



Ako vychovať SIEM?

Obdobie puberty

ITAPA 2018

Ing. Filip Mikuš

Security Specialis, Aliter Technologies

22.05.2018



Potrebujem vlastne SIEM?



The Security Sector Is Dynamic And Vast. We Are Ceaseless & Vigilant In Our Coverage.

The image displays 18 panels of cybersecurity logos, organized into the following categories:

- Infrastructure Security:** Network Firewall (Palo Alto, Fortinet, Cisco, etc.), Network Monitoring (Blue Coat, ThousandEyes, etc.), Intrusion Prevention Systems (Cisco, Snort, etc.), Unified Threat Management (Cisco, Palo Alto, etc.).
- Endpoint Security:** Endpoint Protection & Anti-Virus (McAfee, Symantec, etc.), Endpoint Detection & Response (CrowdStrike, SentinelOne, etc.), Messaging Security (Proofpoint, Mimecast, etc.).
- Application Security:** WAF & Application Security (Akamai, Cloudflare, etc.), Vulnerability Assessment (Checkmarx, SAST tools, etc.), Web Security (Zscaler, Cloudflare, etc.).
- IoT Security:** Various IoT security solutions like MOCANA, ARM, etc.
- Security Operations & Incident Response:** SIEM (Splunk, IBM, etc.), Security Incident Response (IBM, Palo Alto, etc.), Risk & Compliance (RSA, Archer, etc.).
- Threat Intelligence:** BrightPoint, ThreatConnect, etc.
- Mobile Security:** Lookout, MobileIron, etc.
- Data Security:** Veeva, Veracode, etc.
- Cloud Security:** Duo, Okta, etc.
- Transaction Security:** Feedzai, Sift Science, etc.
- Specialized Threat Analysis & Protection:** FORTISCALE, Ray Dynamics, etc.
- Identity & Access Management:** Okta, Ping Identity, etc.

Source: Momentum Partners

Kde mi môže SIEM pomôcť?

- **Rozoznanie bežného a podozrivého správania**
- Dodržiavanie nariadení a štandardov (PCI-DSS, ISO27000, HIPAA, **GDPR**, atď.)
- Pohľad na bezpečnosť - „big picture“
- Zber, analýza, korelácia a retencia logov z jednotlivých zdrojov
- **Urýchlenie detekcie a reakcie** na bezpečnostné incidenty
- **Úspora peňazí** vďaka efektívnemu riadeniu rizík

Ako neúspešne nasadiť SIEM

1. „Pomocou SIEMu riešim všetky bezpečnostné problémy v našej organizácii za jeden deň“
2. „Je to len centrálny kolektor logov, nasadenie nemôže byť technicky náročné“
3. „...aké bezpečnostné politiky?“
4. „To zvládneme sami, admini nemusia o ničom vedieť“
5. „Veď to len nahádzeme do rackov, zapojíme do siete a presmerujeme logovanie, pohoda“
6. „Okej, treba tam na začiatku nastaviť nejaké politiky, ale potom to už bude samostatne fungovať“



Ako vychovať SIEM?



Ako začať s výchovou SIEM-u

■ Definovanie Data Sources

- v prvej fáze sa zamerať na kritické zariadenia
- určiť severitu zbieraných logov

■ Upratovanie udalosti

- normalizácia, parsovanie, filtrovanie logov

■ Korelácie

- definovanie vzťahov medzi udalosťami
- potrebná znalosť, ako systém funguje a čo chcem dosiahnuť koreláciou
- opieranie sa o bezpečnostné procesy a politiky

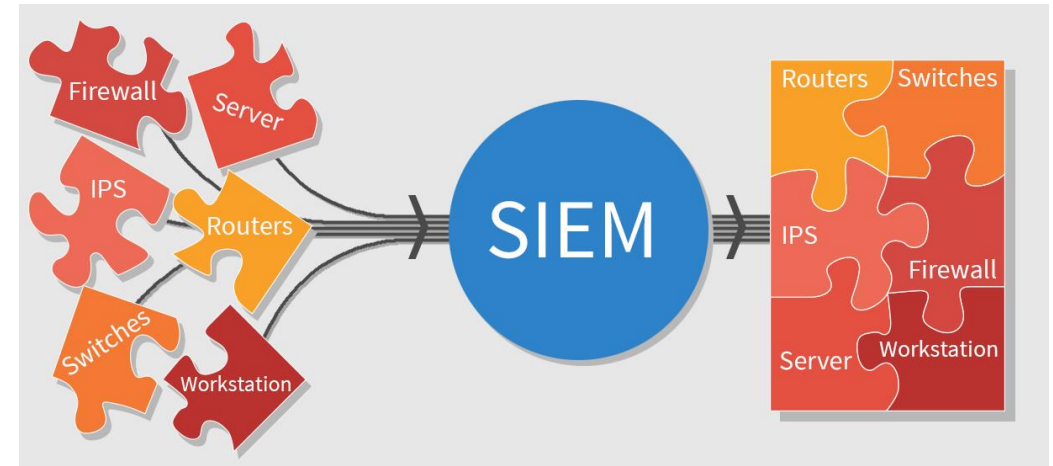
■ Integrácia a obohatenie udalosti

- integrácia so systémami tretích strán AV, VA, Flowmon ADS, MS AD, Cyber Threat Feeds, ...

■ Reporty a alarmy

- prehľad bezpečnosti a kondície systému v podobe grafov, tabuliek a štatistík
- alarmy uľahčia sledovanie niektorých aktivít na ktoré sme upozornení v prípade problému

■ Životný cyklus – aby výchova nezlyhala



Životný cyklus

