AI SOC konzultant

rychleji, kvalitněji, levněji

Tomáš Hlavsa

12. 5. 2025

Atos EVIDEN

SIEM…..jasně, každý ho má…..no jo …..ALE

- Dnešní SIEM - SOC koncepty spoléhají převážně na **ruční analýzu** detekovaných incidentů
- Což je **časově náročný** a na lidskou chybu náchylný přístup
- Skutečnou výzvou je **prioritizace incidentů** se zaměřením na false positives.
- **Reálné hrozby** mohou být přehlédnuty, nebo jejich analýza zpožděna díky této neefektivitě
- Přičemž díky lidskému faktoru zůstává nevyužita **existující Knowledge base** historických incident či postupů, které již vůči danému incident již byly uplatněny

Když do toho vstoupí AI

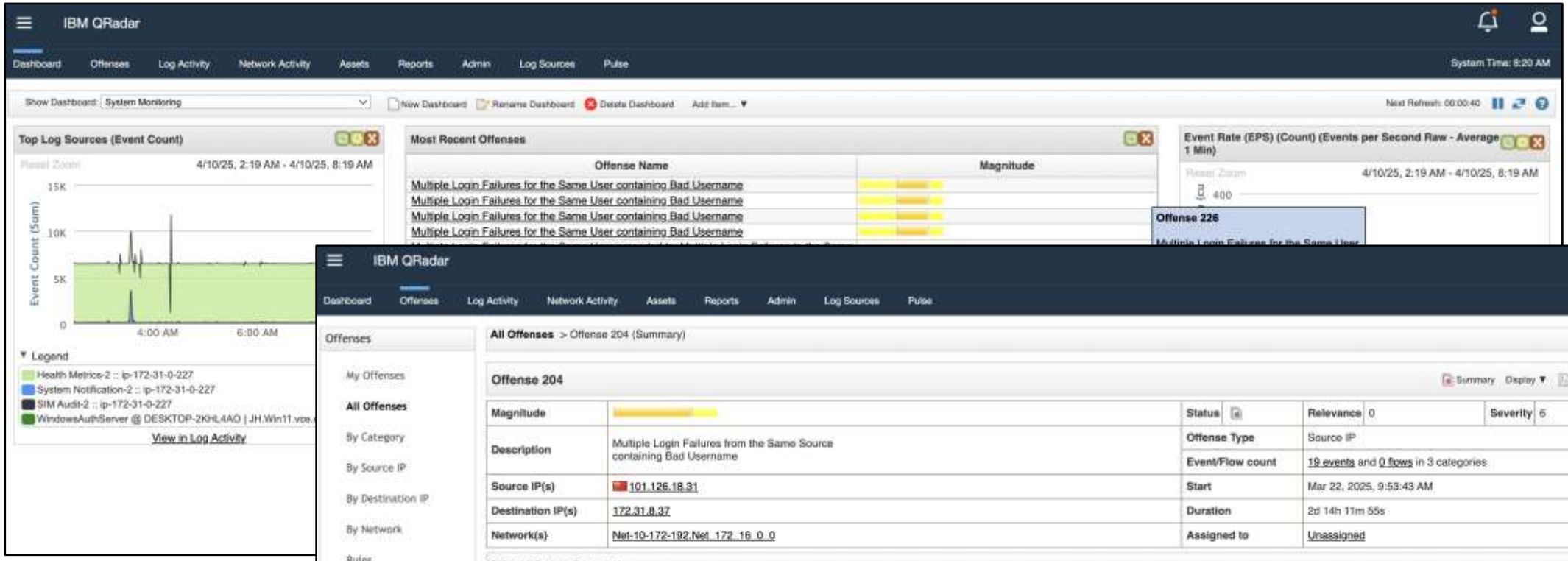
AI SOC Consultant:

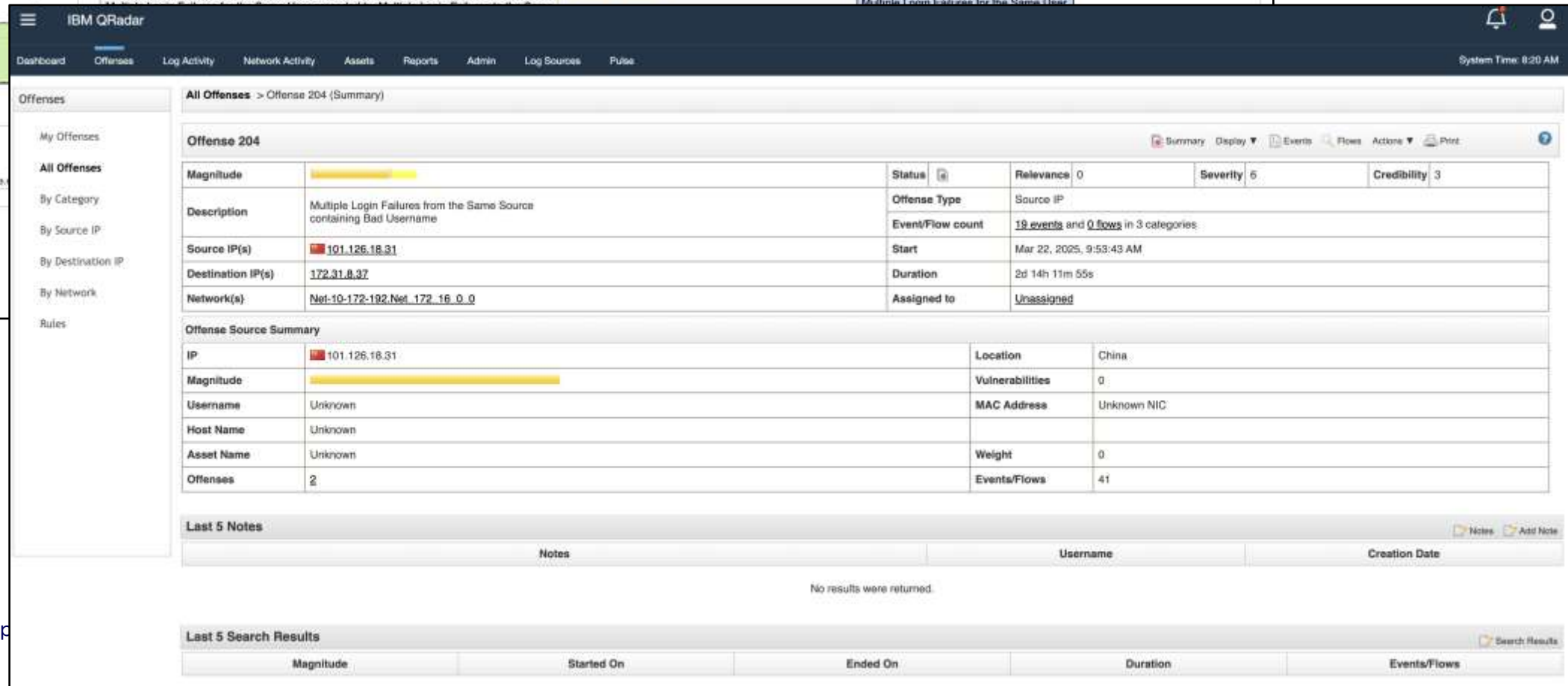
- Vyvinut v Atos/Eviden ČR
- Běží lokálně s využitím **cloud-based** LLM modelů.
- Napojení na SIEM API kdy **extrahuje offenses**.
- Obsahuje **kontrolní mechanismy** předcházející výstupům “mimo context”….. Aby si AI nevymýšlelo ☺

AI workflow (AI Pipeline):

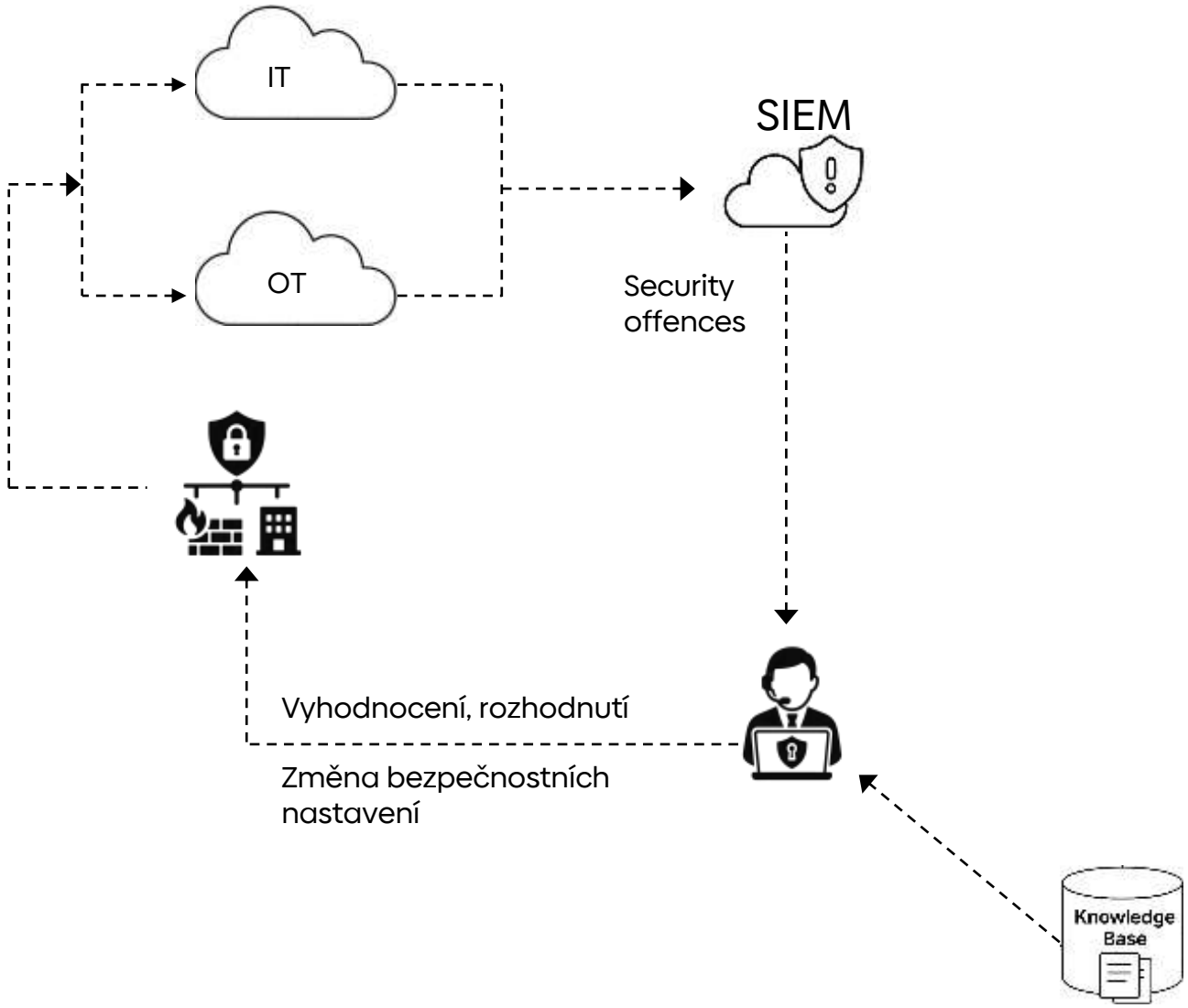
- Framework automatizující workflow s použitím AI
- Umožňuje spouštění vícečetných AI demonů s různými sadami API připojení a různých knowledge base
- Používá přístup “**agentic AI”**

Standardní přístup





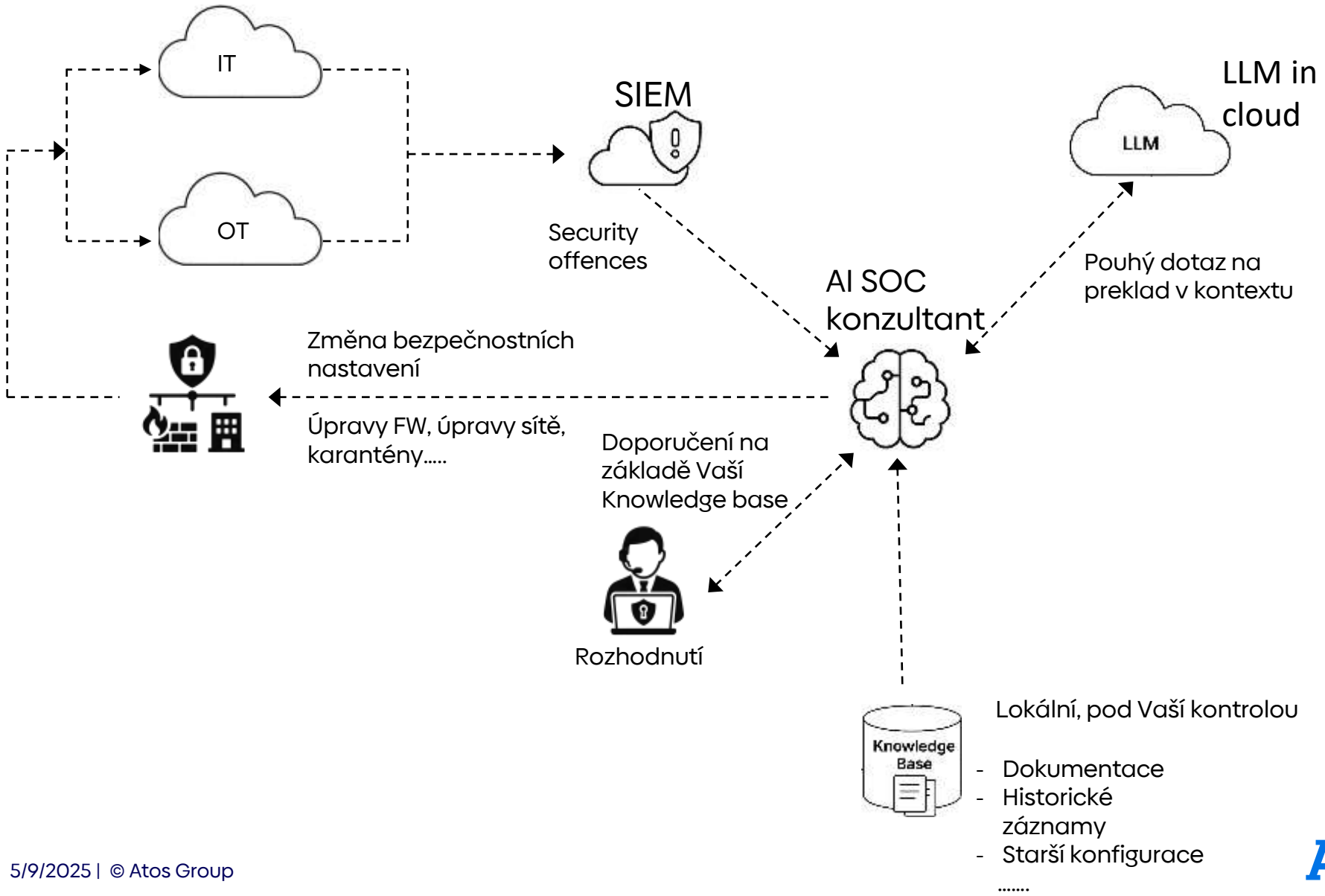
Jak AI SOC konsultant reálně pomáhá



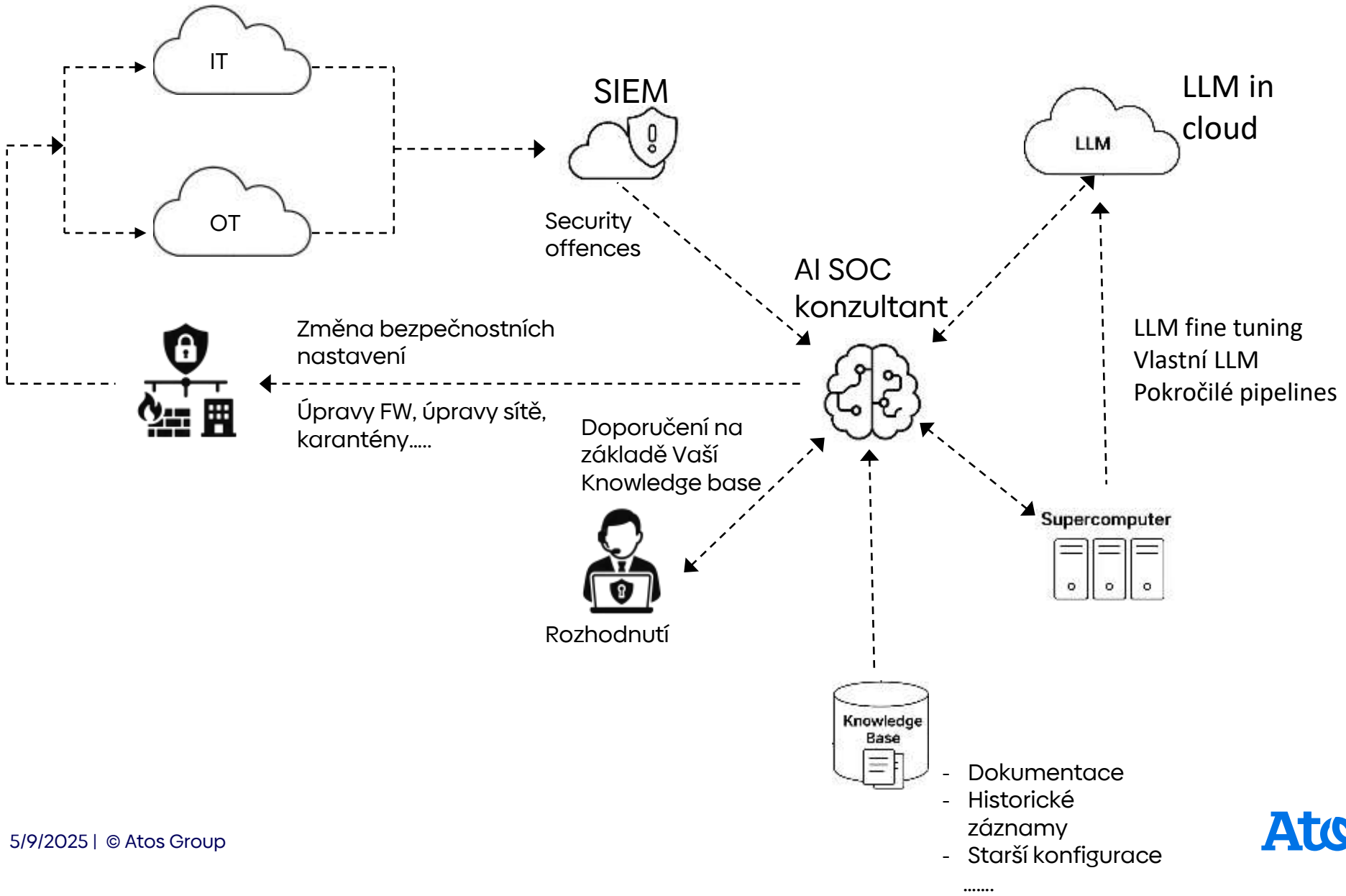
- Dokumentace
- Historické záznamy
- Starší konfigurace

.....

Jak AI SOC konsultant reálně pomáhá



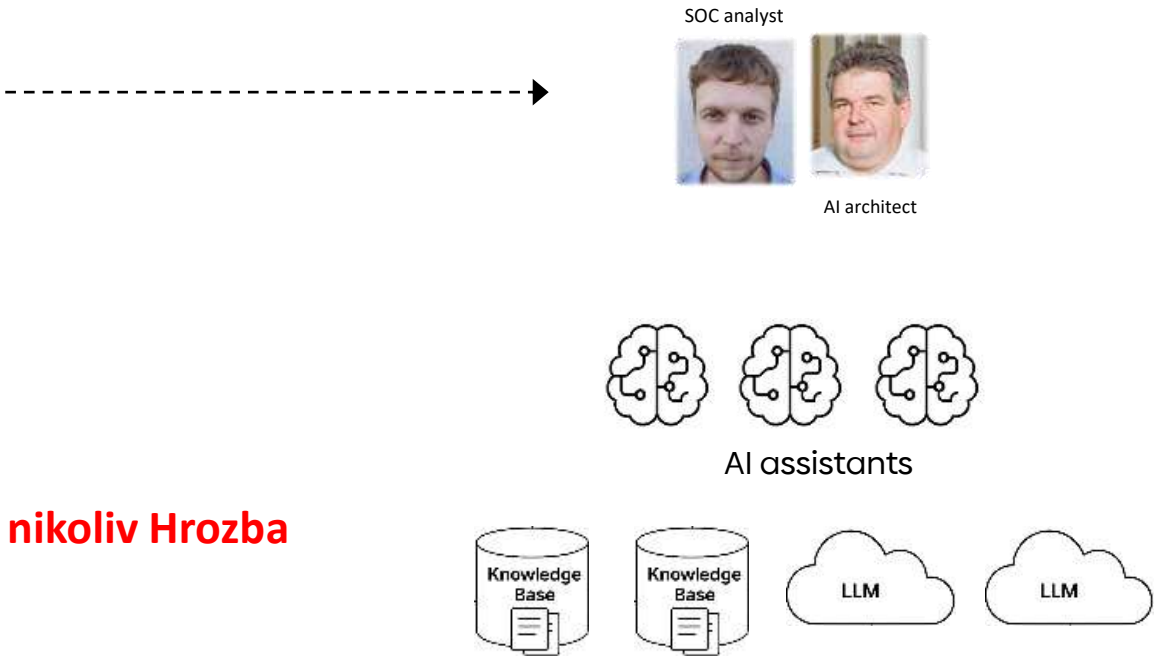
A když přidáte vysoký výpočetní výkon?



Využití expertů se mění

Dnešní SOC jsou proškolení, motivovaní lidé se zájmem o bezpečnostní problematiku

Budoucí SOC bude vyžadovat znalost a odpovědnost pro rozhodování + expertizu k ladění AI / LLM / RAG



Změna -> Výzva -> nikoliv Hrozba

Dopady použití AI pro podporu rozhodování

Preference využití lokální knowledge base (aby si AI nevymýšlelo)

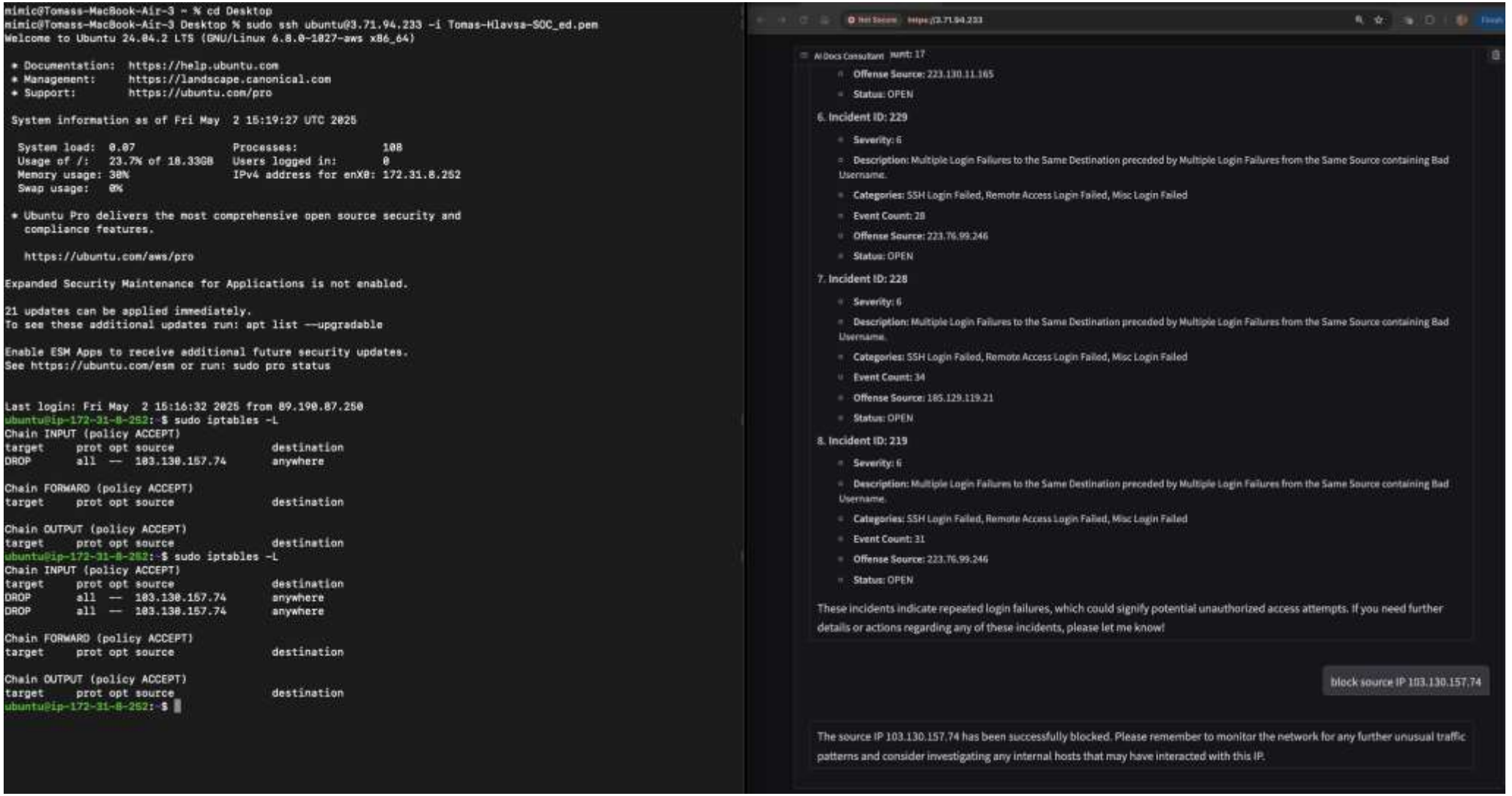
Automatizace bezpečnostních zásahů (rychlost, nevznikají zpoždění)

Kontinuita činností, analytici si nemusejí složitě předávat případy

Rozvoj AI je motivací pro zaměstnance, kteří chtějí věci zlepšovat

AI doplňuje chybějící experty

LIVE DEMO



Otázky?

+420 604 290 196
tomas.hlavsa@eviden.com

Atos EVIDEN