Umelá inteligencia v službách obrany

Riadenie bezpečnostnej infraštruktúry po novom

Judgment Day 2026

Juraj Nemeček, juraj.nemecek@alanata.sk

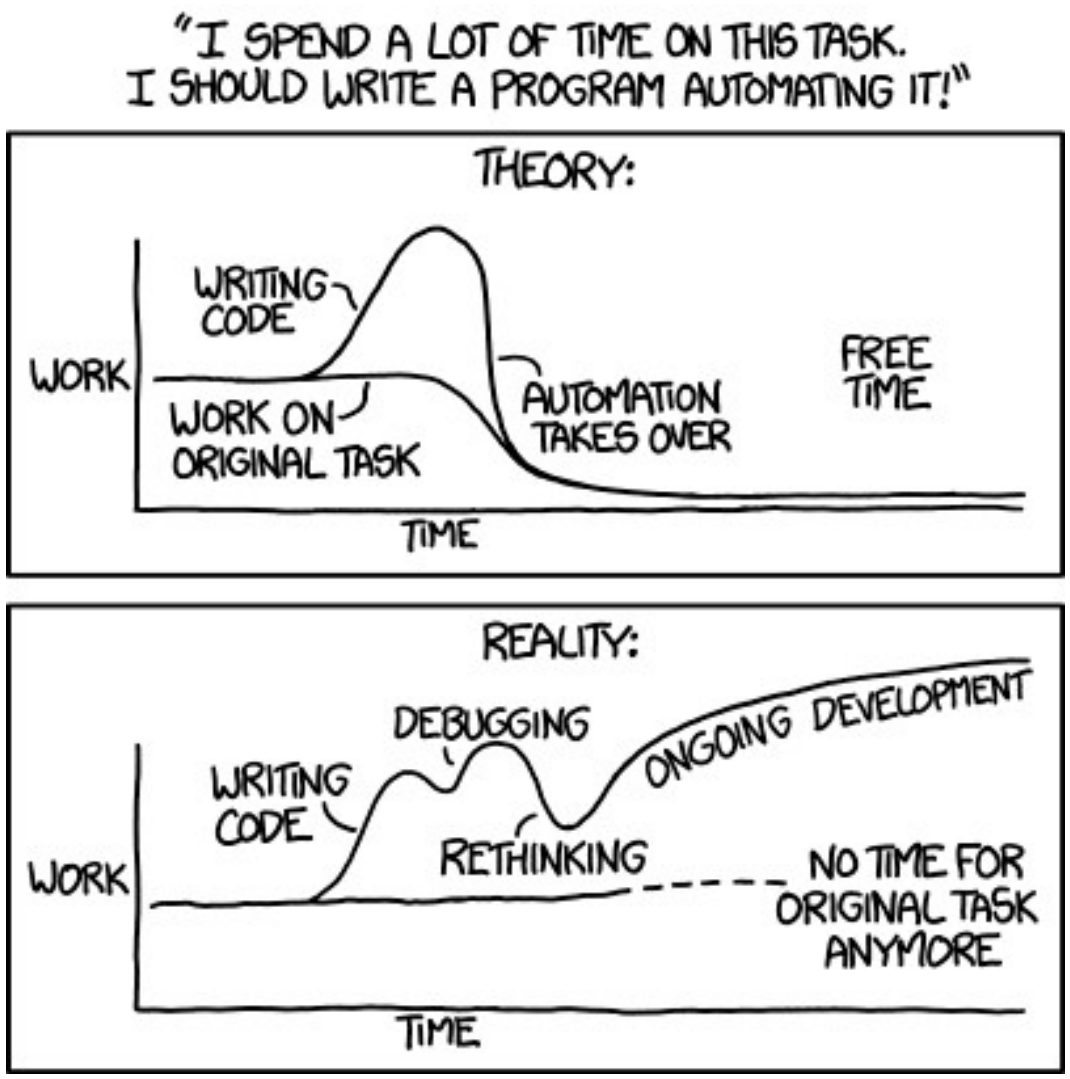
Alanata
Technology Meets Business

Komplexita rastie

- Koncoví agenti, NGFW, SASE, hybridné prostredia, identity management, ...
  - Každý obranný prvok pridáva komplexitu
  - Nekonečný feed potencionálne dôležitých informácií
  - Rastie aj komplexita správy

- Riešenie → Automatizácia 💡

Alanata
Technology Meets Business



XKCD 1319

Alanata
Technology Meets Business

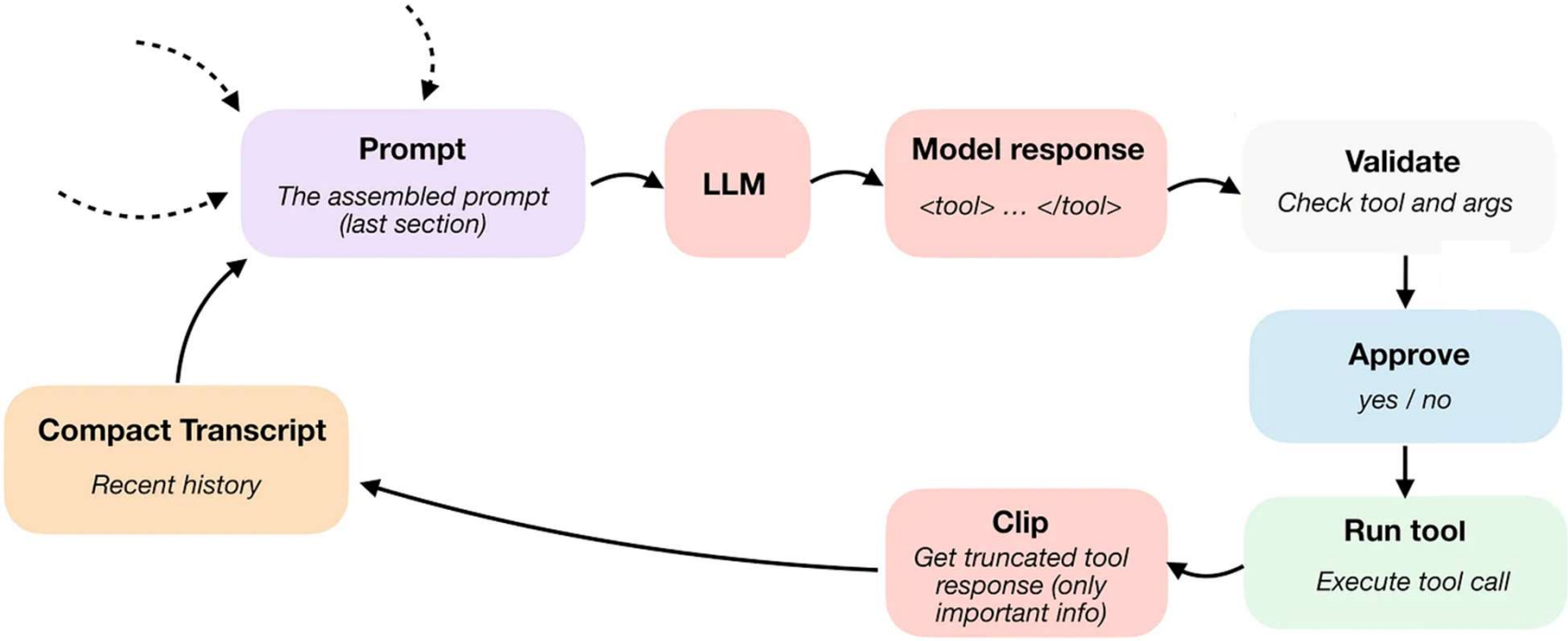
Umelá inteligencia – prečo práve teraz ?

1. Príliš vela dát, príliš málo času

2. Automatizujú aj útočníci

3. AI už nie len o modeloch → Harness

Alanata
nology Meets Business



Zdroj: Sebastian Raschka

Alanata
Technology Meets Business

Ukážky

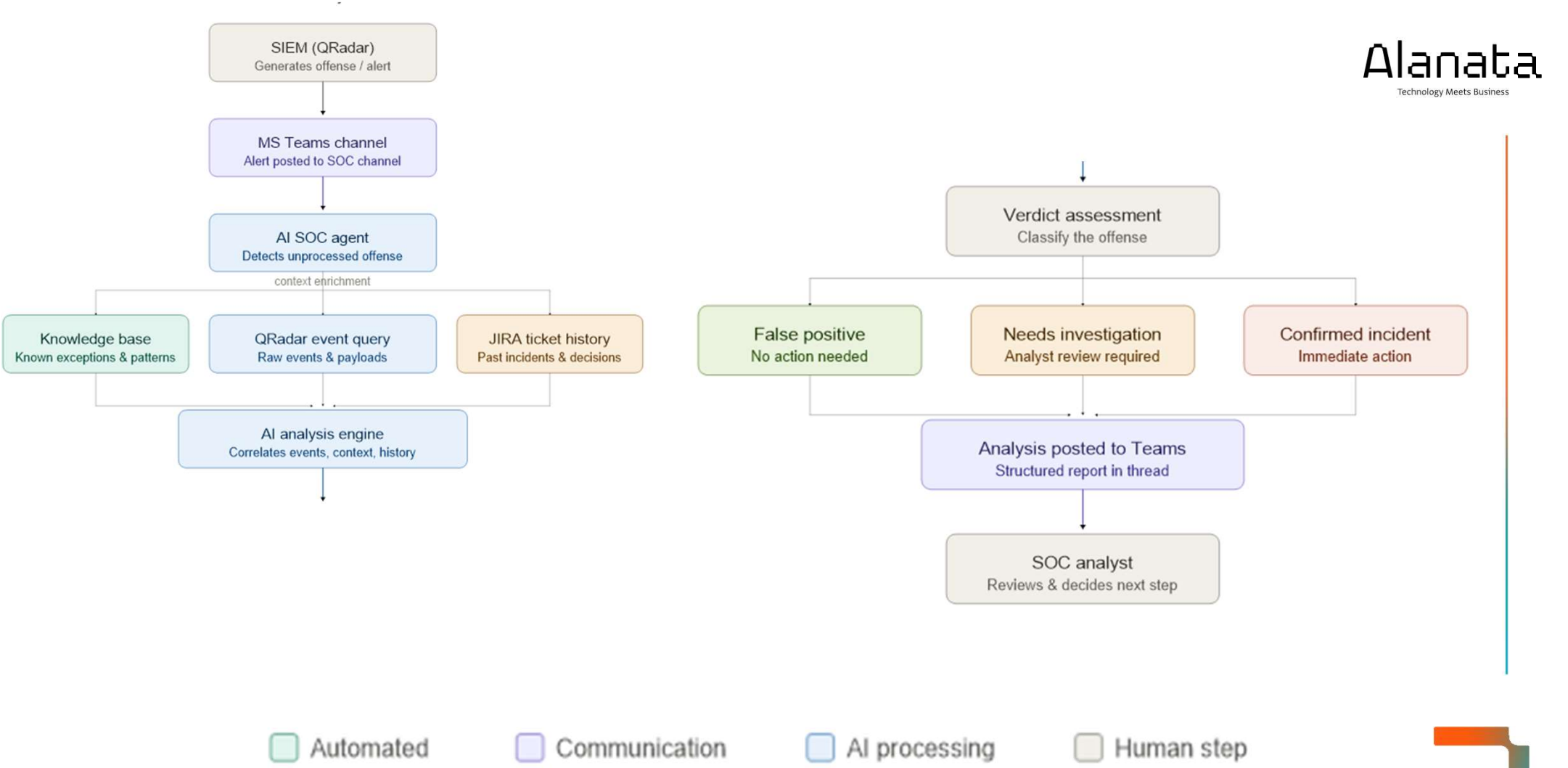
- Automatizácia činnosti SOC
- Automatizácia SecOps
- Automatizácia s použitím Skills

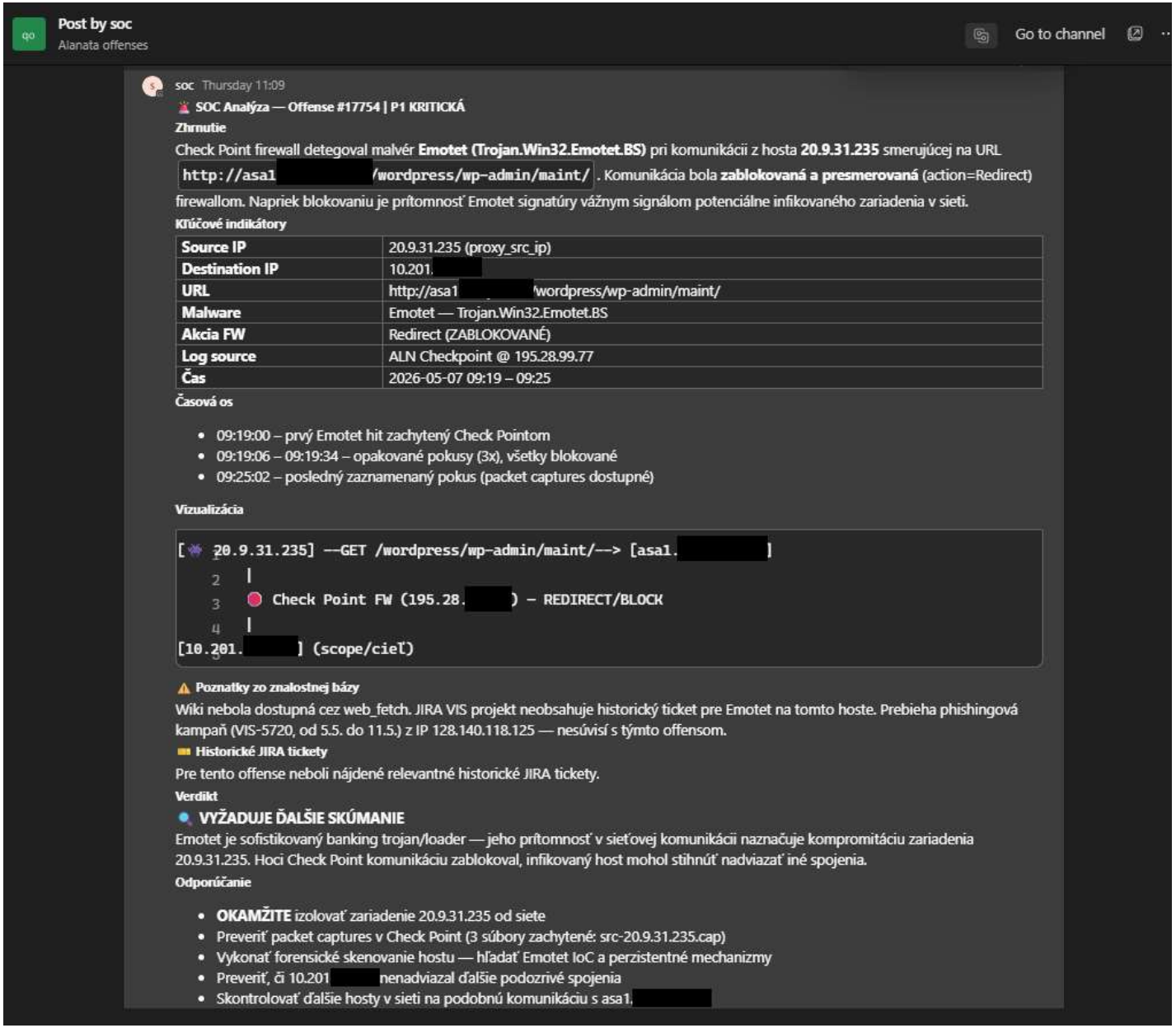
Automatizácia činnosti SOC

- SIEM - množstvo nálezov
- Prioritizácia
- S. Tariq et al - Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities:
  "... 54% of SOC teams feel overwhelmed by alerts, 55% lack confidence in prioritising or responding to them, and security experts spend 27% of their time handling false positives..."

- AI integrované do SOC pipeline
  ↓
- Obohatenie kontextu
  ↓
- Klasifikácia
  ↓
- Report

Alanata
Technology Meets Business





Alanata
Technology Meets Business

Alanata
Technology Meets Business

Automatizácia SecOps

- Model Context Protocol
- MCP client → MCP server → Lokálne nástroje, Externé API
- Komponenty MCP Servera
  - Manžment relácií
  - Autentifikácia
  - Vstupno/výstupné nástroje pre LLM
  - Riešenie chýb
  - ...

Ukážka - MCBP

Ukážka – Lokálny processing

Ukážka – Externá integrácia

Alanata
Technology Meets Business

Automatizácia s použitím Skills

- Skill
  - Kombinácia inštrukcií a kódu ako predpis pre úpravu činnosti modelu
  - Dáva sa ako adresár obsahujúci súbory vo formáte:
    - YAML frontmatter
    - Markdown
  - Vhodný pre opakované činnosti
  - Efektívny – na úvod tokeny len z frontmatter časti
- ❗ Pozor - Obsahuje kód a knižnice ❗

Ukážka – Vytvorenie a využitie Skill

Odporúčania

- Limity
  - Kontextové okno
  - Veľkosti súborov
  - Oprávnenia
- AI už nie len o modeloch
- Dôveruj ale preveruj

Alanata
Technology Meets Business