



AI a szervezetben: üzleti gyorsító vagy információbiztonsági akna?

KUTI ANITA
Információbiztonsági szakterület vezető





**Az AI már itt van a
szervezetben.**

**A kérdés nem a használat,
hanem a kontroll.**

1. Miért most? (Shadow AI)

- A munkavállalók jelentős része már használ **AI-eszközöket**.
- Jellemzően **nem jóváhagyott, nem kontrollált** módon.
- Motiváció: **időnyomás, hatékonyság, alacsony belépési küszöb**.
- Gyors, produktívitás-vezérelt működés → **növekvő kockázat**.

A vezetés gyakran nem tud róla.



**A legtöbb szervezetben nem
AI-bevezetés,
hanem Shadow AI zajlik.**

2. Az AI mint információbiztonsági akna

Hol robbanhat?

- **publikus AI-ba** feltöltött üzleti adatok,
- ismeretlen **adattárolás** és újratanítás,
- **hibás vagy torz output** üzleti döntésekhez,
- **review** nélküli kimenet ügyfél felé.



**A kockázat nem az AI-ban van,
hanem a használat módjában.
Ezen múlik minden.**

3. A fordulópont

Felelős AI =

- Jogszabályi megfelelés (EU AI Act, GDPR)
- Információbiztonság (adat, modell, folyamat)
- Működőképesség és üzleti érték

Stratégiai célok:

- Shadow AI visszaszorítása jóváhagyott alternatívákkal.
- Valódi üzleti haszon gyors elérése, kockázatkontroll mellett.



4. Bevezetés előtt

- Mit automatizálunk vagy támogatunk? (konkrét **use case**)
- Kik használják, mely folyamatokban?
- Milyen **adat** érintett?
(üzleti, személyes, különleges)
- Milyen **kockázatok** jelennek meg már a startnál?

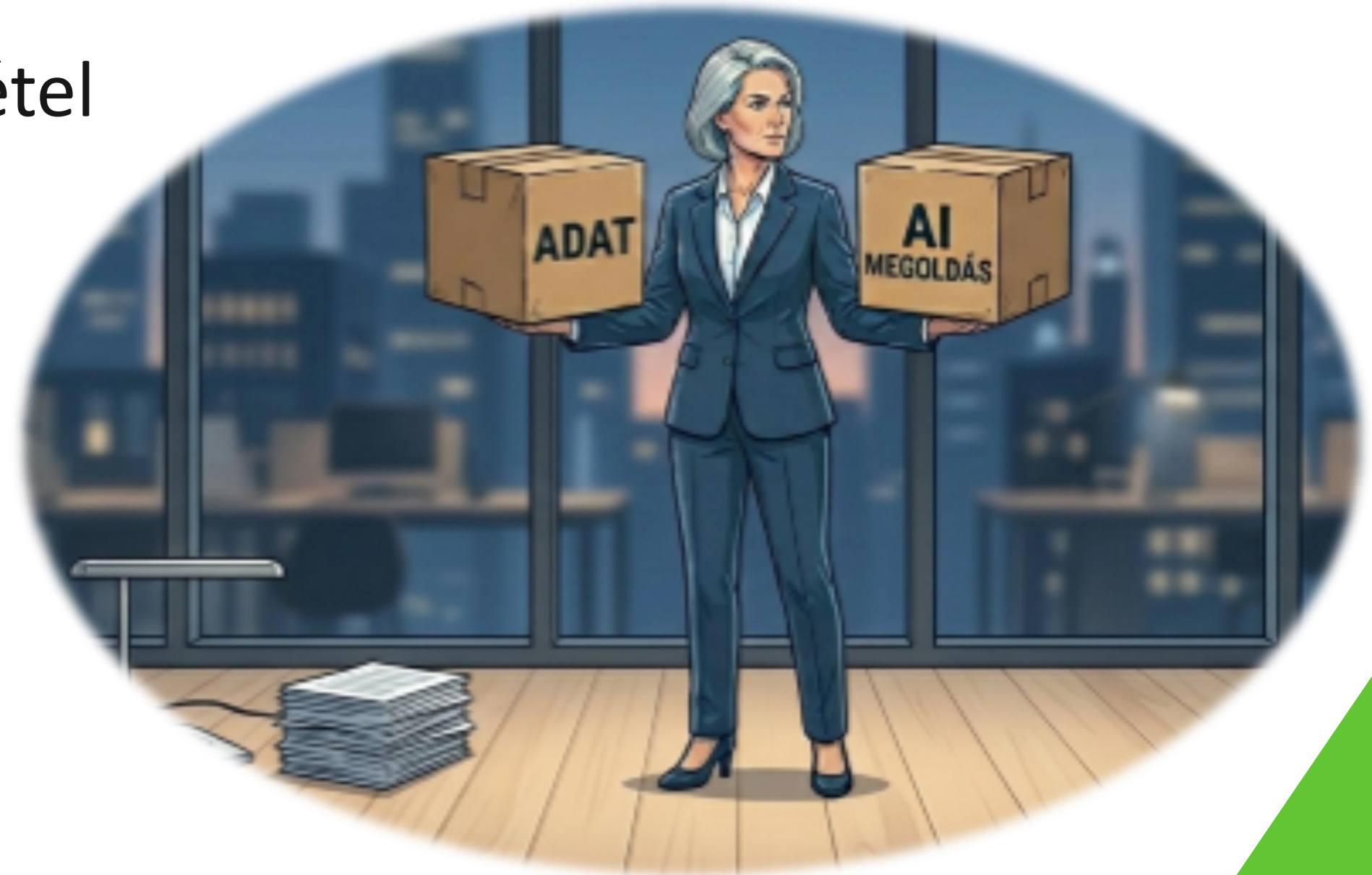
**Bevezetés előtt: közös felmérés –
üzlet + jog + biztonság
Nemcsak IT-feladat!**



5. AI Bevezetés

- Üzleti folyamatok azonosítása
- Adat osztályozás, mint belépési feltétel
- Eszközválasztás és PoC

**Gyors, kontrollált pilot
Kockázat alapján döntés
Go/No-go előre rögzítve**



6. AI biztonságos működés

- Kockázatelemzés és kezelés
- AI hatáselemzés
- Data workflow + **adatminimalizálás**
- **Modellvalidáció és újrapvalidáció**

Fontos:
Nem egyszeri projekt!
Folyamatos monitoring
és szabályozás.



7. AI mint üzleti gyorsító

Hol hozhat valódi értéket?

- Tudatos választás
- Kontrollált működtetés
- Biztonságos üzemeltetés

Feltételek:

- Használati lehetőségek felismerése és kiválasztása
- Ismert adatforrás
- Emberi felügyelet
- AI compliance



- **AI-használati térkép, AI leltár,**
- **engedélyezett/tiltott AI használat,**
- **AI Policy,**
- **vezetői ownership,**
- **tudatosság-növelés.**



0

9. Zárás: a valódi kérdés

**Nem az, hogy használjuk-e az AI-t,
hanem:**

- Ki használja?
- Mire?
- Milyen adatokkal?
- Ki ellenőrzi?
- Ki vállalja a felelősséget?

**A szabályozott AI üzleti gyorsító.
A szabályozatlan AI
információbiztonsági akna.
Policy + technika + monitoring:
együtt működik.**

Kiber & AI Gyorsítósáv

Digitális érettségi felmérés:



Gyors önértékelés • 8 kérdés • 5-10 perc • azonnali eredménnyel