Kybernetická bezpečnost ve zdravotnictví

Odhalení skrytých slabin vaší infrastruktury

3. 12. 2020

Trusted partner for your **Digital Journey**

Atos Gold Business Partner IBM

AGENDA

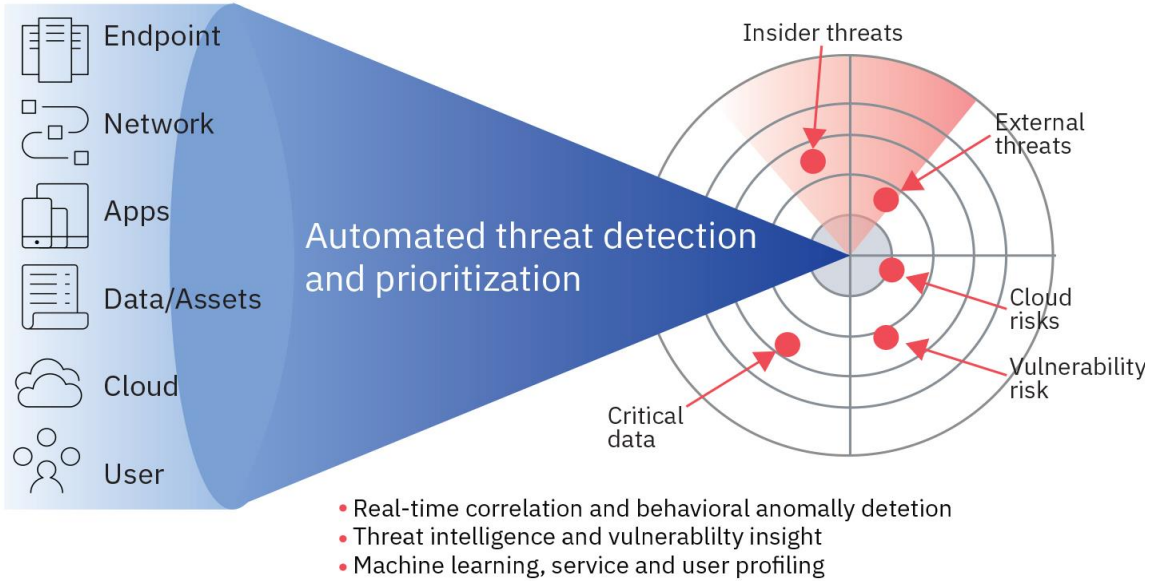
1 SIEM bezpečnostní nástroje pro sběr a vyhodnocení dat

2 Praktické zkušenosti z implementace

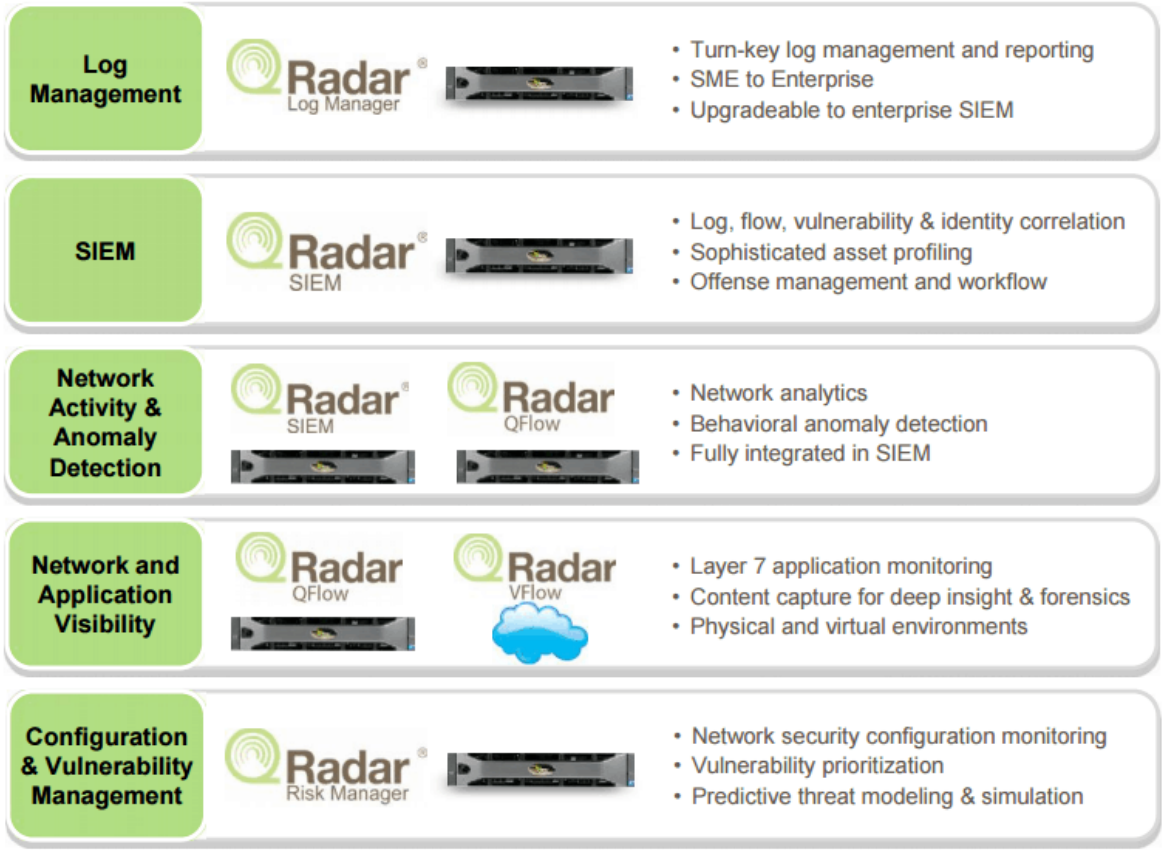
3 Analytika a SOC

Co je to SIEM

- SIEM (Security Information and Event Management) je specializované řešení, které umožňuje sbírat, korelovat a analyzovat události ze všech možných vrstev IT infrastruktury a mnoha zařízení. (Sběr dat | Detekce| Vyšetřování | Reakce)



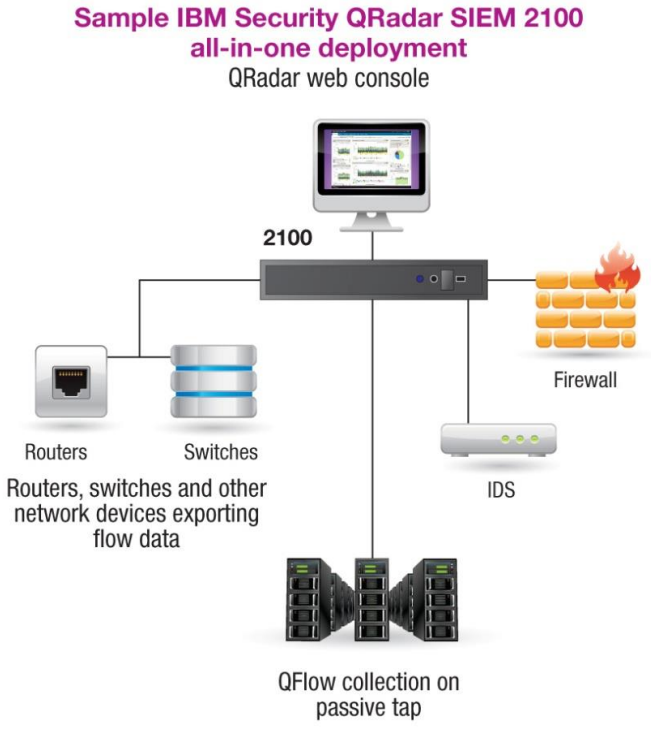
IBM Security QRadar

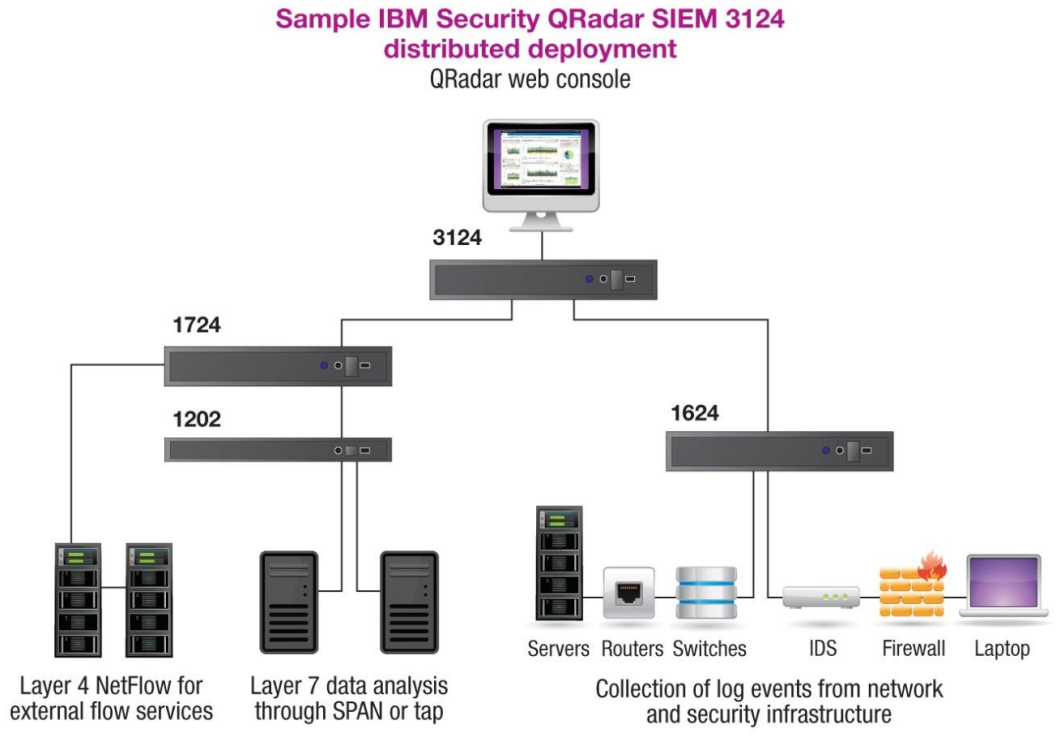


Aktuální verze:
IBM® QRadar® 7.4.1

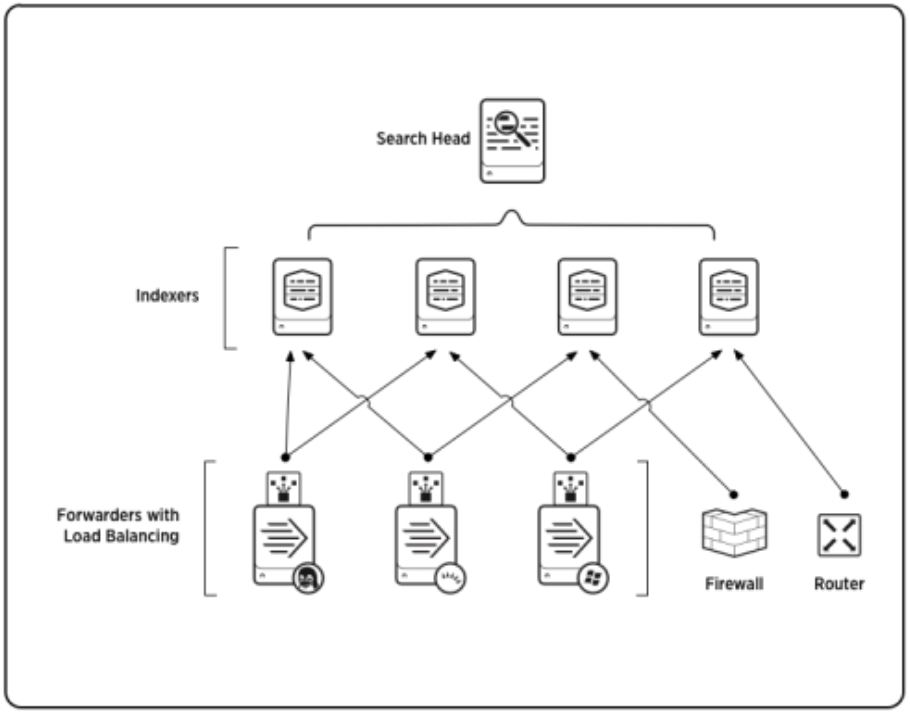
Tato verze přináší celkově vyšší výkon, lepší zabezpečení, vylepšení workflow a lepší kontrolu toků (flow).
Nový update server.

IBM Security QRadar



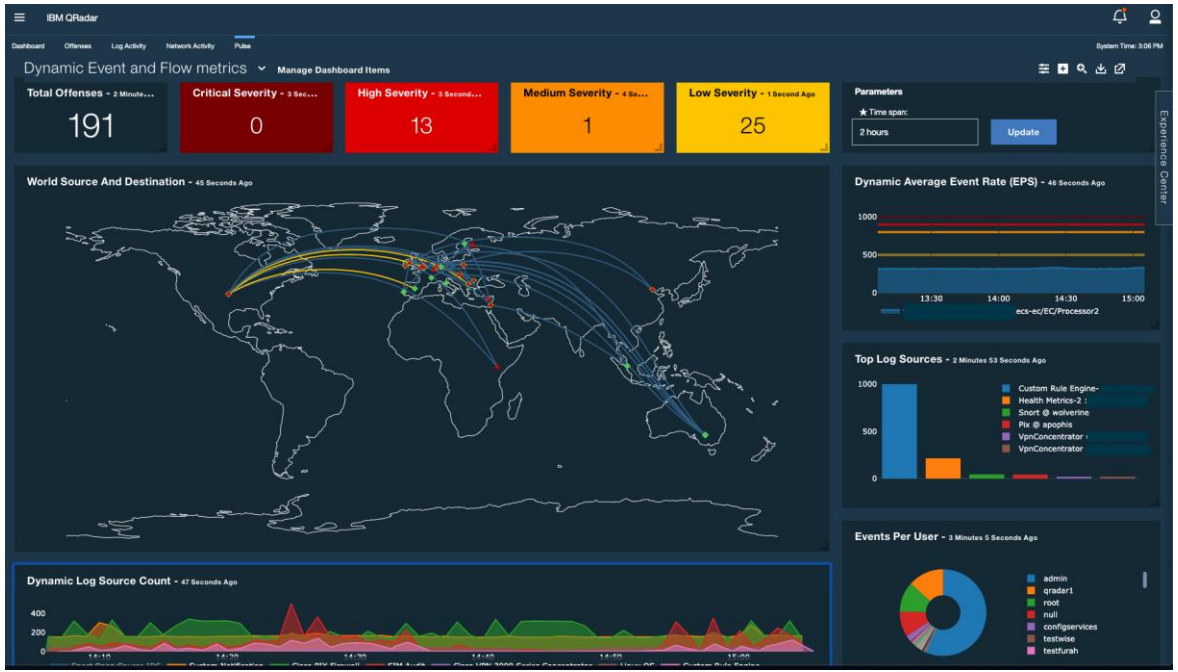


SPLUNK



- **Search head**
- **Indexer**
- **Forwarder**
- **Deployment server**

IBM Security QRadar Apps



- Log Source Manager
- Use Case Manager
- User Behavior Analytics
- Threat Intelligence App
- Advisor with Watson
- QRadar Pulse
- QRadar Assistant

Zkušenosti z implementace

Implementace zaměřené na splnění požadavků Zákona č. 181/2014 Sb.

Vyhlášky č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

- § 11 - Řízení přístupu a bezpečné chování uživatelů
- § 21 - Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů
- § 22 - Nástroj pro detekci kybernetických bezpečnostních událostí
- § 23 - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

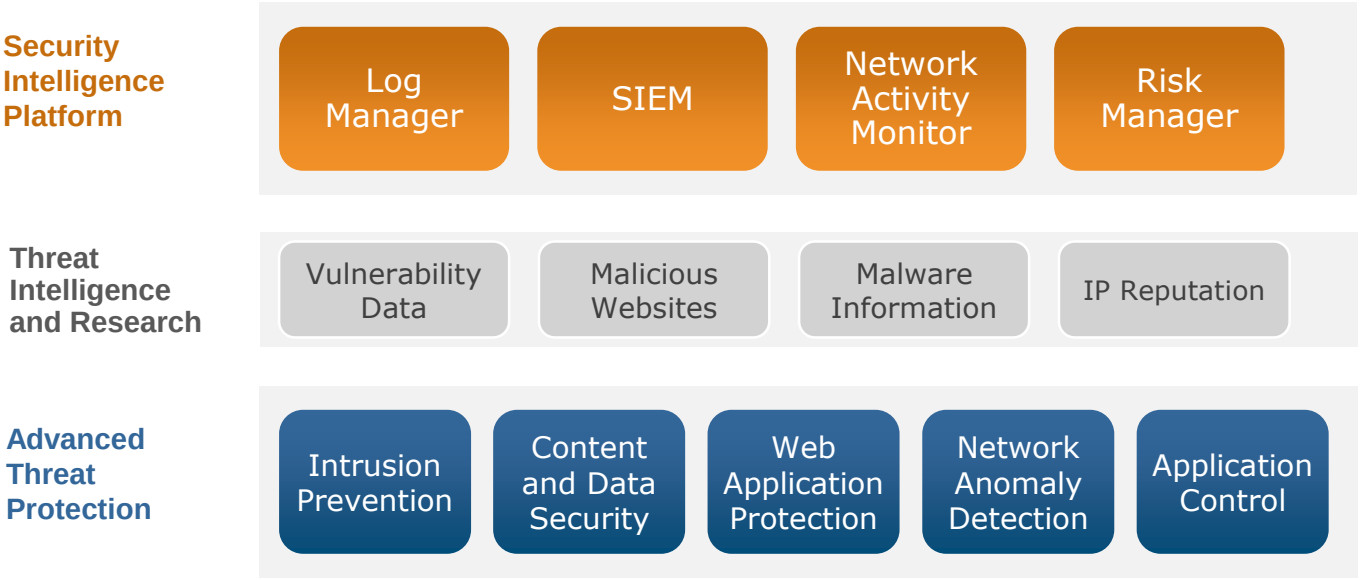
Zkušenosti z implementace

- Při implementaci SIEM nástroje není podstatný počet use case, korelací nebo reportů dodaných od výrobce. Nejdůležitější je možnost konfigurovat stávající korelace a reporty + vytvářet nové korelace a reporty na míru podle zákazníka.

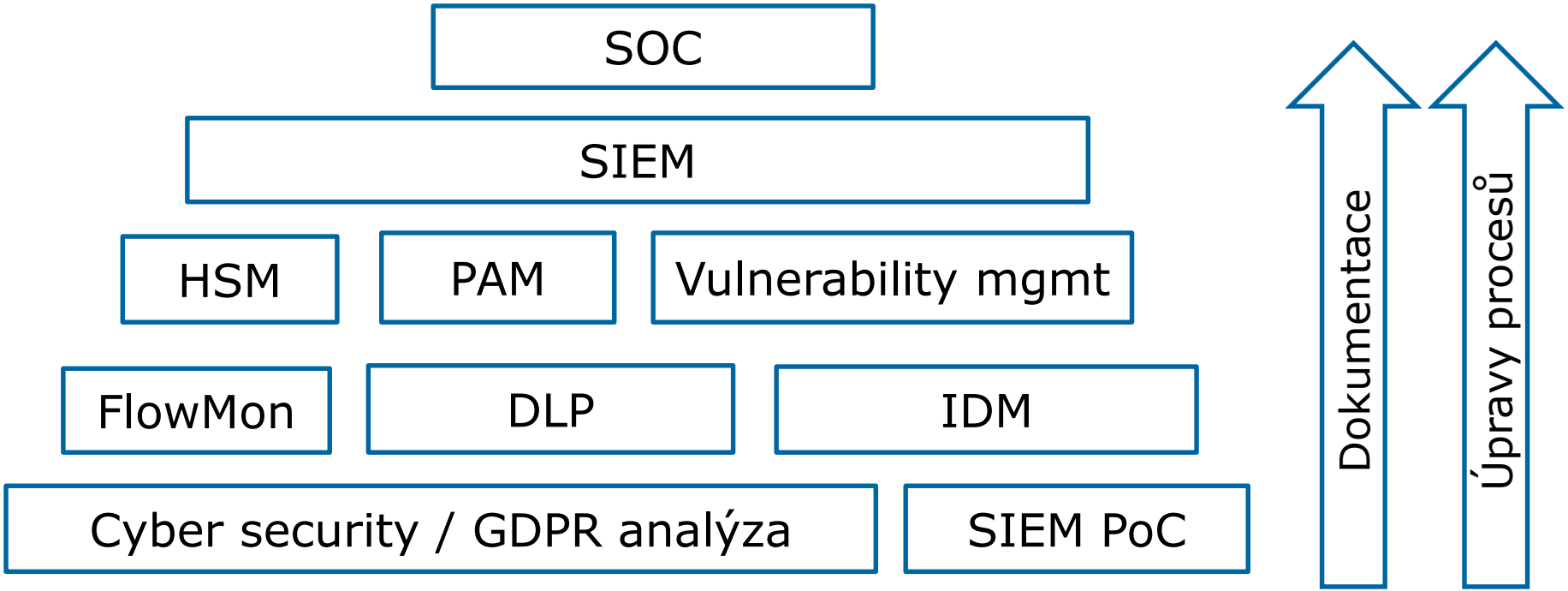
- SIEM nástroje nelze implementovat stylem „nastav a zapomeň (máme splněno)“ SIEM vyžaduje persistentní aktualizace a řádnou provozní a aplikační péči.

- Pro správně fungující SIEM je důležité definovat vhodné use case. Ideálně dopředu včetně zdrojů logů pro korelaci, popisu projevů a požadované reakce.

Zkušenosti z implementace



Zkušenosti z implementace

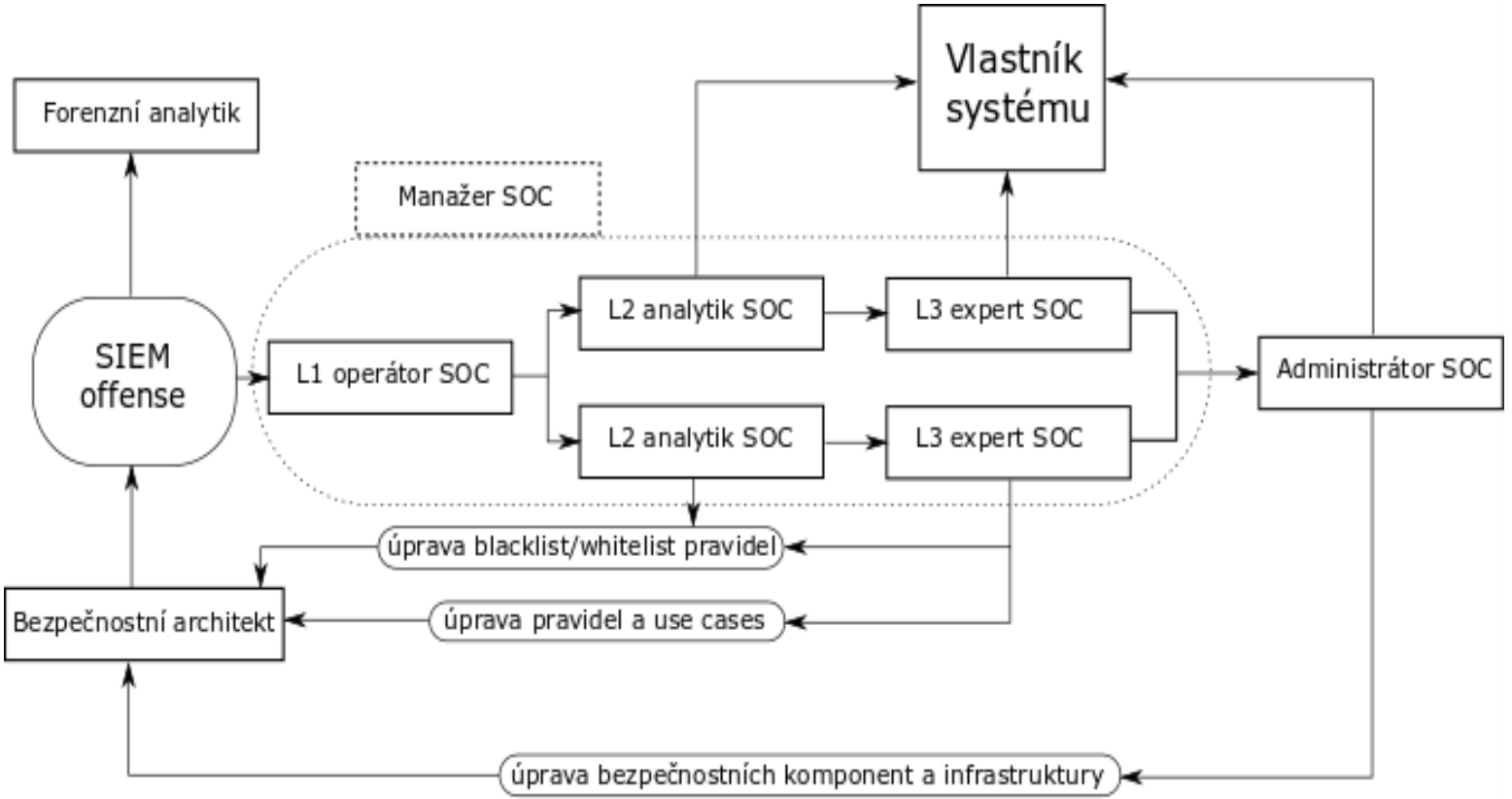


Security Operation Centrum (SOC)

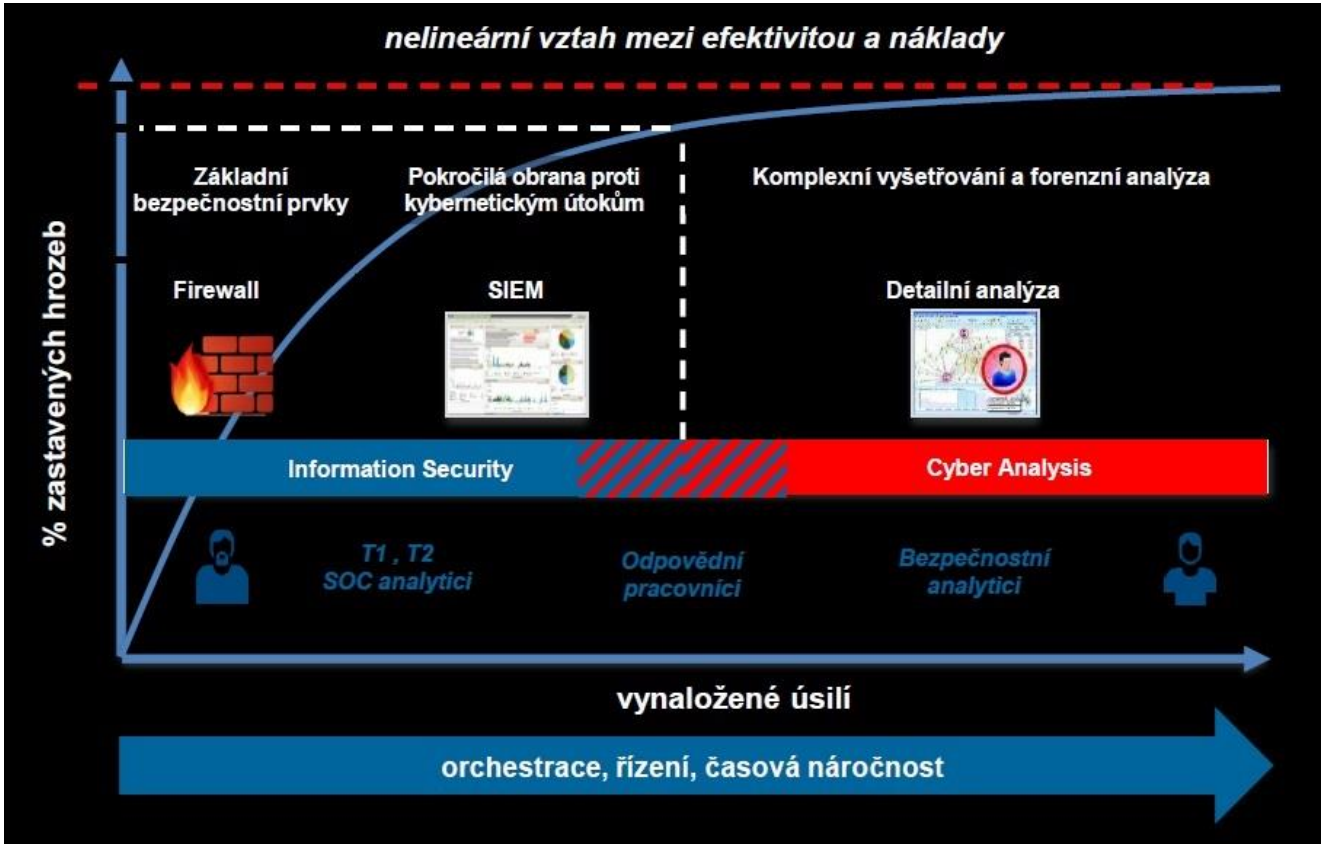
- Security Operation Centrum (SOC)
  - Bezpečnostní dohledové centrum (nikoli provozní dohled)
  - Kontrolní činnosti
  - Operativa a správa bezpečnostních událostí
  - Správa incidentů
  - Vyšetřování
  - Zvládání následků incidentů.

- Zavedení SOC přináší nové role, specifická workflow, procesy a požadavky.

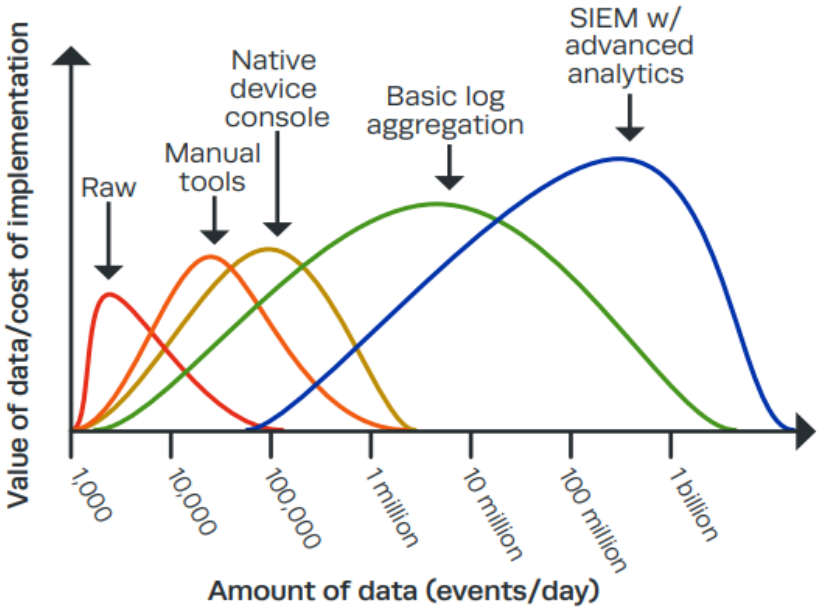
Implementace SOC



Implementace SOC



Hodnota dat


Value of data/cost of implementation
Raw
Manual tools
Native device console
Basic log aggregation
SIEM w/ advanced analytics
1,000
10,000
100,000
1 million
10 million
100 million
1 billion
Amount of data (events/day)

Zdroje

Ten Strategies of a World-Class Cybersecurity Operations Center MITRE
https://www.ibm.com/security
https://cybersecurity.cz/
https://www.splunk.com/

Děkuji

Kontakt:
Petr Němec
M+ +420 739 587 672
petr.nemec@atos.net

Gold
Business
Partner