

M U N I

Automatizovaná analýza bezpečnostních dat

Matúš Raček, Daniel Tovarňák et al.

Masarykova univerzita, CSIRT-MU

Brno, Česká republika

22. ledna, 2026

Kdo?

CSIRT-MU

- Kyberbezpečnostní tým Masarykovy univerzity
- První certifikovaný bezpečnostní tým v ČR
- Oblast působnosti:
 - IPv4 adresy v rozsahu: 147.251.0.0/16,
 - IPv6 adresy v rozsahu: 2001:718:801::/48,
 - doména muni.cz.
- **Kontakt: csirt@muni.cz**

Proč?

Zefektivnění každodenní operativy

- Zvyšující se objem a rychlost generování bezpečnostní telemetrie.
- Rostoucí komplexita chráněného kyberprostoru a následná potřeba korelace více informací.
- Automatizace na straně útočníků.
- Zvýšená zátěž a vysoký počet případů vyhoření pracovníků.
- Doporučením je zvážení investic do automatizace procesů.
- Pokud ale chceme automatizovat, potřebujeme spolehlivý zdroj informací a způsob, jak je efektivně zpracovávat.

Bezpečnostní telemetrie

■ Síťové toky – IPFIX, NSEL

- metadata o provozu na počítačové síti,
- neustále rostoucí rychlosti přenosu dat,
- rostoucí nároky na příjem, zpracování, uchování, prohledávání,
- *velmi vysoký* objem, *nízká* komplexita, *stabilní* implic. struktura.

■ Logy – ECS, Syslog, Winlogbeat

- nejcennější prostředek pro vhled do vnitřní činnosti ICT,
- často v přirozeném jazyce (vývojářů),
- stejně jako výše – výkonnější IT → více logů → vyšší nároky,
- *vysoký* objem, *střední* komplex., *velmi nestabilní* implic. struktura.

■ Kontextové informace – GeolP, výsledky skenů

- *střední* objem, *vysoká* komplexita, *stabilní* implicitní struktura.

Současný stav poznání (a praxe)

■ Současná řešení často

- pracují pouze s podmnožinou bezpečnostní telemetrie,
 - nedisponují dostatečnou flexibilitou,
 - nekladou důraz na definici datových kontraktů,
 - pracují s daty s nízkou kvalitou v nevhodných strukturách (nekvalitní vstupy vedou k nekvalitním výstupům, pravidlo 80/20),
 - naráží na **limity svých базových technologií** při záplavě daty (lze pozorovat nedostatečný výkon, nízkou efektivitu, či nepřiměřené náklady).
- Bezpečná architektura je nutné budovat modulárně, s důrazem na otevřenost, interoperabilitu a průběžnou automatizaci.

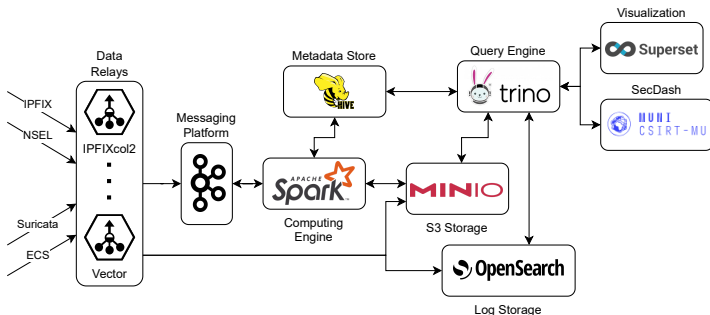
Jak?

Postup řešení

- Referenční systém pro zpracování, retenci a pokročilou analýzu bezpečnostní telemetrie.
- Bázová technologie pro centra bezp. operativy (SOC, CSIRT).
- **Důraz na:**
 - škálovatelnost (1-X uzlů v závislosti na objemu dat),
 - vysoký výkon (diskové úložiště, síť),
 - spolehlivost (redundance, distribuovanost),
 - udržitelnost a udržitelnost (zacílení na analytiku),
 - interoperabilitu (datové kontrakty, API, standardy),
 - otevřenost (otevřený kód a použité nástroje).

Architektura řešení

- Data Lakehouse architektura.
- Oddělení úložiště od výpočtů.



Jak vypadá produkční běh?

- 4x uzel úložiště (2x Intel 6505p, 504 GB RAM, 10x 15TB NVMe).
- 6x výpočetní uzel (2x Intel GOLD 6242, 1.5 TB RAM, 2x 4TB NVMe).
- 2x 100Gbit switch (Cisco Nexus 9336C-FX2).



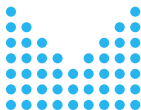
Několik čísel

- Vyšší rychlost dotazování než stávající komerční řešení.
- 6x více dat (2 měsíce vs. 12 měsíců).
- 2x totální výpadek uzlu bez ztráty dat (1 den a 7 dnů).
- Udržitelný datový tok cca 100 tis. záznamů za vteřinu.
- Více než 1 trilion uložených záznamů (1 000 000 000 000).

Co s tím?

- Obohacování uložených údajů -> PassiveDNS, GeoIP obohacování.
- Vytváření agregovaných datových modelů (komunikace IP párů, LiveIP).
- Detekční metody (toky, logy),
- Zavedení NATu -> nový zdroj telemetrie a následná možnost její korelace se síťovými toky.
- ...

Poděkování



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Tento výzkum byl podpořen Programem bezpečnostního výzkumu České republiky v letech 2015-2020 (BV III/1-VS), který je poskytovaný Ministerstvem vnitra ČR, v projektu č. VI20202022164 Pokročilá orchestrace bezpečnosti a inteligentní řízení hrozeb.

Tento výzkum byl podpořen Programem Otevřené výzvy v bezpečnostním výzkumu 2023-2029 (OPSEC), který je poskytovaný Ministerstvem vnitra ČR, v projektu č. VK01030070 Automatizovaná analýza bezpečnostní telemetrie.

**MASARYKOVA
UNIVERZITA**