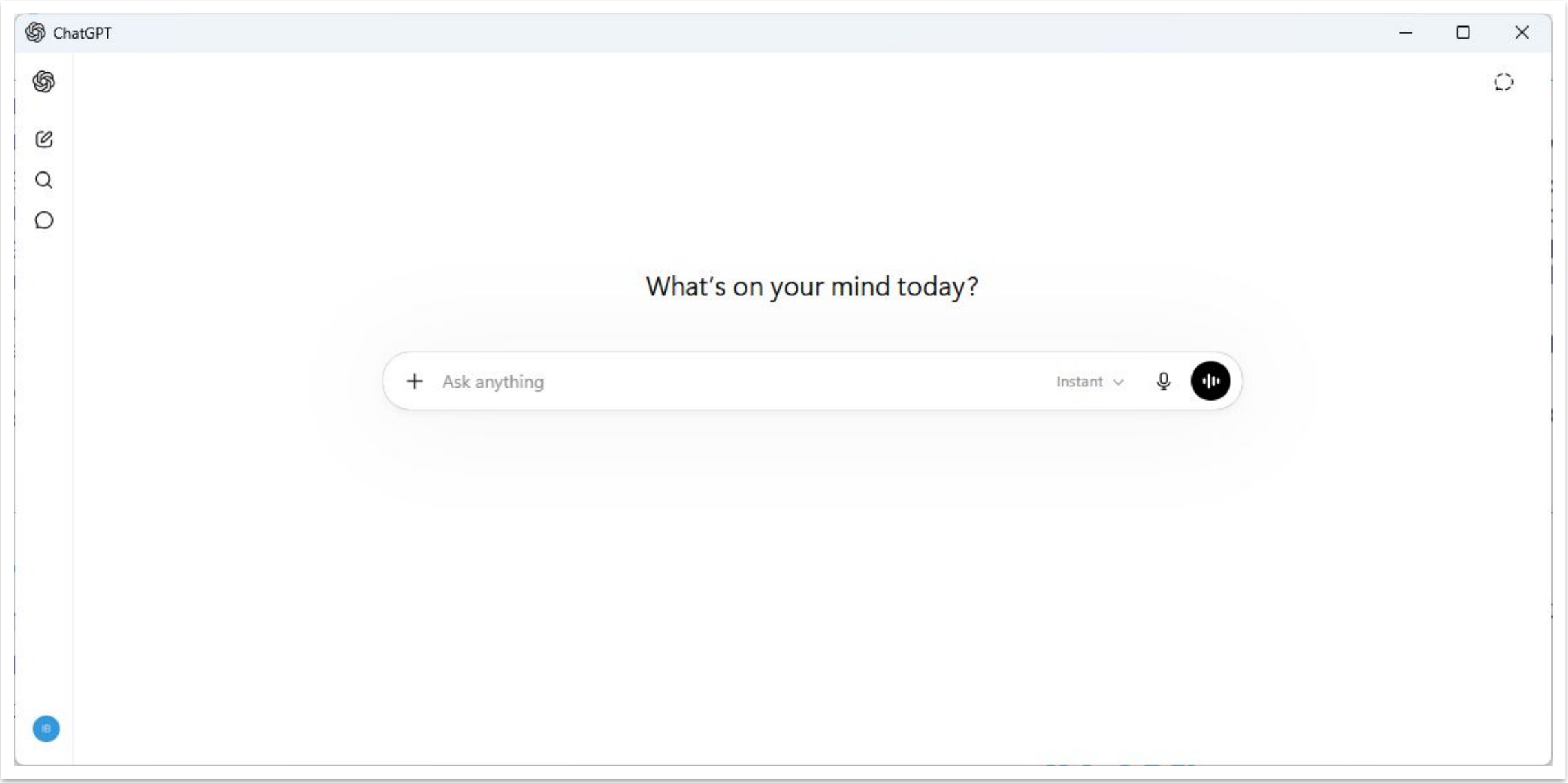
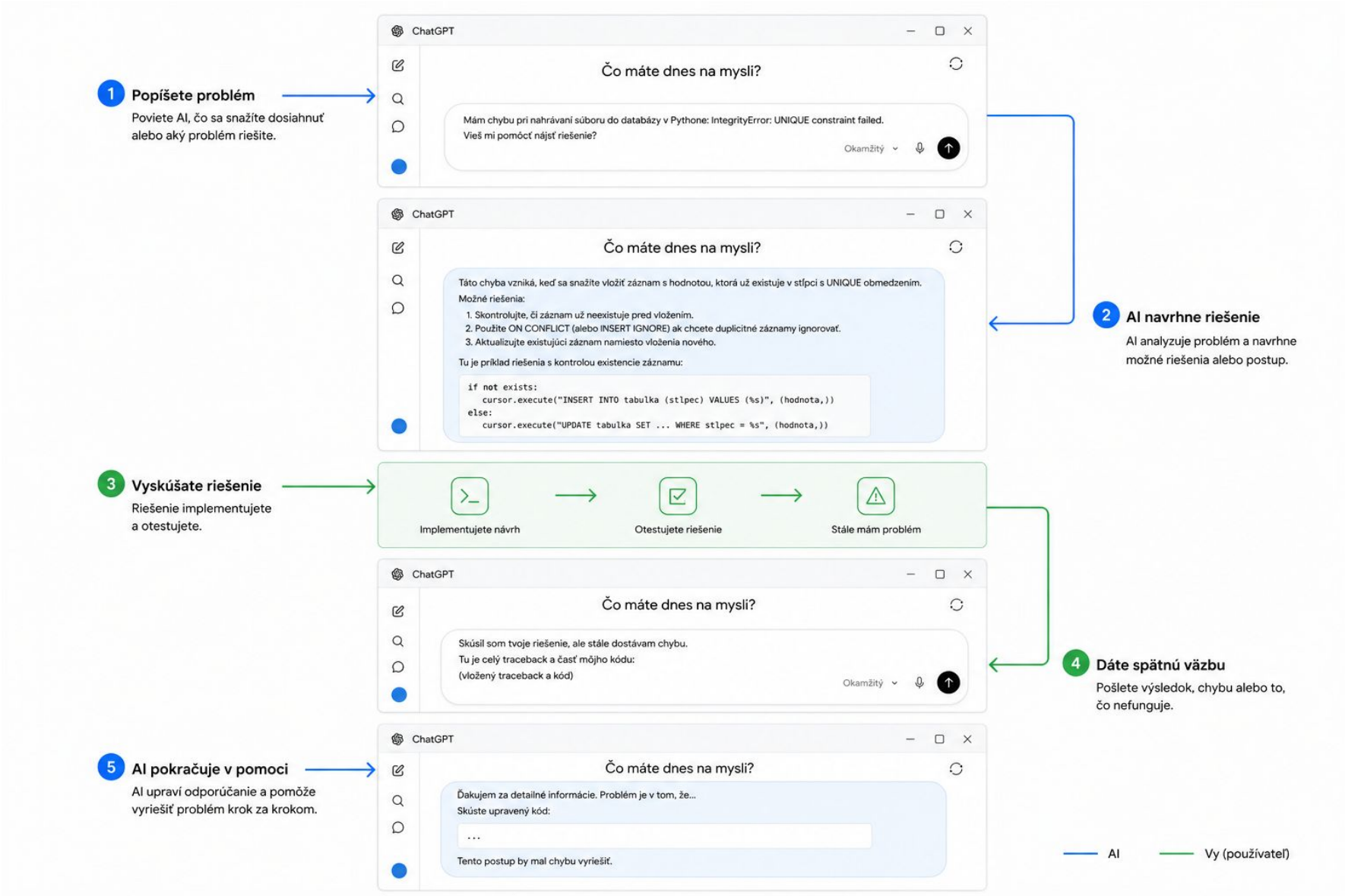
Agentic AI

Od asistenta k autonómnym systémom

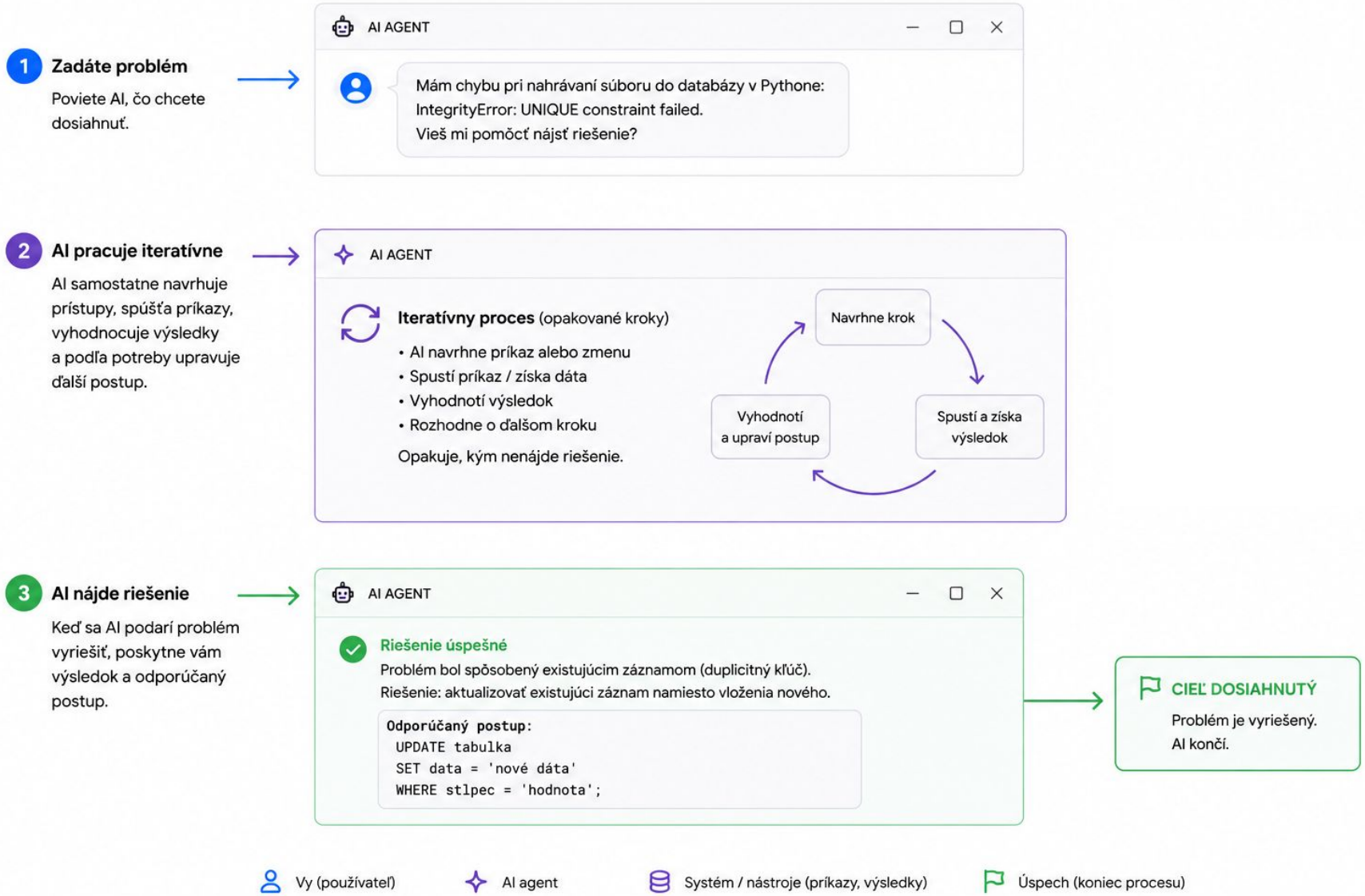
AI asistent - používame a poznáme už dlhší čas



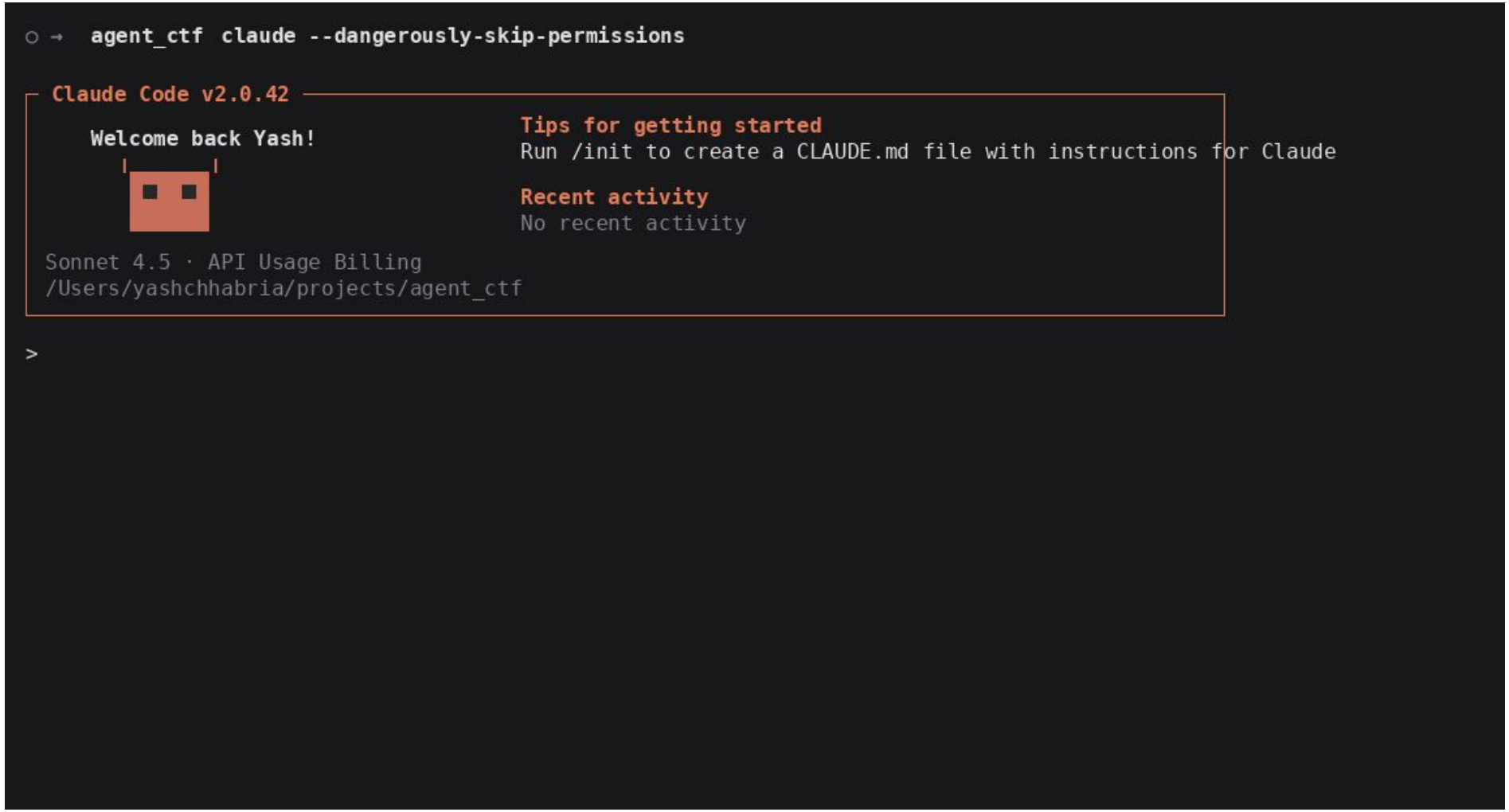
Konverzačná AI nám poradí a poradí aj keď výsledok nefunguje



Agentická AI si svoje odporúčanie vykoná a overí sama

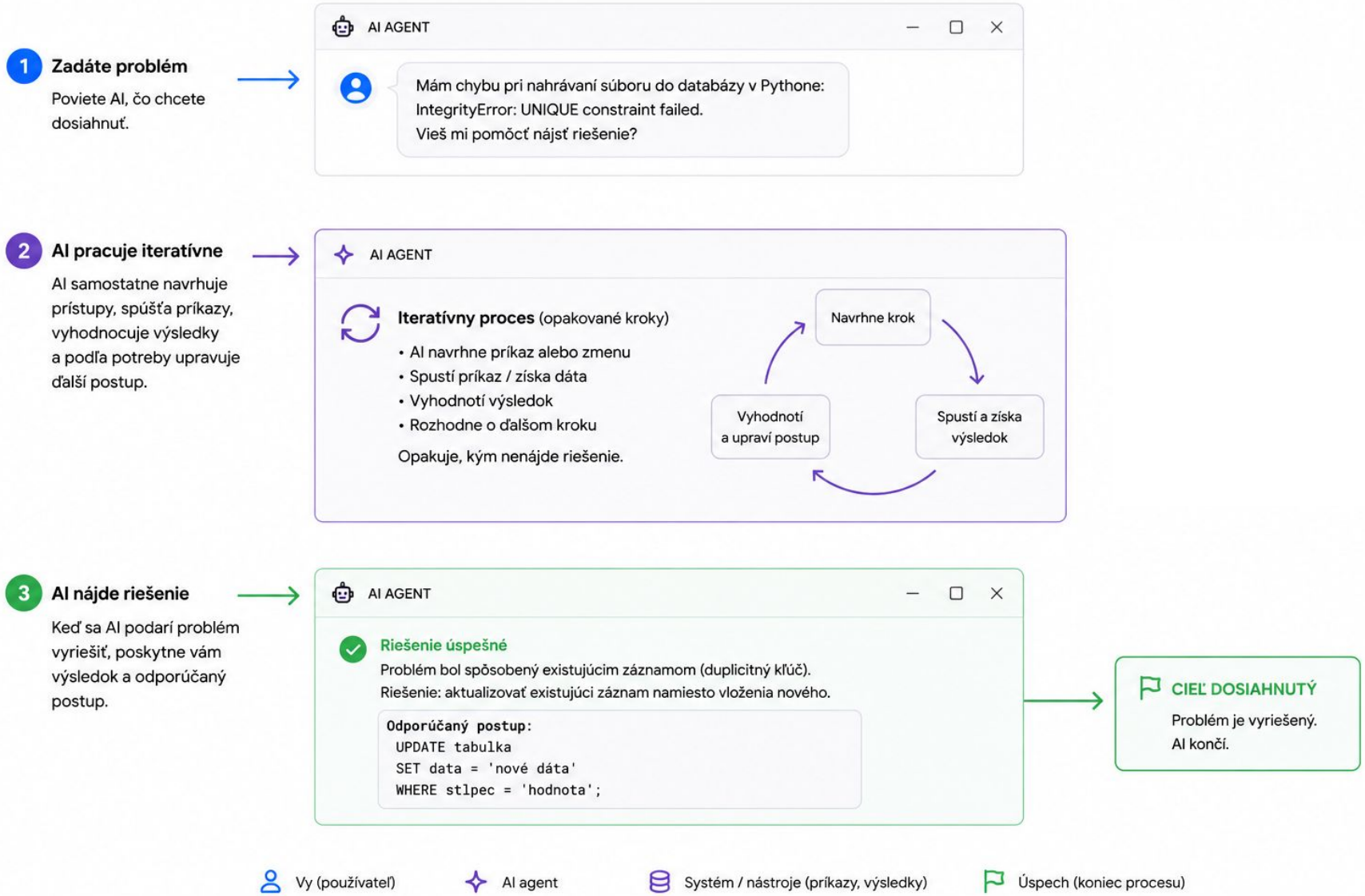


Autonómna činnosť agentickej AI

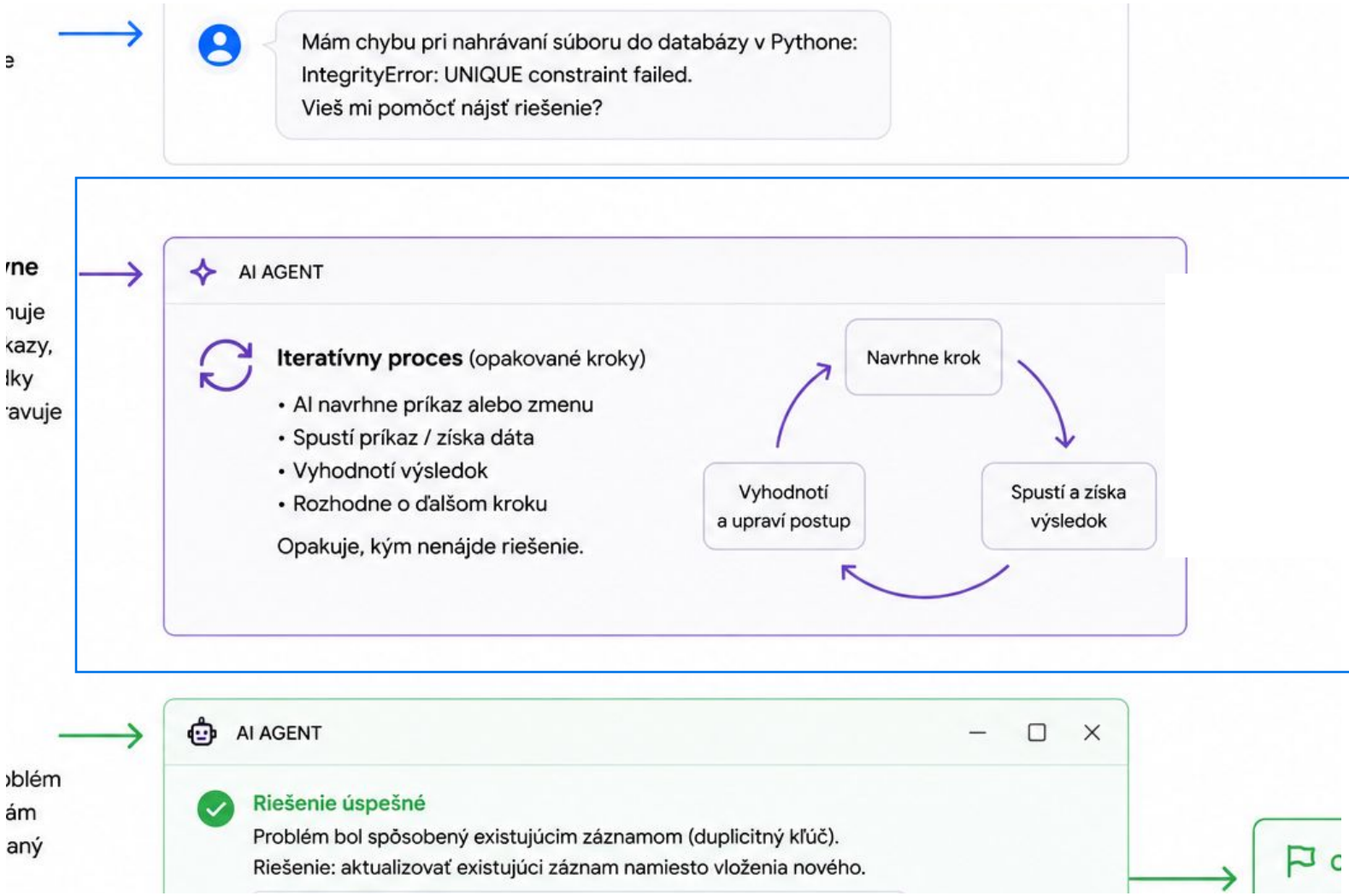


Programovanie je ideálna úloha pre agentickú AI

Agentická AI si svoje odporúčanie vykoná a overí sama



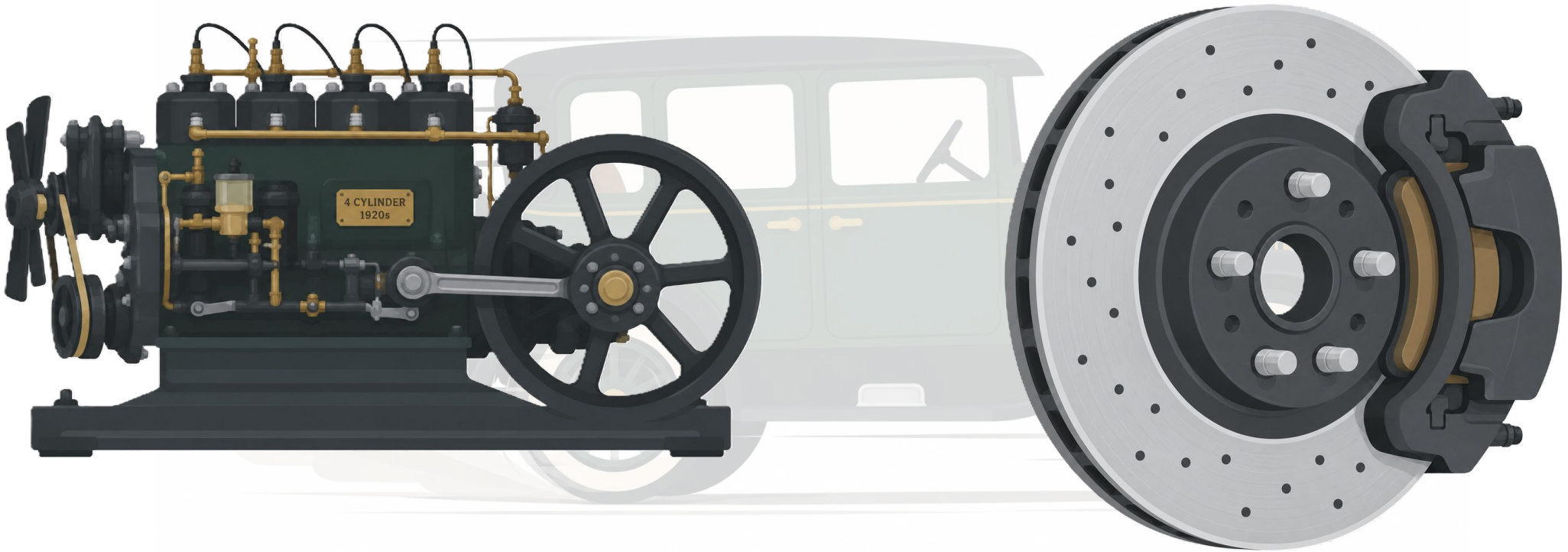
Agentická AI si svoje odporúčanie vykoná a overí sama



- Čo môže spustiť?
- Kde to môže spustiť?
- S aku rolou?
- S akým právami?
- K čomu má prístup?
- Ako auditovať?
- Ako zabrániť omylu?
- **Spustí sa vôbec?**

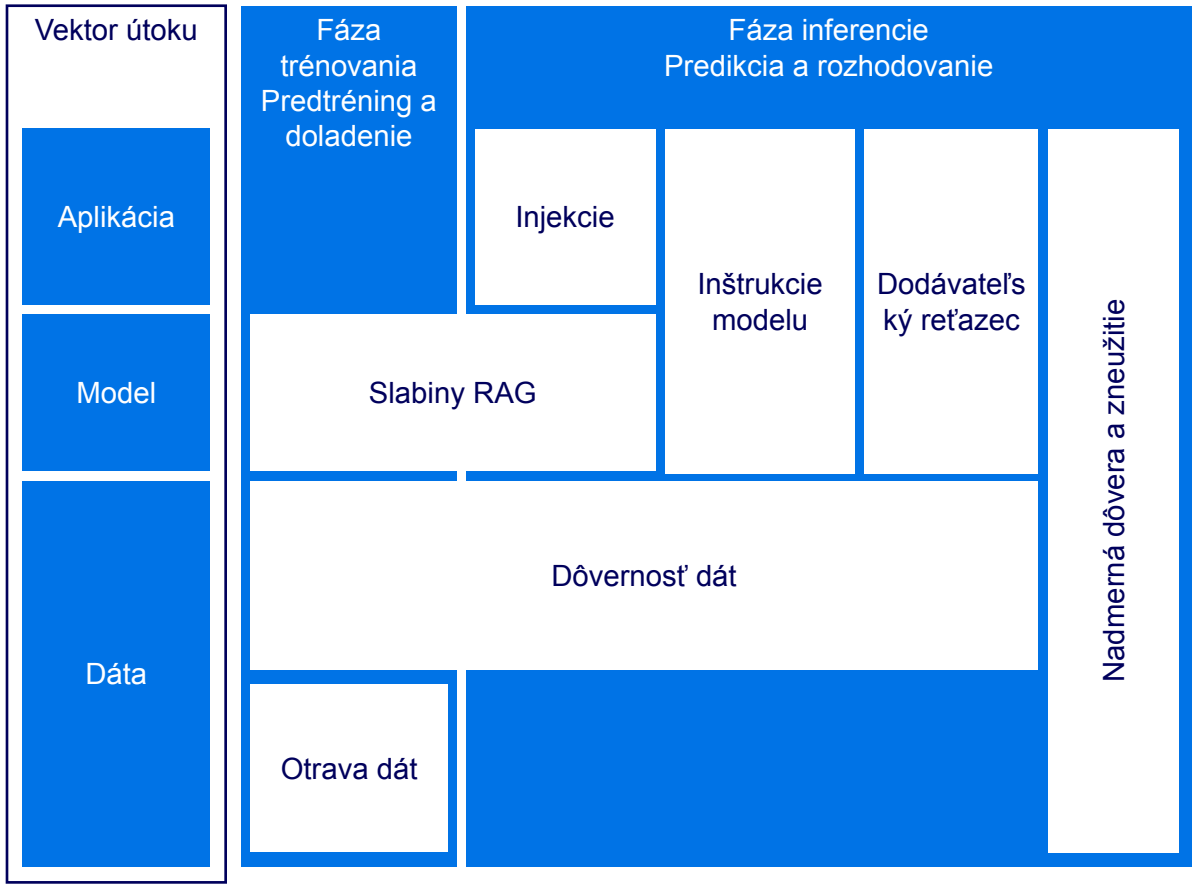
Kedy začali jazdiť auta rýchlejšie?

Kedy začali jazdiť auta rýchlejšie?



Agentická AI prináša hlbšie, širšie a komplexnejšie bezpečnostné riziká

GenAI prináša významné bezpečnostné riziká



Agentná AI prehlbuje tieto riziká rozšírením expozície

Zneužitie autonómnych akcií: manipulácia promptov môže spustiť nezamýšľané alebo škodlivé API a systémové akcie

Rozšírené riziká oprávnení a prístupu: agenti môžu volať nástroje či reťaziť funkcie mimo zamýšľaných hraníc autorizácie

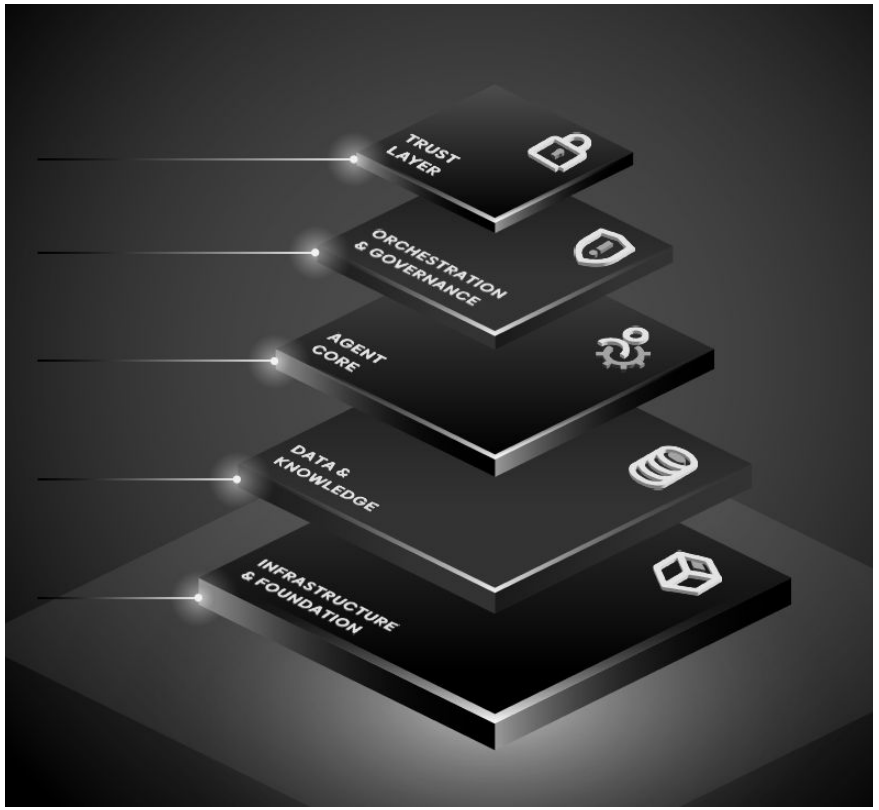
Trvalá pamäť a posun cieľa: otrávený kontext alebo zmanipulované ciele môžu ovplyvniť budúce autonómne rozhodnutia

Obmedzená vysvetliteľnosť a kontrola: autonómne uvažovanie a reťazce akcií znižujú viditeľnosť, auditovateľnosť a izoláciu

Firemná pripravenosť a zodpovedná AI: adopcia/kontroly zamestnancov, etika, správa dát a redizajn AI procesov akcelerátory

Atos Sovereign Agentic Studio

Bezepečnosť a suverenita



Atos Agentic Studion - Agilný prístup k návrhu end-to-end agentových workflowov

Atos Accelerators

- Kritériá výberu agentovej AI
- Rámec priorizácie use case
- Posúdenie pripravenosti dát pre AI
- Digital Data Engineer
- Frictionless Operations Digital Engineer
- Knowledge Pilot

1 Vyber pilot

- Pochop ambície klienta, urči smer
- Vyber jeden účinný a realizovateľný quick-win
- Dohodni, ako vyzerá úspech

2 Premysli workflow

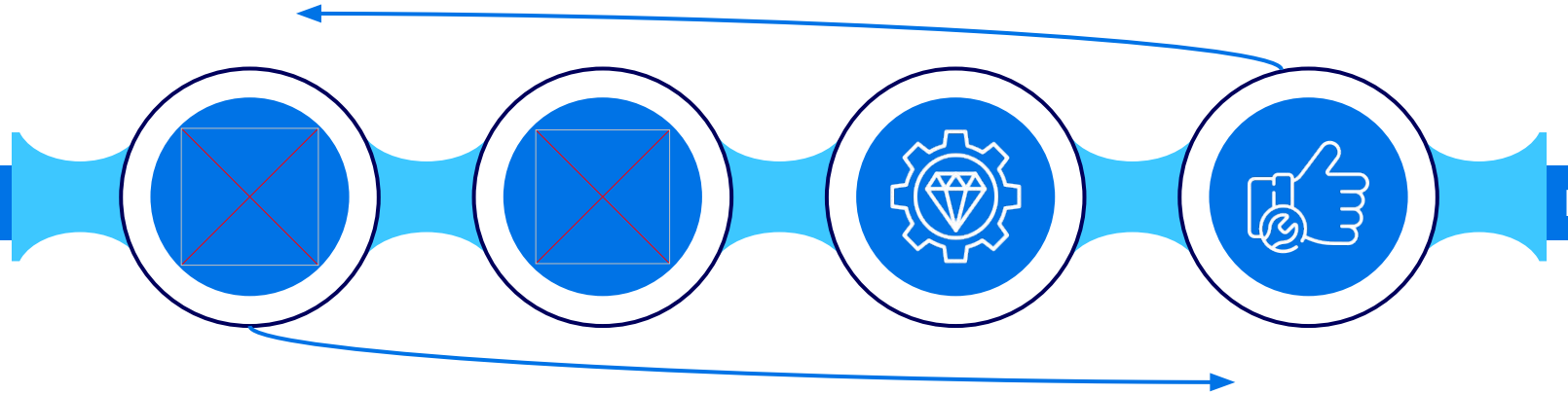
- Posuň sa od „Kde použiť AI?“ k „Čo dosiahneme, ak agenti zvládnu 60 % workflowu?“
- Urči dáta potrebné pre PoV

3 Plánuj a navrhni

- Definuj model Agentic Studio
- Preveď use case na akčný plán a biznis/technickú architektúru

4 Buduj, testuj a meraj

- Over pripravenosť vzorky dát a načítaj
- Postav agentové workflowy a otestuj
- Predveď PoV



Ďalšie kroky

- Návrh na spustenie vrátane posúdenia pripravenosti AI (dáta, integrácie, ľudia atď.)

Atos Scalers program - Široký partnerský ekosystém

Rozhodni, kde konať podľa dôkazov	Urči, ktoré úlohy delegovať	Spúšťaj a prevádzkuj proces s agentmi	Kontroluj náklady a výsledky	Zlepšuj priebežne podľa KPI
Posúdenie hodnoty procesu	Návrh digitálnych rol a zodpovedností	Agentové vykonávanie v reálnom prostredí	Sledovanie nákladov a hodnoty AI	Slučka učenia a optimalizácie
• Pochop, ako proces reálne beží • Identifikuj, kde agenti tvoria hodnotu • Postav business case na faktoch	• Vytvor digitálnych zamestnancov pre konkrétne roly • Definuj úlohy, právomoci, eskalačné pravidlá • Priprav enterprise integráciu	• Daj agentom konať v systémoch a prostrediach • Zahrň human-in-the-loop už v návrhu • Enterprise, regulované a pripravené na suverenitu	• Sleduj cost-to-serve na agenta a workflow • Prepoj vykonávanie s biznis KPI • Umožni informované rozhodnutia o škálovaní	• Monitoruj výkon a odchýlky • Optimalizuj procesy a agentov v čase • Udržuj tvorbu hodnoty
KYP AI	Ema	poolside	Pay-i	KLARITY
Využi task-mining na redefinovanie procesu pre agentifikáciu	Demokratizuj Quick-to-Value agentových AI zamestnancov	Daj plnú kontrolu a vlastníctvo Sovereign LLM modelov	Riaď AI scenáre k najlepšej biznis hodnote s AI FinOps	Posúvaj trvalú a kontinuálnu zmenu s poradenskými AI agentmi

Atos Polaris AI Platform
Agentic AI Foundational Layer

Atos' Scaler Program neustále skúma a hodnotí nových partnerov

Atos

Ďakujem

igor.banduric@atos.ai