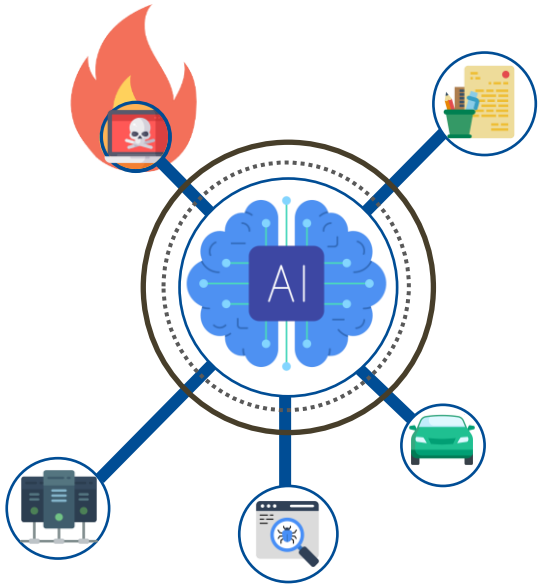
Z normalizovaných dat k inteligentnímu monitoringu. Budoucnost SIEM v éře umělé inteligence

CACIO 2024

Yehor Safonov / SIEM Team Leader (*Aricoma*) / CEO (*LogSolve*) / Ph.D. Student

24.04.2024

Motivace



- Rostoucí počet kybernetických hrozeb;
- Popularita generativních modelů;
- Zásah do všech sfér lidského života;
- Hybridní týmy;
- Vliv na bezpečnostní monitoring.

Cacio

O autorovi

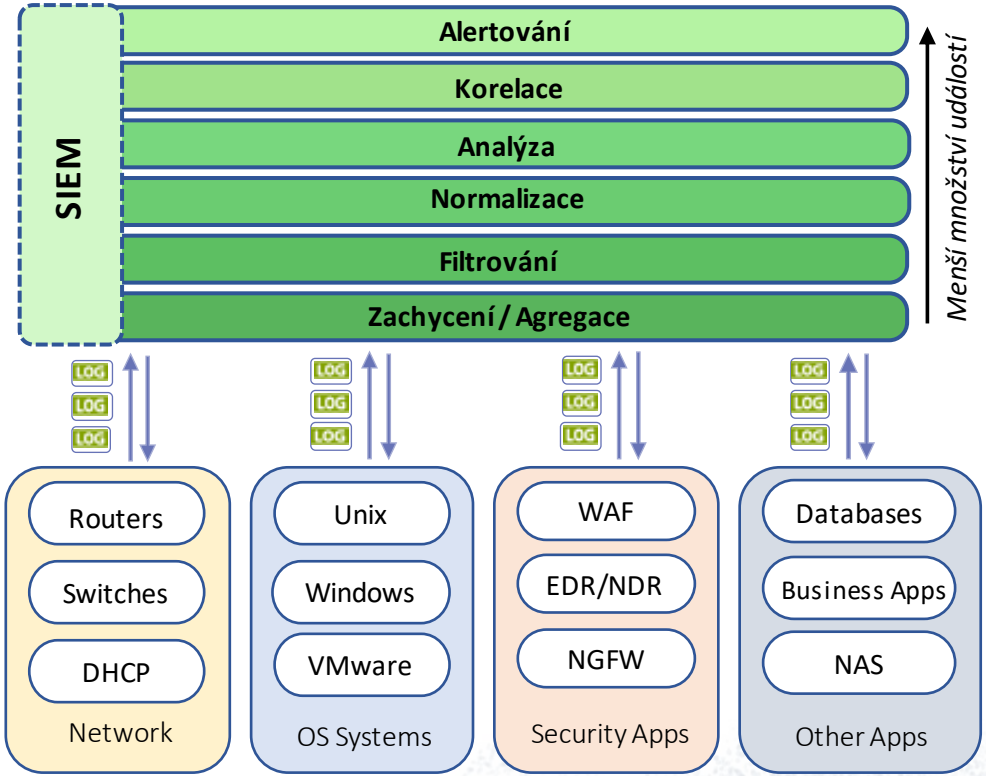
- ARICOMA (SIEM Team Leader);
- Informační bezpečnost a AI (Ph.D. na VUT);
- LogSolve (CEO);
- Automatizace SIEM / SOAR řešení pomocí AI;
- Počítačová bezpečnost, kryptografie, teoretická informatika a strojové učení.

Co si odnesete?

1) Výzvy spojené se SIEM a jejich řešení;
2) Jaké procesy SIEM / SOC AI dokáže nahradit?
3) Dolování znalostní z logových záznamů.
4) Rizika spojená s AI.

Cacio

Hlavní principy SIEM systémů

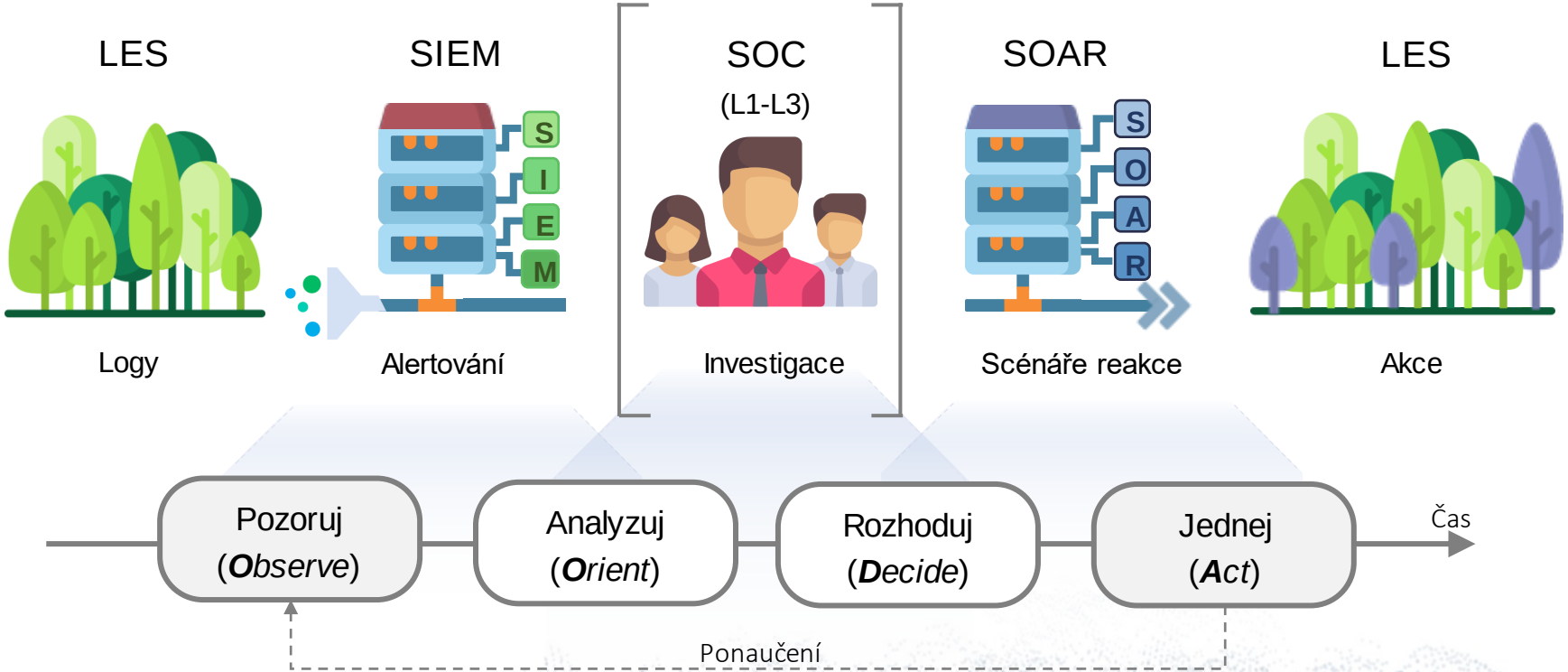


- ***Security Information and Event Management***
- Velké počítačové infrastruktury;
- Složitá konfigurace a optimalizace;
- Ideální místo pro aplikování AI.

- Sběr dat napříč infrastrukturou;
- Různé zdroje logů:
  - LES (*Log Event Sources*),
  - PES (*Packet Event Sources*).

Cacio

Potravní řetězec bezpečnostního monitoringu



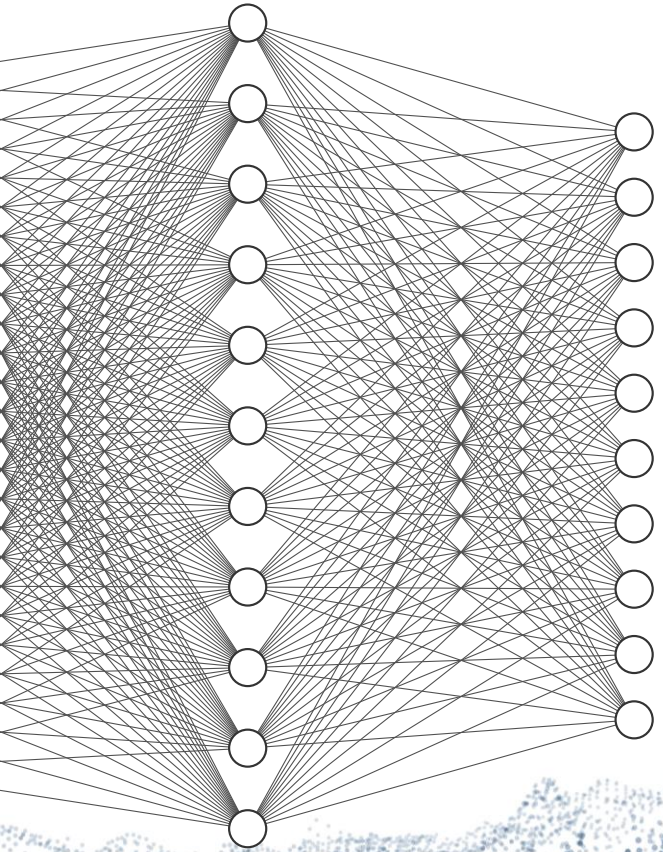
Cacio

Hlavní výzvy SIEM řešení

- Iluze bezpečnosti;
- Nedostatečné využití umělé inteligence;
- Problematické napojení technologií;
- Chybovost dekodérů;
- Aktualizace;
- Nefunkčnost korelačních pravidel;
- Dlouhodobá udržitelnost.

Cacio

Překonání očekávání: Neuvěřitelný boom *Deep Learning*



- 2012 – výrazný pokrok CNN (Toronto);
- Revoluce v algoritmech s příchodem DL;
- HW akcelerace výpočtů (NV CUDA);
- Vznik frameworků (Tensorflow, Pytorch, Keras);
- 2017 – Transformer networks (GPT, BERT);
- NLP (*Natural Language Processing*).

Cacio

Jak to může fungovat v praxi?

Transformer Networks

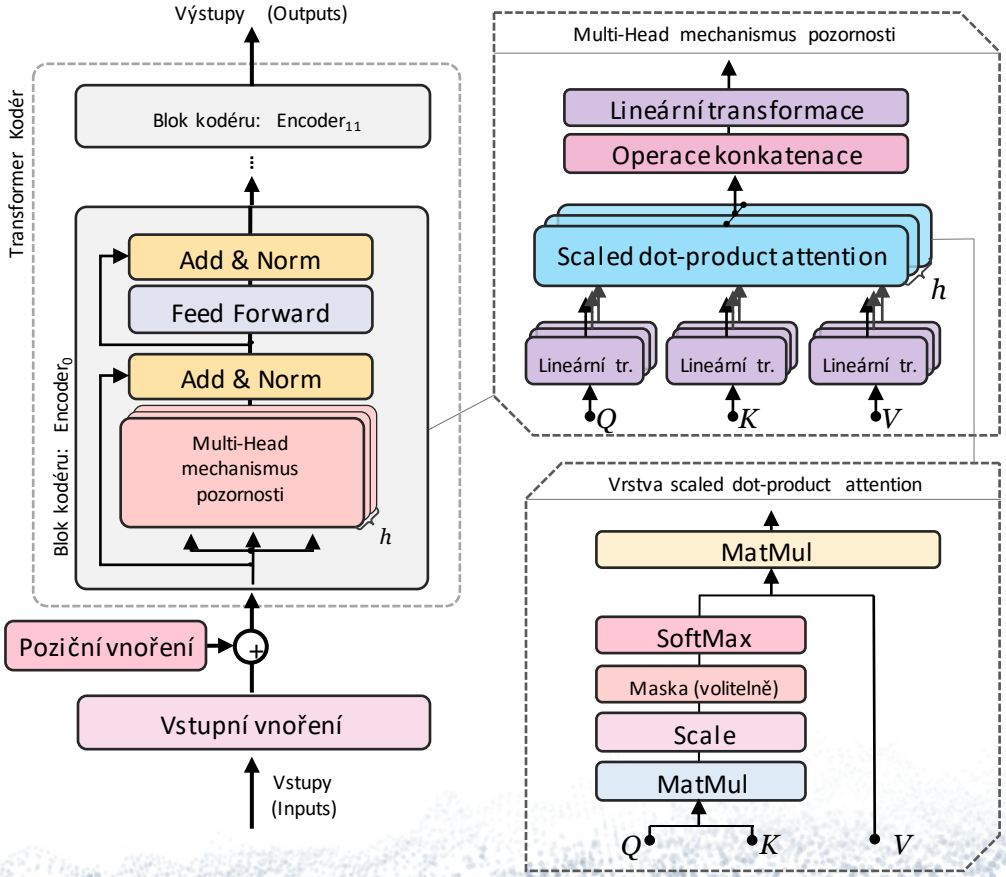
NLP (*Natural Language Processing*)

Green Apple tastes good to me.

I bought a new generation of Apple.

Cacio

Jak to může fungovat v praxi?



Transformer Networks

GPT 4

1.5 tril.

12 288 dim.

6 TB

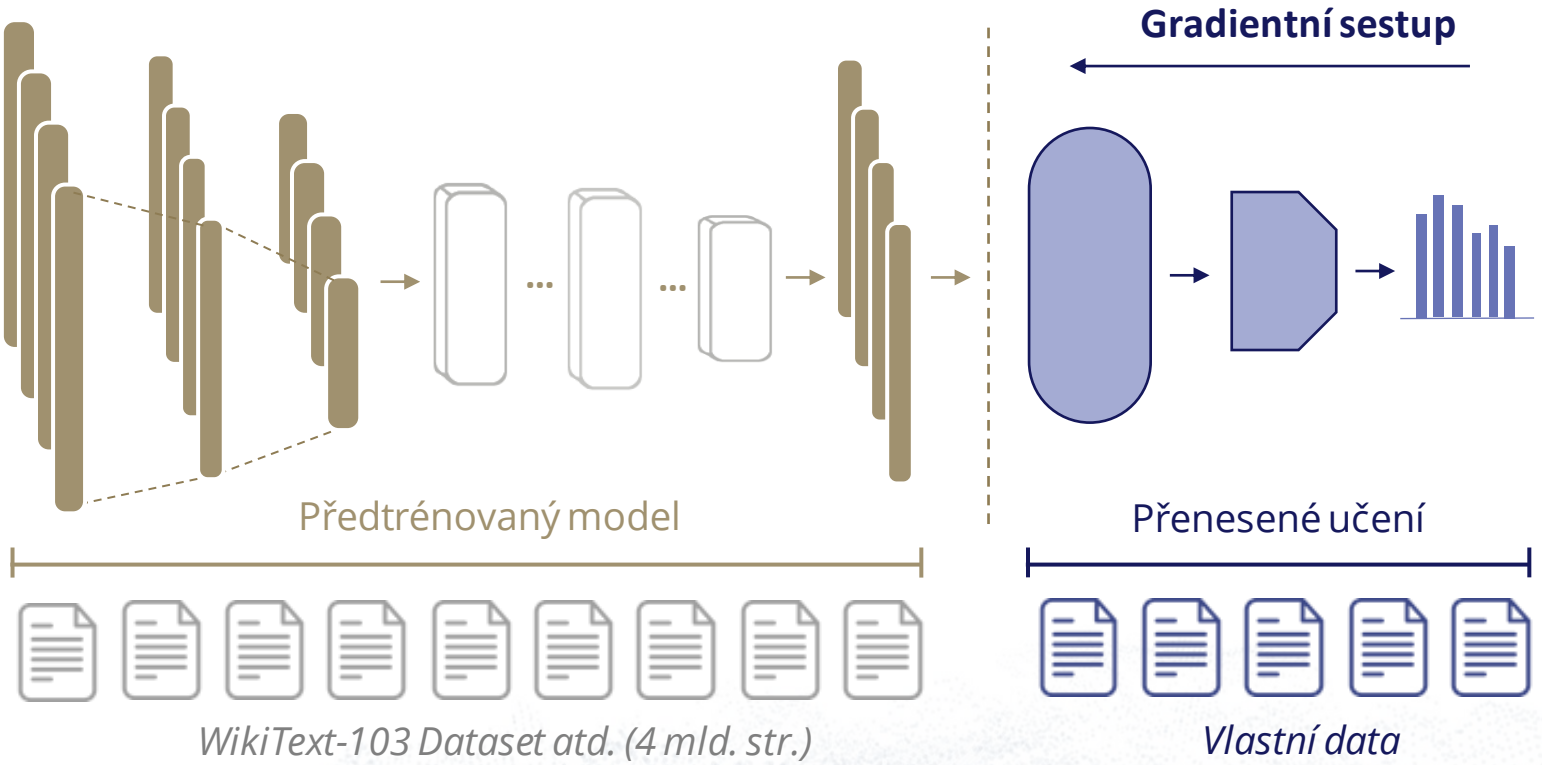
1065 let

$63 mld.

4 mld. str.

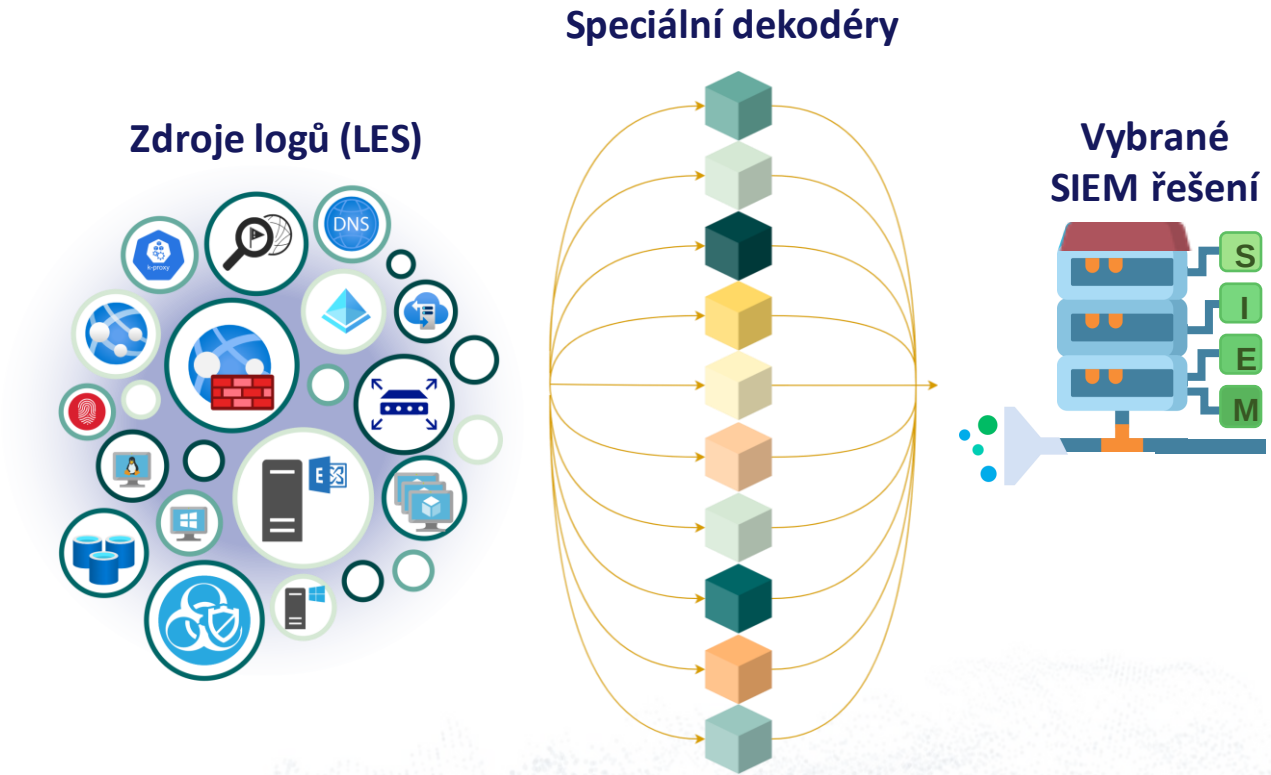
Cacio

Aplikování na doménu bezpečnostního monitoringu



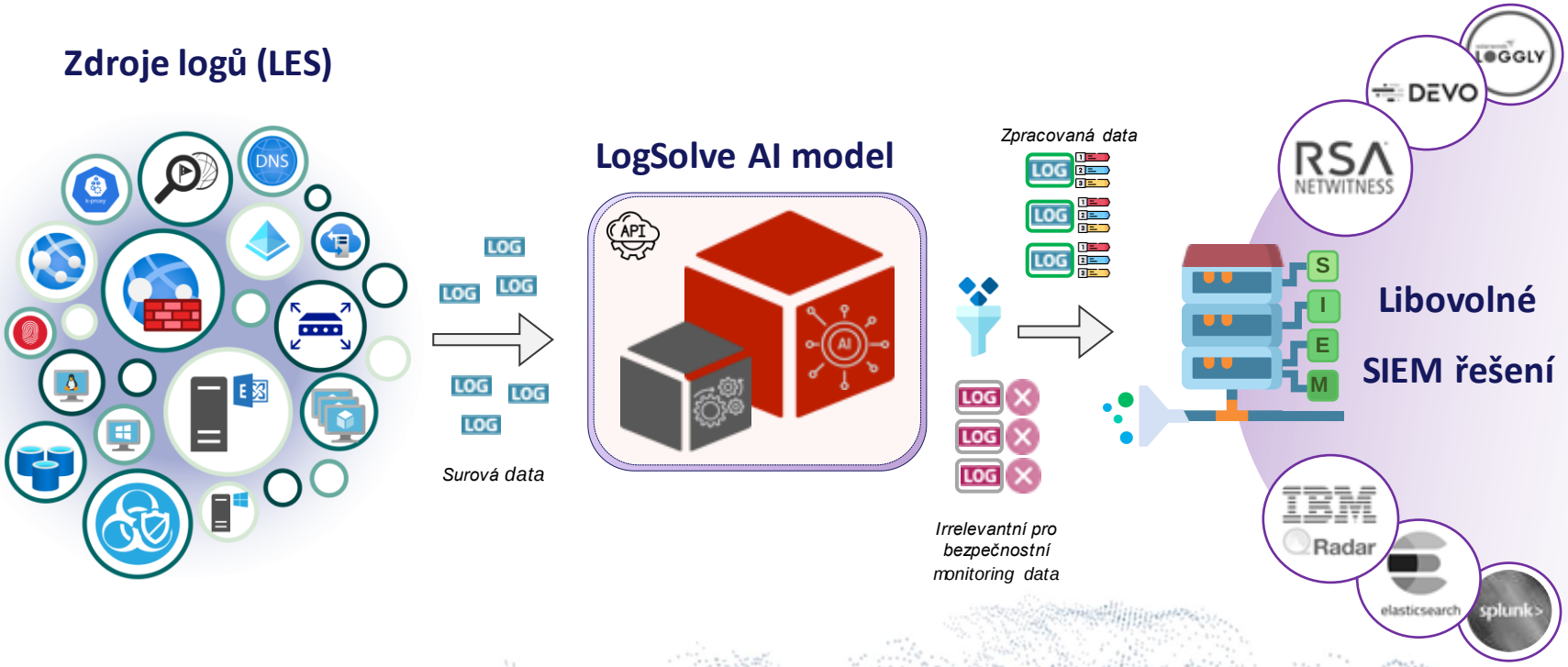
Cacio

Dolování znalostí z logů: *Aktuální stav*



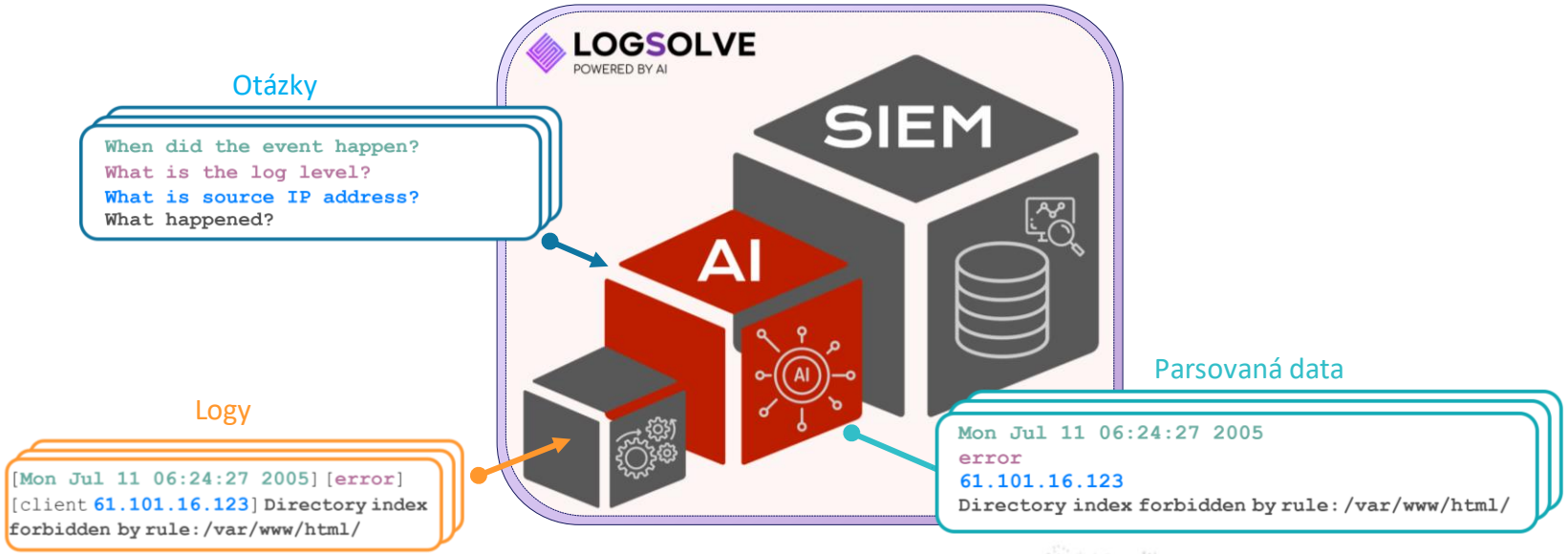
Cacio

Dolování znalostí z logů: *Navrhované řešení*



Cacio

Dolování znalostí z logů: *Navrhované řešení*



Dolování znalostí z logů: *Kvantifikace výhod*

Výhody

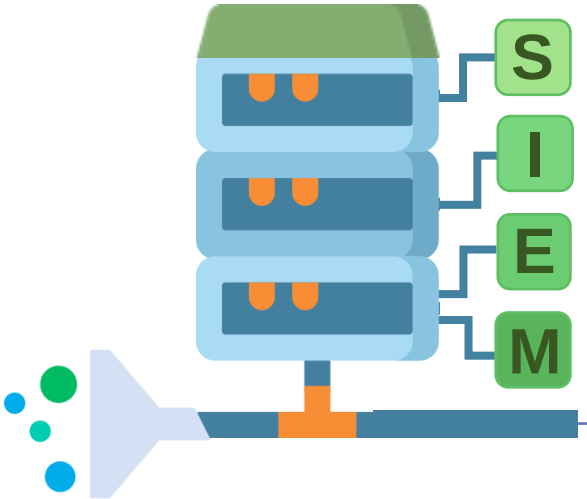
- Úspora nákladů na obsluhu:
- Jednoduché napojení LES:
- Licenční úspora (EPS):
- Flexibilita na dodavateli SIEM;
- Jeden model **VS** speciální konektory;
- Jednoduchá údržba, automatizace.

Kvantifikace

- ✓ minimálně cca 3 024 000 Kč ročně;
- ✓ úspora cca 60 000 Kč za jeden LES;
- ✓ minimálně cca 500 000 Kč;
- ✓ snížení míry zapojení správců;
- ✓ zvýšení míry konkurence na trhu SIEM.

Cacio

Jaké budeme mít SIEMy v budoucnu?



- Automatizováno
- Z části automatizováno
- Nové funkcionality

Agregace a sběr dat

- Vyčítání dat (pull)
- Příjem dat (push)
- Dolování znalostí (parsování)
- Sledování napojených technologií

Filtrování a Indexace dat

- Základní Vyhodnocení a Filtrování
- Normalizace a generalizace

Analýza a Korelace

- Pokročilá analýza dat
- Pokročilá korelace a monitoring

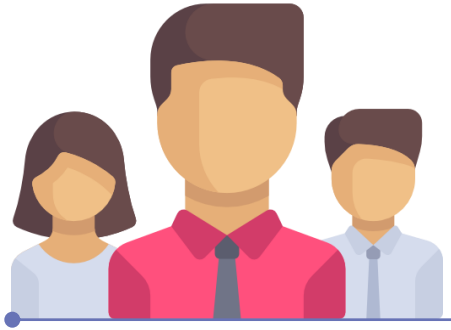
Reportování / Alertování / Expertní systém

- Reportování
- Prediktivní analýza
- Alertování
- Vyhledávání hrozeb
- Adaptivní napojení na jiné systémy
- Pokročilý Expertní Systém

Cacio

Jaká je budoucnost *Security Operation Center* (SOC)?

SOC



L1-L3

- Nahrazeno
- Z části nahrazeno / Asistence
- Minimální míra asistence

SOC L1 (*Level 1*)

- Základní monitorování událostí
- Třídění alertů
- Dokumentace incidentů
- Základní reakce (playbooks)

SOC L2 (*Level 2*)

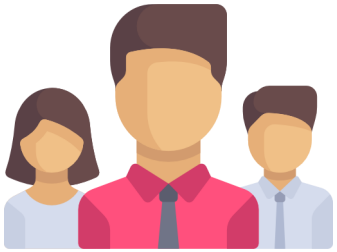
- Reakce na incidenty
- Proaktivní vyhledání hrozeb
- Spoluúčast na rozvoji SIEM, tvorba playbooks
- Komunikace a spolupráce s externími subjekty

SOC L3 (*Level 3*)

- Pokročilá analýza útoků
- Řízení a koordinace incidentů
- Bezpečnostní architektura (analýza, návrh, doporučení)
- Vývoj a zdokonalení procesů SOC

Cacio

Jaká je budoucnost?



L1-L3

Log Manager

Rozhraní

Základní
Bezpečnostní monitoring

SIEM / SOAR

Rozhraní

Pokročilý
Bezpečnostní monitoring

AI-SIEM / AI-SOAR

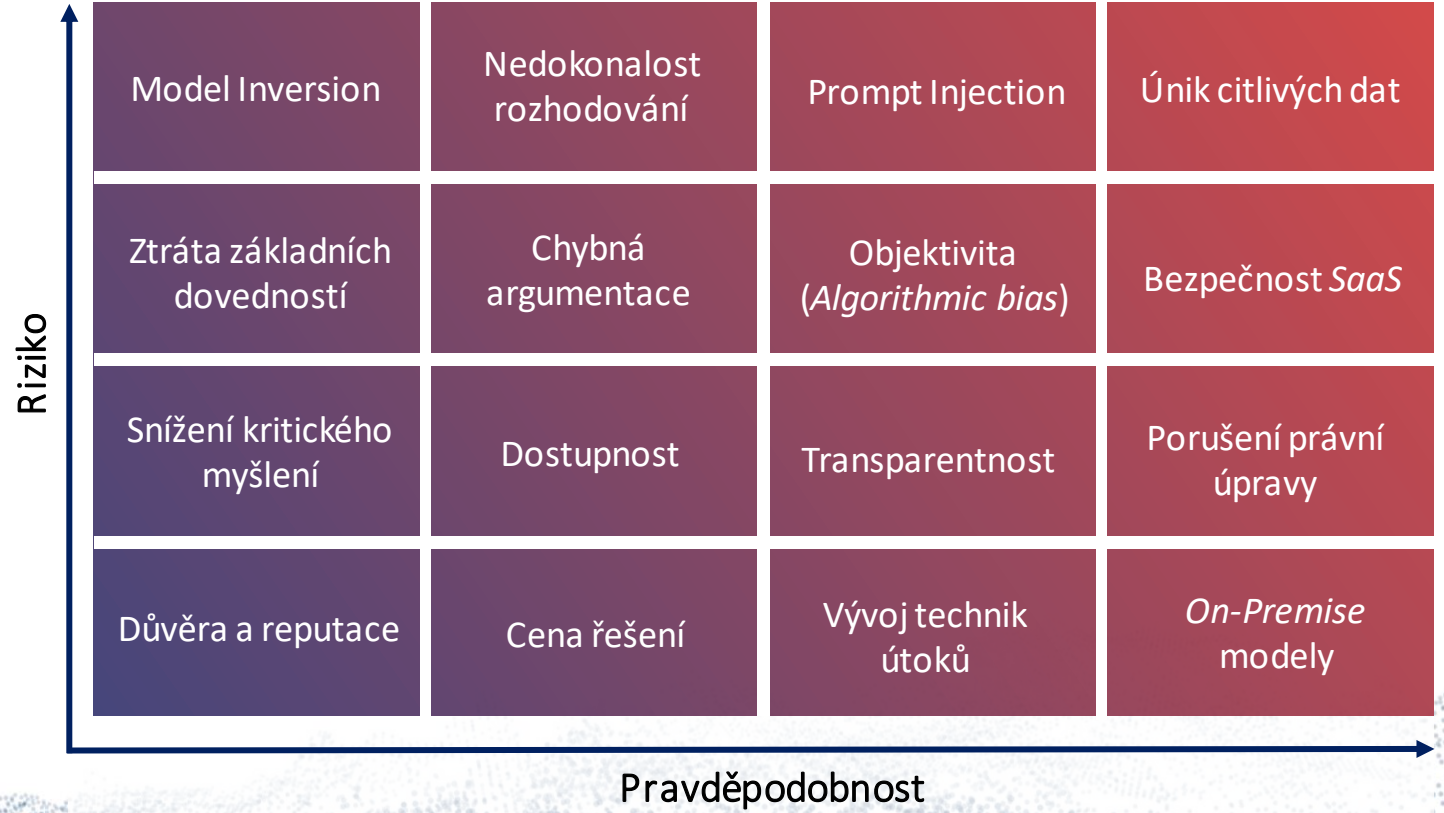
Rozhraní

AI Powered
Bezpečnostní monitoring

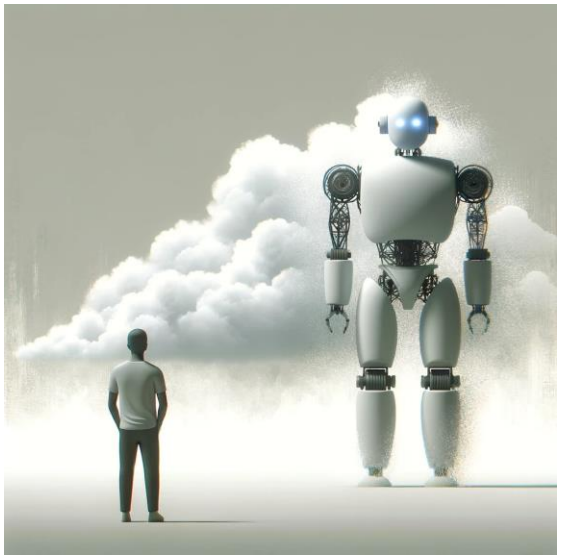
Čas

Cacio

Rizika generativních modelů v *Enterprise* sektoru



Doporučení a závěr



- Velký potenciál AI modelů;
- Dopad na bezpečnostní monitoring;
- Hybridní týmy;
- Kritické myšlení 3.0;
- Limitace datových sad;
- Rizika AI modelů;
- Rizika poskytovatelé *SaaS*.

Cacio

Děkuji za pozornost!

Yehor Safonov

SIEM Team Leader / CEO LogSolve / Ph.D. Student

yehor.safonov@gmail.com / +420 771 132 753