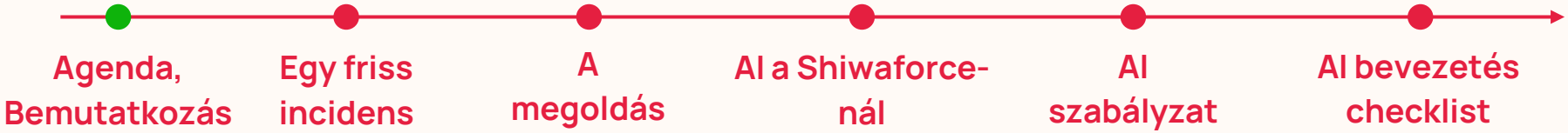
shiwaforce

Biztonságos AI használat szoftverfejlesztői nézőpontból


Agenda,
Bemutatkozás
Egy friss
incidens
A
megoldás
AI a Shiwaforce-
nál
AI
szabályzat
AI bevezetés
checklist

shiwaforce

Bemutatkozás

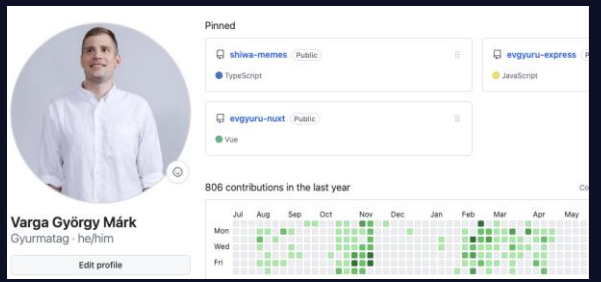
Varga György Márk

Product Developer

gyorgymarkvarga.me

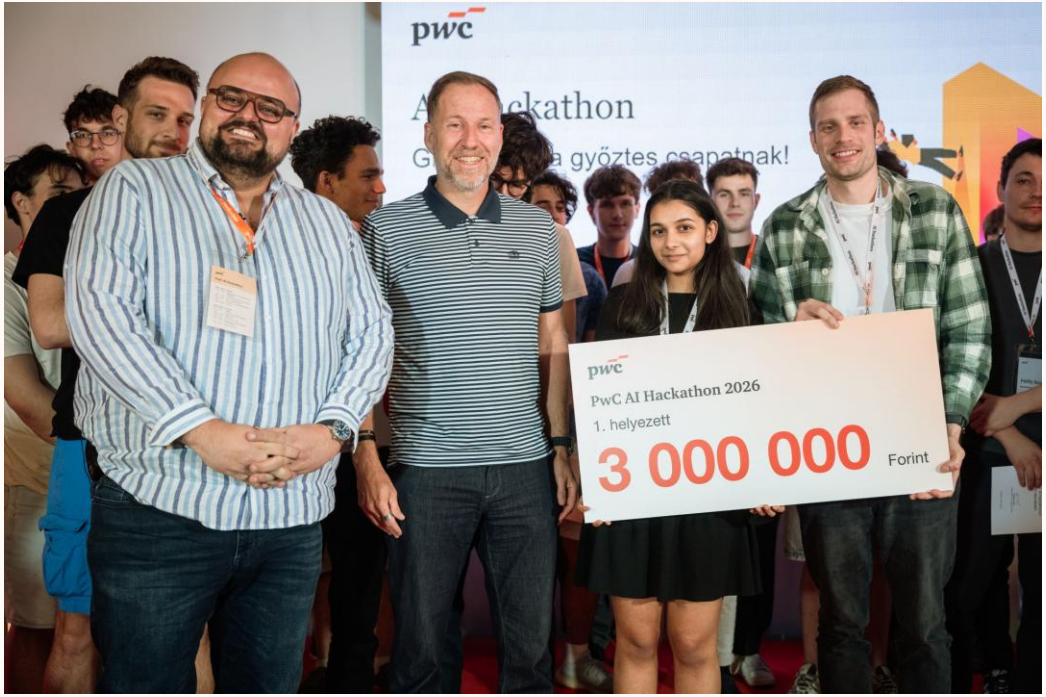
@Gyurmatag

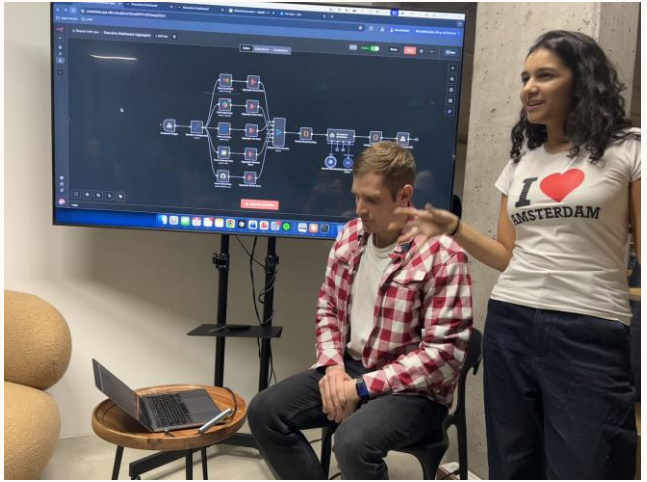
@Gyurmatag

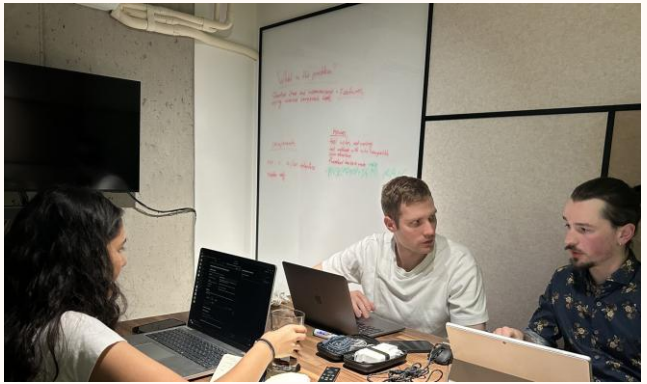



TEDx
Danubia


Cloudflare


pwc
PwC AI Hackathon 2026
1. helyezett
3 000 000
Forint


I
AMSTERDAM

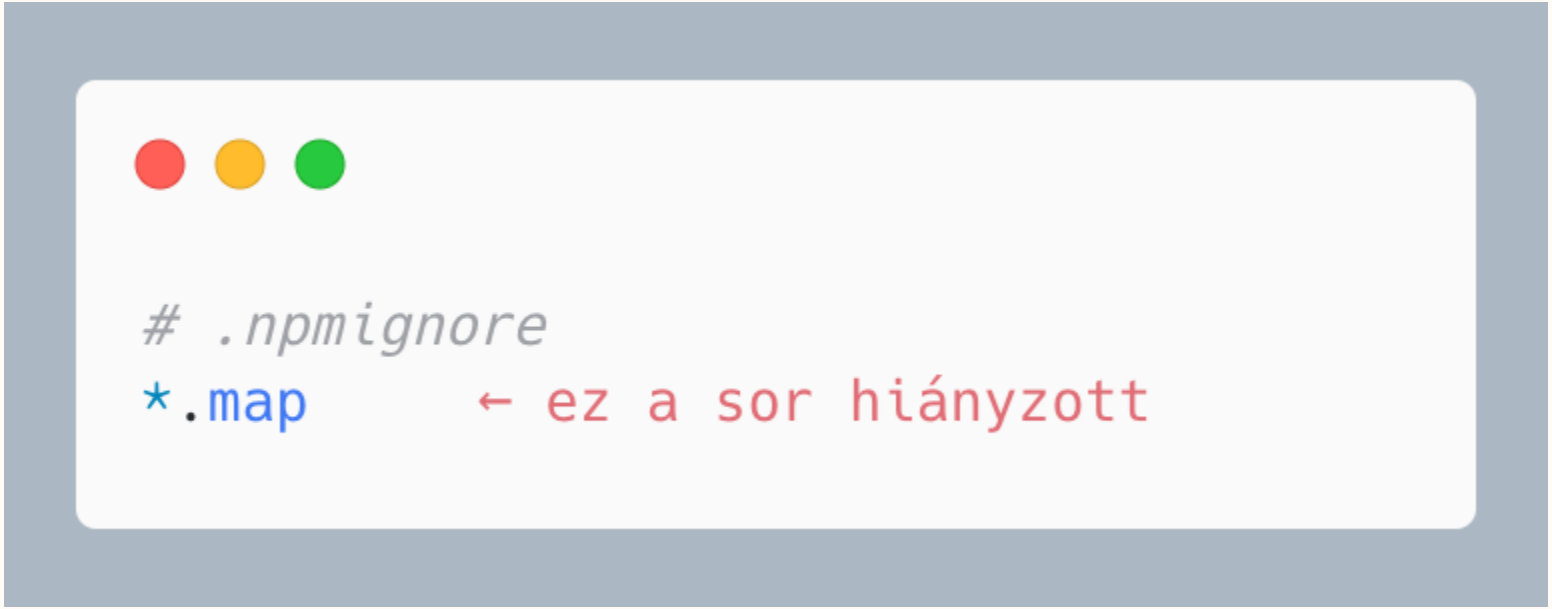



How we onboarded engineers on Cursor in a highly regulated sector?

shiwaforce

Egy friss incidens

2026. március 31. — egy hiányzó sor



A 72 óra

Két független supply chain esemény egy éjjel

T + 0h

Source code leak

512 ezer sor TypeScript az npm-en, egy hiányzó .npmignore sor miatt

T + 3h

Független axios támadás

Külön szereplő (DPRK, Microsoft). RAT-tal fertőzött axios csomag — heti 83M letöltés. 3 órás ablak.

T + 24h

Hamis GitHub repók

„Leaked Claude Code" repók a Google találatok között, malware-rel

T + 72h

Typosquat csomagok

Hamis npm csomagok - a build-folyamatokat várják

Ha ez egy banki fejlesztői környezet lenne...

Tudnánk-e róla?

Tudnánk pontosan, melyik fejlesztő, melyik gépen, mikor frissített Claude Code-ot npm-en keresztül?

Mennyi idő alatt?

3 órás támadási ablakban malware került a fejlesztői gépekre. Mennyi idő alatt érne be a riasztás a SOC-hoz?

Mit jelentenénk?

Az MNB 13/2025 AI Ajánlása szerint bejelentésköteles? NKI felé 24 órán belül kötelező?

Ezekre nincs rossz válasz — csak felkészült és felkészületlen szervezet.

shiwaforce

Megoldás

Tudnánk-e róla?

Eszköz-leltár

Élő nyilvántartás: melyik AI eszköz, melyik verzió, melyik telepítési mód. Ha valahol incidens van, tudjuk, érint-e minket.

Központi hozzáférés

Vállalati SSO, nincs személyes account. Ki, mikor, milyen tool-t használ - egy helyen látható.

Audit

Minden AI-művelet naplózva. Egy auditor előtt 5 percen belül elő tudjuk venni, ki mit csinált.

Mennyi idő alatt?

Vendor monitoring

Nem akkor értesülünk egy AI tool sebezhetőségéről, amikor a Hacker News-on felmegy. Push értesítés a gyártóktól, automatikus alert a CVE-kre.

Verziókontroll

Nem auto-update vakon. Minden új verzió release notes review után megy élesbe.

AI-incidens forgatókönyv

Külön playbook, nem általános IT incident response. Eszkalációs lánc dev-től CISO-ig.

Mit jelentenénk?

Vendor risk - minden AI eszközre

Mielőtt egy tool bekerül a céges használatba: tanúsítványok (SOC 2, ISO), adatkezelés, EU adatszuverenitás, tanítási opt-out. Évente felülvizsgálva.

Adatkezelés

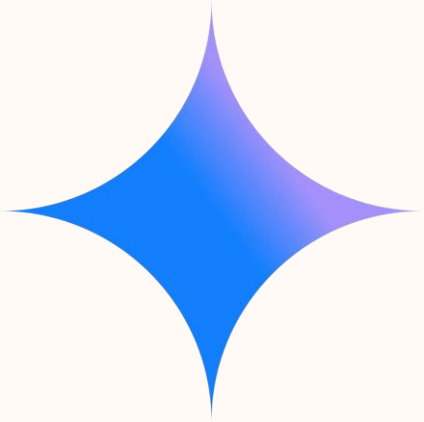
Mit lehet „AI-ba küldeni”, mit nem.

Dokumentáció és transzparencia

Auditálható nyomvonal: ki, melyik vendor, melyik modell, milyen adatkezeléssel. Incidens esetén ügyfél felé előre megírt eszkalációs út.

AI a Shiwaforce-nál

Eszközök



Gemini

Cursor

Claude

Dashboard

Complete AI activity history

View Leaderboard →

Team Overview

Total Activity Score

6,314,863

Combined team score

Accepted Lines (All AI)

3,097,101

Lines accepted across Tab, Composer & Agent

Total Requests

37,081

Chat: 1,123 | Composer: 594 | Agent: 35,364

Tab Accepts

9,418

Inline completions accepted

Top Performer

György Márk Varga

Score: 3,572,480

Active Users

46

Team members with activity

Chat Requests

1,123

AI chat interactions

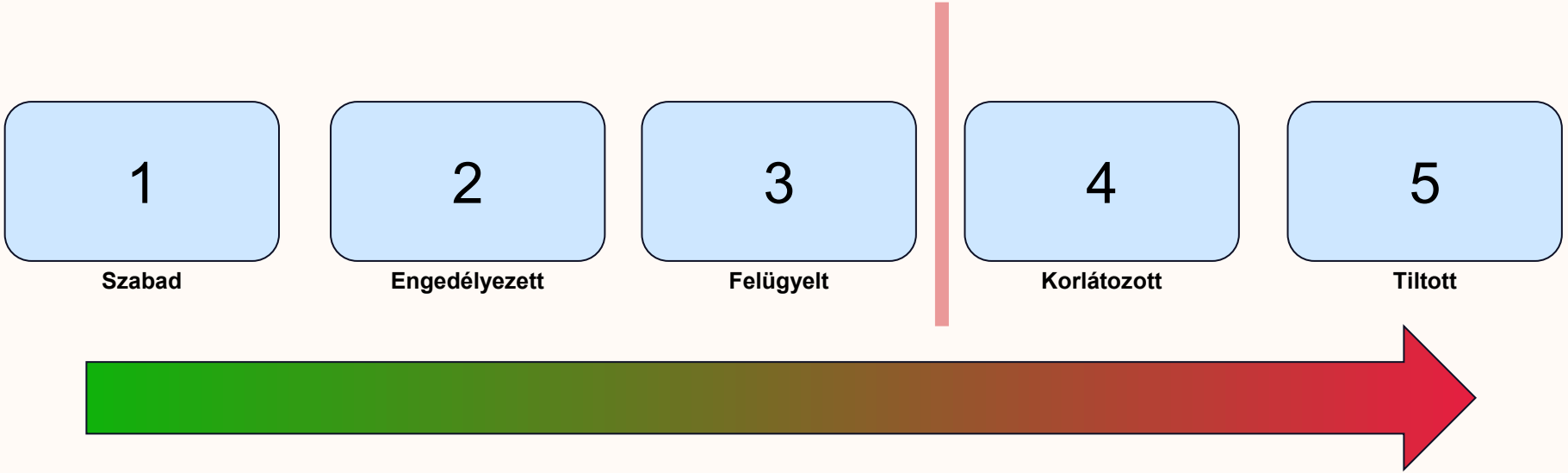
Agent Requests

35,364

Autonomous task requests

Shiwaforce AI szabályzat

AI Szabályzat



shiwaforce

AI Bevezetés Checklist

AI Bevezetés Checklist

1. **Stratégia és felelősségi körök**
   Ki jóváhagy, ki üzemeltet, ki auditál. Keret, nem eszközlista.

2. **Vendor due diligence**
   Tanúsítványok, EU adatszuverenitás, audit log képesség. Évi felülvizsgálat.

3. **Központi hozzáférés**
   SSO, RBAC, audit nyomvonal. Egy helyen látszik, ki mit használ.

4. **Adatosztályozás**
   Mi "mehet AI"-ba, mi nem. Ügyféladatra szigorú szabály, banki kontextusban szegregált környezet.

5. **Verzió- és telepítés-kontroll**
   Pinned, jóváhagyott verziók. Native installer preferencia, release notes review után.

6. **AI-incidens playbook**
   Külön az általános IT incident response-tól. Eszkalációs lánc előre megírva, évi tabletop.

7. **Folyamatos képzés és felülvizsgálat**
   Fejlesztők AI-jártassága mérve. A szabályzat élő dokumentum, nem egyszeri compliance.

8. **Naprakészség és visszacsatolás**
   Új AI-eszközök és kockázatok rendszeres áttekintése; tapasztalatok megosztása csapatok között.

shiwaforce

Köszönöm a figyelmet!

György Márk Varga
Product Developer

+36 (30) 647 2771
gyorgy.varga@shiwaforce.com