

Kybernetická bezpečnost ve zdravotnictví

Odhalení skrytých slabín vaší infrastruktury



3. 12. 2020

Trusted partner for your Digital Journey

© Atos

Atos
Gold
Business
Partner

IBM.

AGENDA

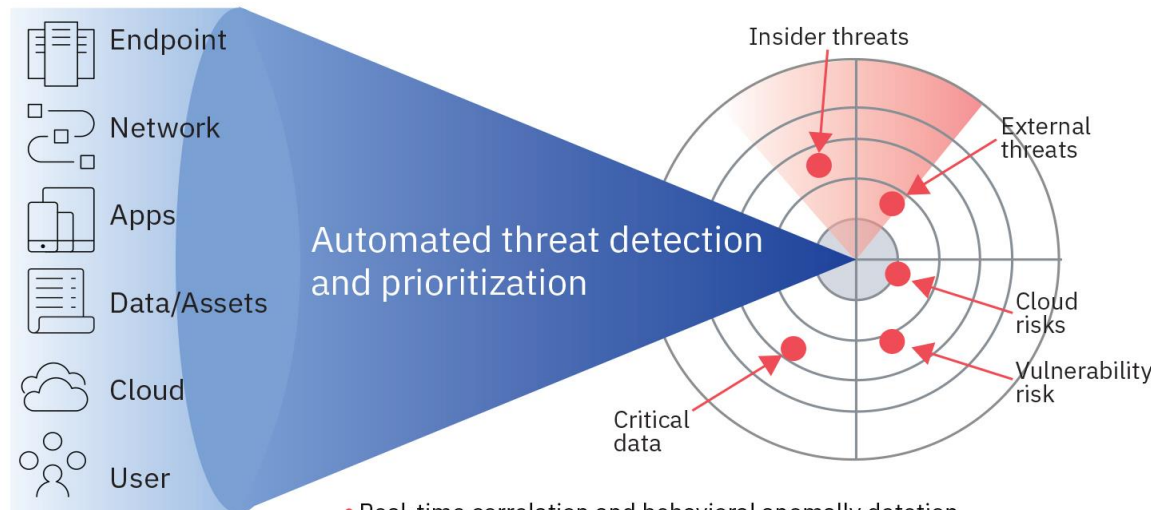
1 SIEM bezpečnostní nástroje pro sběr a vyhodnocení dat

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)



- Real-time correlation and behavioral anomaly detection
- Threat intelligence and vulnerability insight
- Machine learning, service and user profiling



IBM Security QRadar

Log Management	 	<ul style="list-style-type: none">• Turn-key log management and reporting• SME to Enterprise• Upgradeable to enterprise SIEM
SIEM	 	<ul style="list-style-type: none">• Log, flow, vulnerability & identity correlation• Sophisticated asset profiling• Offense management and workflow
Network Activity & Anomaly Detection	   	<ul style="list-style-type: none">• Network analytics• Behavioral anomaly detection• Fully integrated in SIEM
Network and Application Visibility	   	<ul style="list-style-type: none">• Layer 7 application monitoring• Content capture for deep insight & forensics• Physical and virtual environments
Configuration & Vulnerability Management	 	<ul style="list-style-type: none">• Network security configuration monitoring• Vulnerability prioritization• Predictive threat modeling & simulation

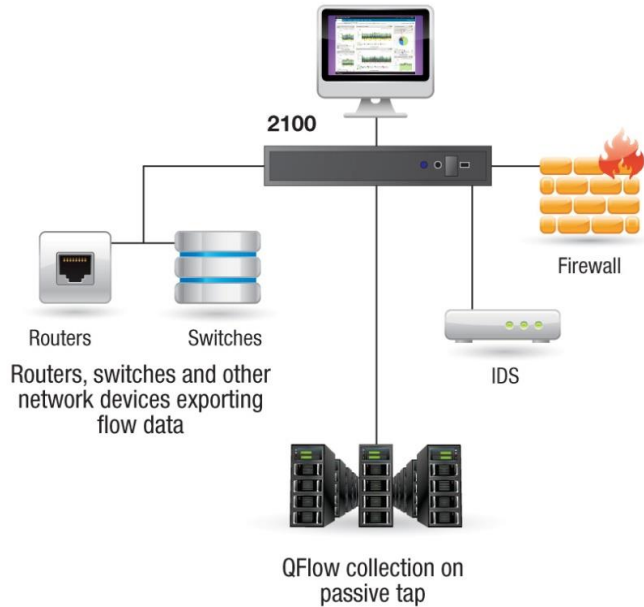
Aktuální verze:
IBM® QRadar® 7.4.1

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

IBM Security QRadar

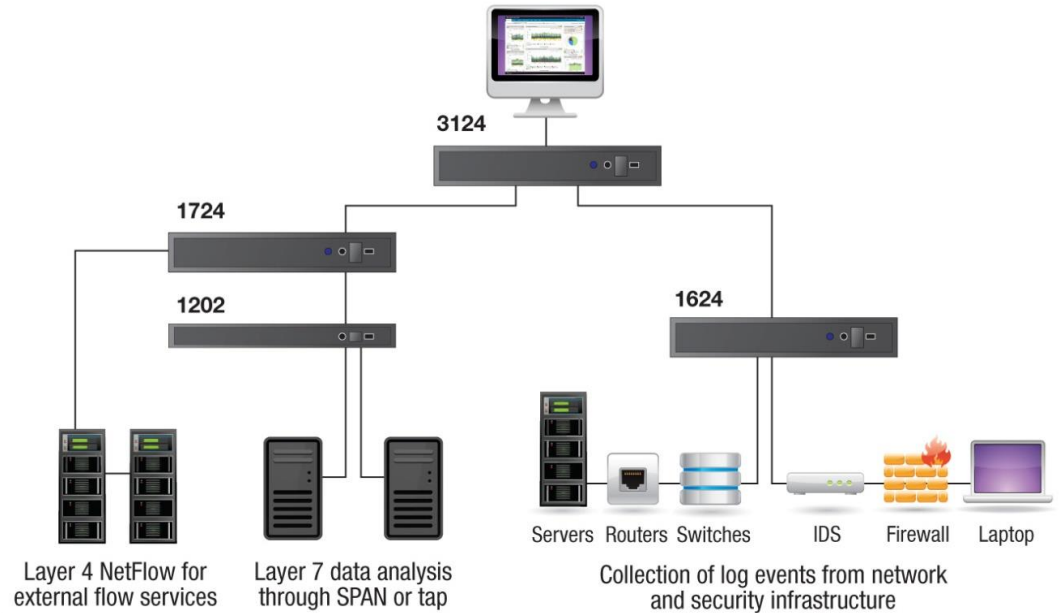
Sample IBM Security QRadar SIEM 2100 all-in-one deployment

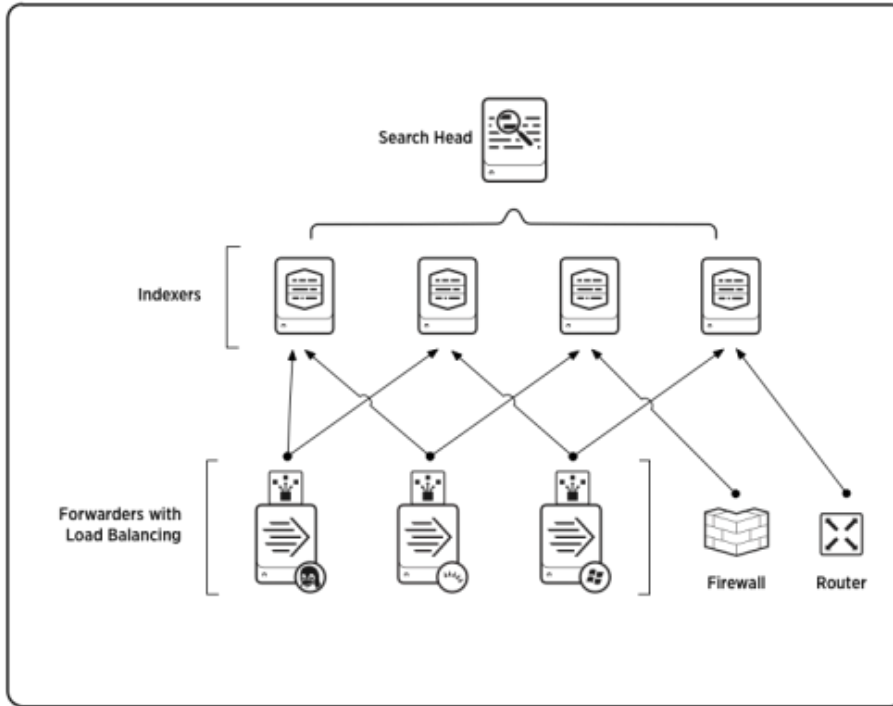
QRadar web console



Sample IBM Security QRadar SIEM 3124 distributed deployment

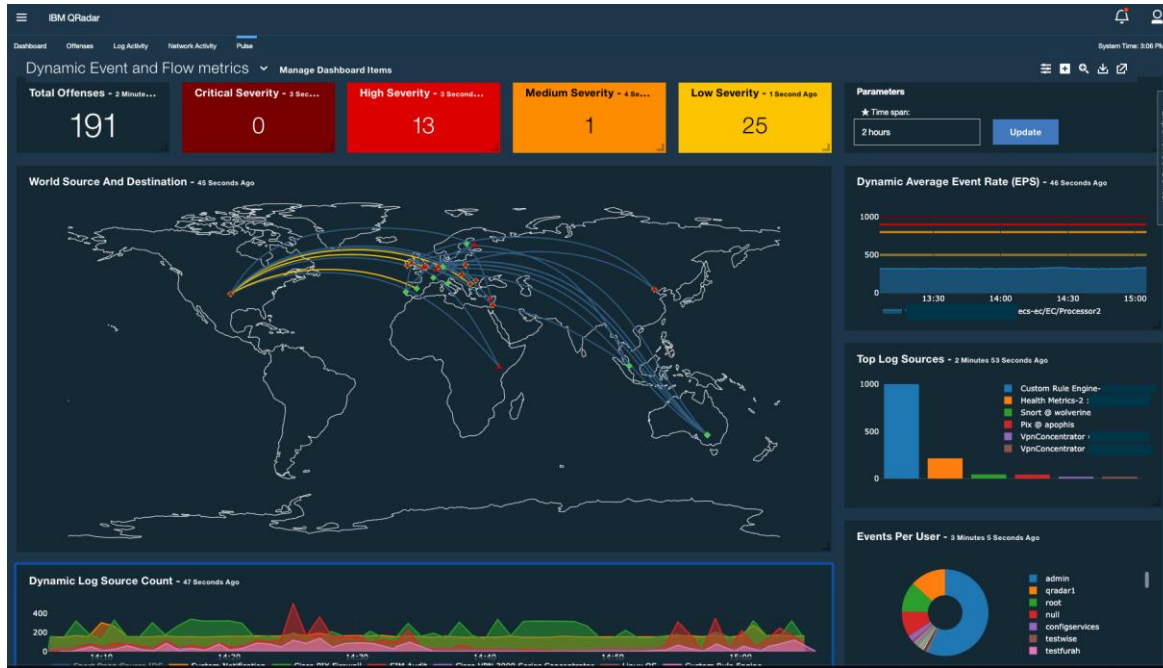
QRadar web console





- ▶ **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

Security Intelligence Platform

Log Manager

SIEM

Network Activity Monitor

Risk Manager

Threat Intelligence and Research

Vulnerability Data

Malicious Websites

Malware Information

IP Reputation

Advanced Threat Protection

Intrusion Prevention

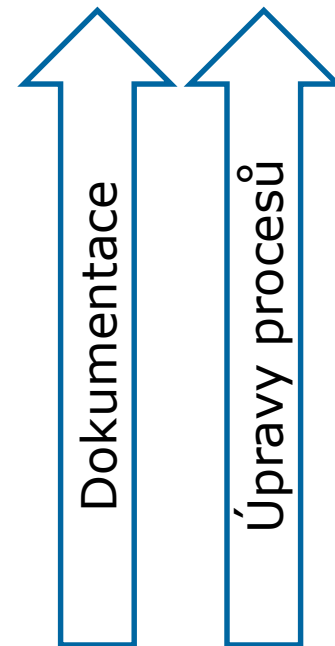
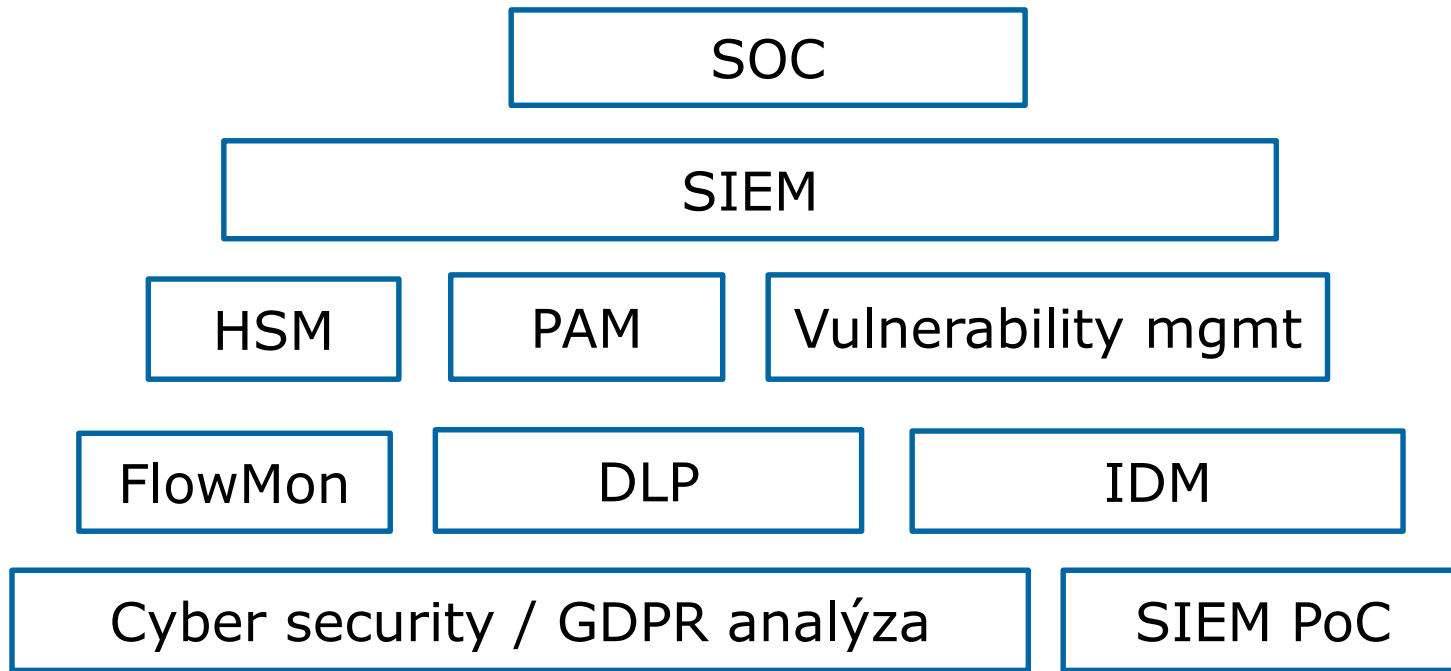
Content and Data Security

Web Application Protection

Network Anomaly Detection

Application Control

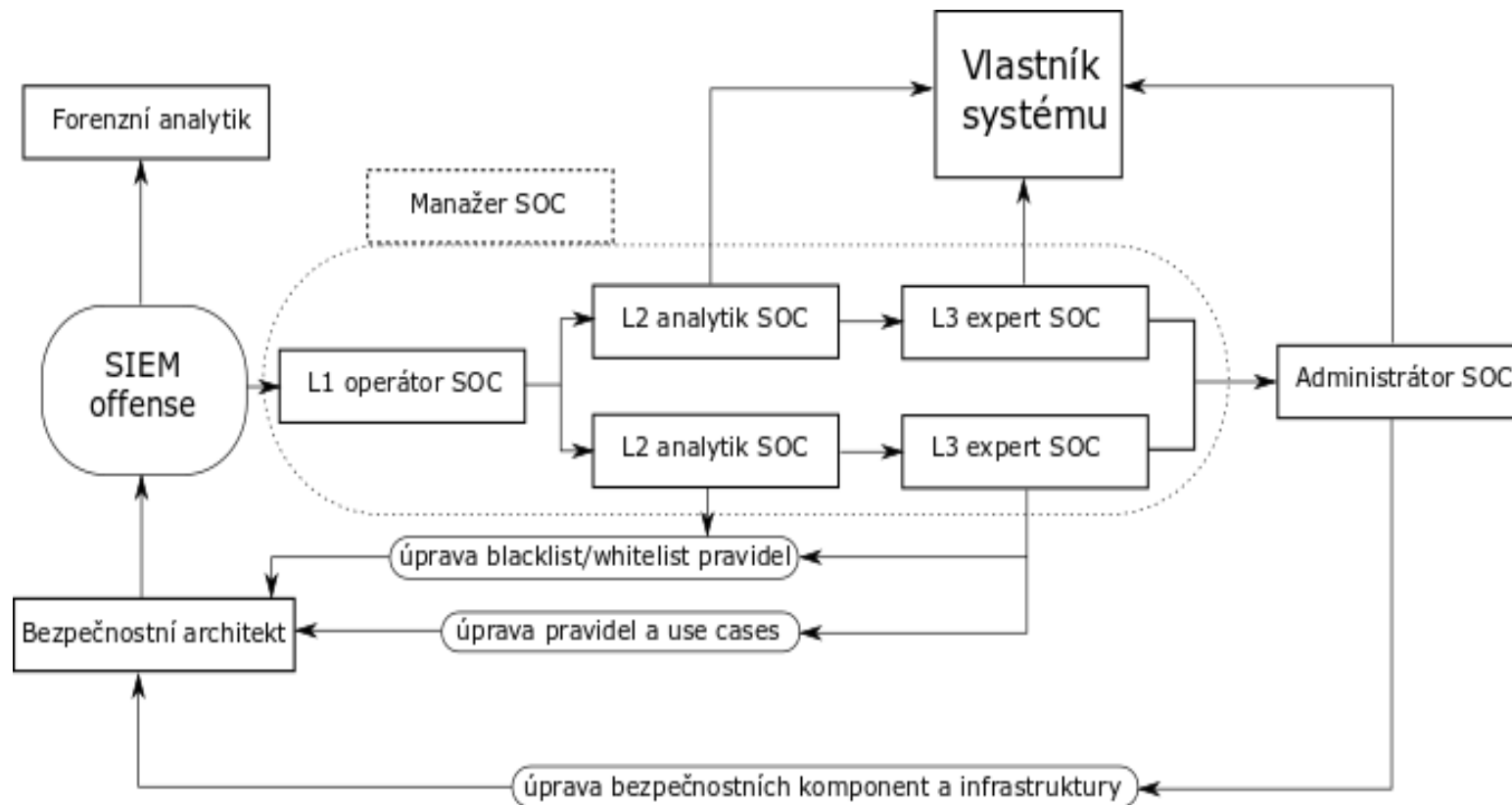
Zkušenosti z implementace



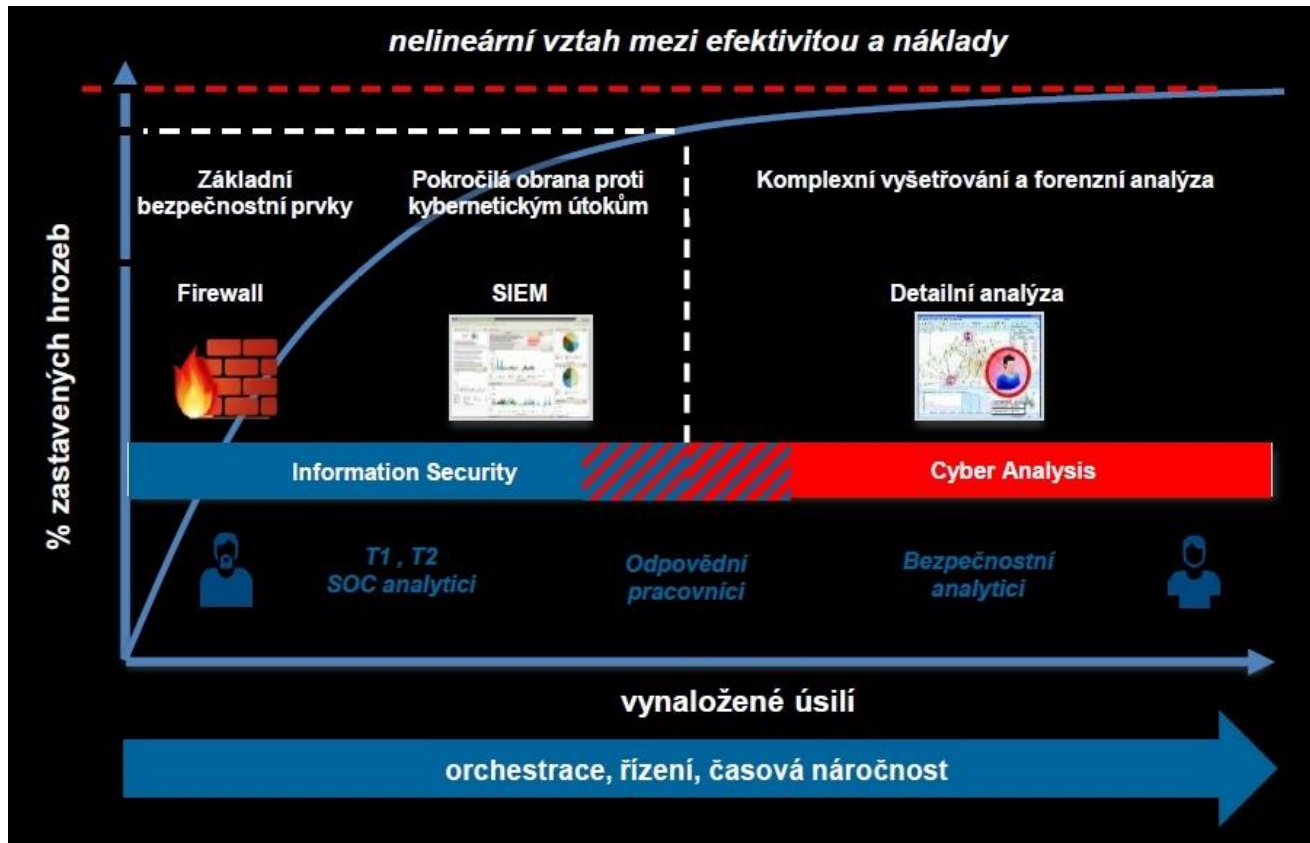
Security Operation Centrum (SOC)

- ▶ 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.

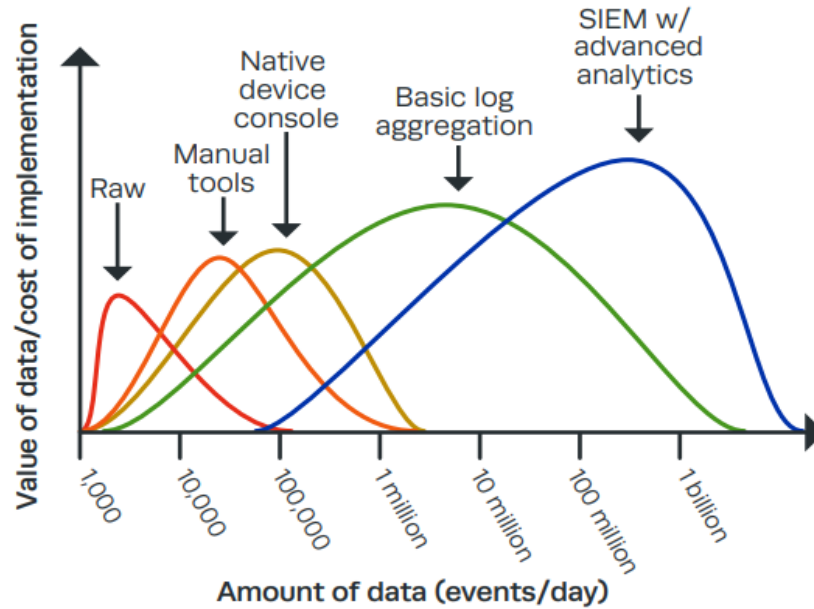
Implementace SOC



Implementace SOC



Hodnota dat



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

Atos, the Atos logo, and Atos|Syntel are registered trademarks of the Atos group. October 2020. © 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

Atos

**Gold
Business
Partner**

IBM