Cesta k efektívnej kybernetickej bezpečnosti

Security Operation Center

Peter Jankovský, CTO & Principal Security Architect, **AXENTA a.s.**

AGENDA

- Čo je to „bezpečnostný dohľad“?
- Čo je to SOC?
- Čo je to SOC 2.0?
- Prevádzka SOC

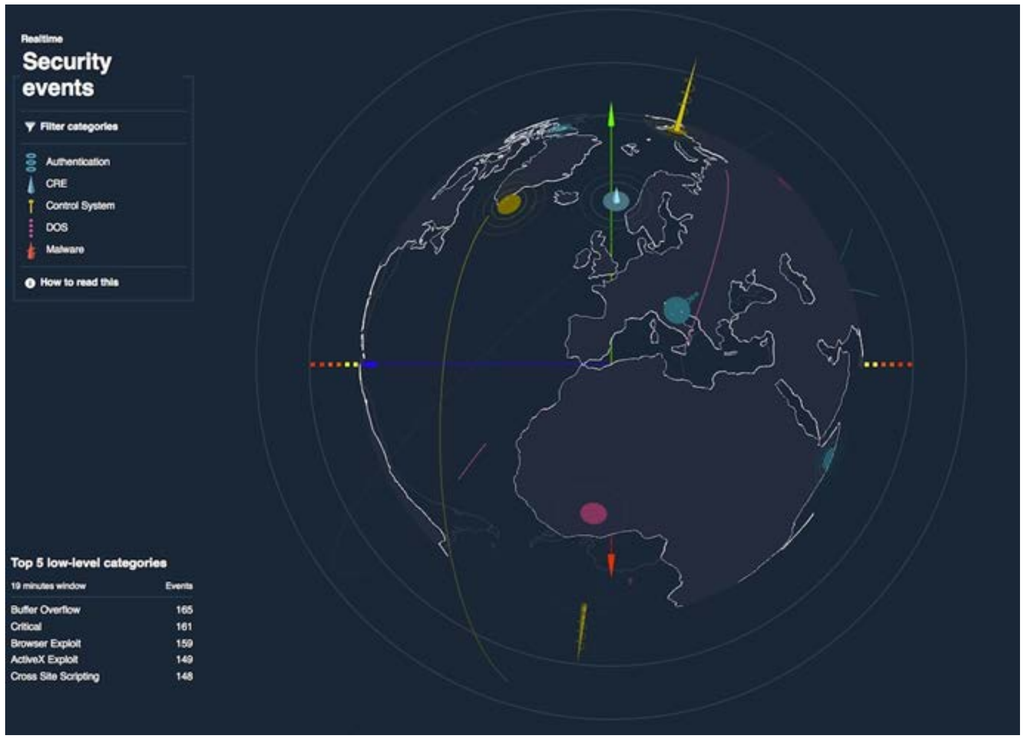
Čo je to „bezpečnostný dohľad“?

Log Management
Auditná stopa - RAW, archivácia, full-text search
Identifikácia logov, ich analýza a napojenie

SIEM
Korelácia v reálnom čase, reporting, dashboardy
Rule based

Ľudia
Bezpečnostný špecialista
20% FTE

Assety
Informácie o prostredí, IP plány
bez procesov o vzniku/zániku zariadení



Čo je to „SOC“? A hlavne čo nie je SOC!

Security Operation Center
Bezpečnostné Prevádzkové Centrum

SOC vs Managed Security Services
Externé a Interné penetračné testy
FW konfigurácie
WAF, NAC, DLP...

SOC -> Incident Response (CSIRT)
Zakladanie incidentov
Riešenie incidentov / CSIRT tím

SOC & Kybernetický zákon (ČR)
+/- 85 požiadaviek na súlad
Menej než 20% je o dohľade bezpečnosti

SOC ≠ Incident Response (CSIRT)

Log Management + SIEM
Auditná stopa, Detekcia, Reporting, Dashboardy
Hunting – hľadanie neznámeho v neznámom

Tickety
Service Desk / Help Desk
Štart Incident Response

Procesy a Ľudia
Interné predpisy a postupy
24/7

Assesment
Informácie o prostredí, zraniteľnosti
Business Impact

Čo je to „SOC 2.0“?

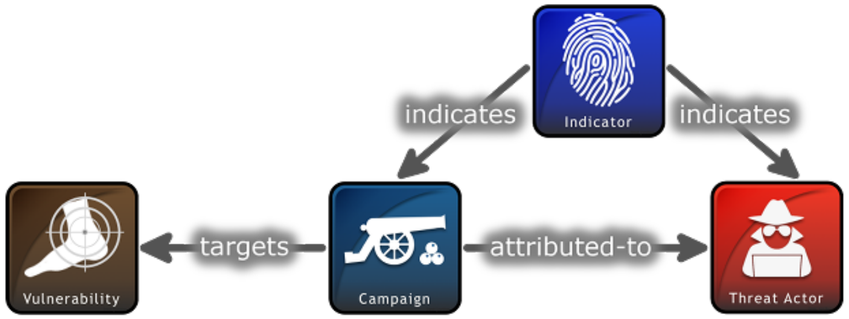
Threat Inteligence

Global EARLY-warning system

- Tactical
- Technical
- Operational

STIX, TAXII

- Structured Threat Information Expression
- Trusted Automated Exchange of Intelligence Information



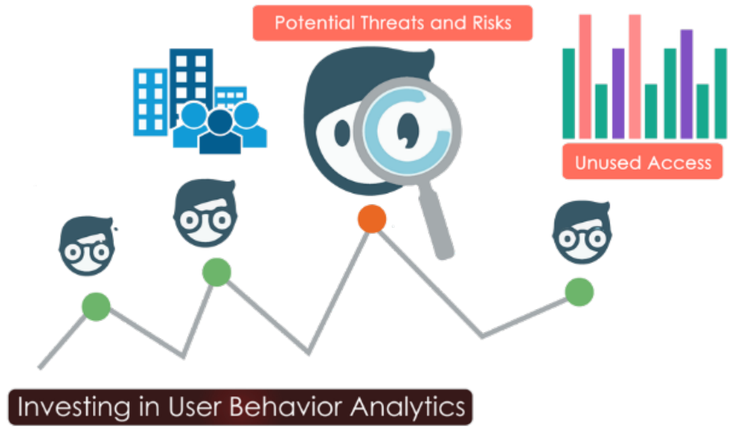
Advanced Analytics

User and (E)ntity Behavior Analytics

Network Behavior Analytics

Machine Learning / Statistics / Baselines

- *Time*
- *Biometrics (Keystroke, Mouse Movements)*



Prevádzka SOC 2.0

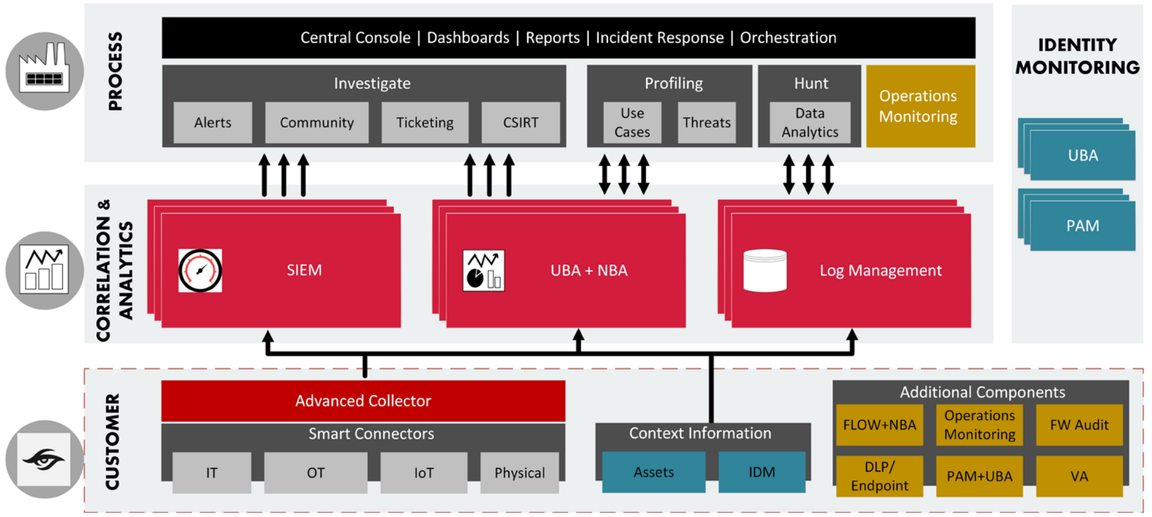
Software
Event Management, SIEM, UBA, NBA,
Prevádzkový monitoring, Ticketing, Dashboardy

Analytika
Hunting Unknown Unknowns
Reporting/KPI
Threats Exchange

Ľudia

Procesy
Incident Response, konzultácie, tvorba obsahu, vzdelávanie

Cyber SOC



Ďakujem za pozornosť

Peter Jankovský

Principal Security Architect

AXENTA
Bezpečnost informací je pro nás na prvním místě

efocus.sk