Biztonsági tanulmány

Enterprise Security Overview - AI Interview Analyzer

Szolgáltató:	AI Interview Analyzer Sp. z o.o.
Cím:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Besorolás:	PUBLIC
Dátum:	24.06.2026

Contents

Biztonsági tanulmány

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

Célközönség: Vállalati biztonsági, IT- és beszerzési csapatok

Besorolás: Nyilvános

1. Vezetői összefoglaló

Az AI Interview Analyzer egy vállalati toborzási platform, amely a jelölt kifejezett hozzájárulásával rögzíti az interjúkat, átírja és strukturálja azokat, valamint bizonyítékokon alapuló értékelési támogatást nyújt a toborzók számára. Mivel a platform jelöltek személyes adatait kezeli és toborzási folyamatokat támogat, a biztonságot és az adatvédelmet elsődleges tervezési korlátként kezeljük, nem pedig utólag hozzáadott funkcióként.

Ez a tanulmány konkrét és ellenőrizhető módon írja le, hogyan védjük az ügyfél- és jelöltadatokat. Azoknak szól, akik beszállítókat értékelnek: biztonsági mérnököknek, IT-adminisztrátoroknak, adatvédelmi tisztviselőknek és beszerzési szakembereknek. A dokumentumban szereplő minden adat közvetlenül a saját mérnöki rendszereinkből származik, nem marketinganyagokból.

A központi üzenet egyszerű: **nem pusztán állítjuk, hogy a platform biztonságos, hanem folyamatosan teszteljük is azt.** Kódbázisunk **3,171 automatizált tesztet** tartalmaz, beleértve egy dedikált biztonsági tesztcsomagot, amely a hitelesítést, jogosultságkezelést, szervezetek közötti elkülönítést, injektálás elleni védelmet és adattörlést vizsgálja. Ezen felül ismételhető penetration testing keretrendszert futtatunk éles telepítéseken, és írásos auditjelentéseket készítünk. Hét belső biztonsági audit során 2026 márciusában és áprilisában **zero critical findings** eredményt rögzítettünk, legutóbbi auditunk pedig **PASS** minősítéssel zárult. (Ezeknek a kontrolloknak a formális külső tanúsítása szerepel az ütemtervünkben; lásd a 18. szakaszt.)

Biztonsági jellemző	Összefoglaló
Hosztolás	Microsoft Azure, kizárólag EU-régiók
Hálózati modell	Privát végpontok, alapértelmezett tiltású hálózati szegmentáció, nincs nyilvános adatbázis
Titkosítás	Nyugalmi állapotban AES-256, átvitel közben TLS 1.2 vagy újabb
Identitás	Rövid élettartamú aláírt tokenek, bcrypt jelszóhash-elés, SSO támogatás
Hozzáférés-szabályozás	Szerepköralapú hozzáférés-szabályozás szigorú szervezetenkénti elkülönítéssel
Titkok	Központi titokkezelő tár felügyelt identitásalapú hozzáféréssel
Adatvédelem	Kifejezett hozzájárulás, konfigurálható megőrzés, egységenkénti törlés
Felelős AI	Kizárólag döntéstámogatás, ember mindig része a folyamatnak
Bizonyosság	3,171 automatizált teszt, valamint ismétlődő penetration testing és auditok

1.1 A dokumentum olvasása

A 3–11. szakaszok az adatokat védő kontrollokat írják le: architektúra, hálózat, identitás, alkalmazás, adatvédelem, adatkezelés és a biztonságos fejlesztési életciklus. A 12. és 13. szakasz a megkülönböztető folyamatos tesztelési programunkat és auditelőzményeinket tárgyalja. A 14–17. szakaszok az üzemeltetést, a fenyegetésmodellezést, a sérülékenységkezelést és a megfelelőségi leképezést fedik le. A mellékletek kontrollkatalógust, értékelői GYIK-et és egy szójegyzéket tartalmaznak, amelyet egy biztonsági csapat közvetlenül felhasználhat az értékelés során.

2. A dokumentum hatóköre és megközelítése

2.1 Mit fed le ez a dokumentum

Ez a tanulmány az AI Interview Analyzer szolgáltatás biztonsági architektúráját és gyakorlatait fedi le: a hosztolási környezetet, a hálózati kialakítást, az identitás- és hozzáférés-kezelést, az alkalmazásszintű kontrollokat, az adatvédelmet, az adatkezelési és szabályozási illeszkedést, a biztonságos fejlesztési életciklust és a folyamatos biztonsági tesztelési programunkat.

2.2 Mitől ellenőrizhető

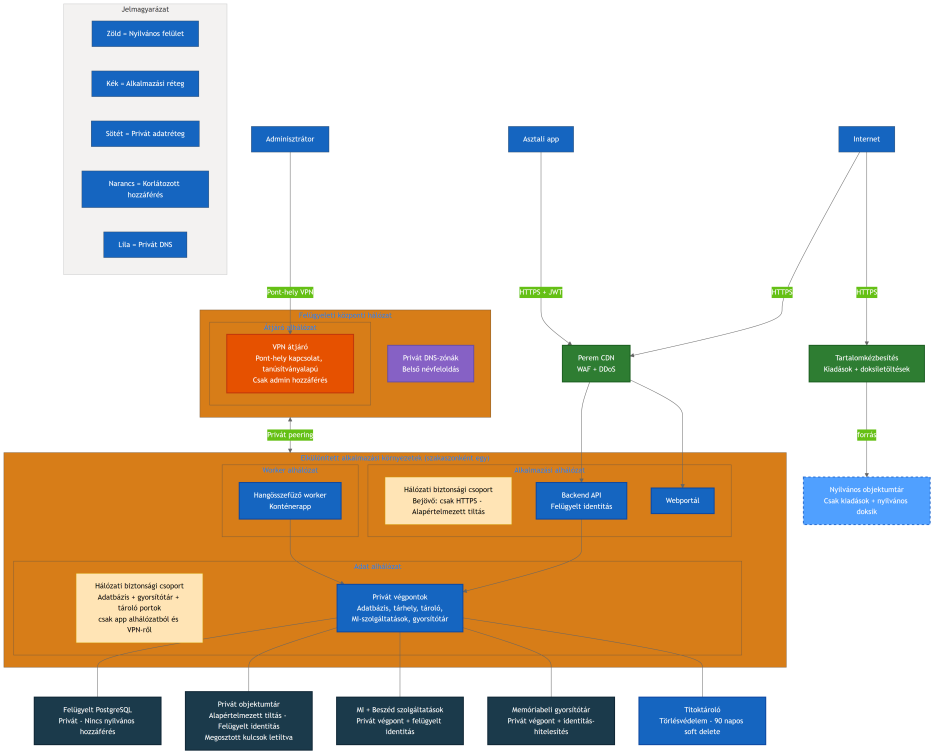
A beszállítói biztonsági állításokat könnyű megfogalmazni és nehéz megbízni bennük. Ezért a dokumentumban szereplő minden jelentősebb állítást valami konkrét és számszerűsíthető elemhez kötöttünk a mérnöki rendszereinken belül: egy kódban megvalósított kontrollhoz, egy teszthez, amely bizonyítja, hogy a kontroll működik, egy infrastruktúra-definícióhoz, amely kikényszeríti azt, vagy egy auditjelentéshez, amely dokumentált ellenőrzést rögzít. Ahol egy kontroll a jövőbeli ütemterv része, és még nem áll rendelkezésre ma, azt kifejezetten jelezzük. Inkább állítunk kevesebbet és maradunk hitelesek, mintsem túlzó állításokat tegyünk és lebukjunk.

2.3 Megosztott felelősség

A platformot szoftver mint szolgáltatás formájában nyújtjuk. Mi üzemeltetjük az infrastruktúrát, az alkalmazást, az AI-folyamatot és az adatkezelést. Az ügyfél felelős saját felhasználói fiókjainak és szerepköreinek kezeléséért, az adatmegőrzési időablakok belső szabályzatához igazodó konfigurálásáért, valamint annak biztosításáért, hogy a jelölti hozzájárulást a platform által biztosított hozzájárulási munkafolyamaton keresztül szerezzék be. A 14. szakasz ezt a felosztást részletesebben ismerteti.

3. A biztonsági architektúra áttekintése

A platform nem egyetlen monolitként, hanem együttműködő szolgáltatások kis számaként épül fel. Asztali alkalmazás és webes portál szolgál kliensként. Egy központi backend API kezeli a teljes adattárolást, hitelesítést, számlázást, az AI-folyamatot, a hozzájárulást, az e-mailt, a fájlkezelést és a dashboardokat. Egy audio merge worker aszinkron módon dolgozza fel a felvételeket. Minden érzékeny állapot a backend API mögött található; a kliensek soha nem kommunikálnak közvetlenül az adatbázissal, a tárolóval vagy az AI-szolgáltatásokkal.



A fenti ábra az éles topológiát mutatja, szándékosan általánosított erőforrásnevekkel. Három alapelv látható rajta:

- **Nincs közvetlen kitettsége az adatszolgáltatásoknak.** Az adatbázis, a privát objektumtároló, az AI-szolgáltatások és a gyorsítótár nyilvános hálózati hozzáférése le van tiltva, és csak privát végpontokon keresztül érhetők el egy elszigetelt virtuális hálózaton belül. A titokkezelő tárat az alkalmazás privát végponton keresztül éri el, és azt platformidentitás-hitelesítés, valamint legkisebb jogosultság elvén alapuló hozzáférési szabályzatok is védik, így bármilyen hozzáféréshez érvényes, engedélyezett identitás szükséges, függetlenül a hálózati útvonaltól.
- **Elkülönített nyilvános felület.** Az egyetlen nyilvános objektumtároló kiadási letöltéseket és nyilvános dokumentumokat tárol. Jelöltadatokat soha nem tartalmaz. Az ügyféloldali alkalmazásforgalom egy peremrétegen halad át, amely web application firewall, distributed-denial-of-service védelem és tartalomkiszolgálás funkciót nyújt.
- **A rendszergazdai hozzáférés kapuzott.** Az üzemeltetők a belső erőforrásokat kizárólag tanúsítványalapú point-to-site VPN-en keresztül érik el egy menedzsment hub hálózatba, nem pedig a nyilvános interneten át.

Minden telepítési szakasz (fejlesztési és éles) teljesen elszigetelt környezet, saját hálózattal, tárolófiókokkal, adatbázissal és titkokkal. Az ügyfél éles adatai soha nem jelennek meg alacsonyabb szintű környezetekben. A megosztott menedzsment hub kizárólag a VPN-átjárót és a privát DNS-t tartalmazza, privát peeringgel minden környezethez.

4. Többrétegű védelem

Egyetlen kontrollra sem támaszkodunk abban, hogy minden támadást megállítson. A platform egymástól független kontrollokat rétegez, így bármelyik egyes réteg hibája sem teszi elérhetővé az adatokat. Az alábbi rétegek mindegyike megvalósított, és ahogy a 12. szakasz leírja, külön-külön tesztelt.

Réteg	Jellemző kontrollok
Hálózati perem	Kizárólag TLS-alapú átvitel, peremoldali WAF és DDoS védelem, privát végpontok, alapértelmezett tiltású szegmentáció
Identitás és hozzáférés	Rövid élettartamú aláírt tokenek, bcrypt hash-elés, szerepköralapú hozzáférés-szabályozás, szervezetenkénti elkülönítés
Alkalmazás	Sémavalidáció minden bemeneten, kizárólag ORM-alapú adathozzáférés, kimeneti kódolás, rate limiting
Adatvédelem	Titkosítás nyugalmi állapotban, titokkezelő tár felügyelt identitással, EU adatlokalizáció, hozzájáruláshoz kötött feldolgozás
Irányítás és adatkezelés	Konfigurálható megőrzés, egységenkénti törlés, ember a folyamatban AI, auditnaplózás
Folyamatos bizonyosság	Automatizált tesztcsomag, ismételhető penetration testing, rendszeres belső biztonsági auditok

A dokumentum fennmaradó része ezeket a rétegeket egyenként ismerteti, majd bemutatja, hogyan bizonyítjuk folyamatosan, hogy a rétegek valóban működnek.

5. Hálózati biztonság

5.1 Privát alapértelmezés szerint

Az adatréteg kialakításánál fogva privát. A felügyelt PostgreSQL adatbázis nyilvános hálózati hozzáférése le van tiltva, és csak privát végponton keresztül érhető el. A privát objektumtároló alapértelmezés szerint minden hálózati hozzáférést tilt, teljes mértékben letiltja a megosztott hozzáférési kulcsokat, és kizárólag az alkalmazás alhálózatából, felügyelt identitáson keresztül érhető el. A gyorsítótár, az AI-szolgáltatások és a titokkezelő tár ugyanígy privát végpontokon és privát DNS-feloldáson keresztül érhetők el.

A gyakorlatban ez azt jelenti, hogy nincs internet felé nyitott kapcsolatkarakterlánc az adatbázishoz, és nincs nyilvános tárolási URL a jelöltek hanganyagához: az adatbázis és a privát tároló nyilvános hálózati hozzáférése teljesen le van tiltva. A titokkezelő tárat az alkalmazás privát végponton keresztül éri el, és platformidentitás-hitelesítés, valamint legkisebb jogosultság elvén alapuló hozzáférési szabályzatok védik, ahol az alkalmazásidentitások kizárólag olvasási hozzáférést kapnak csak azokhoz a titkokhoz, amelyekre szükségük van, így a titkok érvényes, engedélyezett identitás nélkül nem kérhetők le. Az a támadási felület, amelyet egy külső támadó egyáltalán elérhet, az alkalmazás HTTPS-végpontjaira korlátozódik a peremréteg mögött.

5.2 Hálózati szegmentáció

Minden környezet külön alhálózatokra van osztva az alkalmazási réteg, az adatréteg és az aszinkron worker számára. Minden alhálózatot olyan network security group szabályoz, amelynek utolsó szabálya minden bejövő forgalmat tilt. Az alkalmazási alhálózat csak bejövő HTTPS-forgalmat fogad. Az adatalhálózat kizárólag a meghatározott adatbázis-, gyorsítótár- és vault-portokat fogadja, és csak az alkalmazási alhálózat vagy az adminisztratív VPN felől. Ez azt jelenti, hogy még ha egy támadó valamilyen módon el is érné az alkalmazási réteget, nem tudna szabadon továbblépni az adatrétegbe; csak azok az útvonalak engedélyezettek, amelyeket az alkalmazás jogosan használ.

5.3 A perem

A nyilvános alkalmazásforgalmat egy peremréteg szolgálja ki, amely web application firewall, DDoS védelem és content delivery network funkciókat biztosít. A kiadási és dokumentumletöltések egy dedikált nyilvános tárolófiókból kerülnek kiszolgálásra egy content-delivery front dooron keresztül, teljesen elkülönítve attól a privát tárolótól, amely a jelöltadatokat tárolja. A két tárolási sík soha nem keveredik: a nyilvános sík hibás konfigurációja nem tárhatja fel a privát jelöltadatokat, mert eltérő fiókokról van szó eltérő hálózati szabályokkal.

5.4 Rendszergazdai hozzáférés

Nincs nyilvános rendszergazdai végpont a privát hálózatba. Az üzemeltetők point-to-site VPN-átjárón keresztül csatlakoznak, amely tanúsítványalapú hitelesítést használ. Az adminisztratív adatbázis- és gyorsítótár-hozzáférés csak ezen az alagúton belül lehetséges, mivel ezeknek a szolgáltatásoknak a nyilvános hálózati hozzáférése le van tiltva. Ez a mindennapi üzemeltetést teljes mértékben távol tartja a nyilvános internettől.

6. Identitás- és hozzáférés-kezelés

6.1 Hitelesítés

A felhasználói munkamenetek egy harminc percig érvényes aláírt hozzáférési tokennel jönnek létre, amelyhez egy különálló, nem átlátszó, szerveroldali frissítési token tartozik. A hozzáférési tokenek minden kérésnél ellenőrzésre kerülnek, és a felhasználó az adatbázissal szemben újra validálásra kerül (beleértve az aktív fiók ellenőrzését), ahelyett hogy kizárólag a token tartalmára hagyatkoznánk. Kijelentkezéskor a szerveroldali frissítési munkamenet azonnal visszavonásra kerül, így egy ellopott frissítési token nem élheti túl a kijelentkezést.

A jelszavakat soha nem tároljuk olvasható formában. Ezeket bcrypt segítségével hash-eljük, jelszavanként egyedi salt használatával. Azoknak a szervezeteknek, amelyek egyszeri bejelentkezést preferálnak, a platform Microsoft és Google OAuth bejelentkezést támogat, ebben az esetben egyáltalán nem tárolunk jelszót.

Az e-mail tulajdonjoga egyszer használatos, időkorlátos ellenőrző hivatkozáson keresztül kerül megerősítésre, mielőtt egy önregisztrált fiókot ellenőrzöttnek tekintenénk, és az ellenőrző e-mail újraküldései rate limiting alatt állnak a visszaélések megelőzése érdekében.

6.2 Szerepköralapú hozzáférés-szabályozás

Az engedélyezés egy négy, növekvő jogosultságú szerepkört tartalmazó modell segítségével érvényesül: interviewer, hiring manager, recruiter és administrator. A kiemelt műveletekhez való hozzáférést szerveroldali függőségek érvényesítik, amelyek ellenőrzik mind a hívó szerepkörét, mind annak ellenőrzött státuszát. Ezek a szerepkörellenőrzések jóval több mint száz különálló API-műveletet védenek.

Szerepkör	Tipikus képességek
Interviewer	Kiosztott interjúkat bonyolít le; csak a számára kiosztott interjúkat látja
Hiring manager	Az általa birtokolt vagy amelynek tagja toborzásokat kezeli
Recruiter	Teljes toborzási és jelöltkezelés a szervezeten belül
Administrator	Szervezeti beállítások, számlázás, felhasználó- és API-kulcs-adminisztráció

A durva szerepkörellenőrzéseken túl a platform adatszintű láthatósági szabályokat is alkalmaz. A hiring managerek csak azokat a toborzásokat látják, amelyeket létrehoztak vagy amelyeknek tagjai; az interviewerek csak a nekik kiosztott interjúkat látják. A jogosultság tehát egyszerre érvényesül a „milyen művelet” és a „mely rekordok” szintjén.

6.3 Szervezetenkénti elkülönítés

A platform több-bérlős, és a bérlők elkülönítését első osztályú biztonsági kontrollként kezeljük. Minden hitelesített identitás szervezetazonosítót hordoz, és az adatlekérdezések erre a szervezetre vannak szűkítve. Amikor egy felhasználó egy másik szervezethez tartozó rekordot kér le, a platform „not found” választ ad, ahelyett hogy felfedné a rekord létezését. Belső adatbázis-azonosítók soha nem kerülnek a kommunikációs rétegre; az API megjelenítési azonosítókat mutat, és azokat kérésenként újratérképezi, ami megszünteti a szervezetek közötti felsorolásos támadások egy gyakori osztályát.

Ez nem csupán tervezési szándék. Ahogy a 12. szakasz ismerteti, automatizált tesztcsomagunk egy kiterjedt szervezetek közötti mátrixot futtat, amely megkísérli az egyik szervezet adatainak elérését egy másik szervezet hitelesítő adataival, és ellenőrzi, hogy minden ilyen kísérlet meghiúsul.

6.4 Programozott hozzáférés

Integrációkhoz az arra jogosult csomagokban lévő szervezetek API-kulcsokat bocsáthatnak ki. A kulcsok felismerhető prefixet használnak, 128 bites entrópiával rendelkeznek, és csak hash formájában tároljuk őket; a nyers kulcs a létrehozáskor egyszer látható, utána soha többé. Minden kulcs kifejezett jogosultsági kört hordoz (olvasás, írás vagy ATS-integráció), korlátozható meghatározott forráshálózatokra, azonnal visszavonható, és kulcsonkénti rate limiting vonatkozik rá, amely a szervezet

csomagszintjéből származik. A kulcsellenőrzés timing-safe összehasonlítást használ, hogy ne szivárogjon információ a válaszidőkön keresztül.

7. Alkalmazásbiztonság

Az alkalmazást úgy írjuk, hogy teljes sérülékenységi kategóriákat küszöböljön ki, ne pedig eseti alapon javítsunk hibákat.

- **Injektálás.** Minden adatbázis-hozzáférés objektum-relációs leképezőn keresztül történik paraméterezett lekérdezésekkel. A kódbázis nem tartalmaz nyers, karakterlánc-formázott SQL-t. Ez szerkezeti szinten szünteti meg az SQL injection lehetőségét.
- **Bemenetvalidáció.** Minden kérés törzse szigorú sémával kerül validálásra, mielőtt elérné az üzleti logikát. A túlméretezett payloadok elutasításra kerülnek, a lista-végpontok pedig lapozottak az erőforrás-felhasználás korlátozására.
- **Kimeneti kódolás és cross-site scripting.** A felhasználó által megadott és az AI által generált szöveget nem megbízhatónak tekintjük. Ahol a tartalmat HTML-ként kell megjeleníteni, az íráskor engedélyezési listás tisztítón halad át, és egy dedikált tesztcsomag megerősíti, hogy a script tagek, eseménykezelők és javascript URL-ek eltávolításra kerülnek.
- **Mass assignment.** A frissítési műveletek kifejezett sémákat használnak, amelyek kizárják a privilegizált mezőket, például a szerepkört, szervezetet és kreditegyenleget, így egy kliens nem emelhet jogosultságot extra mezők beküldésével.
- **Rate limiting.** A hitelesítési és visszaélésre hajlamos végpontok rate limiting alatt állnak egy tartós, adatbázis-alapú limiter segítségével, amely újraindítások után is működik, és több alkalmazáspéldány között is helyesen viselkedik. A bejelentkezés, regisztráció, jelszó-visszaállítás és ellenőrző újraküldések mind saját limitet kapnak. A kliens IP-feloldása megerősített a továbbítási fejlécek hamisítása ellen.
- **Webhookok.** A fizetési és e-mail szolgáltatóktól érkező bejövő webhookokat a nyers kérés törzsén a szolgáltatói aláírásokkal szemben ellenőrizzük feldolgozás előtt.
- **Fájlfeltöltések.** A feltöltések méretkorlátozottak, validáltak, generált azonosítók alatt kerülnek tárolásra felhasználó által megadott nevek helyett, és kérésenként, valamint szervezetenként is korlátozottak.
- **Biztonsági fejlécek.** Éles környezetben a válaszok szigorú szállítási biztonságot, content-type és frame opciókat, referrer policy-t és korlátozó permissions policy-t hordoznak, valamint elnyomják a szerver- és keretrendszer-bannereket.

8. Adatvédelem

8.1 Titkosítás

Minden adat nyugalmi állapotban AES-256 használatával titkosított az Azure platform tárolási és adatbázis-titkosítási rétegein keresztül. Minden hálózati forgalom kizárólag HTTPS-en keresztül szolgálódik ki TLS 1.2 vagy újabb használatával; a titkosítatlan HTTP minden rétegben HTTPS-re kerül átirányításra. Éles környezetben az API és a webes portál szigorú szállítási biztonsági fejléceket küld egy további megerősítő fejléckészlettel együtt, valamint elnyomja a szerver- és keretrendszer-verzióbannereket.

8.2 Titokkezelés

Az alkalmazástitkok egy központi titokkezelő tárban találhatók, ahol a purge protection engedélyezett, és kilencvennapos soft-delete időablak van beállítva. Az alkalmazások Azure-erőforrásokhoz system-assigned managed identity segítségével hitelesítenek, nem pedig hosszú élettartamú kulcsokkal; például a privát tárolóban a megosztott hozzáférési kulcsok teljesen le vannak tiltva, így a hozzáférés csak identitásalapú szerepkör-hozzárendeléseken keresztül lehetséges, az egyes erőforrásokra szűkítve. A vault hozzáférési szabályzatai az alkalmazásprincipáloknak csak olvasási hozzáférést adnak a konkrétan szükséges titkokhoz, a legkisebb jogosultság elvét követve.

8.3 Adatlokalizáció

Minden ügyfél- és jelöltadat tárolása és feldolgozása az Európai Unión belül történik. Az alkalmazás hosztolása, az adatbázis, a tároló, a gyorsítótár és a titkok West Europe régióban találhatók, az AI-feldolgozás pedig EU-régiókban fut. Az AI-szolgáltató nem használja fel az ügyféladatokat modelljei tanításához.

8.4 Egyetlen interjú életútja

Az adatvédelmi kontrollok megértésének legvilágosabb módja egy interjú teljes végigkövetése. A hozzájárulás rögzítésre és naplózásra kerül, mielőtt bármi feldolgozás történne. A feltöltés átvitel közben titkosított. Az átírás és elemzés EU-beli adatközpontokban fut. Az eredmények titkosított tárolóba kerülnek. Minden rekordot ezután egyetlen megőrzési óra szabályoz, amely naplózott, kaszkádos törlésben végződik. A jelölti jogok, például a visszavonás, törlés, hozzáférés vagy hordozhatóság, bármely ponton megszakíthatják ezt a folyamatot.

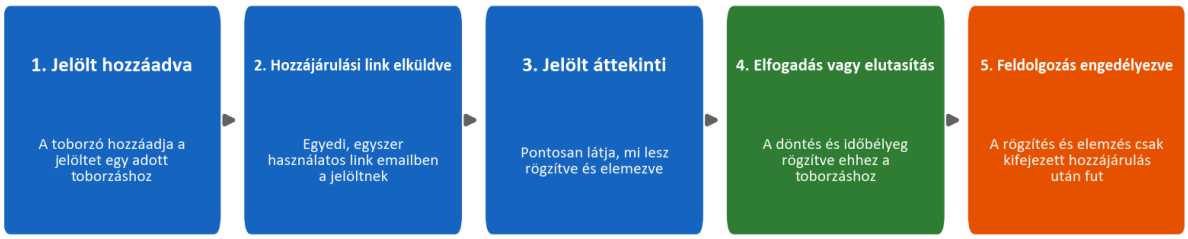
9. Privacy by Design és GDPR

Az adatvédelem be van építve az adatmodellbe és a munkafolyamatba, nem csupán szabályzatokkal van utólag hozzáillesztve.

9.1 Hozzájárulás

Egyetlen interjút sem rögzítünk vagy elemzünk a jelölt kifejezett hozzájárulása nélkül. Amikor egy jelöltet hozzáadnak egy toborzáshoz, a platform e-mailben egyedi, egyszer használatos hozzájárulási linket küld. A jelölt áttekinti, mi fog történni, majd elfogadja vagy elutasítja azt. A hozzájárulási állapot, beleértve a válasz idejét is, az adott toborzáshoz kerül rögzítésre, így a hozzájárulás mindig egy konkrét felvételi folyamathoz kötött, és nem globálisan megadott.

Jelölti hozzájárulás: kifejezett és rögzített minden feldolgozás előtt

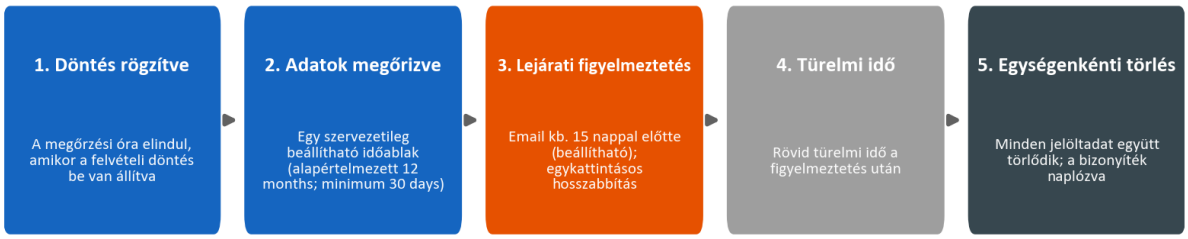


9.2 Megőrzés és törlés

Az adatmegőrzés szervezetenként konfigurálható, alapértelmezés szerint tizenkét hónap, konfigurálható minimuma harminc nap, és jelöltenként felül is bírálható. A jelölt adatainak egyetlen megőrzési órája van, nem pedig külön időzítő minden egyes műtermékhez. Az óra akkor indul, amikor a felvételi döntés rögzítésre kerül. Az adatok lejárta előtt a platform figyelmeztetést küld (alapértelmezés szerint körülbelül tizenöt nappal korábban), és egykattintásos hosszabbítást kínál. Amikor az adatok törlésre kerülnek, egyetlen egységként törlődnek: a jelöltrekord, az interjúk, az átiratok, a hangfelvételek, a dokumentumok és az összehasonlítások együtt kerülnek eltávolításra, és a törlés auditnaplóba kerül. Nincs részleges vagy árva maradvány.

Az alábbi életciklus ezt az egyetlen órát mutatja, és azt, hogyan fut össze egyetlen kaszkádos törlésbe naplózott törlési bizonyítékkal.

Adatmegőrzés: egy óra jelöltenként, egységenkénti törlés



9.3 Érintetti jogok és alfeldolgozók

A platform támogatja a GDPR által előírt érintetti jogokat, beleértve a hozzáférést, törlést, hordozhatóságot, tiltakozást és magyarázathoz való jogot. A feldolgozás adatfeldolgozási megállapodás alapján történik, amelyet az ügyfelek regisztrációkor fogadnak el, és amely szervezetenként verziózott. Alfeldolgozóink és szerepeik, mind az EU-n belül vagy megfelelő garanciák

mellett, ebben a megállapodásban kerülnek közzétételre, és az ügyfelek előzetes értesítést kapnak minden változásról. A 17. szakasz tartalmazza az alfeldolgozói nyilvántartást és a cikkenkénti megfelelőségi leképezést.

10. Felelős AI és az EU AI Act

A platform az EU AI Act magas kockázatú kategóriájába tartozik, mivel foglalkoztatási döntéseket támogat, és ezt a besorolást komolyan vesszük.

A termék meghatározó szabálya az, hogy **az AI döntéstámogatás, nem döntéshozó.** A rendszer soha nem fogad el vagy utasít el automatikusan egy jelöltet. Beszédet ír át, kérdéseket és válaszokat strukturál, a válaszokat a toborzó által meghatározott kritériumok szerint pontozza, és visszajelzést fogalmaz meg, majd minden kimenetet ember vizsgál felül, mielőtt azt felhasználnák. Ez biztosítja, hogy az ember szilárdan része marad a folyamatnak.

Ugyanilyen fontos az is, amit az AI nem tesz. Nem értékel személyiséget, „kulturális illeszkedést", érzelmi állapotot, hangszínt, akcentust, nemet, életkort, etnikai hovatartozást, megjelenést vagy testbeszédet. A pontozás az átiratból származó bizonyítékokra és a toborzó által meghatározott kritériumokra épül, és a jelöltek nevei ki vannak zárva az értékelési bemenetből az elfogultság csökkentése érdekében. Közzéteszünk átláthatósági kártyát, felhasználói dokumentációt és megfelelőségi nyilatkozatot, amely leírja a rendszert, annak korlátait és védelmi intézkedéseit.

Felelős AI kontroll	Működése
Ember a folyamatban	Minden pontszámot és minden visszajelzést toborzó vizsgál felül felhasználás előtt
Nincs automatizált döntés	A rendszer soha nem fogad el vagy utasít el automatikusan egy jelöltet
Bizonyítékalapú pontozás	A pontszámok az átiratból származó alátámasztó bizonyítékokra hivatkoznak
Elfogultságcsökkentő kialakítás	A nevek kizárva az értékelésből; a tartalom fontosabb, mint a stílus
Hatókör-korlátok	Személyiség, érzelem, akcentus és védett jellemzők soha nem kerülnek értékelésre
Jelölti visszajelzés biztonsága	A privát jelölti visszajelzés egy generálási és validálási biztonsági korláton halad át

Ezek a korlátok nem csupán dokumentációban szerepelnek; az AI prompt rétegbe vannak kódolva, és egy dedikált AI-biztonsági tesztprogram vizsgálja őket, amelyet a 12.3 szakasz ismertet.

11. Biztonságos fejlesztési életciklus

A biztonságot abban is érvényesítjük, ahogyan a szoftvert építjük és szállítjuk, nem csak a futó rendszerben.

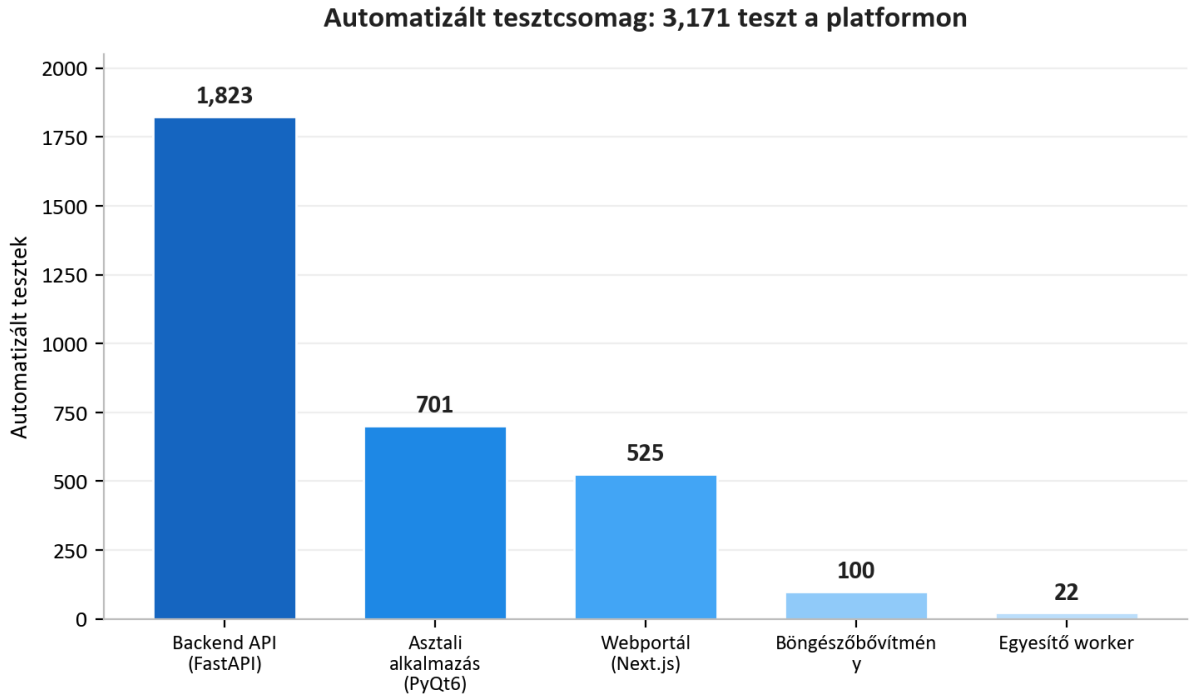
- **Környezetek elkülönítése.** A fejlesztési és éles környezet teljesen különálló, mindegyik saját infrastruktúrával, tárolófiókokkal, adatbázissal, titkokkal és aldomainnel. Nincs megosztott állapot.
- **Infrastructure as code.** A teljes felhőkörnyezet kódként van definiálva és kódként felülvizsgálva, ami ellenőrizhetővé és reprodukálhatóvá teszi a biztonsági állapotot. Egy felülvizsgáló pontosan meg tudja nézni, mely portok vannak nyitva, mely erőforrások privátak, és mely identitások milyen jogosultságokkal rendelkeznek.
- **Rögzített, kapuzott telepítések.** A continuous-integration folyamat minden lépése pontos, megváltoztathatatlan verzióhoz van rögzítve. Az éles telepítések tag-alapúak, csak a védett éles pipeline-on keresztül futnak, és kötelező jóváhagyás mögé vannak helyezve. Az automatizált tesztcsomag kiadási kapuként működik: ha a tesztek sikertelenek, a telepítés nem mehet ki.
- **Függőségi higiénia.** Az automatizált függőségfigyelés hetente javasol frissítéseket a backend, az asztali alkalmazás, a web, az infrastruktúra és a pipeline-definíciók területén, a függőségi auditok pedig rendszeres biztonsági felülvizsgálatunk részei.
- **Aláírt műtermékek.** Az asztali telepítők kóddal aláírtak, így az ügyfelek ellenőrizhetik, hogy a telepített szoftver valóban tőlünk származik.
- **Titokkezelési fegyelem.** A titkok a vaultban és a védett pipeline-titkokban találhatók, soha nem a forráskódban.

12. Folyamatos biztonsági tesztelés

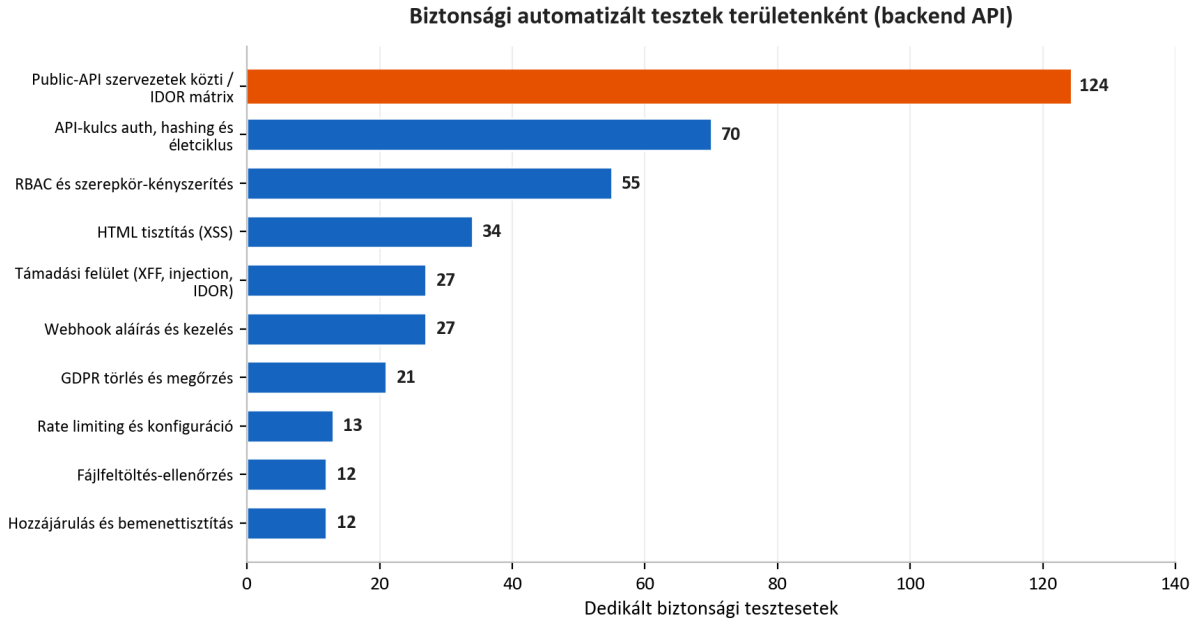
Ez a bizonyossági történetünk központi eleme és az a rész, amelyet a legtöbb beszállító nem tud bemutatni. A biztonságot folyamatosan mérendő dolognak tekintjük, végrehajtható ellenőrzésekkel, nem pedig egyszer megfogalmazott állításnak.

12.1 Az automatizált tesztcsomag

A platformot **3,171 automatizált teszt** fedi le a backend API, az asztali alkalmazás, a webes portál, a böngészőbővítmény és az audio merge worker területén.



Ezek nem csupán funkcionális tesztek. Egy jelentős, dedikált biztonsági tesztcsomag vizsgálja a dokumentumban korábban ismertetett kontrollokat. Az alábbi ábra a backend API biztonság-specifikus tesztjeit bontja le területenként.



Sok más mellett ez a csomag tartalmaz egy kiterjedt nyilvános API-mátrixot, amely minden végpontot lefuttat legitim felhasználóként, a szervezet saját API-kulcsaként, valamint egy rivális szervezet API-kulcsaként, és ellenőrzi, hogy minden szervezetek közötti kísérlet blokkolva van. Tartalmaz több tucatnyi támadói szemléletű tesztet a továbbítási fejléc hamisítására, fejlécinjektálásra és azonosítószivárgásra, egy fókuszált HTML-tisztítási csomagot a cross-site scripting ellen, szerepkör-érvényesítési teszteket a teljes szerepkörmodellre, valamint olyan teszteket, amelyek bizonyítják, hogy a jelöltadatok valóban egységként törlődnek. Mivel ezek a tesztek kiadási kapuként futnak, bármely regresszió, amely gyengítené ezeket a kontrollokat, megállítaná a kiadást ahelyett, hogy eljutna az ügyfelekhez.

12.2 Élő penetration testing

Az automatizált egységtesztek azt bizonyítják, hogy a kontrollok helyesen viselkednek elszigetelten. Annak bizonyítására, hogy egy valós telepítésben együtt is működnek, fenntartunk egy ismételhető penetration testing módszertant, amely valós támadószkripteket futtat egy élő környezet ellen. Ez hat fázisba szerveződik:

Fázis	Fókusz	Vizsgált példák
1. Statikus elemzés	Forráskód	Titkok, injektálási minták, veszélyes függvények, hiányzó auth, nem biztonságos HTML
2. Architektúra-felülvizsgálat	Infrastruktúra	Privát végpontok, szegmentáció, TLS, titokkonfiguráció
3. Támadási vektor elemzés	Forráskódkezelés és felhő	Ágvédelem, identitási hatókör, nyilvános kitettség
4. Élő penetration testing	Futó környezet	Hitelesítés nélküli szondázás, szervezetek közötti hozzáférés, injektálás, tokenmanipuláció, SSRF, rate-limit burstök
5. Vállalati pontozás	Érettség	Tizenhat biztonsági kategória pontozása vállalati alapvonalhoz mérten
6. Függőségi és ellátási lánc	Harmadik fél kockázata	Függőségi CVE audit, rögzített pipeline-akciók, lock-file integritás

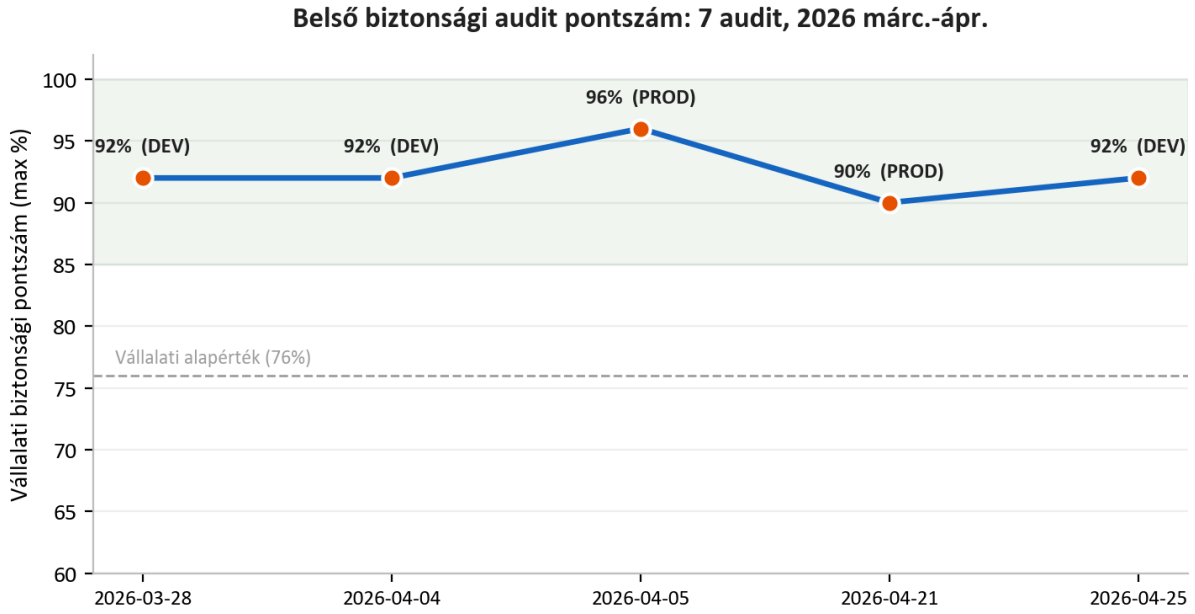
A 4. fázis valódi támadói tesztelés egy telepített rendszer ellen, nem ellenőrzőlista. Védett végpontokat vizsgál hitelesítő adatok nélkül, és megerősíti, hogy azok megtagadják a hozzáférést; két szervezetet regisztrál, majd megpróbálja az egyik szervezet rekordjait elérni a másik fiókjával; cross-site-scripting és server-side-template payloadokat injektál, és megerősíti, hogy azok semlegesítésre kerülnek; manipulálja a hitelesítési tokeneket, és megerősíti, hogy azokat elutasítják; server-side request forgery kísérleteket tesz a felhő metaadat-végpontjai ellen; és burst jellegű terhelést küld a hitelesítési végpontokra, hogy megerősítse: a rate limiting valóban aktiválódik az élő környezetben, nem csak elméletben.

12.3 Jelölti visszajelzés biztonsági tesztelése

Mivel a platform privát fejlesztési visszajelzést tud generálni a jelöltek számára, ehhez a funkcióhoz külön támadói biztonsági programot futtatunk. Szándékosan durva és ellenséges toborzói megjegyzésekkel táplálja a rendszert, és ellenőrzi, hogy a jelöltnek szóló kimenet soha ne tartalmazzon vulgaritást, soha ne fedje fel vagy tulajdonítsa egy toborzó identitását vagy magánvéleményét, és soha ne alkalmazzon ítélkező személyiségcímkéket. Ez védi a jelöltet, akinek konstruktív és tiszteletteljes visszajelzést kell kapnia, valamint az ügyfelet, akinek belső véleménye soha nem szivároghat kifelé.

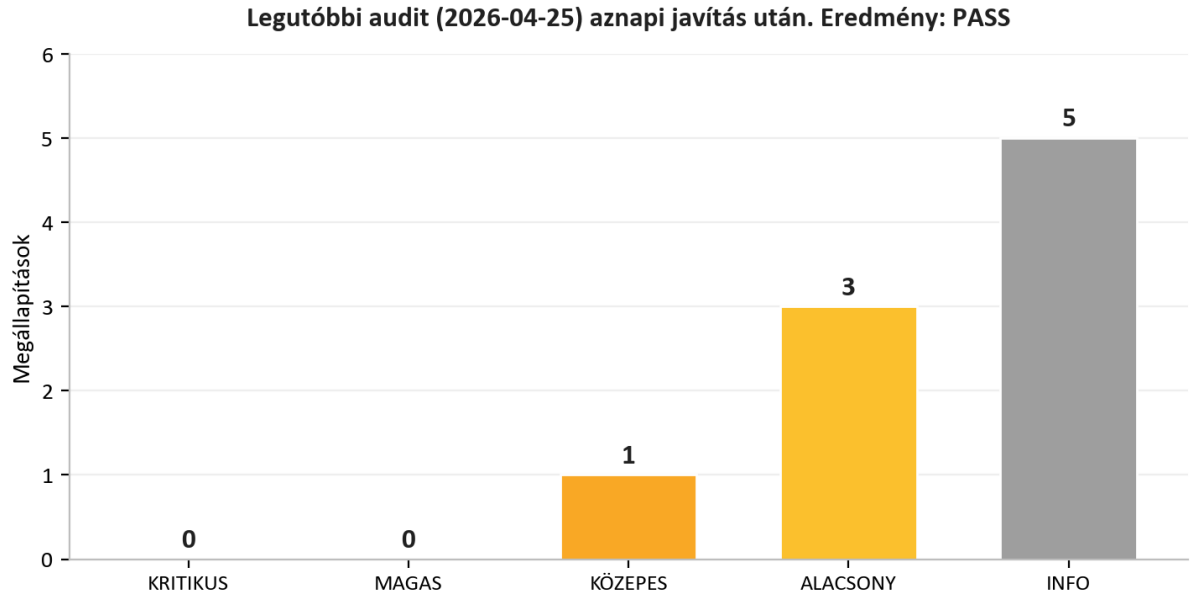
13. Biztonsági auditeredmények

Rendszeres biztonsági auditokat végzünk strukturált, ismételhető penetration testing módszertan használatával, és mindegyikről dátummal ellátott jelentést készítünk súlyosság szerint besorolt megállapításokkal, bizonyítékokkal és javításokkal. Ezek belső auditok, amelyeket saját biztonsági folyamatunk működtet; ugyanezen kontrollok formális külső tanúsítása szerepel az ütemtervünkben. 2026 márciusának vége és áprilisának vége között **seven such audits** készült fejlesztési és éles környezetekben.



A leendő ügyfél számára a legfontosabb eredmény a következetesség: **across all seven audits there were zero critical findings.** Azokban a ritka esetekben, amikor magasabb súlyosságú probléma merült fel, azt gyorsan, gyakran még aznap javítottuk és újraellenőriztük. A pontozási szempontrendszert ebben az időszakban szándékosan szigorítottuk (a maximálisan elérhető pontszám emelkedett, ahogy több értékelendő kategóriát adtunk hozzá), ezért marad magas a normalizált pontszámvonal akkor is, amikor a léc magasabbra került.

Legutóbbi auditunk, 25 April 2026 dátummal, jól szemlélteti, hogyan működik a folyamat a gyakorlatban. Két magasabb súlyosságú problémát azonosítottunk, mindkettőt még aznap kijavítottuk és újraellenőriztük, az audit pedig **PASS** minősítéssel zárult, úgy hogy az aktuális fenyegetési modell szerint nem maradt kihasználásra kész probléma.



Audit	Környezet	Kritikus	Verdikt
2026-03-28	Fejlesztési	0	Készen áll éles használatra
2026-04-04	Fejlesztési	0	Vállalati használatra kész
2026-04-05	Éles	0	Vállalati használatra kész
2026-04-20	Fejlesztési	0	Készen áll éles használatra, megjegyzésekkel
2026-04-20	Fejlesztési	0	Megfelelt megjegyzésekkel
2026-04-21	Éles	0	Biztonságos, nincs kihasználható megállapítás
2026-04-25	Fejlesztési	0	Megfelelt

Az ezekben az auditokban megfigyelhető minta a legőszintébb bizonyíték, amit nyújthatunk: a problémákat megtaláljuk, mert keményen keressük őket, és gyorsan lezárjuk őket, mert a folyamatot úgy alakítottuk ki, hogy erre képes legyen. Az a beszállító, amely soha nem jelent megállapítást, általában olyan beszállító, amely nem keres.

---

14. Üzemeltetési ellenálló képesség és megosztott felelősség

14.1 Monitorozás és naplózás

Az alkalmazás- és platformtelemetria központosított naplóelemző munkaterületre és alkalmazásmonitorozó szolgáltatásba áramlik, ami láthatóságot biztosít számunkra az elérhetőség és a viselkedés felett. Az olyan érzékeny műveletek, mint az adattörlés, jogi megállapodás elfogadása és AI-meghívások, dedikált audittáblákban kerülnek rögzítésre, így tartós nyoma marad annak, ki mit tett a fontos adatokkal.

14.2 Mentés és helyreállítás

A felügyelt adatbázis automatizált biztonsági mentéseket őriz meg, és a privát tárolót mind blob-, mind konténerszinten soft-delete megőrzés védi, így a véletlen vagy rosszindulatú törlés a megőrzési ablakon belül helyreállítható. A kritikus infrastruktúra törlési zárral védett az éles erőforrások véletlen lebontása ellen.

14.3 A megosztott felelősség összefoglalása

Terület	AI Interview Analyzer	Ügyfél
Infrastruktúra, hálózat, patch-elés	Igen	-
Alkalmazásbiztonság és AI-folyamat	Igen	-
Titkosítás, titokkezelés, adatlokalizáció	Igen	-
Felhasználó- és szerepkör-adminisztráció	Biztosítja a kontrollokat	Kezeli a felhasználókat és szerepköröket
Megőrzési szabályzat konfigurálása	Biztosítja a kontrollokat	Beállítja a megőrzési időablakot
Jelölti hozzájárulás	Biztosítja a munkafolyamatot	Biztosítja annak használatát
Erős végfelhasználói hitelesítő adatok és SSO	Támogatja az SSO-t és a szabályzatot	Kikényszeríti a belső szabályzatot

15. Fenyegetési modell és OWASP leképezés

Konkrét támadói kör ellen tervezünk: hitelesítő adatokkal nem rendelkező külső támadó, egy szervezet kíváncsi vagy rosszindulatú hitelesített felhasználója, aki egy másik szervezet adatait próbálja elérni, kompromittált függőség, valamint belső hiba. Az alábbi táblázat a széles körben használt OWASP Top 10 kockázati kategóriákat térképezi fel azokra a konkrét kontrollokra, amelyek ezeket a platformban kezelik, és amelyek mindegyikét a 12. szakaszban ismertetett tesztelés vizsgálja.

OWASP kockázat	Hogyan mérsékli a platform
Hibás hozzáférés-szabályozás	Szerepköralapú hozzáférés-szabályozás minden privilegizált végponton; szervezetenkénti szűkítés; „not found” szervezetek közötti hozzáférésnél; azonosító-újratérképezés; szervezetek közötti tesztmátrix
Kriptográfiai hibák	TLS 1.2+ átvitel közben; AES-256 nyugalmi állapotban; bcrypt jelszóhash-elés; titkok felügyelt vaultban
Injektálás	Kizárólag ORM-alapú paraméterezett lekérdezések; szigorú sémavalidáció; íráskori HTML-tisztítás
Nem biztonságos tervezés	Rétegezett többrétegű védelem; fenyegetésmodellezés és architektúra-felülvizsgálat minden auditban
Biztonsági hibás konfiguráció	Infrastructure as code; alapértelmezett tiltású hálózati csoportok; biztonsági fejlécek; letiltott megosztott tárolási kulcsok; API-séma nincs közzétéve éles környezetben
Sérülékeny komponensek	Heti automatizált függőségfigyelés; függőségi CVE auditok rendszeres felülvizsgálat során
Azonosítási és hitelesítési hibák	Rövid élettartamú tokenek; rate limited bejelentkezés; e-mail-ellenőrzés; SSO támogatás; nincs olvasható jelszó
Szoftver- és adatintegritási hibák	Rögzített, megváltoztathatatlan pipeline-lépések; aláírt asztali telepítők; webhook-aláírás ellenőrzése; tag által kapuzott éles telepítések
Biztonsági naplózási és monitorozási hibák	Központosított telemetria; dedikált audittáblák érzékeny műveletekhez
Server-side request forgery	Kimenő hívások megbízható végpontokra korlátozva; SSRF próbák a penetration testing keretrendszerben

Ez a leképezés a bizonyossági érvelésünk gerince: minden ismert támadási osztályhoz tartozik egy megnevezett kontroll, és minden megnevezett kontrollhoz tartozik egy teszt.

16. Sérülékenységkezelés és felelős közzététel

A biztonság soha nem készül el véglegesen, ezért folyamatos felfedezési és javítási ciklust működtetünk.

- **Felfedezés.** A sérülékenységek négy forrásból kerülnek felszínre: az automatizált tesztcsomagból, a rendszeres penetration testing auditokból, az automatizált függőségfigyelésből, valamint az ügyfelektől vagy kutatóktól érkező jelentésekből.
- **Triázs.** Minden megállapítás súlyossági besorolást kap (critical, high, medium, low vagy informational), bizonyítékkal és javítási felelőssel, pontosan úgy, ahogy auditjelentéseinkben rögzítjük.
- **Javítási célok.** A critical és high megállapítások azonnali javítási prioritást élveznek; auditelőzményeinkben a magasabb súlyosságú megállapításokat jellemzően még aznap javítottuk és újraellenőriztük. A medium és alacsonyabb besorolású megállapítások a rendszeres karbantartási ütembe kerülnek.
- **Ellenőrzés.** A javítások újratesztelésre kerülnek, és ahol releváns, élő ellenőrzést végzünk a telepített környezet ellen, hogy megerősítsük: a probléma valóban lezárult, nem csupán a kódban lett lezárva.
- **Közzététel.** A biztonsági aggályok közvetlenül bejelenthetők nekünk. A jelentéseket visszaigazoljuk, kivizsgáljuk, és a bejelentőt a megoldásig tájékoztatjuk.

17. Megfelelőségi leképezés

17.1 GDPR

GDPR-terület	Platformmegvalósítás
Jogszerű alap (Art. 6)	Kifejezett jelölti hozzájárulás rögzítve a feldolgozás előtt
Adatminimalizálás és tároláskorlátozás (Art. 5)	Csak interjú szempontjából releváns adatok kerülnek feldolgozásra; konfigurálható megőrzés automatikus törléssel
Törléshez való jog (Art. 17)	Minden jelöltadat egy egységként történő törlése naplózott törlési bizonyítékkal
Érintetti jogok (Art. 15 to 20)	Hozzáférés, törlés, hordozhatóság és tiltakozás támogatott
Feldolgozói kötelezettségek (Art. 28)	Regisztrációkor elfogadott, szervezetenként verziózott adatfeldolgozási megállapodás
Feldolgozás biztonsága (Art. 32)	Titkosítás, hozzáférés-szabályozás, elkülönítés és folyamatos tesztelés a dokumentumban leírtak szerint
Alfeldolgozói átláthatóság	Az adatfeldolgozási megállapodásban közzétéve, változás esetén előzetes értesítéssel

17.2 EU AI Act

A platformot foglalkoztatási döntéseket támogató magas kockázatú AI-rendszerként kezeljük, és a szabályozással összhangban álló dokumentációt tartunk fenn, beleértve az átláthatósági kártyát, a felhasználói dokumentációt és a megfelelőségi nyilatkozatot. Az alapvető védelmi intézkedéseket, az emberi felügyeletet, az átláthatóságot, a bizonyítékalapú pontozást és az AI által értékelt dolgok szigorú hatókör-korlátait a 10. szakasz írja le. Tovább fejlesztjük formális megfelelőségi dokumentációnkat, ahogy a szabályozás végrehajtási ütemterve előrehalad.

17.3 Hosztolási tanúsítások

A platform teljes egészében Microsoft Azure szolgáltatáson fut, amelynek adatközpontjai független tanúsításokkal rendelkeznek, beleértve az ISO 27001 és SOC 2 tanúsításokat. Ezek a tanúsítások az alkalmazásunk alatti fizikai és platformrétegekre terjednek ki; az alkalmazásszintű kontrollok azok, amelyeket ez a dokumentum végig ismertet.

17.4 Alfeldolgozói nyilvántartás

Alfeldolgozó	Cél	Régió
Microsoft Azure	Hosztolás, AI- és beszédfeldolgozás, tárolás, tranzakciós e-mail	EU (West Europe, Sweden Central)
Stripe	Előfizetés- és fizetésfeldolgozás	EU (Ireland)
Fakturownia	Számlázás	EU (Poland)
ATS connector (optional)	Jelöltkövetési integráció, csak kérésre engedélyezve	EU

18. Biztonsági ütemterv

A biztonságot folyamatosan fejlődő programként kezeljük. Jelenlegi ütemtervünk kezdeményezései közé tartozik a többtényezős hitelesítési lehetőségek erősítése adminisztratív fiókokhoz, az adathozzáférés központosított auditnaplózásának bővítése, a függőségek naprakészségének további szigorítása rendszeres ütemben, valamint a dokumentumban leírt kontrollok formális külső tanúsításának előmozdítása. Ezek egyike sem olyan hiányosság, amely ma ügyféladatokat tenne ki; mindegyik egy már most is rétegezett biztonsági állapot további erősítése.

19. Összefoglalás

Az AI Interview Analyzer többrétegű architektúrával védi a jelölt- és ügyféladatokat: privát alapértelmezésű hálózattal nyilvános adatszolgáltatások nélkül, erős identitáskezeléssel és szervezetenkénti elkülönítéssel, olyan alkalmazáskóddal, amely teljes sérülékenységi osztályokat tervez ki, valamint titkosítással, EU adatlokalizációval és az adatmodellbe épített adatvédelmi kontrollokkal. A platformot az különbözteti meg, hogy ezek mögött bizonyíték áll. 3,171 automatizált teszttel, ismételhető élő penetration testing módszertannal, dedikált AI-biztonsági programmal és hét belső biztonsági audit eredményével, amelyekben zero critical findings szerepelt, nemcsak állítani tudjuk, hanem meg is tudjuk mutatni, hogy a platform biztonságos.

A melléklet: Biztonsági kontrollkatalógus

Az elsődleges kontrollok és az azokat alátámasztó bizonyítékok tömör összefoglalója.

Kontroll	Mechanizmus	Bizonyíték
Átviteli titkosítás	Kizárólag HTTPS, TLS 1.2+, HTTP átirányítva	Infrastructure as code; architektúra-audit
Titkosítás nyugalmi állapotban	AES-256 platformtitkosítás tárolón és adatbázison	Platformkonfiguráció; architektúra-audit
Jelszóvédelem	bcrypt jelszavankénti salt használatával	Forráskódkezelés; hitelesítési tesztek
Munkamenet-kezelés	30 perces aláírt tokenek, visszavonható szerveroldali frissítés	Forráskódkezelés; hitelesítési tesztek
Jogosultságkezelés	Négy szerepkörös hozzáférés-szabályozás privilegizált végpontokon	Szerepkör-érvényesítési tesztcsomag
Bérlői elkülönítés	Szervezetenkénti lekérdezésszűkítés; 404 szervezetek között	Szervezetek közötti tesztmátrix
API-kulcs biztonsága	Hash-elt tárolás, szűkített jogosultságok, kulcsonkénti rate limiting	API-kulcs tesztcsomag
Injektálás elleni védelem	Kizárólag ORM-alapú paraméterezett lekérdezések	Statikus elemzés; injektálási tesztek
Cross-site scripting elleni védelem	Íráskori HTML-tisztítás	HTML-tisztítási tesztcsomag
Rate limiting	Tartós, adatbázis-alapú limiter auth végpontokon	Rate-limit tesztek; élő burst ellenőrzések
Webhook integritás	Szolgáltatói aláírás ellenőrzése a nyers törzsön	Webhook tesztcsomag
Titokkezelés	Felügyelt vault, purge protection, managed identity	Infrastructure as code; architektúra-audit
Hálózati elkülönítés	Privát végpontok; alapértelmezett tiltású szegmentáció	Infrastructure as code; architektúra-audit
Adattörlés	Egységenkénti kaszkádos törlés auditnaplóval	GDPR törlési tesztcsomag
Ellátási lánc	Rögzített pipeline-lépések; heti függőségfigyelés	Pipeline-konfiguráció; függőségi audit

B melléklet: Gyakran ismételt kérdések biztonsági értékelők számára

Hol tárolják az adatainkat? Teljes egészében az Európai Unión belül, Microsoft Azure szolgáltatáson, West Europe régióban, az AI-feldolgozás pedig EU-régiókban történik. A jelöltadatok soha nem hagyják el az EU-t.

Felhasználják az adatainkat AI-modellek tanítására? Nem. Az AI-szolgáltató nem használja fel az ügyféladatokat tanításhoz.

Elérhető az adatbázis az internetről? Nem. A nyilvános hálózati hozzáférés le van tiltva, és az adatbázis csak a virtuális hálózaton belüli privát végponton keresztül érhető el.

Láthatja egy ügyfél egy másik ügyfél adatait? Nem. Minden lekérdezés a hívó szervezetére van szűkítve, a szervezetek közötti hozzáférés „not found” választ ad, és egy automatizált mátrix folyamatosan teszteli ezt az elkülönítést.

Hogyan tárolják a jelszavakat? bcrypt-tel hash-elve és egyedi jelszavankénti salt használatával. Microsoft és Google egyszeri bejelentkezés támogatott, ebben az esetben jelszót nem tárolunk.

Támogatják az egyszeri bejelentkezést? Igen, Microsoft és Google OAuth segítségével.

Meddig érvényesek a hozzáférési tokenek? Harminc percig, egy visszavonható szerveroldali frissítési munkamenettel párosítva, amely kijelentkezéskor érvénytelenítésre kerül.

Hogyan kezelik a jelölti hozzájárulást? Minden jelölt egyedi, egyszer használatos hozzájárulási linket kap, és bármilyen rögzítés vagy elemzés előtt el kell fogadnia azt. A hozzájárulás az adott felvételi folyamathoz kerül rögzítésre.

Hogyan történik az adattörlés? Egyetlen egységként, amely magában foglalja a jelöltrekordot, interjúkat, átiratokat, hanganyagot, dokumentumokat és összehasonlításokat, konfigurálható megőrzési ütemezéssel, naplózott törlési bizonyítékkal. A jelöltek közvetlenül is kérhetik a törlést.

Van adatfeldolgozási megállapodásuk? Igen, regisztrációkor elfogadott és szervezetenként verziózott, beleértve az alfeldolgozói nyilvántartást.

Az AI hoz felvételi döntéseket? Nem. Kizárólag döntéstámogatást nyújt; minden kimenetet ember vizsgál felül, és minden döntést ember hoz meg.

Hogyan bizonyítják a biztonsági állításaikat? 3,171 automatizált teszttel, köztük dedikált biztonsági tesztcsomaggal, élő környezetek ellen futtatott ismételhető hatfázisú penetration testing módszertannal, AI-biztonsági tesztprogrammal és rendszeres írásos auditjelentésekkel.

Mi történik, ha sérülékenységet találnak? Súlyossági besorolást kap bizonyítékkal és felelőssel, prioritás szerint javításra kerül, újraellenőrzik, adott esetben élő ellenőrzéssel együtt, és auditjelentésben rögzítik.

Futtathatunk saját penetration testet? Biztonsági értékelések megfelelő hatókör és ütemezés mellett megszervezhetők az ügyfélkapcsolati képviselőn keresztül.

C melléklet: Szójegyzék

Kifejezés	Jelentés
AES-256	Erős szimmetrikus titkosítási szabvány, amelyet nyugalmi állapotban lévő adatok védelmére használnak
bcrypt	Kifejezetten jelszóhash-elésre tervezett függvény jelszavankénti salt használatával
Managed identity	Platform által kiadott identitás, amely lehetővé teszi egy szolgáltatás számára a hitelesítést tárolt kulcsok nélkül
Private endpoint	Privát hálózati cím, amely a felhőszolgáltatást távol tartja a nyilvános internettől
Network security group	Engedélyezési és tiltási szabályok halmaza, amely szűri az alhálózat felé irányuló hálózati forgalmat
RBAC	Szerepköralapú hozzáférés-szabályozás, amely a felhasználó szerepköre szerint biztosít jogosultságokat
IDOR	Insecure direct object reference, egy hozzáférés-szabályozási hiba, amely ellen a platform védekezik
SSRF	Server-side request forgery, egy támadási osztály, amelyet penetration testingjeink során vizsgálunk
Web application firewall	Peremoldali kontroll, amely szűri a rosszindulatú webforgalmat
Data processing agreement	Az a szerződés, amely szabályozza, hogyan kezeli a feldolgozó a személyes adatokat az adatkezelő nevében

D melléklet: Kapcsolat és dokumentumkezelés

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Biztonsági értékelés, adatfeldolgozási megállapodás másolata vagy EU AI Act megfelelőségi dokumentációnk ügyében kérjük, lépjen kapcsolatba ügyfélkapcsolati képviselőjével.

Ez a dokumentum az AI Interview Analyzer szolgáltatás biztonsági helyzetét írja le a láblécben feltüntetett létrehozási dátum időpontjában. Kizárólag értékelési célokra szolgál, és nem képezi szerződés részét. A konkrét szerződéses biztonsági kötelezettségvállalásokat a vonatkozó megállapodás és adatfeldolgozási megállapodás tartalmazza.