

Umelá inteligencia v službách obrany

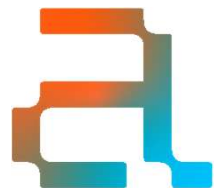
Riadenie bezpečnostnej infraštruktúry po novom

Judgment Day 2026

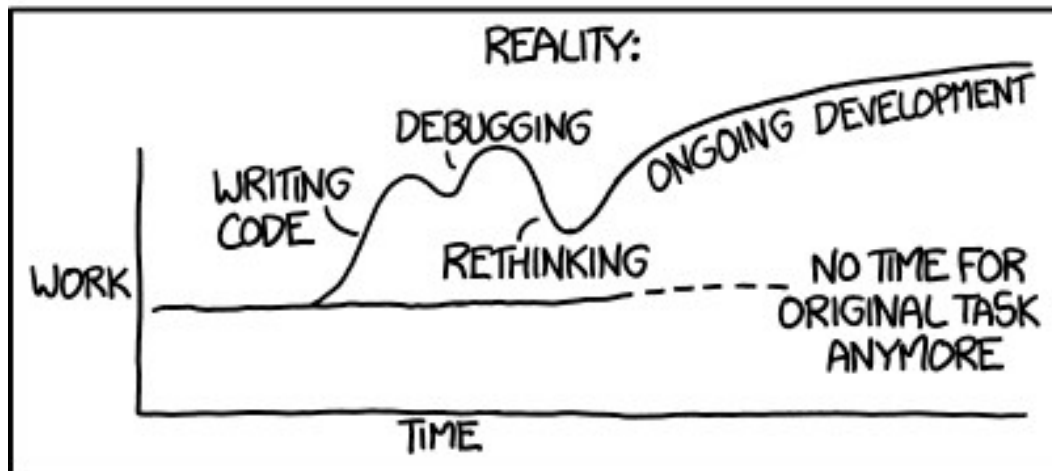
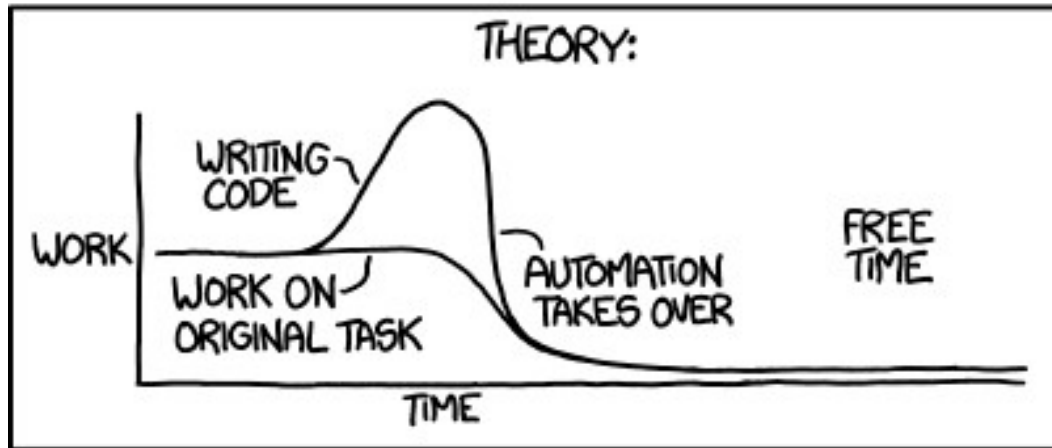
Juraj Nemeček, juraj.nemecek@alanata.sk

Komplexita rastie

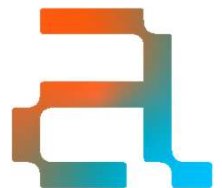
- Koncoví agenti, NGFW, SASE, hybridné prostredia, identity management, ...
 - Každý obranný prvok pridáva komplexitu
 - Nekonečný feed potencionálne dôležitých informácií
 - Rastie aj komplexita správy
- Riešenie → Automatizácia 💡



"I SPEND A LOT OF TIME ON THIS TASK.
I SHOULD WRITE A PROGRAM AUTOMATING IT!"



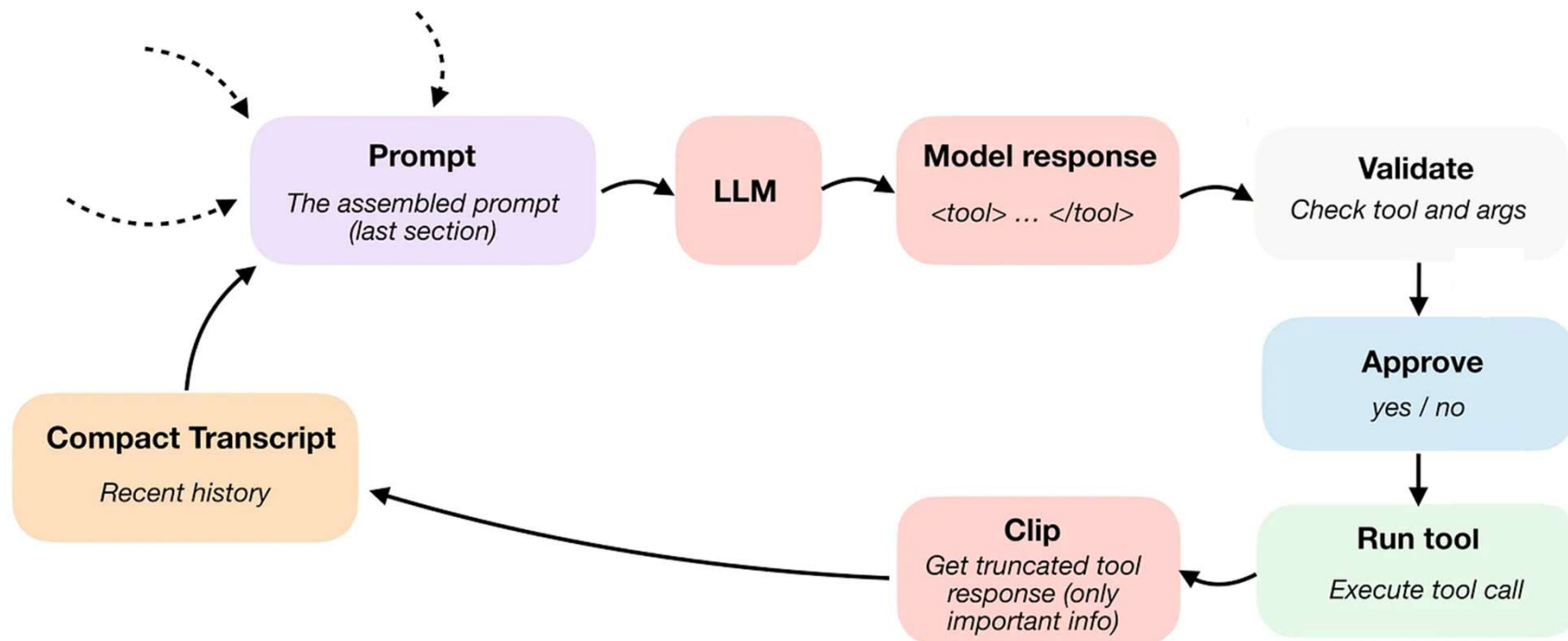
XKCD 1319



Umelá inteligencia – prečo práve teraz ?

1. Príliš vela dát, príliš málo času
2. Automatizujú aj útočníci
3. AI už nie len o modeloch → Harness





Zdroj: [Sebastian Raschka](#)



Ukážky

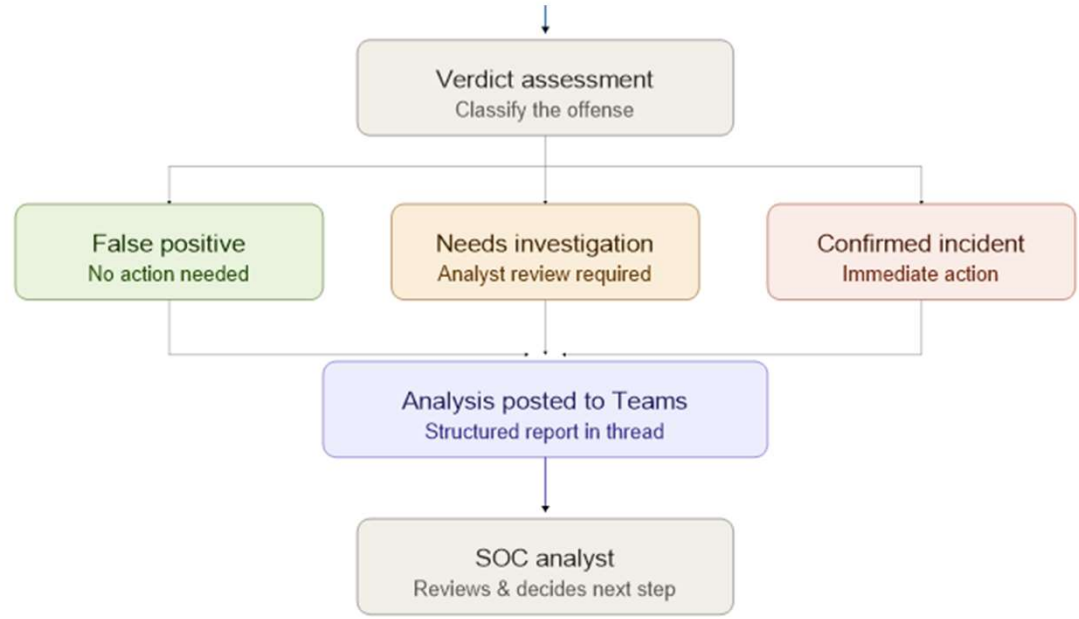
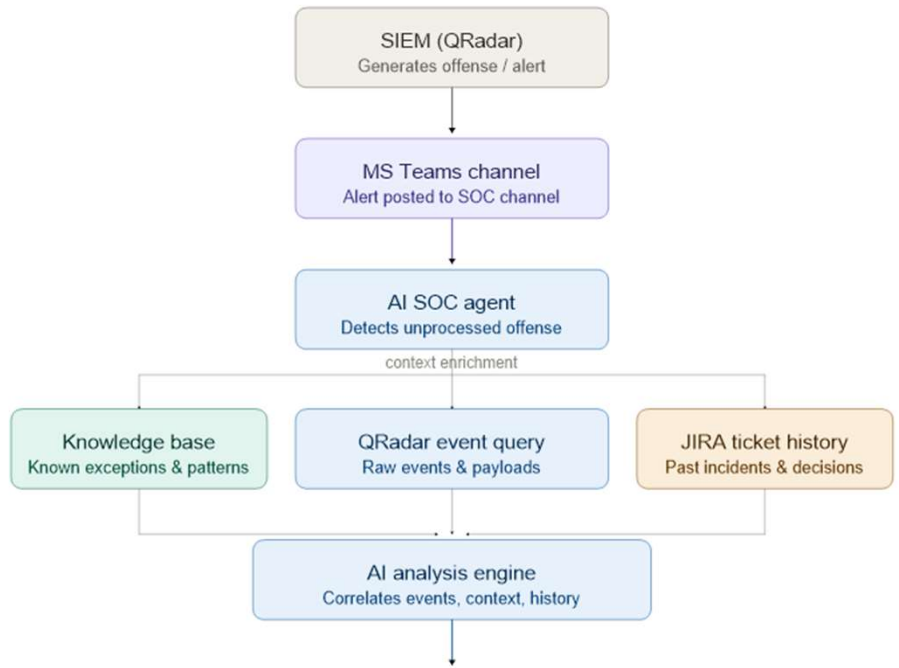
- Automatizácia činnosti SOC
- Automatizácia SecOps
- Automatizácia s použitím Skills



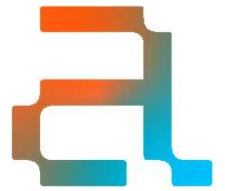
Automatizácia činnosti SOC

- 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





□ Automated
 □ Communication
 □ AI processing
 □ Human step



Post by soc Alanata offenses

soc Thursday 11:09

SOC Analýza — Offense #17754 | P1 KRITICKÁ

Zhrnutie

Check Point firewall detegoval malvér **Emotet (Trojan.Win32.Emotet.BS)** pri komunikácii z hosta **20.9.31.235** smerujúcej na URL `http://asa1[redacted]/wordpress/wp-admin/maint/`. Komunikácia bola **zablokovaná a presmerovaná** (action=Redirect) firewallom. Napriek blokovaníu je prítomnosť Emotet signatúry vážnym signálom potenciálne infikovaného zariadenia v sieti.

Kľúčové indikátory

Source IP	20.9.31.235 (proxy_src_ip)
Destination IP	10.201.[redacted]
URL	http://asa1[redacted]/wordpress/wp-admin/maint/
Malware	Emotet — Trojan.Win32.Emotet.BS
Akcia FW	Redirect (ZABLOKOVANÉ)
Log source	ALN Checkpoint @ 195.28.99.77
Čas	2026-05-07 09:19 – 09:25

Časová os

- 09:19:00 – prvý Emotet hit zachytený Check Pointom
- 09:19:06 – 09:19:34 – opakované pokusy (3x), všetky blokované
- 09:25:02 – posledný zaznamenaný pokus (packet captures dostupné)

Vizualizácia

```
[ * 20.9.31.235 ] --GET /wordpress/wp-admin/maint/--> [ asa1.[redacted] ]
2 |
3 | ● Check Point FW (195.28.[redacted]) - REDIRECT/BLOCK
4 |
[ 10.201.[redacted] ] (scope/cieľ)
```

▲ Poznámky zo znalostnej bázy

Wiki nebola dostupná cez web_fetch. JIRA VIS projekt neobsahuje historický ticket pre Emotet na tomto hoste. Prebieha phishingová kampaň (VIS-5720, od 5.5. do 11.5.) z IP 128.140.118.125 — nesúvisí s týmto offensom.

■ Historické JIRA tickety

Pre tento offense neboli nájdené relevantné historické JIRA tickety.

Verdikt

- VYŽADUJE ĎALŠIE SKÚMANIE**

Emotet je sofistikovaný banking trojan/loader — jeho prítomnosť v sieťovej komunikácii naznačuje kompromitáciu zariadenia 20.9.31.235. Hoci Check Point komunikáciu zablokoval, infikovaný host mohol stihnúť nadviazať iné spojenia.

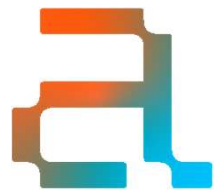
Odporúčanie

- OKAMŽITE** izolovať zariadenie 20.9.31.235 od siete
- Preveriť packet captures v Check Point (3 súbory zachytené: src-20.9.31.235.cap)
- Vykonať forensické skenovanie hostu — hľadať Emotet IoC a perzistentné mechanizmy
- Preveriť, či 10.201.[redacted] nenadviazal ďalšie podozrivé spojenia
- Skontrolovať ďalšie hosty v sieti na podobnú komunikáciu s asa1.[redacted]

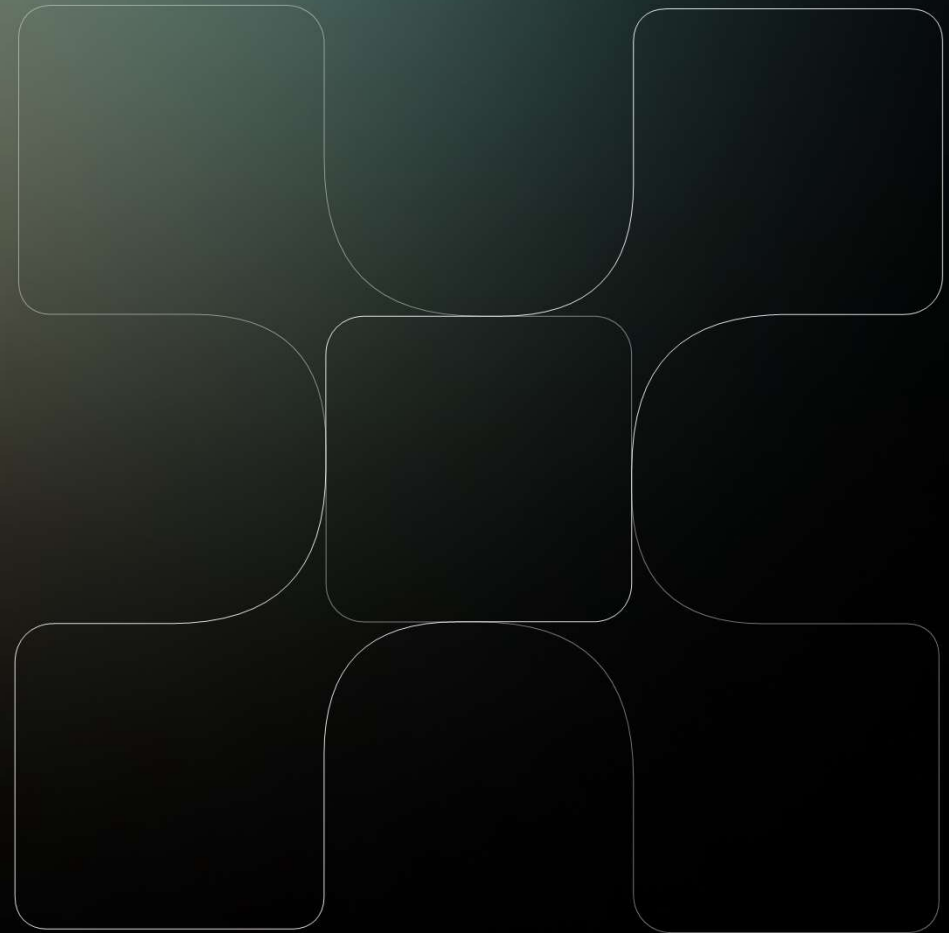


Automatizácia SecOps

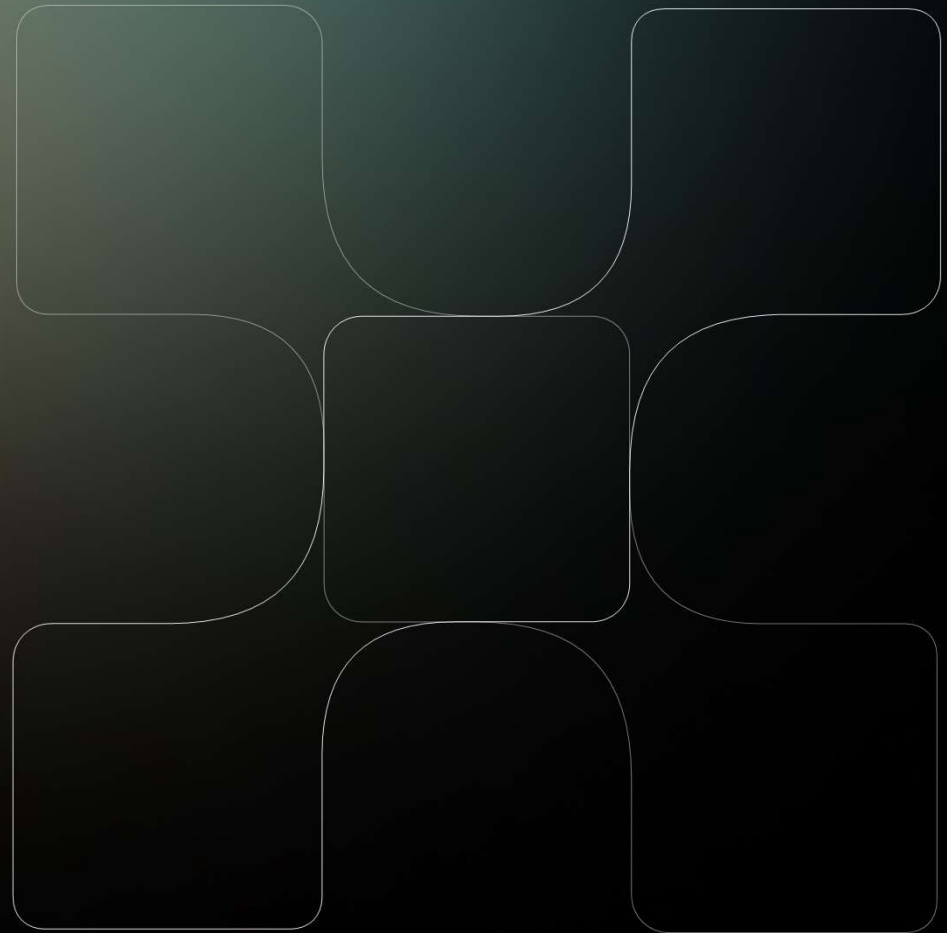
- Model Context Protocol
- MCP client → MCP server → Lokálne nástroje, Externé API
- Komponenty MCP Servera
 - Manžment relácií
 - Autentifikácia
 - Vstupno/výstupné nástroje pre LLM
 - Riešenie chýb
 - ...



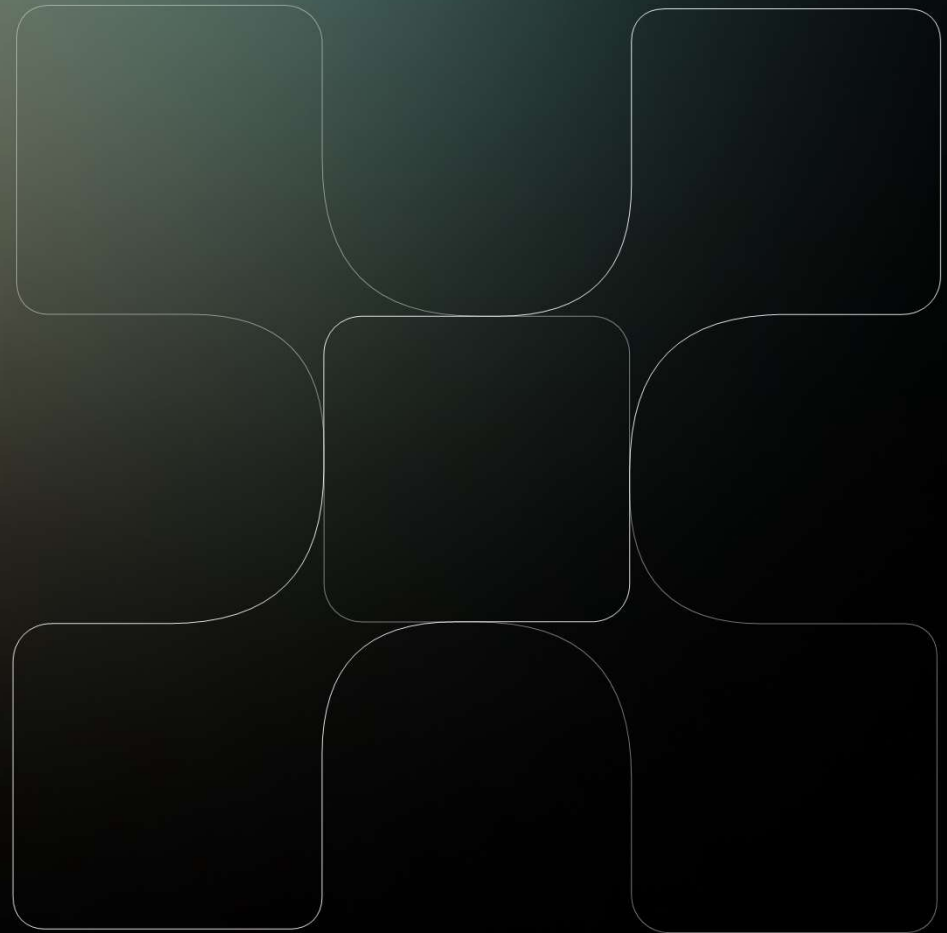
Ukážka - MCBP



Ukážka – Lokálny processing

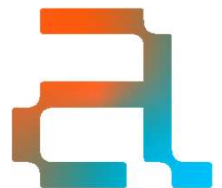


Ukážka – Externá integrácia



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

