ISACA MÁSODIK SZERDAI ELŐADÁS

Mihály Tamás

Túlzott jogosultság, mint az auditokon leggyakrabban feltárt hiányosság - le kéne küzdeni végre, de hogyan!?

2024. április 10.

ISACA®
Budapest Chapter

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

ISACA®
Budapest Chapter

Agenda

- Előadóról
- Információbiztonsági helyzetkép 2023 (ISACA) – a leggyakrabban feltárt probléma: a túlzott jogosultságok
- Legfrissebb szabályozások, elvárások, felelősségek
- A túlzott jogok feltárási módjai, csökkentési lehetőségei
- Tipikus hibák felhasználói felülvizsgálat során
- Hol tartanak most a felhasználói jogosultsági felülvizsgálatok?
- Felhasználói jogosultsági felülvizsgálati folyamat fejlesztése
- Milyen eszközzel és hogyan tehetjük a kockázatokat mérhetővé és könnyebben kezelhetővé?
- A felülvizsgálati folyamatban hol segíthet a mesterséges intelligencia?

Előadó- Mihály Tamás CISA, CISM

25 éve az IT biztonsági szakmában:

- Big4 IT security tanácsadó, auditor
- Banki IT belső ellenőr,
- IT biztonsági vezető, 10+ év CISO-ként jelentős hazai kereskedelmi bankokban.

Főbb tapasztalatok:

- Törvényi megfelelőség, nemzetközi szabványok
- Biztonság szervezés, kontroll folyamatok
- Kockázatfelmérés
- Csalásfelderítés / csalásmegelőzés
- Adatszivárgás gátlás
- Jogosultsági kockázatok, felülvizsgálatok

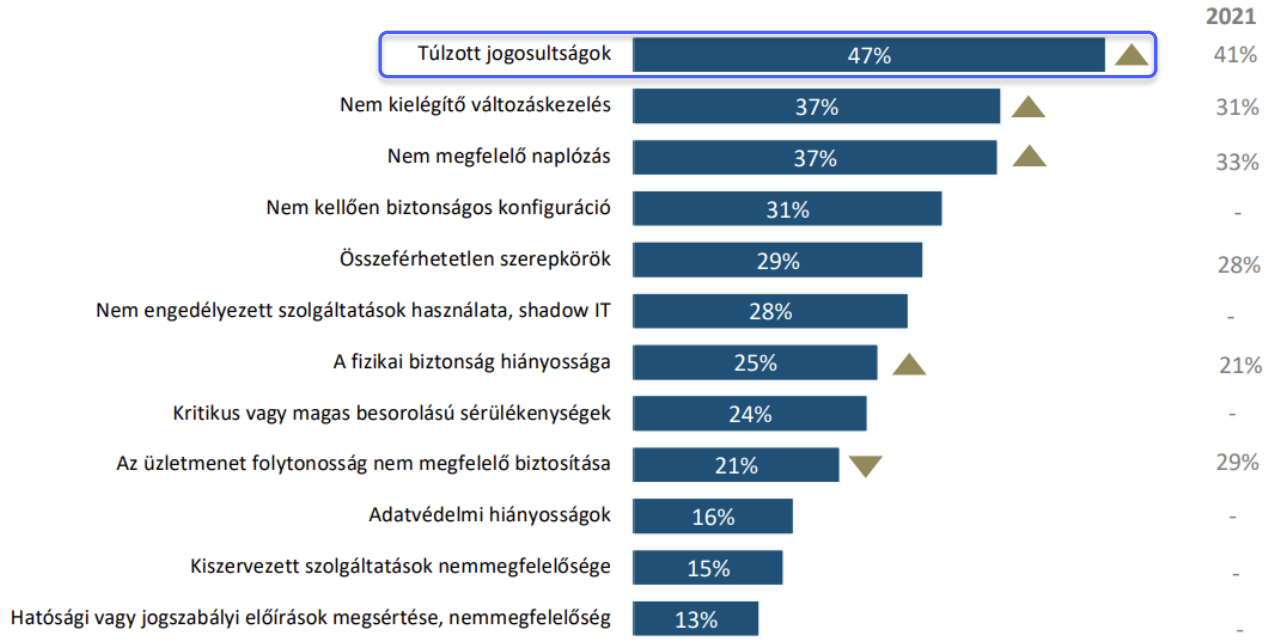
ISACA Budapest Chapter

ISACA - Információbiztonsági helyzetkép 2023 – a leggyakrabban feltárt probléma

IT auditok során észlelt biztonsági hiányosságok leggyakoribb problémája a **túlzott jogosultságok (47%),** amely növekedést mutatott az elmúlt 2 évben.

Sok éve élen áll a feltárt hiányosságokat tekintve.

6. ábra: Az IT auditok során azonosítottak-e hiányosságokat az alábbi területeken az elmúlt 12 hónapban?



Bázis: IT auditot rendszeresen végző szervezetek

ISACA Budapest Chapter

Legfrissebb szabályozások, elvárások

Jogszabályi háttér:

Least privilege (v. need-to-know) elvként megtalálható az alábbiakban:

ISO 27002, COBIT, PCI DSS, NIST 800-53, GDPR, SOX, HIPAA-ban

a legfrissebb, legszélesebb kört érintőek közül pedig a **DORA és a NIS2** részletszabályaiban

- DORA: JC 2023/86 – Article 20, 21 és 30. fejezetek (**féléves UAR, egyéves UAR a ritkán használt rendszerekre**, data owner v. jóváhagyó viszont nem szerepel, megkülönbözteti az adminisztrációs és privilegizált jogokat!)
- NIS2 (MK Rendelet - Norma): 2. Hozzáférés felügyelet (2.67 **Felhasználói jogosultságok felülvizsgálata „meghatározott időközönként**))

Feladatok és felelősségek I.

Elsődlegesen érintett területek:

- Üzleti vagy szakmai területek vezetői (data owners), mint jóváhagyók
- Rendszer- és folyamatszervezők (a belső folyamatok módosulásának mindig lehet jogosultsági vonatkozása)
- Jogosultságkezelési folyamatot rendszeresen, operatívan ellenőrző területek (pl. Információ biztonsági csoport)
- Jogosultságkezelési folyamat végrehajtói (pl. IT adminisztrátorok, IT biztonsági adminisztrátorok)

Feladatok és felelősségek II.

További érintett területek:

• Belső ellenőrzés (az éves tervezett üzleti/szakterületi vizsgálatai során, vagy IT biztonság vizsgálatakor)

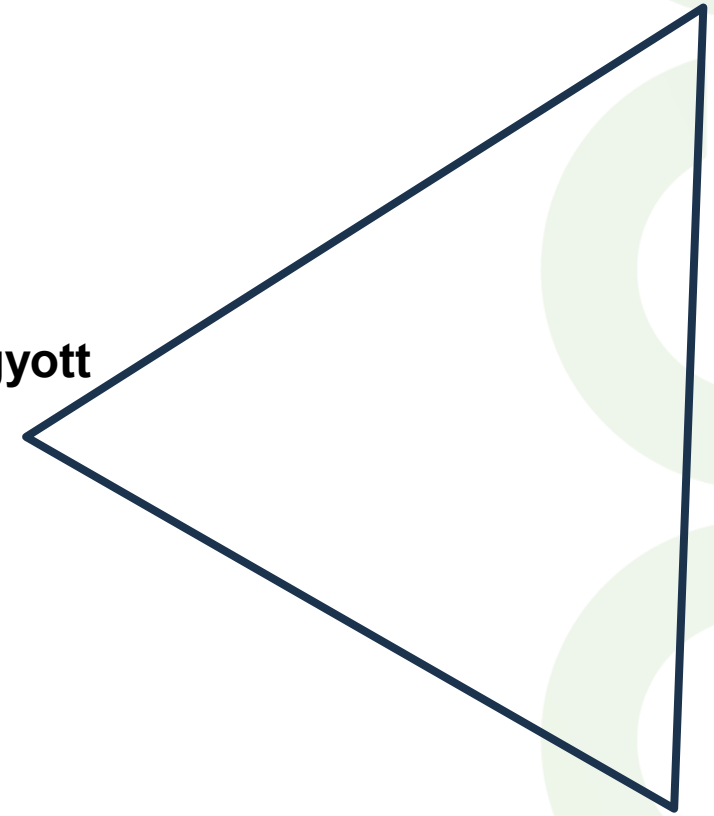
• Egyéb biztonsági területek (pl. fizikai biztonság vagy bankbiztonság)

• Esetlegesen jogi vagy compliance területek (összeférhetetlenségek meghatározása, változó törvényi követelmények feltárása, stb.)

A feladatok és a felelősségek megoszlanak

Adatgazdák, jóváhagyók:
- igényelt szerepkörök jóváhagyása
- szerepkörök tesztelése
- szerepkör módosítási javaslatok
- jogosultság felülvizsgálatok

IT adminok, rendszerszervezők:
- szerepkörök kialakítása
- felhasználó létrehozás, jóváhagyott szerepek beállítása (ha az nem automatikus)
- szerepkörök módosítása
- felhasználó inaktiválás, törlés

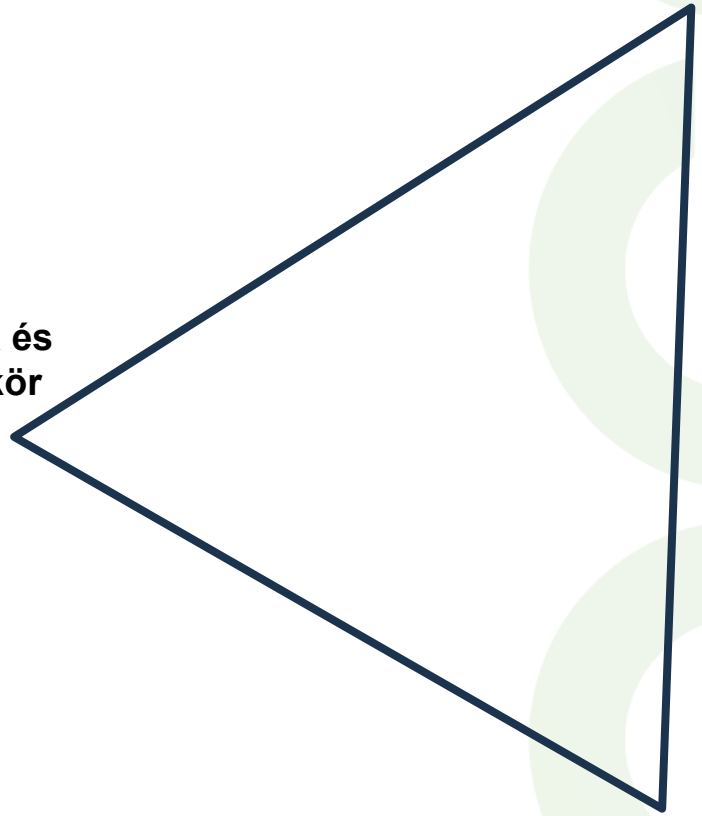


IT security:
- least privilege kötelezettség
- IAM folyamat felügyelete
- visszakereshetőség
- kockázatarányosság

Mi történik egy túlzott jogosultsági incidens során?

ISACA®
Budapest Chapter

Ki, mivel hárítaná a felelősséget?



IT adminok, rendszerszervezők:

- „A kérést az adatgazda jóváhagyta és amúgy sem kértek minket a szerepkör átdolgozásra, és mi nem tudtuk pontosan, hogy mit csinál majd ténylegesen a kolléga!”

Adatgazdák, jóváhagyók:

- „Nem tudtam pontosan, hogy mi van a szerepkörben, nem vagyok IT-s, amúgy meg nem felületes voltam a jóváhagyásnál, hanem csak gyors, hogy mielőbb dolgozzon a kolléga!”

IT security:

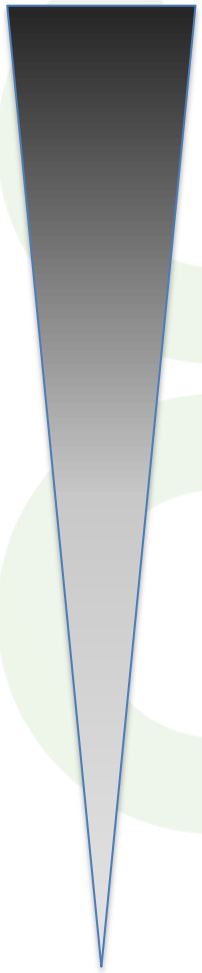
- „Én a kontrol rendszer meglétéért vagyok felelős, nem én hagytam jóvá az adott jogosultságot!”

ISACA Budapest Chapter

Mik lehetnek egyáltalán túlzott jogosultságok? „Szürke zóna”

Értelmezhetőség erőssége szerinti csökkenő sorrendben:

- Gyártói, default felhasználók telepítéshez, frissítéshez
- Átfogó, általános rendszeradminisztrátori jogosultságok, felhasználók
- Fejlesztői jogok (dev, debugger jogok), felhasználók
- Szűkebb, célhoz kötött, de még adminisztratív jogok (pl. backup admin)
- Felhasználó menedzsment funkciókkal bíró szerepek
- Security konfigurációs szerepek
- Adatkommunikációs, interfész jogok
- Szakmai, üzleti konfigurációs szerepek
- „Üzleti vezető és titkárnője mindent is csinálhat” szerepek
- Közvetlen adatbázis elérési jogok (vagy adott rendszer alatti technológiai szintek)
- Széles körű tesztelési jogok, összevont profilok éles rendszerben
- Szakmailag, üzletileg összeférhetetlen profilok
- Mindent látó auditori jogosultságok
- Elavult, széles körű profilok



És ezeket még tovább lehetne variálni azzal, hogy belsős dolgozókról vagy külsősökről beszélünk, aktív szerződésük van vagy lejárt, aktív vagy inaktívak a userek, technikai vagy csoportuserekről, kiosztott vagy ki nem osztott szerepekről beszélünk, éles, teszt vagy fejlesztői környezetről, stb. …

ISACA Budapest Chapter

A túlzott jogok feltárási módjai, csökkentési lehetőségek I.

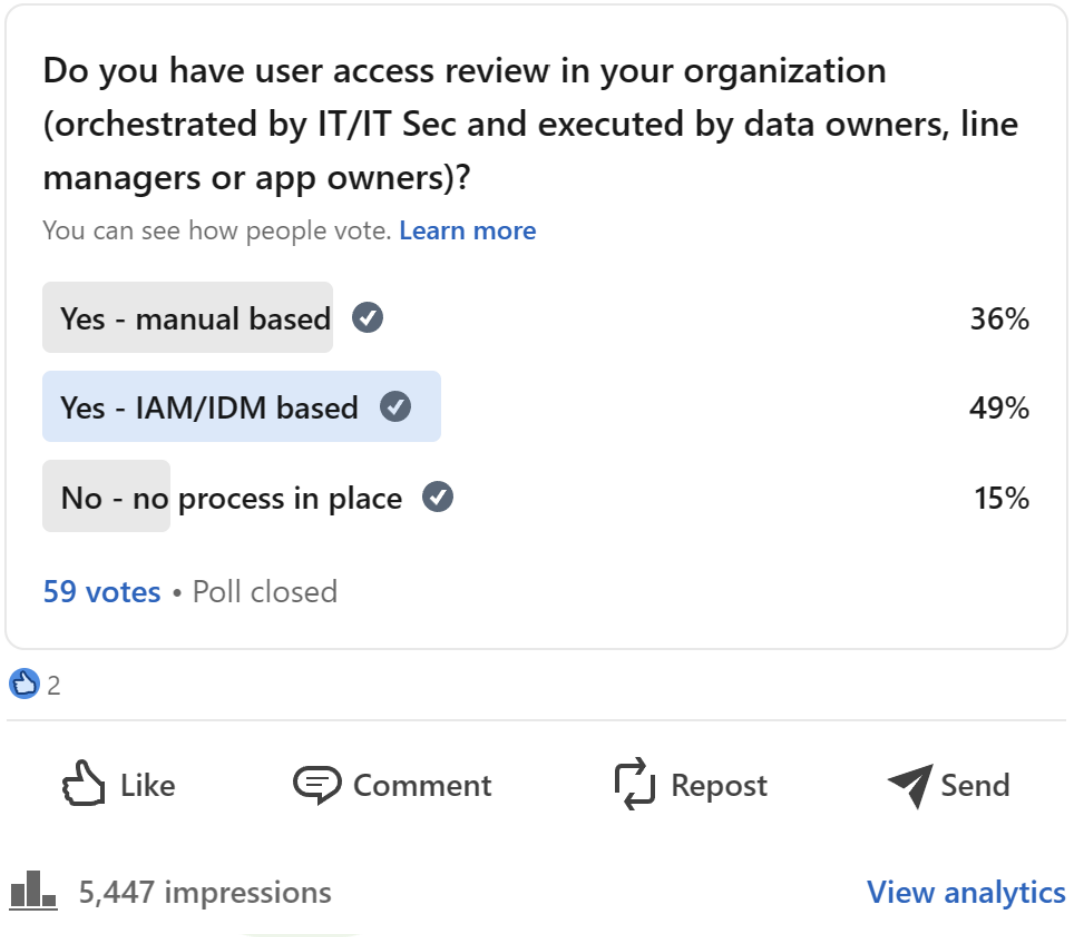
• Rendszeres felhasználói jogosultsági felülvizsgálatok (de ez sok munka, nehéz szervezni, összefogni, eredményeit összegezni és megvalósítani – az IAM rendszer ilyen funkciója segíthet!)

• Privileged Identity (v. Access) Management PIM/PAM használata (manuális felhasználó definiálás, és ennek nem ez a fő célja, hanem az activity monitoring és a credential management)

• Folyamatos, automatizált jogosultsági kockázatmérés és jogosultság felügyelet (szerepkör tartalomban jogosultsági kockázatokat és nem használt, inaktív felhasználókat felderítő eszköz)

Hol tartanak most a felhasználói jogosultsági felülvizsgálatok?

- LinkedIn-en megkérdezett szakmabeliek **53%**-a még mindig manuális végzi a felhasználói jogosultsági felülvizsgálatokat
- Idő- és energiaigényes folyamat
- A szakemberek sok esetben elhanyagolják a feladatot, a problémák miatt általában csak **évente** végzik el a felülvizsgálatot, bízva az auditorok jó szándékában.
- Nem áll rendelkezésre megfelelő eszköz.



ISACA Budapest Chapter

Tipikus hibák felhasználói jogosultsági felülvizsgálat során

A FELHASZNÁLÓI JOGOSULTSÁGI FELÜLVIZSGÁLATI (User Access Review) FOLYAMAT NEM TELJESKÖRŰ:

- Csak a felhasználók munkavállalói státuszát ellenőrzik a jogait és szerepköreit nem.
- A felülvizsgálati folyamatot nem dokumentálják, így nem lehet nyomon követni, hogy ki, mit és mikor vizsgált felül.
- Az azonosított problémákat jelentős késéssel vagy egyáltalán nem javítják ki.
- Az összeférhetetlen jogok vizsgálata ki van zárva a felülvizsgálati folyamatból.
- A felülvizsgálati folyamat nem következetes, és nincs belső szabályozása.

Tipikus hibák felhasználói jogosultsági felülvizsgálat során

A VIZSGÁLT ADATOK KÖRE NEM TELJES:

- Csak a munkavállalók felhasználóit vizsgálják felül
- A külső felhasználók is ki vannak zárva a felülvizsgálatból.
- A felhasználók jogait külső, kézzel egyszerűsített listák alapján ellenőrzik.
- A technikai felhasználók jogait senki sem ellenőrzi.
- A szerepkörök tartalmát nem gyűjtik össze és nem vizsgálják felül.

ISACA® Budapest Chapter

Tipikus hibák felhasználói jogosultsági felülvizsgálat során

A VIZSGÁLATOT NEM A MEGFELELŐ SZEMÉLY VÉGZI:

- A felülvizsgálatot nem az business owner/data owner végzi, hanem az informatikai rendszergazdák, így senki nem veszi észre és nem követi a hozzáférési profilok tartalmában bekövetkező üzleti változásokat.
- A felülvizsgálatot végző személy átadja a feladatot valaki másnak (megfelelő ismeretekkel vagy anélkül).
- A felülvizsgálók szakértelme széles skálán mozog, és néhányan nem rendelkeznek megfelelő ismeretekkel a felülvizsgálathoz.
- A felülvizsgálónak a saját jogosultságait is ellenőriznie kell, ami természeténél fogva ellentmondásos.
- A felülvizsgáló nincs tisztában a hozzáférési jogosultságokkal kapcsolatos üzleti kockázatokkal és konfliktusokkal.

ISACA Budapest Chapter

Tipikus hibák felhasználói jogosultsági felülvizsgálat során

NEM VAGY ROSSZ ESZKÖZÖKET HASZNÁLNAK A FELÜLVIZSGÁLAT SORÁN:

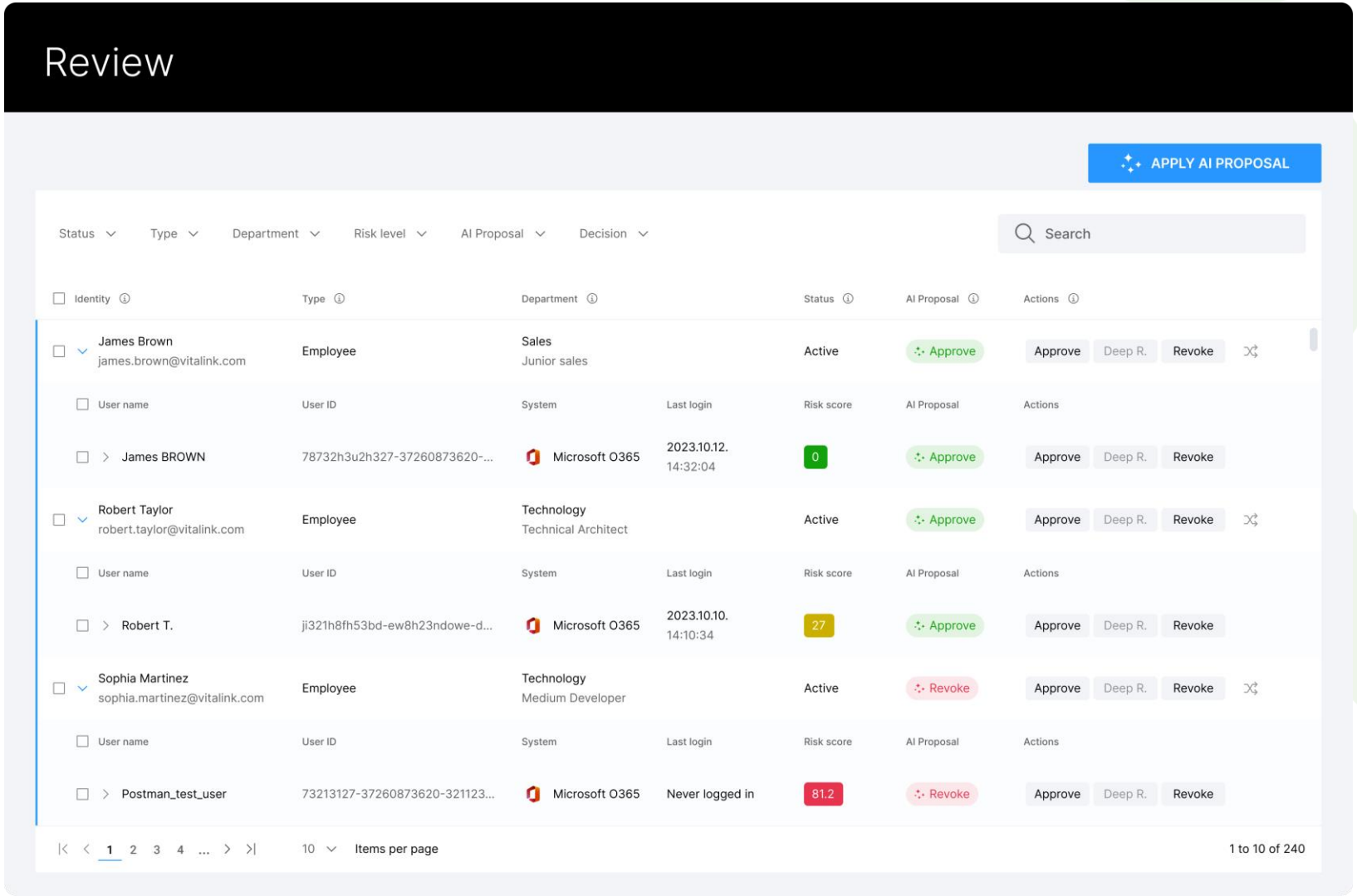
- Manuálisan irányítják, koordinálják és ellenőrzik a felülvizsgálati folyamatot.
- A felülvizsgálat összetett, hiányos és nehezen érvényesíthető az egész szervezeten keresztül.
- A folyamat hosszú időt vesz igénybe, és nehéz válaszokat kapni a felülvizsgálók részéről.
- Az IAM-eszköz (ha van ilyen) nem konfigurálható a felhasználói hozzáférések felülvizsgálati folyamatához.

ISACA Budapest Chapter

Milyen eszközzel és hogyan tehetjük a kockázatokat mérhetővé és könnyebben kezelhetővé?

- A felhasználói és alacsonyabb szintű felülvizsgálatoknál a **hozzáférési kockázati pontozás** segíti az adattulajdonosokat abban a döntésben, hogy mit és miért kell visszavonni!
- **Scoring-alapú mérőszámrendszer**, amely kvantitatív módon számszerűsíthetővé és összemérhetővé teszi a felhasználók jogosultsági kockázatait;
- **Granularitás és mélység** a jogosultsági kockázatok feltárásában és kiértékelésében a lehető legmélyebb – a szerepkör-tartalmakat is érintő – elemi jogosultsági objektumok szintjéig;
- **Rendszerek közti (cross-system/cross-application) összeférhetetlenségek** feltárásának képessége;
- **AI/ Machine Learning/ Automation** – segít abban, hogy megmutatja mit kell ténylegesen felülvizsgálni

A felülvizsgálati folyamatban hol segíthet a mesterséges intelligencia?



- Magában a döntéshozatal támogatásában - co-pilot javaslattétel
- Az adat előkészítésben - sok különböző, gyakran legacy rendszerekből hosszadalmas előállítani a vizsgálni kívánt adatokat, adatmezők felismerése, adattisztítás, merge

THEFENCE

XS MATRIX

ISACA®
Budapest Chapter

KÖSZÖNÖM A FIGYELMET!