Bezpečnost komplexně
SOC 2.0

kozak@axenta.cz

Jan Kozák, Presale Technical Specialist

AXENTA

AGENDA

- KDO JSME
- BEZPEČNOST KOMPLEXNĚ
- SOC
- SOC 2.0
- REFERENCE

AXENTA

Kdo jsme / víme jak na to

© 2009 [2002]

AXENTA

Technologická Spolupráce

Sdružení českých a slovenských firem a expertů zabývajících se **kyber. bezpečností**

NSM
NETWORK SECURITY MONITORING CLUSTER

Založeno 2010

20 členů

Výrobci
Systémoví integrátoři
Konzultační specialisté

MUNI

CKB
cluster kybernetickej bezpečnosti

Založeno 2018

8 členů

Bezpečnost. Jak ji vnímáme?

Bezpečnost

Procesy

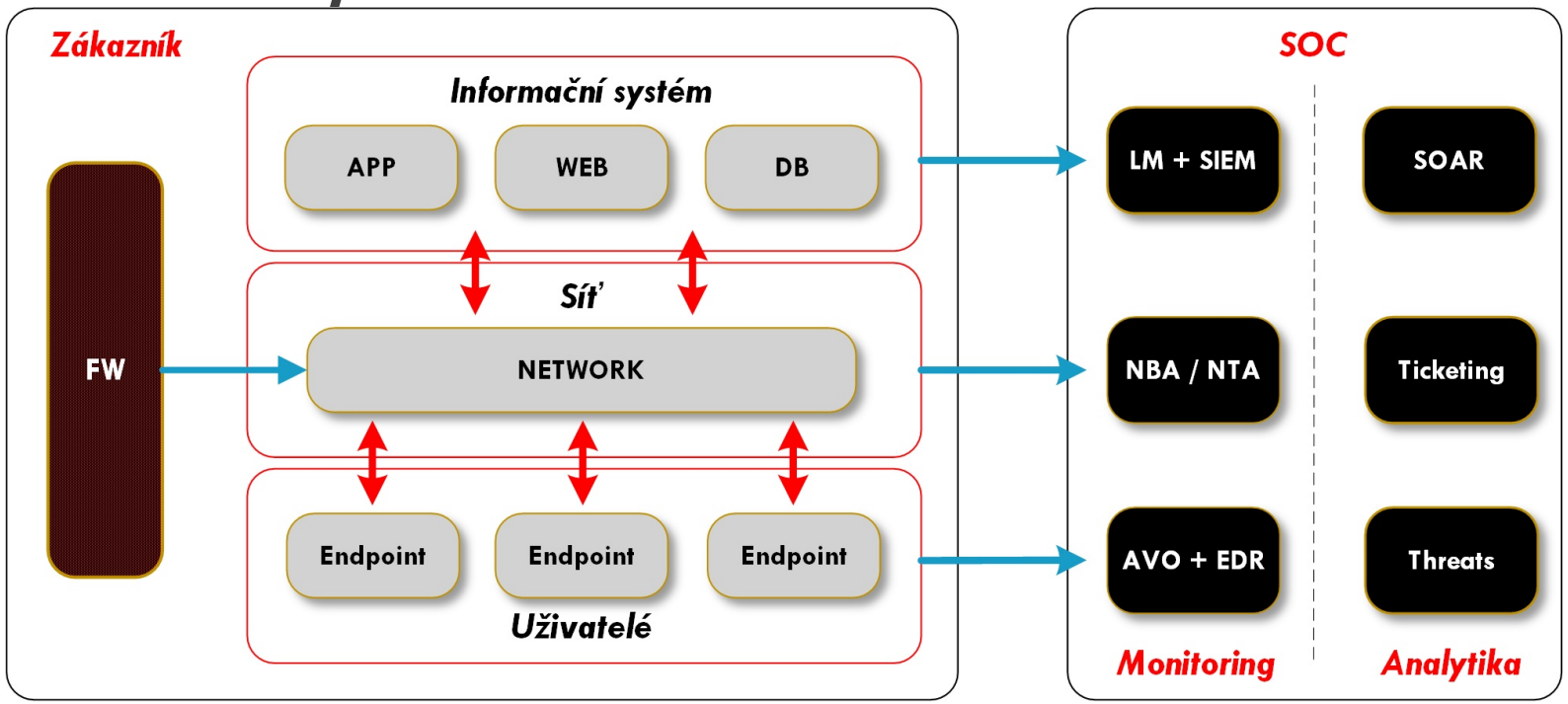
- ***CSIRT***
- *Analýzy rizik, procesů a informací*
- ***Kybernetická bezpečnost***
- *Incident Response*
- *Školení*

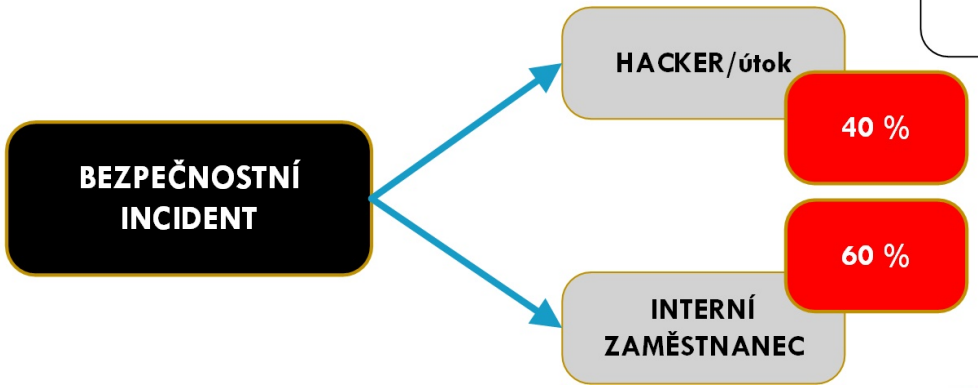
Monitoring

- ***Security Operation Center***
- *Network Behavior Analytics (NBA)*
- *Log Management*
- *Endpoint Detection and Response (EDR)*
- ***SIEM***
- *Řízení privilegovaných přístupů (PIM/PAM)*

AXENTA

Dokonalá bezpečnost / Proti čemu a čím se chránit





AXENTA

PDCA vs NIST Cybersecurity Framework

SOC 2.0

Analytics - Future of Security Monitoring

AXENTA

Co je to „bezpečnostní dohled“?

Log Management

Auditní stopa, archivace, vyhledávaní

SIEM

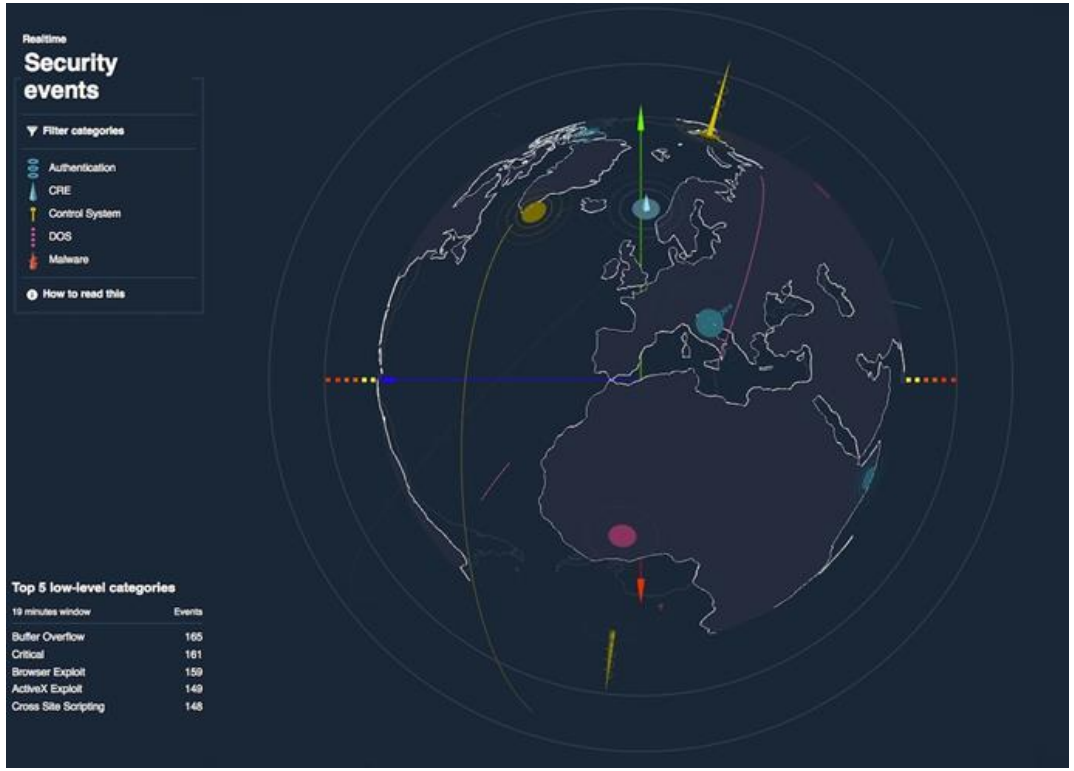
Korelace + Reporting + Dashboardy

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 & Kybernetický zákon

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

SOC 1.0 ≠ Incident Response

Log Management + SIEM

Auditní stopa, detekce, reporting, dashboardy

Tickety

Service Desk / Help Desk

Start Incident Response

Procesy a Lidé

Interní předpisy a postupy

Provoz 24/7

Runbooks

Assety

IP plány, CMDB, zranitelnosti

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

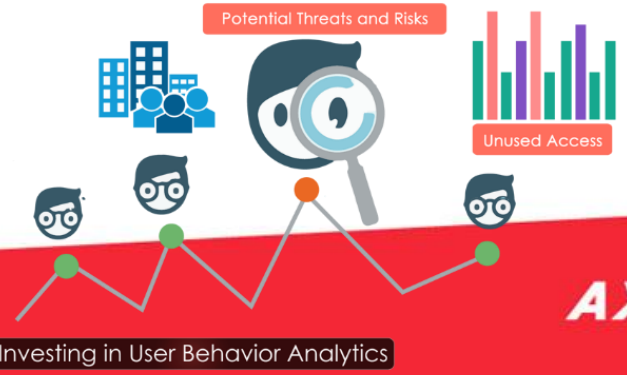
Endpoint Detection and Response

User and (E)ntity Behavior Analytics

Network Behavior Analytics

Machine Learning / Statistics / Baselines

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



Co je to „SOC 2.0“?

Security

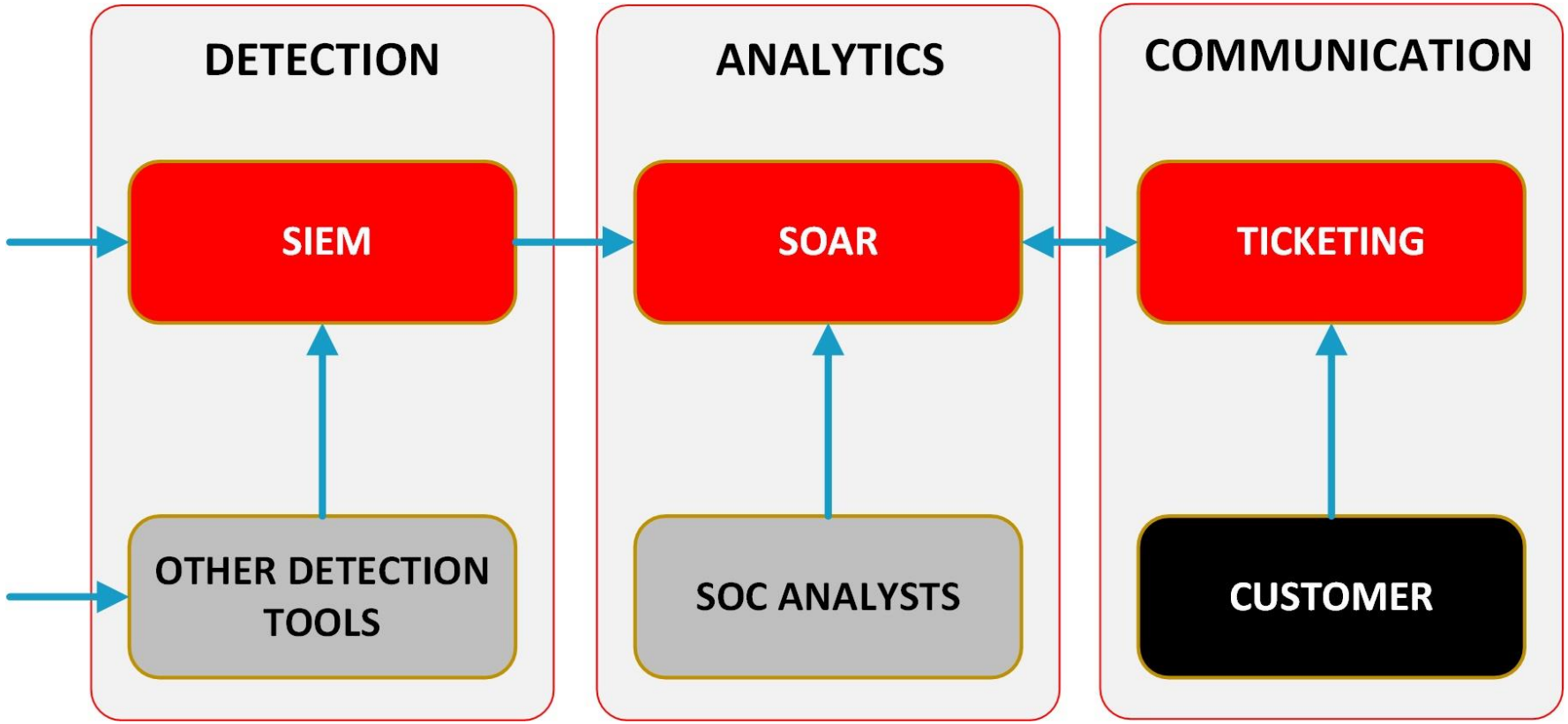
Orchestration

Automation and

Response

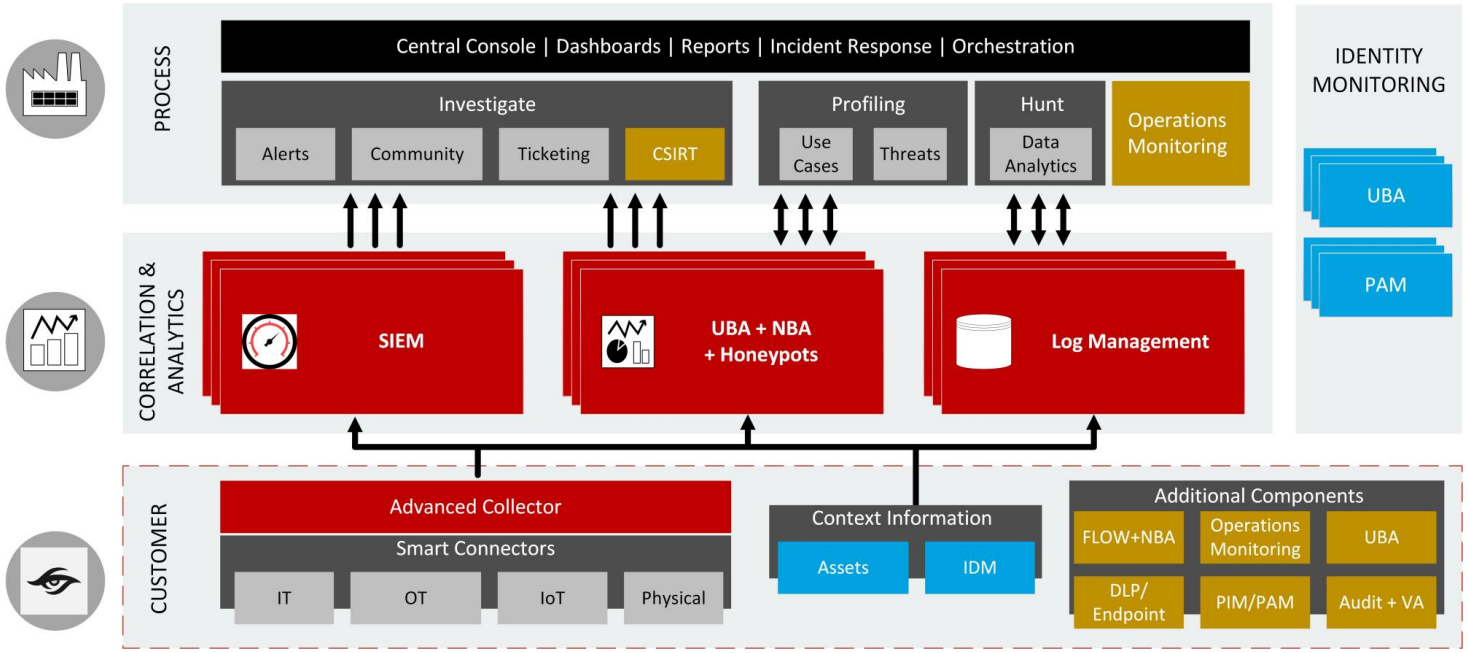
AXENTA

Jak to děláme?



Detekce
Analytika
Komunikace

Cyber SOC



Software

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

Analytika

Hunting Unknown Unknowns

Reporting/KPI

Threats Exchange / MISP

Runbooks / The Hive

Lidé

Procesy

Incident Response, konzultace, tvorba obsahu, vzdělávání

CSIRT

AXENTA

Reference

Finance

Utility

Public + ostatní

Reference

Security monitoring/LM

PIM/PAM

Procesy

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