SPCSS

Státní pokladna
Centrum sdílených služeb

Optimální vstupy pro efektivní bezpečnostní monitoring

18. 5. 2026

TLP: GREEN

Mgr. Martin Kotyk CISM

Manažer kybernetické bezpečnosti

martin.kotyk@spcss.cz

Řízení kybernetických rizik

OBLAST	HLAVNÍ CÍL	TYPICKÉ AKTIVITY	ODPOVĚDNOST
Detekce hrozeb	Včasné odhalení incidentu	Nepřetržité monitorování, korelace logů, alerting	Security Operations Centre (SOC)
Reakce na incidenty	Minimalizace dopadů	Containment, analýza, obnova systémů	SOC, IT, Management
Hlášení dle zákona č. 264/2025 Sb.	Splnění regulatorních povinností	24 h early warning, 72 h hlášení, závěrečná zpráva	Management

Zákon č. 264/2025 Sb.

Rozsah pro Bezpečnostní monitoring

- § 13 Bezpečnostní opatření
  - Obligatorní povinnost zavedení bezpečnostních opatření
- § 14 Seznam bezpečnostních opatření
  - **Vyšší povinnosti 1. b) 5. 6. 7.**
    - **409/2025 § 21 Detekce kybernetických bezpečnostních událostí**
    - **409/2025 § 22 Zaznamenávání událostí**
    - **409/2025 § 23 Vyhodnocování kybernetických bezpečnostních událostí**
  - **Nižší povinnosti 2. i); j)**
    - **410/2025 § 9 Detekce a zaznamenávání kybernetických bezpečnostních událostí**
- § 15 – Hlášení kybernetických bezpečnostních incidentů
  - Povinnost hlásit KBI NÚKIBu
- § 16 – Postup hlášení kybernetických bezpečnostních incidentů
- § 17 – Zvládání kybernetických bezpečnostních incidentů

Security Operations Center

Nepřetržitý bezpečnostní monitoring

- 24/7 Monitoring IT prostředí
- Odhaluje Bezpečnostní události a zajišťuje včasnou reakci na ně
- ***Útoky dnes probíhají v minutách, ne dnech***

Technologie a lidská expertíza

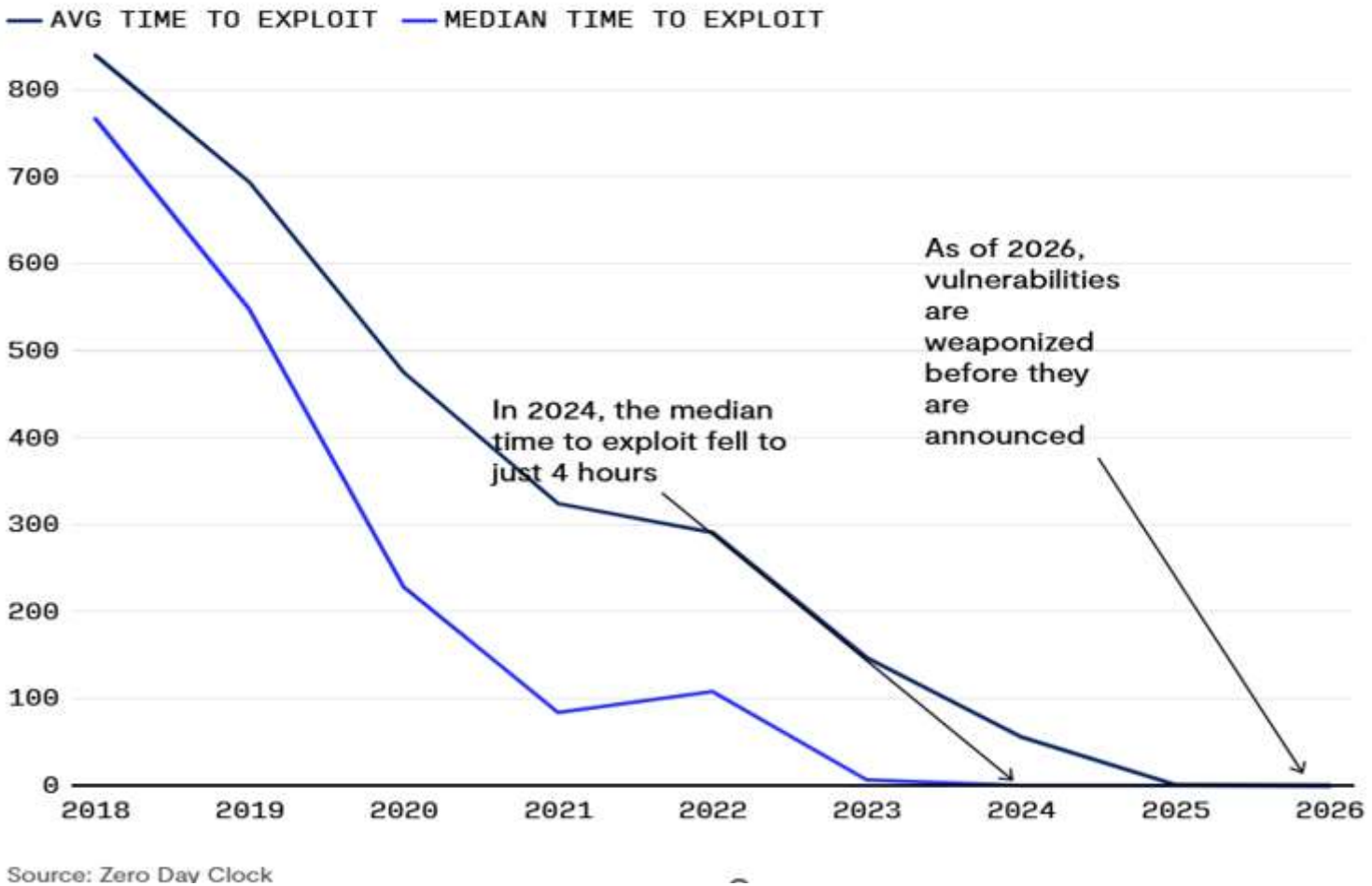
- Nástroje + odbornost analytiků = vyhodnocení Bezpečnostní události

Zvyšování bezpečnostní zralosti

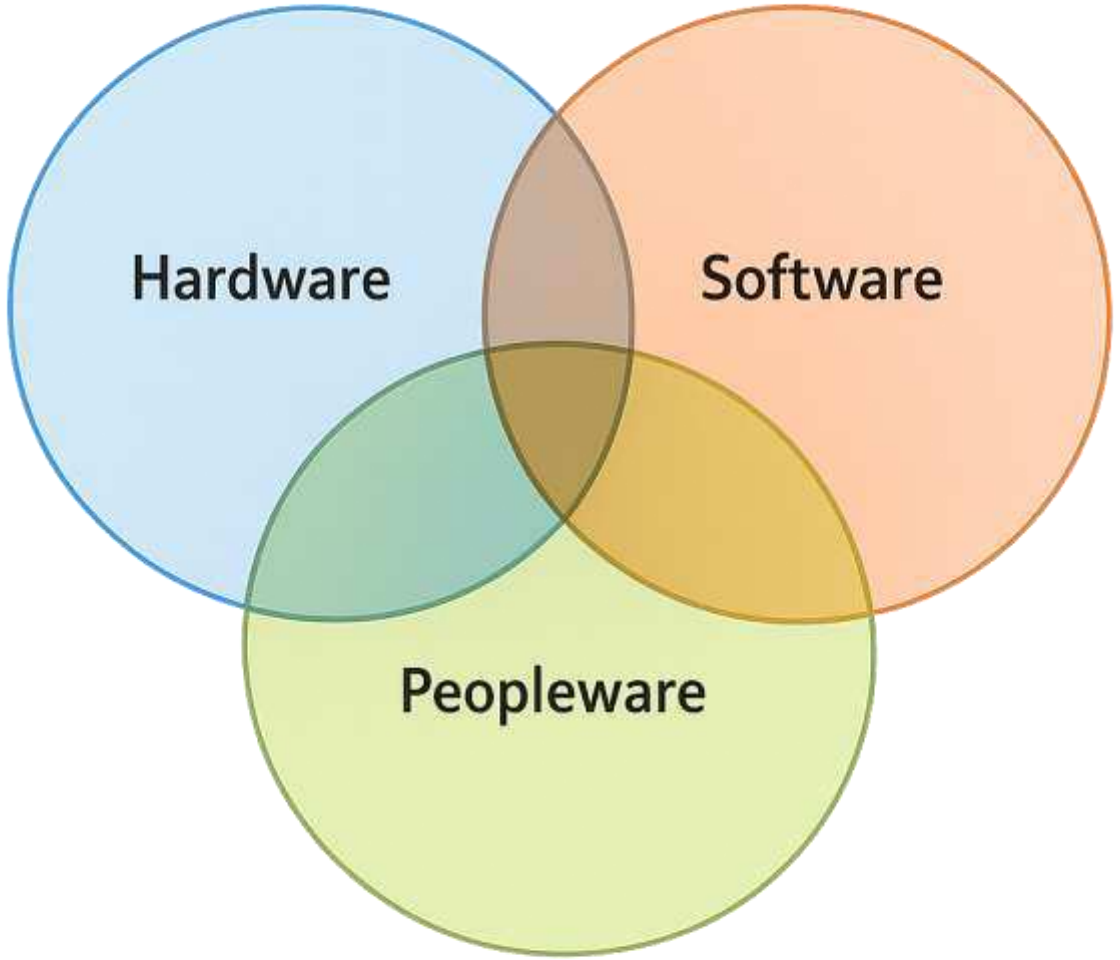
- Analýza a optimalizace SOC na základě Bezpečnostních událostí

Doba od zranitelnosti k zneužití

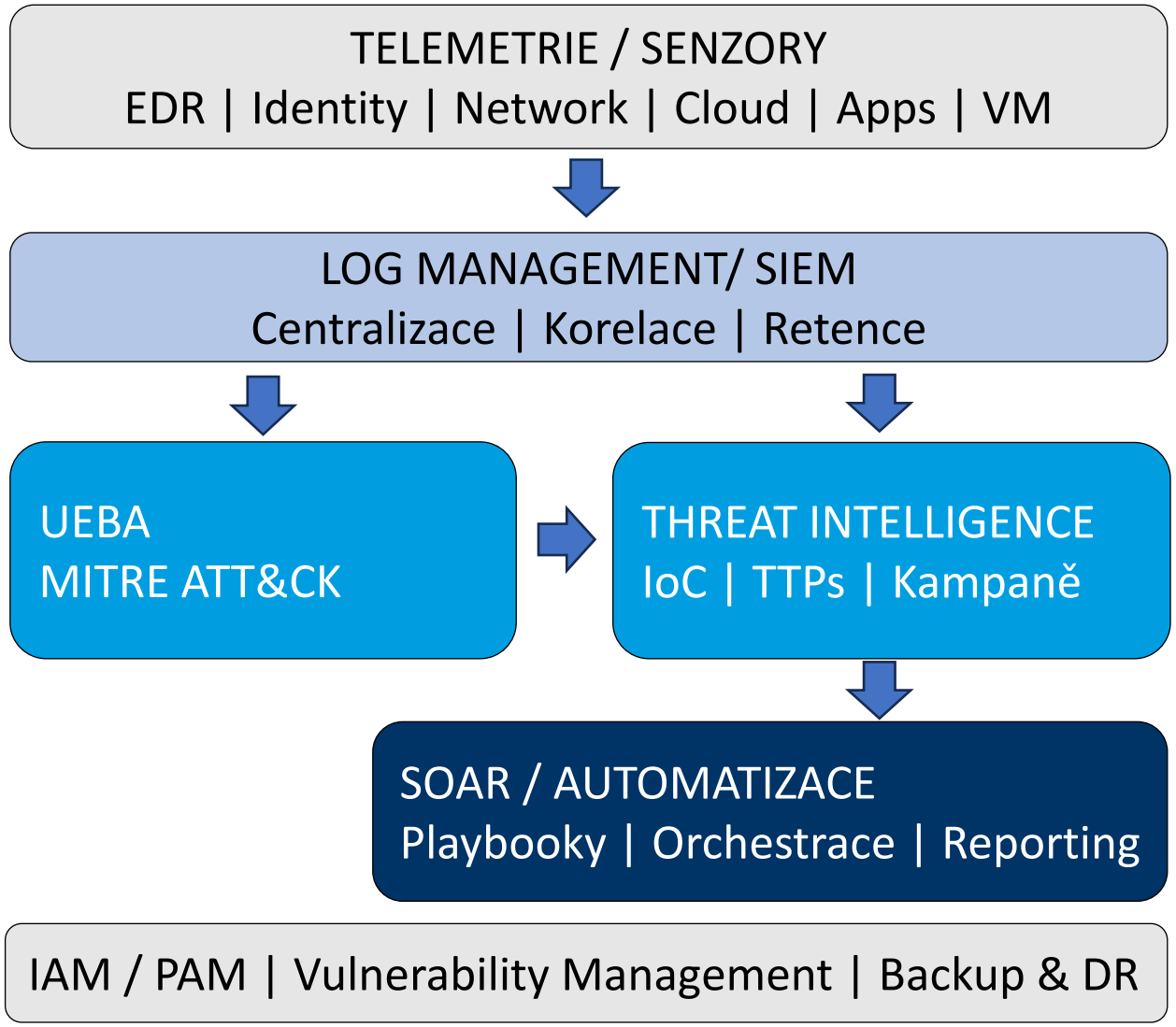
Doba od oznámení zranitelnosti k jejímu zneužití se kvůli AI významně zkrátila



Co potřebujeme pro SOC



Cílová Architektura SOC



Hardware (on-prem)

- Compute vrstva (SIEM / XDR / SOAR) 2–5 mil. Kč
  - 3–6 node cluster CPU: 16–32 cores / node RAM: 64–256 GB / node
- Storage 2–6 mil. Kč
  - Vstup: 50–200 GB/den
  - Hot storage: 5–10 TB; Cold storage: 50–200 TB
- Network vrstva 0,5–2 mil. Kč
  - Log collectors / forwardery; Load balancing ingestion; TLS šifrování
- Security appliances 1–3 mil. Kč
  - NDR / IDS senzory; Malware sandbox; Email / web security gateway

Celkem: 5–15 mil. Kč

Software (on-prem)

- Telemetrie / senzory (1,3 – 3,3 mil. Kč / rok)
- SIEM / Log Management (2,5 – 7,5mil. Kč / rok)
- CDR / XDR (1,1 – 2,8 mil. Kč / rok)
- Threat Intelligence (0,3 – 2,2 mil.Kč / rok)
- SOAR / Automatizace (1,6 – 5 mil.Kč / rok)
- Podpůrné domény (1,6 – 6 mil. Kč /rok)

Celkem: 12 – XX mil.Kč / rok

Hardware+Software (Cloud/Hybrid)

- Cloud nebo Hybrid
  - *Soulad s zákonem č. 264/2025 Sb., a prováděcími předpisy?*
  - *SLA?*
  - *Vendor lock?*
  - *Kde máte uložena data?*
  - *Veřejná zakázka?*
  - *Kdo provede integraci?*

Celkem: 5 – 18 mil.Kč / rok

Peopleware SOC

Role	Počet	Pokrytí	Poznámka	Průměrná měsíční mzda
L1 (Tier 1 monitoring)	10–14	24/7	1–2 analytici na směnu	56 000 min 560 000
L2 (Incident response)	6–10	24/7	min. 1 L2 na směnu (eskalace)	69 000 min 414 000
L3 (Threat hunting / expert)	2–4	pracovní doba	+ on-call	113 000 min 226 000
SOC Manager	4–5	24/7	duty manager / eskalace	89 000 min 356 000
SIEM / Detection engineer	2–3	pracovní doba	tuning, use cases	102 000 min 204 000
SOAR / automation engineer	1–2	pracovní doba	automatizace	96 000 min 96 000
Threat intelligence	1–2	pracovní doba	enrichment (CVE to KEV apod.)	79 000 min 79 000
Celkem	**26–40**			**1 935 000**

Počet zaměstnanců pro 24/7 = (počet lidí na směně × 5.5)

Peopleware pro provoz SOC

Oblast	Role	Počet	Průměrná mzda (Kč/měs)	Měsíční náklad min
Security & IT Support	Compliance + admin (mix)	4–8	70 000	280 000
	IAM / PAM + Vulnerability	3–5	90 000	270 000
	IT provoz (sysadmin, network)	6–10	108 000	648 000
Infrastructure & Facility	Facility management	3–5	63 000	189 000
	Fyzická ostraha 24/7	10–15	31 000	310 000
Další provoz	Úklid	1–2	27 000	27 000
	Recepce	2–3	33 000	66 000
	Údržbář	1–2	40 000	40 000
	BOZP / požární ochrana	1	57 000	57 000
	Administrativa / koordinace	1	38 000	38 000

AI driven SOC?

„AI SOC výrazně zvyšuje efektivitu, ale bez ochrany proti prompt injection může útočník ovlivnit samotné rozhodování SOC.“

Prompt injection = nové kritické riziko

- Útok na AI SOC skrz vstupní data -> manipulace s AI SOC
- **Vstupní data:** Logy (HTTP, DNS, User-Agent); Email / phishing; Threat Intelligence feedy; Externí data (API, OSINT)
- **Dopad na AI SOC:** False negatives (plánovaný útok projde); Manipulace priorit incidentů; Exfiltrace dat; Degradace modelu (poisoning)

= AI nesmí být plně autonomní, AI musí být kontrolován člověkem

Bezpečnostní monitoring - výstup

- Zvolíte On-Prem, Hybrid či Cloud
  - *Postavíte si jej sami, či vám jej bude provozovat třetí strana?*
- SPCSS
  - Od založení provádíme Bezpečnostní monitoring
    - CSIRT - SPCSS
    - „Řízená bezpečnostní služba“ pro bezpečnostní úrovně 3 a 4
  - To, co již máte, jsme schopni integrovat

Děkuji za pozornost

Prostor pro vaše dotazy