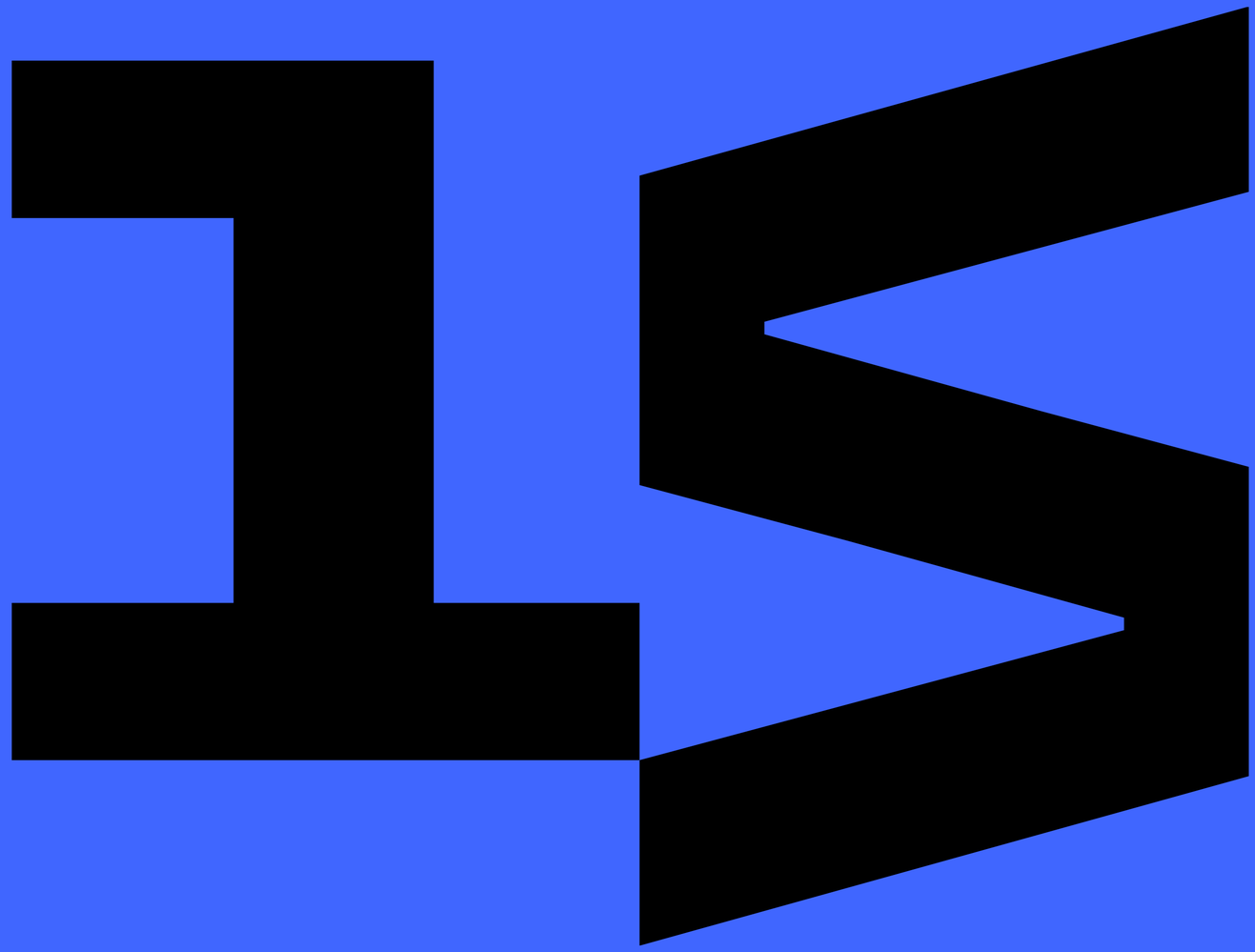
Kódolás AI használatával

Ott Károly



A (kiber)biztonság gyakorlatAI konferencia

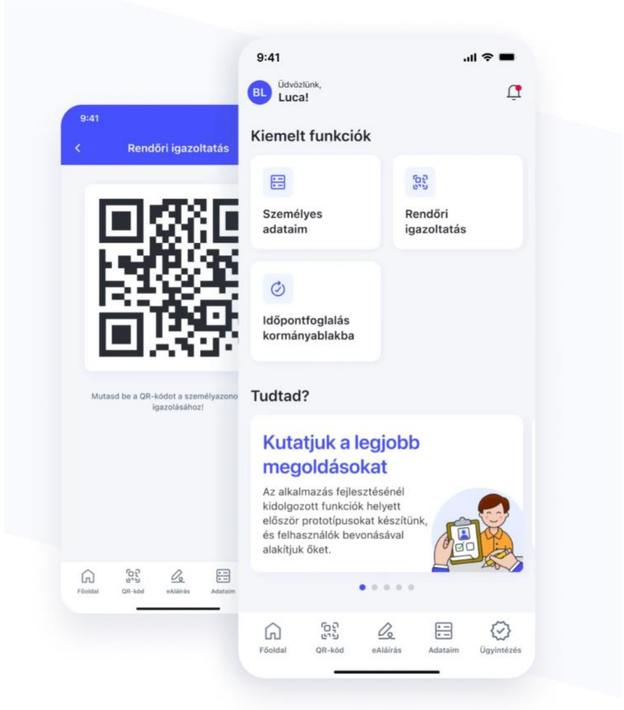
2025/04/10

idomsoft

IdmSoft Zrt.

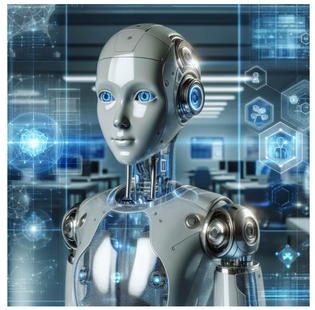
Visszaadjuk az állampolgároknak az időt, hogy azzal foglalkozzanak, amivel szeretnének.

- Állami tulajdonú fejlesztő cég
- A Digitális Magyarország Ügynökség (DMÜ) irányítás alatt
- Közigazgatási ügyintézések és eljárások digitális rendszereinek fejlesztése ügyintézők és állampolgárok számára
  - Digitális Állampolgár (DÁP) mobilalkalmazás
  - Árfigyelő
  - Választási Tájékoztatási Rendszer, Nemzeti Választási Rendszer
  - Nyilvántartások: Személyi Adat és Lakcím, Országos Jármű, Okmány

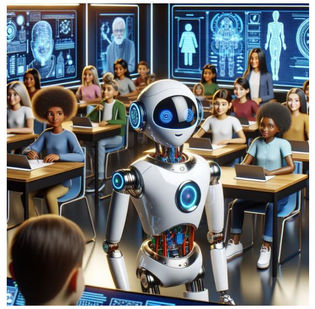


Mi az AI?

- **AI (Artificial Intelligence) – Mesterséges Intelligencia**: *„egy gép, program vagy mesterségesen létrehozott tudat által megnyilvánuló intelligencia” (Wikipédia)*



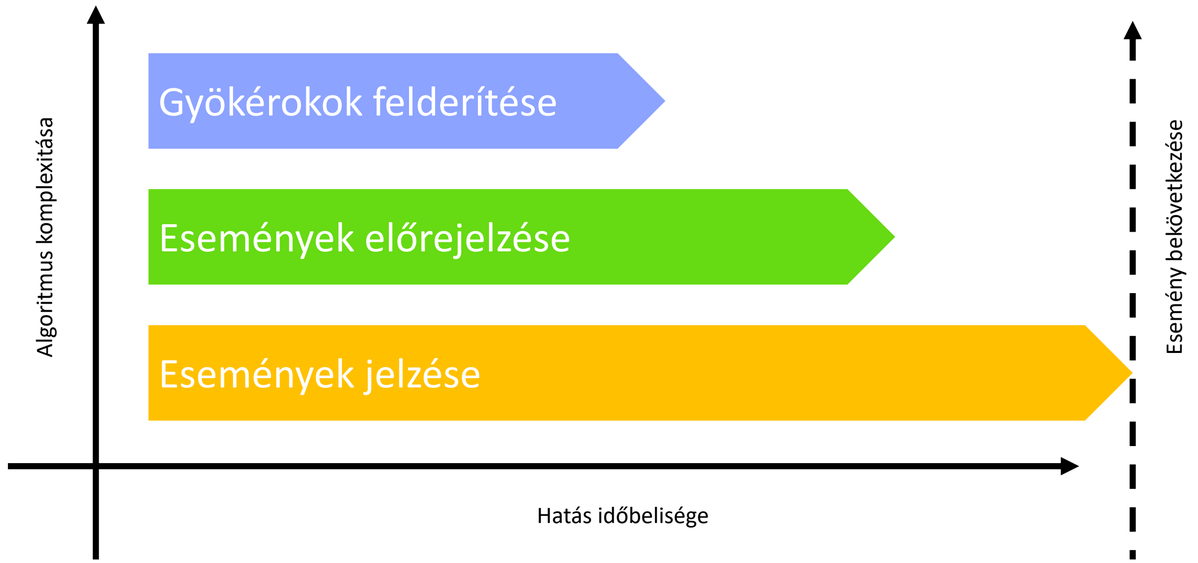
- **ML (Machine Learning) – Gépi Tanulás**: (korábban adatbányászat) matematikai algoritmusok gyűjteménye nagy adatmennyiségek átvizsgálására, minták felimerésére, előrejelzésekre



- **GenAI (Generative AI) – Generáló AI**: nagy nyelvi modellek ember-gép kommunikációra

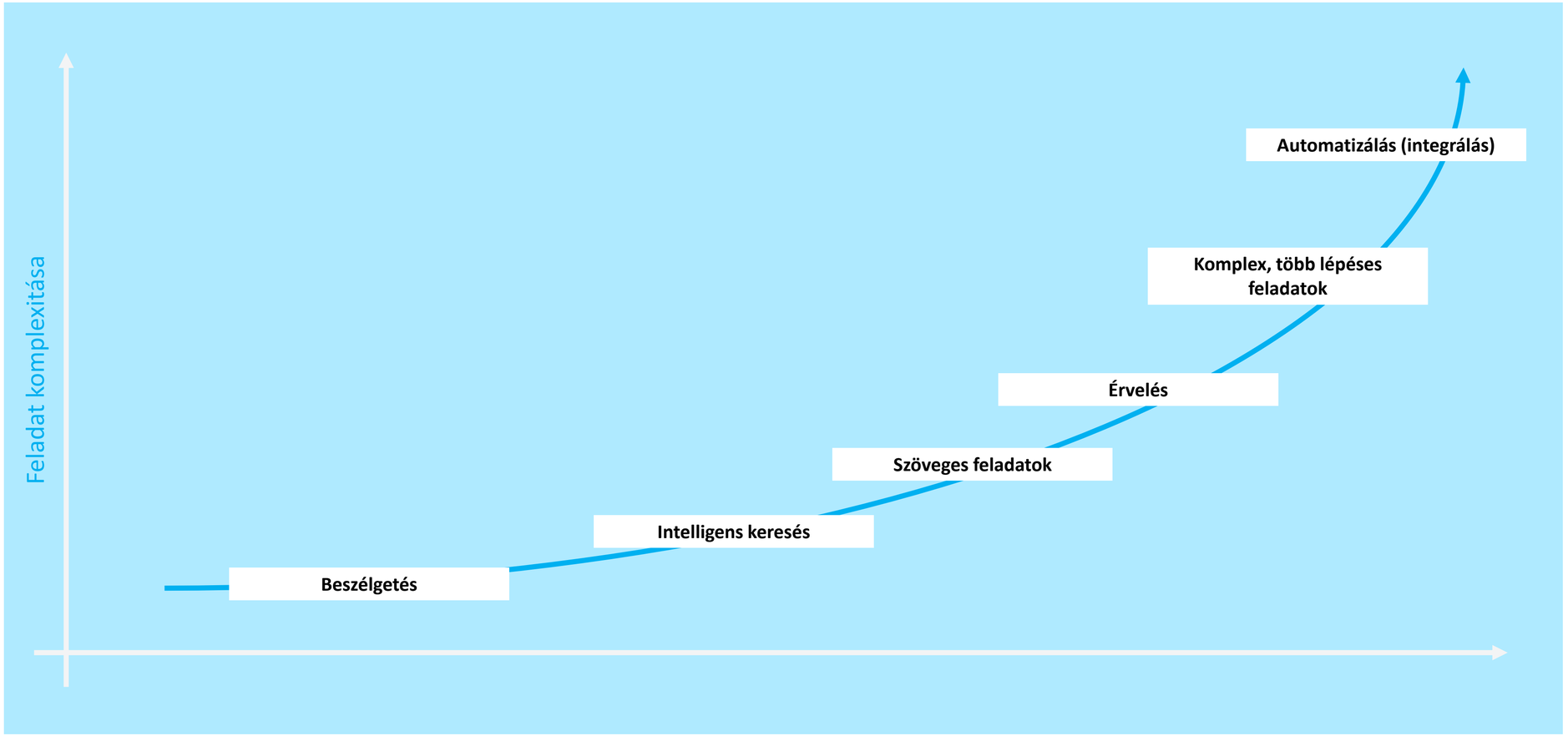
AI alkalmazása

- **Machine Learning**
  - Események jelzése
  - Események előrejelzése
  - Gyökérokok felderítése
  - Felhasználók: kutatók, ipar, bank, biztosítás

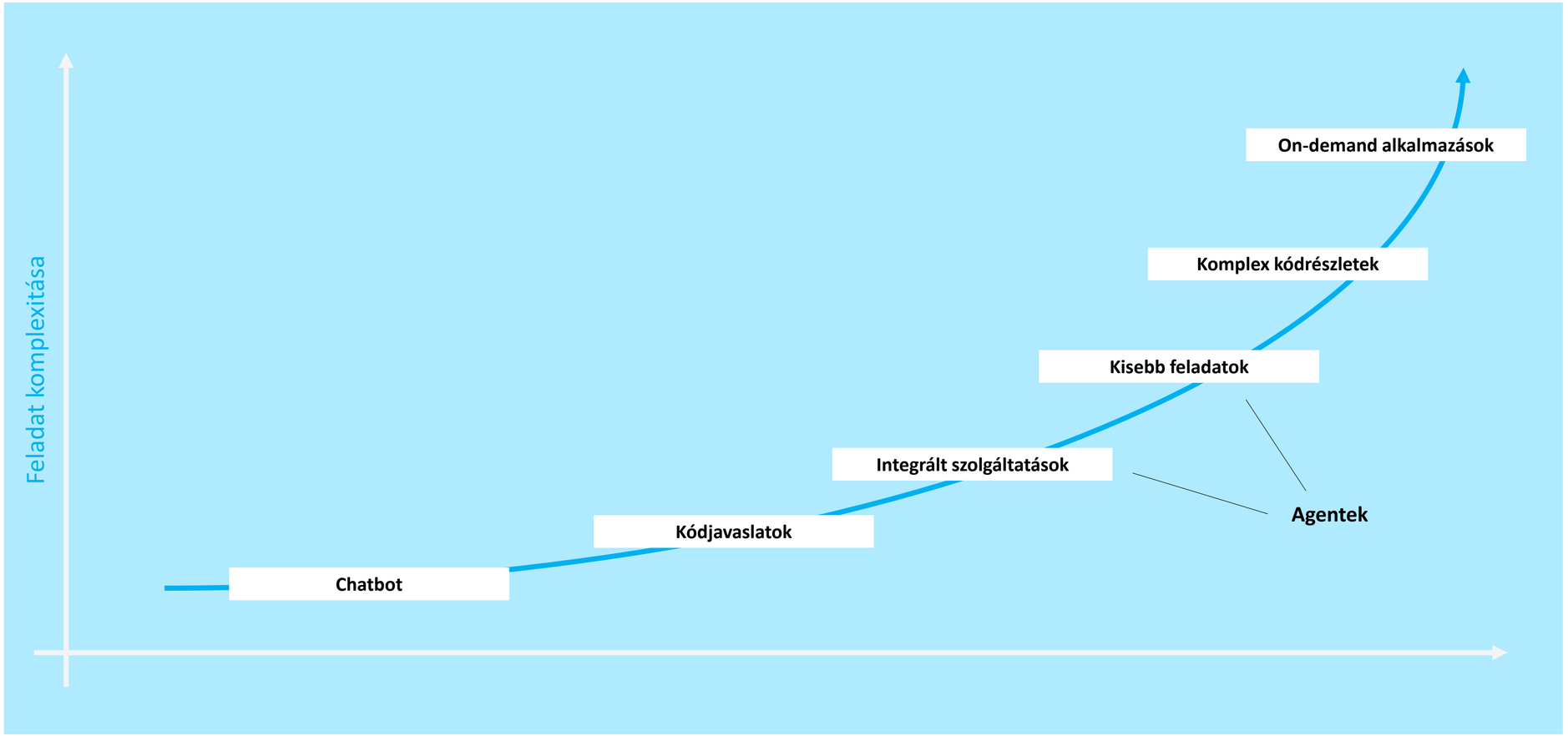


- **GenAI**
  - Munkánk támogatására: repetitív, manuális feladatok elvégzésére szöveges környezetben
  - Beszélgetésre: tudáskinyerés az összes interneten elérhető információból
  - Automatizálásra: szöveges utasítások alapján feladatok elvégzése
  - Felhasználók: irodai dolgozók

GenAI használatának fejlődése



GenAI használata a kódolásban



Nemzetközi trendek a GenAI kódolásban

Github Copilot Adoption Trends

Metric	Industry Average	Technology	Healthcare	Industrial Conglomerate	Banking and Finance	Insurance	Startups
Acceptance Rate	65%	70%	60%	55%	65%	50%	75%
Suggestion Rate	30%	35%	25%	20%	30%	25%	35%
License Usage (Business)	80% Paid	90% Paid	70% Paid	60% Paid	80% Paid	70% Paid	90% Paid
Code Completion	60%	70%	50%	60%	70%	50%	70%
Function Generation	20%	15%	25%	20%	15%	25%	15%
Bug Fixing	10%	10%	15%	10%	10%	15%	10%
Refactoring	10%	5%	10%	10%	5%	10%	5%
Productivity Gains	10-20%	15-25%	5-15%	10-20%	15-25%	5-15%	15-25%

OPSERA

2025. Március 25.

GenAI kódolási hibák és megoldásaik

- **Kódolt hitelesítő adatok:** A mesterséges intelligencia véletlenül API-kulcsokat vagy érzékeny adatokat tartalmazó kódot generálhat
- **Harmadik féltől származó függőségek:** A mesterséges intelligencia ismert sebezhetőséggel rendelkező kódtárakat javasolhat
- **Nem érvényesített bemenetek:** Előfordulhat, hogy az AI által generált űrlapok vagy API-k nem rendelkeznek megfelelő bemeneti ellenőrzéssel, ami biztonsági résekhez vezet

- **Engedélyek és függőségek áttekintése:** A megvalósítás előtt mindig ellenőrizze, hogy az AI milyen külső függőségeket javasol
- **Biztonsági szkennerek használata:** Az olyan eszközök, amelyek képesek észlelni a javasolt kódtárak biztonsági réseit
- **Soha ne használjon mesterséges intelligenciát érzékeny kódokhoz:** Kerülje a mesterséges intelligencia használatát hitelesítés, titkosítás vagy más biztonsági szempontból kritikus funkciók kezelésére szakértői felülvizsgálat nélkül

GenAI használata az IdomSoftban

- **GitHub Copilot**: műszaki területek támogatására
- **M365 Copilot Chat**: GenAI megoldás szöveges feladatokhoz
- Tesztelés alatt további megoldások
  - Microsoft GenAI Agentek
  - GitHub Agentek
  - Onprem GenAI megoldások védett információkra
- GenAI szolgáltatások (100+) szabályozása

GitHub Copilot

Microsoft Copilot Chat

Microsoft Copilot Studio

M365 Copilot

Kódolás és GenAI veszélyei

- **Megbízhatatlan AI modell használata**
  - adat vagy kód lopás/szivárgás modell használat közben
- **Felelőtlen AI modell használat**
  - javaslat felületes vizsgálata
- **Rosszindulatú AI modell használata**
  - rosszindulatú kód elhelyezés a kódban
- **Hibás vagy rosszindulatú modell beépítése a programba**

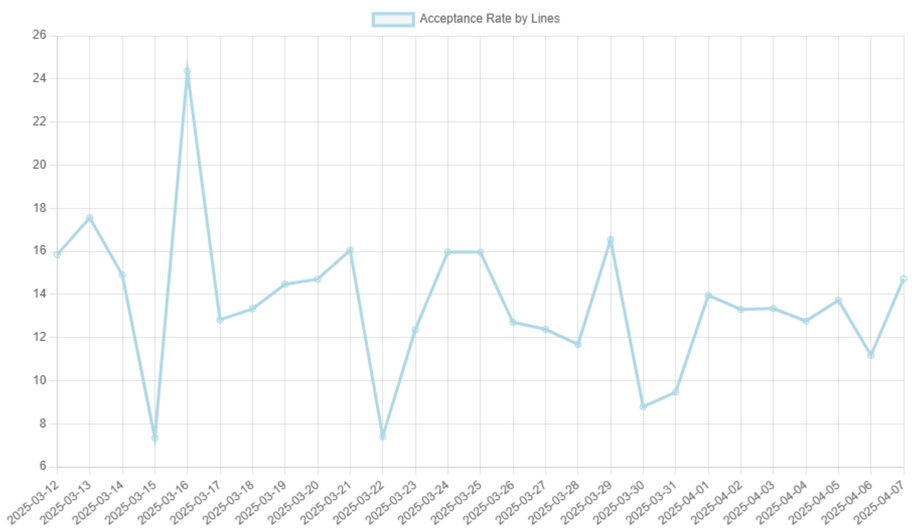
GitHub Copilot használat

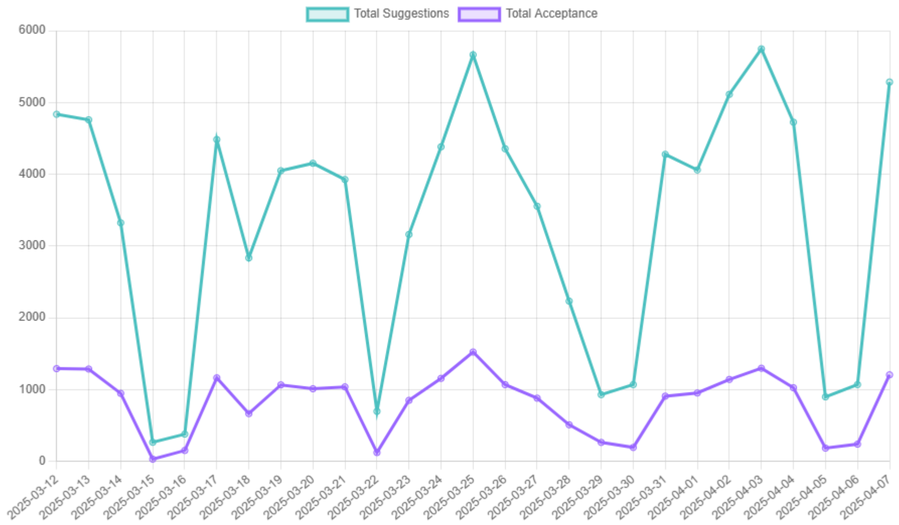
Összes felhasználó száma: 130

Általagos napi felhasználók száma: 75

Javasolt sorok elfogadási aránya: 15%

Havi elfogadott sorok száma: 30.000





M365 Copilot Chat használat

Filters: Periods: **Past 30 days (Mar 8, 2025 - Apr 6, 2025)**

Active users
233

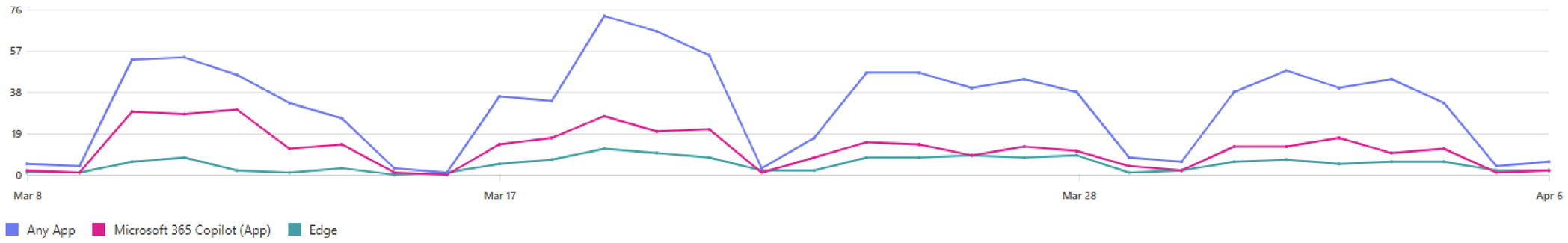
Average daily active users
31

Adoption

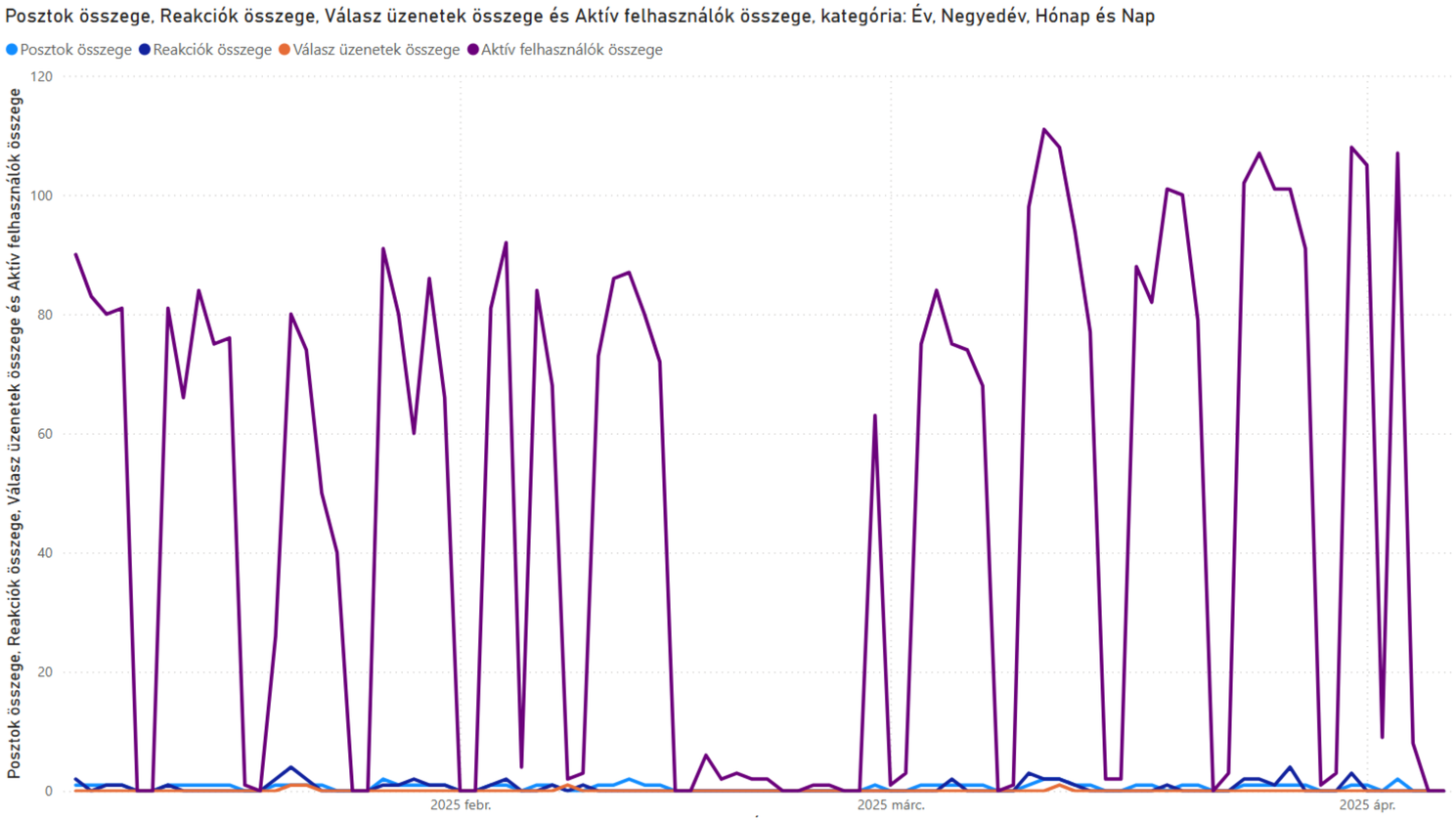
Adoption trend by app

Summary | Trend | Apps: **All**

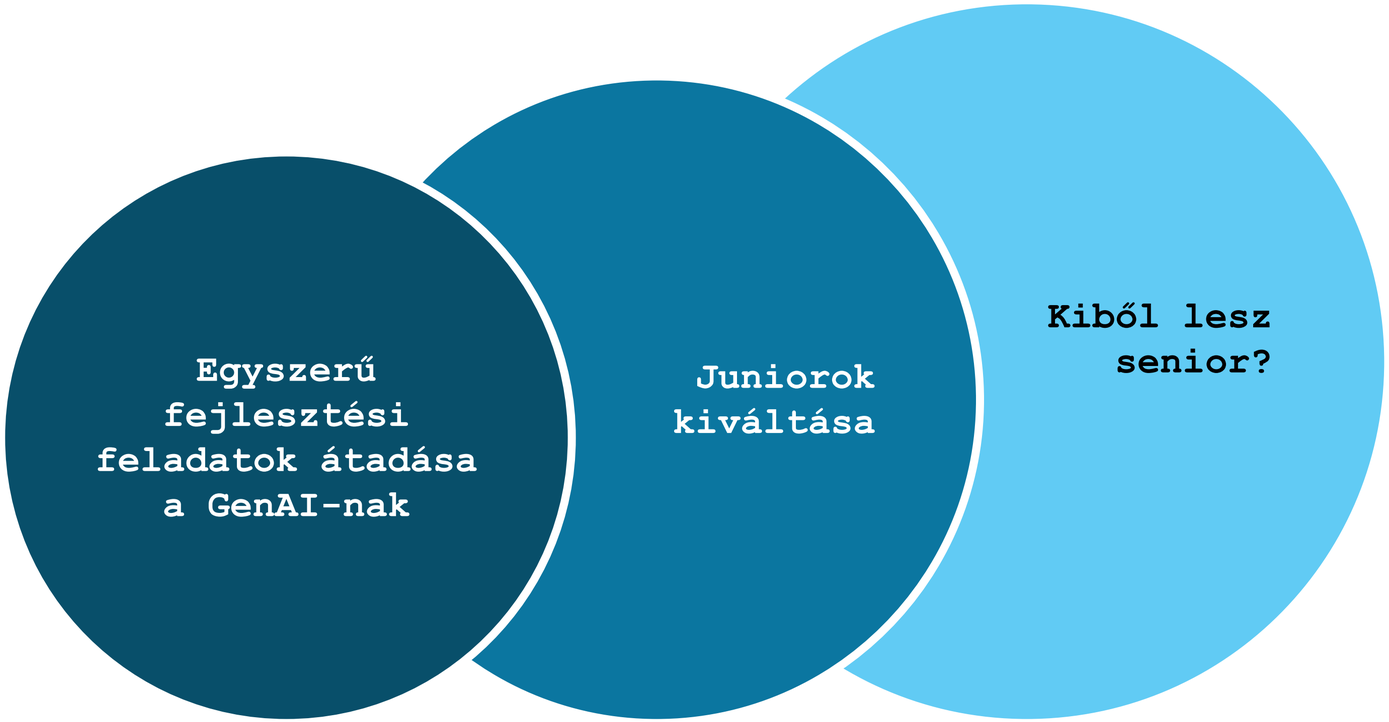
The number of active users of Microsoft 365 Copilot Chat for the selected period. See metric definitions



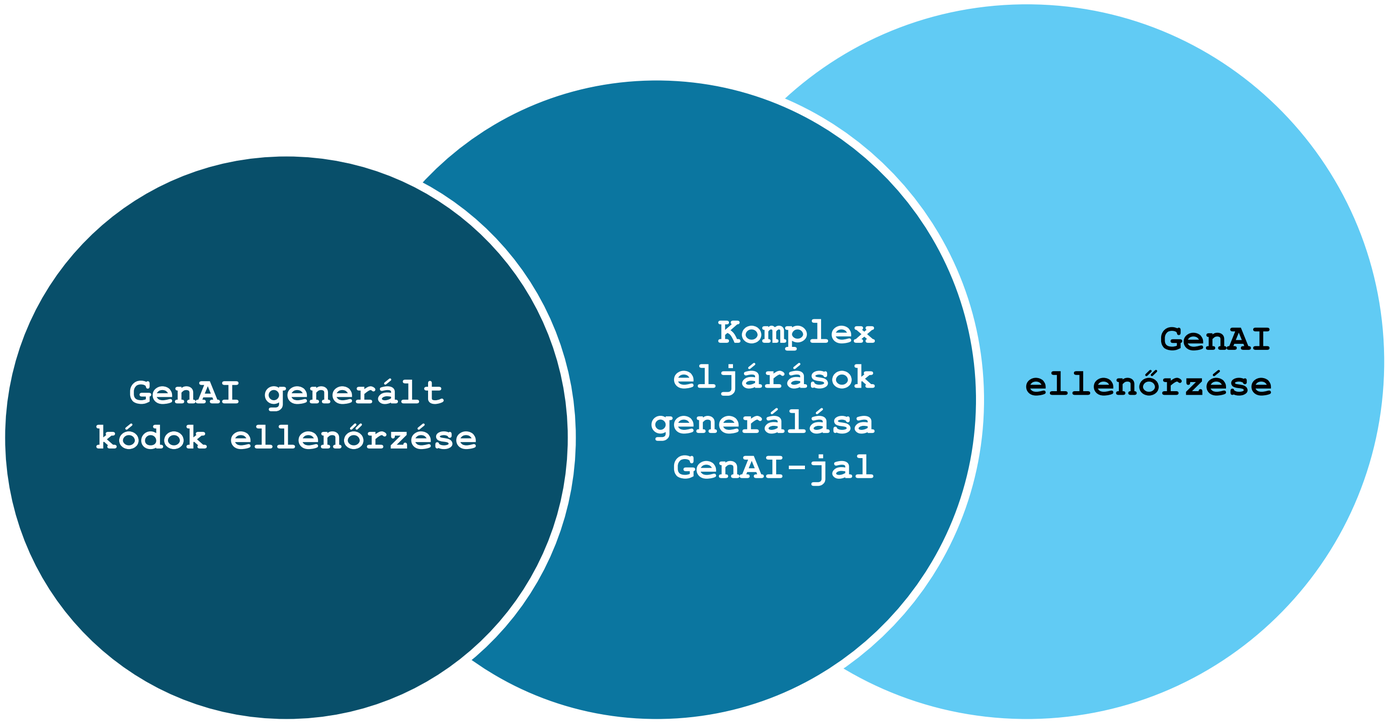
AI community of practice – Teams csatorna



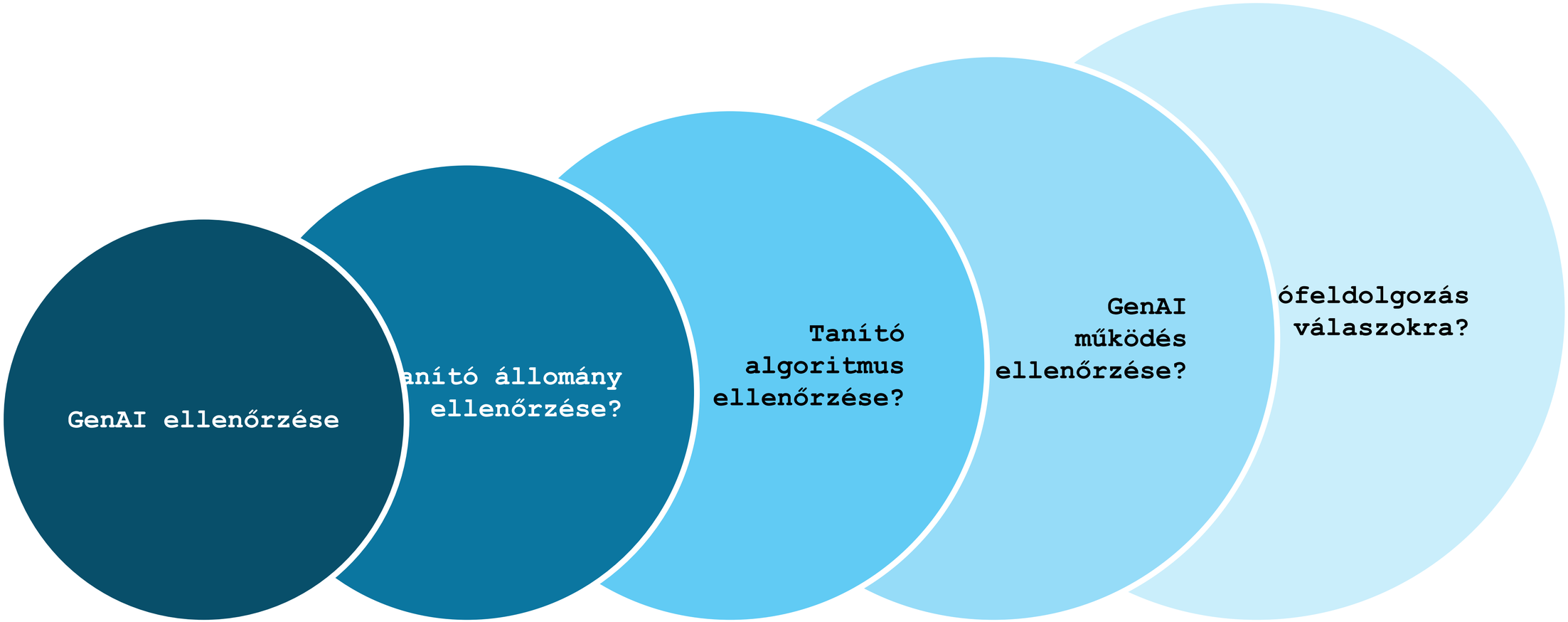
GenAI alkalmazásának kérdései



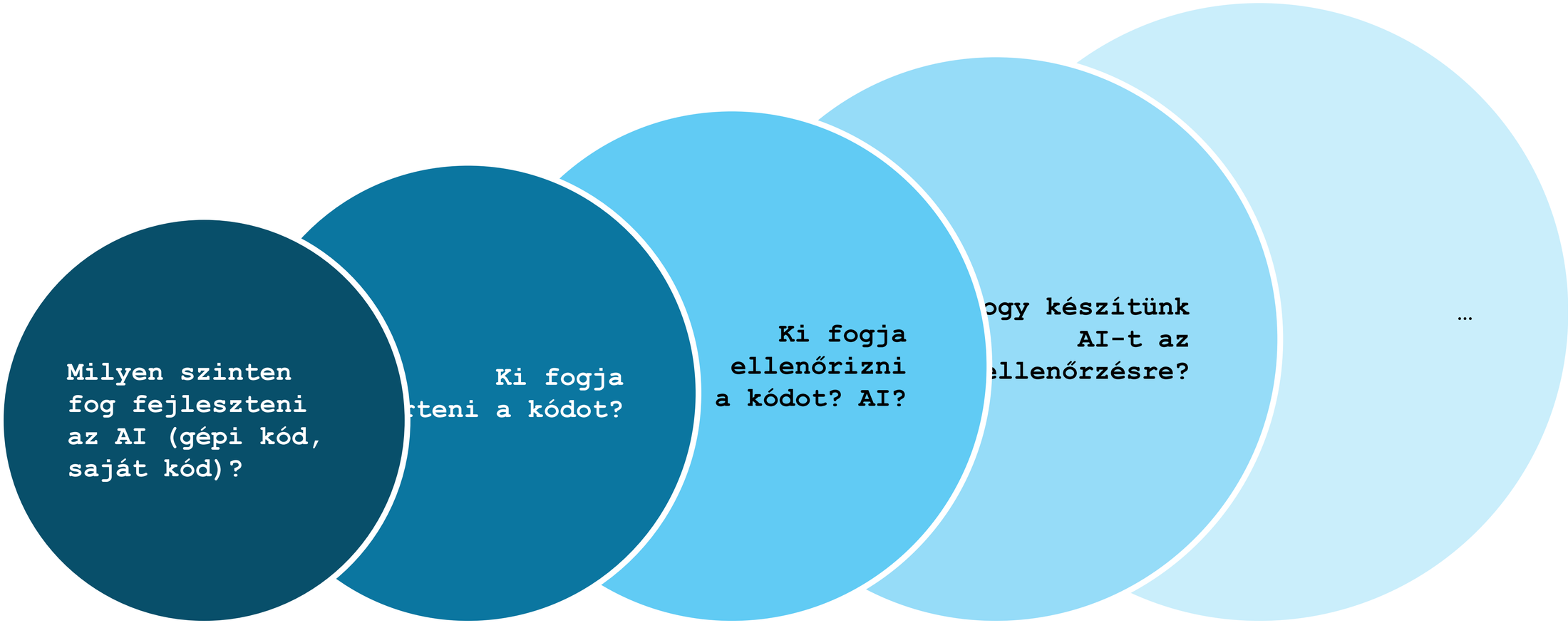
GenAI alkalmazásának kérdései



GenAI alkalmazásának kérdései



GenAI alkalmazásának kérdései



Köszönöm a figyelmet!

Ott Károly
IdomSoft Zrt.