Security Operation Center (nejen) jako řešení požadavků Zákona o Kybernetické Bezpečnosti

marec@axenta.cz

Denis Marec, manažer rozvoje a obchodu

AXENTA

Kdo jsme / víme jak na to

© 2009 [2002]

Reference

Financial

Česká průmyslová zdravotní pojišťovna
STÁTNÍ TISKÁRNA CENIN, státní podnik
CREDITAS
ČESKÁ POJIŠŤOVNA
ČMSS
Na těchto základech můžete stavět
KB
Allianz
VÚB BANKA
MONETA MONEY BANK
DanubePay
ŠKODA PRAHA Invest
ERSTE Group IT
ČS ÚVĚRNÍ DRUŽSTVO
SPRÁVA ŠTÁTNYCH HMOTNÝCH REZERV SLOVENSKEJ REPUBLIKY
PPF Banka

Utility

T-Mobile
orange
TEPLÁRNY BRNO
Teko TEPLÁREŇ KOŠICE
O2
O2 IT Services
DISTRIBUCE
ČEZ
Řízení letového provozu České republiky
SAKO
ČEPRO
ČEPS, a.s.

Public + ostatní

Jihomoravský kraj
Ministerstvo obrany České republiky
ASBIS
Ministerstvo dopravy
MINISTERSTVO ZEMĚDĚLSTVÍ
MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR
PRAHA MĚSTSKÁ ČÁST
MINISTERSTVO OBRANY SLOVENSKEJ REPUBLIKY
Oblastní nemocnice Kladno, a.s.
ZOS Trnava, a.s.
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
ombudsman veřejný ochránce práv
GoodData
NOVARTIS

Reference

Security monitoring/LM

PIM/PAM

Procesy

Bezpečnost

Procesy

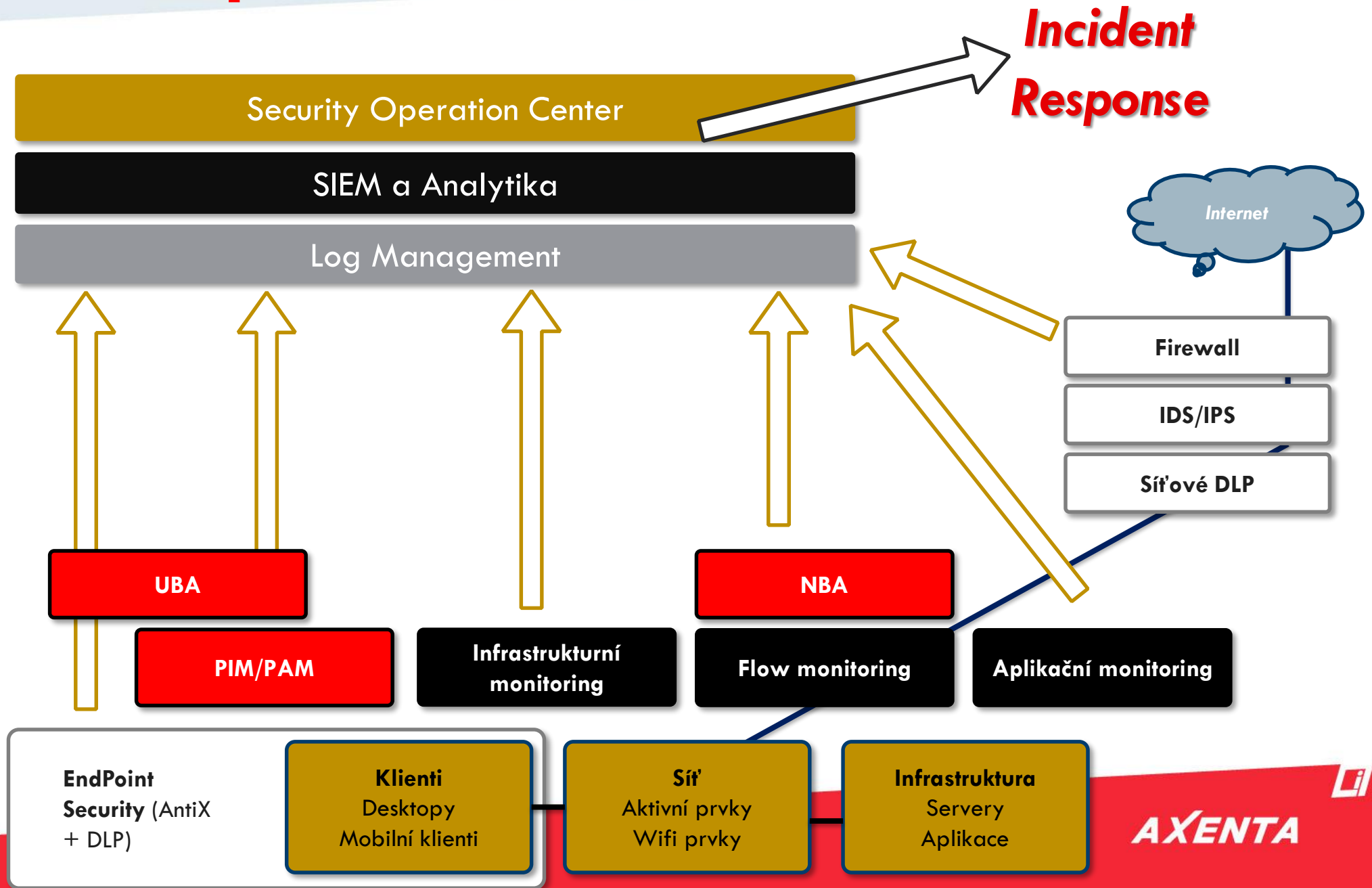
- ***GDPR***
- *Analýzy rizik, procesů a informací*
- ***Kybernetická bezpečnost***
- *Incident Response*
- *Školení*

Monitoring

- ***Security Operation Center***
- *Network Behavior Anomaly (NBA)*
- *Log Management*
- *User Behavior Anomaly (UBA)*
- ***SIEM***
- *Řízení privilegovaných přístupů (PIM/PAM)*

AXENTA

Dokonalá bezpečnost



AXENTA

Plan
Do
Check
Act

SOC 2.0

Analytics - Future of Security Monitoring

Kybernetický zákon

- Fyzická bezpečnost
- Ochrana integrity komunikačních sítí
- Ověřování identity uživatelů
- Řízení přístupových oprávnění
- Ochrana před škodlivým kódem
- **Zaznamenávání činností**
- **Detekce kybernetických bezpečnostních událostí**
- **Sběr a vyhodnocení kybernetických bezpečnostních událostí**
- Aplikační bezpečnost
- Kryptografické prostředky
- Ostatní technologie podporující org. a tech. opatření

Co je to „bezpečnostní dohled“?

Log Management

Auditní stopa, archivace, vyhledávaní

SIEM

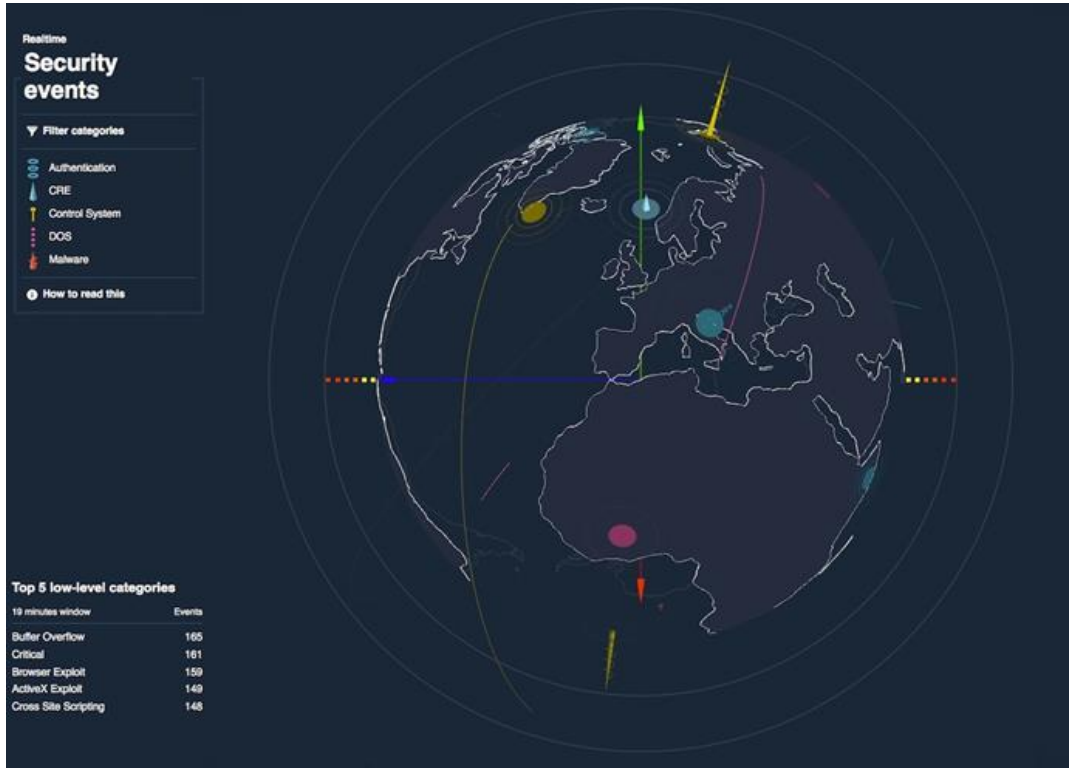
Korelace + Reporting + Dashboardy

Lidé

Bezpečnostní specialista

Assety

IP plány, CMDB, kategorizace



Co je to SOC? A hlavně co není SOC!

Security Operation Center

Bezpečnostní Provozní Centrum

SOC vs Managed Security Services

Externí a Interní penetrační testy
FW konfigurace
WAF, NAC, DLP...

SOC -> Incident Response <-> CSIRT

Řešení incidentů
CSIRT tým (forenzní šetření)

SOC & ZoKB

+/- 85 požadavků, více než polovina požadavků mimo rámec SOC

AXENTA

Co je to „SOC 2.0“?

Threat Inteligence

Global EARLY-warning system

- Tactical
- Technical
- Operational

Malware Information Sharing Platform (MISP)

Honeypots

Advanced Analytics

DNS Firewall

User and (E)ntity Behavior Analytics

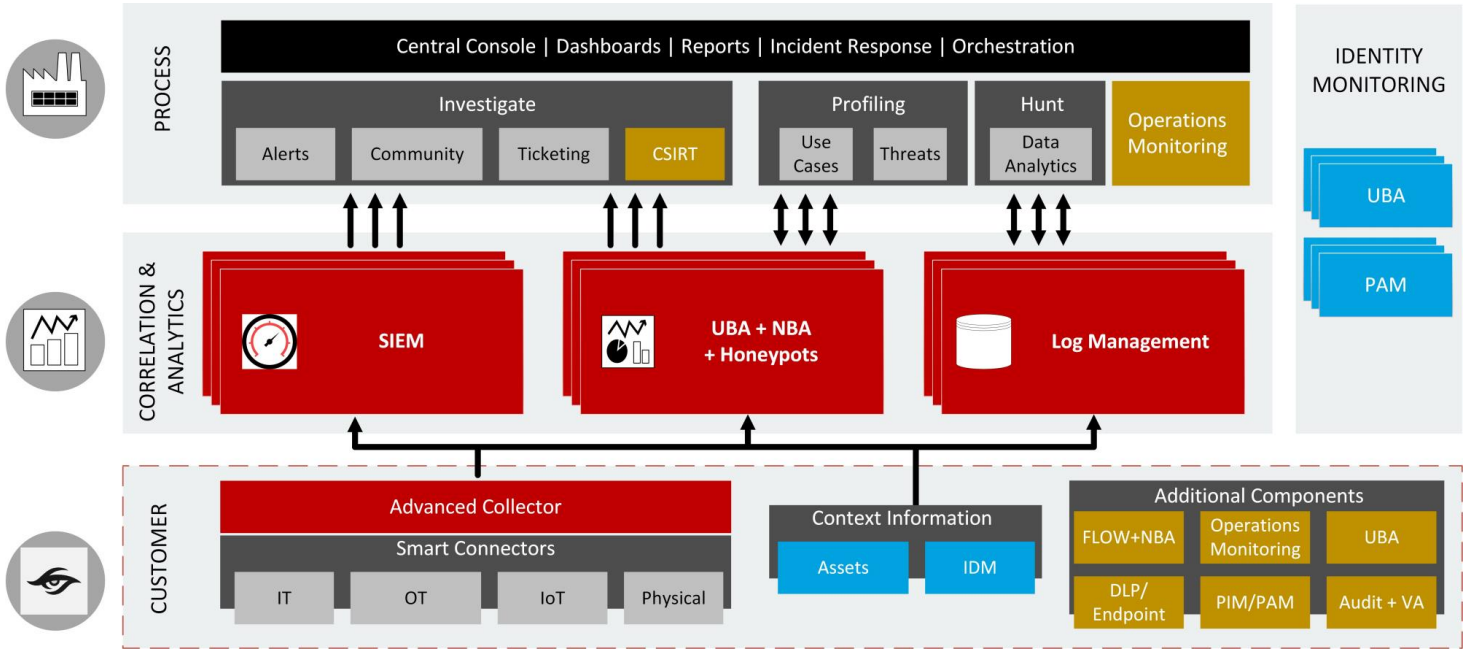
Network Behavior Analytics

Machine Learning / Statistics / Baselines

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

Investing in User Behavior Analytics

Cyber SOC



Software

Event Management, SIEM, UBA, NBA,
Provozní monitoring, Ticketing, Dashboardy

Analytika

Hunting Unknown Unknowns

Reporting/KPI

Threats Exchange

Runbooks/The Hive

Lidé

Procesy

Incident Response, konzultace, tvorba obsahu, vzdělávání

CSIRT

AXENTA

Děkuji

SIEM

Investigate

Security

User Behavior Anomaly

IT operations

Mobile Monitoring

Continuous compliance

Security Analytics

Storage

Log Management

Big Data

Workbench

managed cloud

in-house/legacy custom apps

Apps

Applications

SaaS

Systems Monitoring

Insider threats

Virtual

Cloud security

350+ CEF partners

Contextual Security Intelligence

AXENTA