغل من خلال

ويعاد التحقق منها بما في ذلك الفحوصات الحية عند الاقتضاء، وتسجل في تقرير تدقيق.**ماذا يحدث عندما تكتشفون ثغرة؟**
تسند إليها شدة مع أدلة ومالك، وتعالج وفق جدول أولويات،

يمكن ترتيب تقييمات أمنية عبر ممثل حسابكم ضمن نطاق وجدولة مناسبين.**هل يمكننا إجراء اختبار اختراق خاص بنا؟**

# الملحق C: المعجم

| المصطلح | المعنى |
|---|---|
| AES-256 | معيار تشفير متماثل قوي يستخدم لحماية البيانات أثناء التخزين |
| bcrypt | دالة مصممة خصيصا لتجزئة كلمات المرور مع salting لكل كلمة مرور |
| Managed identity | هوية تصدرها المنصة وتتيح للخدمة المصادقة دون مفاتيح مخزنة |
| Private endpoint | عنوان شبكة خاص يبقي خدمة سحابية خارج الإنترنت العام |
| Network security group | قواعد السماح والرفض التي ترشح حركة الشبكة إلى شبكة فرعية مجموعة من |
| RBAC | في الوصول المستند إلى الدور، ويمنح الأذونات وفقا لدور المستخدم التحكم |
| IDOR | غير آمن إلى كائن، وهو خلل في التحكم بالوصول تدافع المنصة ضده مرجع مباشر |
| SSRF | من جانب الخادم، وهو فئة هجوم تفحص في اختبارات الاختراق لدينا تزوير طلب |
| Web application firewall | ضابط طرفي يرشح حركة الويب الخبيثة |
| Data processing agreement | يحكم كيفية تعامل المعالج مع البيانات الشخصية نيابة عن المتحكم العقد الذي |

# الملحق D: معلومات الاتصال والتحكم في المستند

**AI Interview Analyzer Sp. z o.o.**

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

NIP: 5253079974

أمنية، أو الحصول على نسخة من DPA الخاصة بنا، أو وثائق المطابقة الخاصة بنا مع EU AI Act، يرجى الاتصال بممثل حسابكم. لإجراء مراجعة

وقد قدم لأغراض التقييم ولا يشكل جزءا من أي عقد. وتحدد الالتزامات الأمنية التعاقدية المحددة في الاتفاقية المعمول بها وDPA.*
*يصف هذا المستند الوضع الأمني لخدمة AI Interview Analyzer اعتبارا من تاريخ الإنشاء المبين في التذييل.