SOC
Security Operation Center vs KyBez

kozak@axenta.cz

Jan Kozák, Presale Technical Specialist

AXENTA

AGENDA

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

AXENTA

Kdo jsme / víme jak na to

© 2009 [2002]

Reference

Financial

Utility

Public + ostatní

AXENTA

Reference

Security monitoring/LM

PIM/PAM

Procesy

Technologická Spolupráce

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

NSM
NETWORK SECURITY MONITORING CLUSTER

Založeno 2010

22 členů

Výrobci
Systémoví integrátoři
Konzultační specialisté

CKB
cluster kybernetickej bezpečnosti

Založeno 2018

6 členů

AXENTA

Bezpečnost. Jak ji vnímáme?

Bezpečnost

Procesy

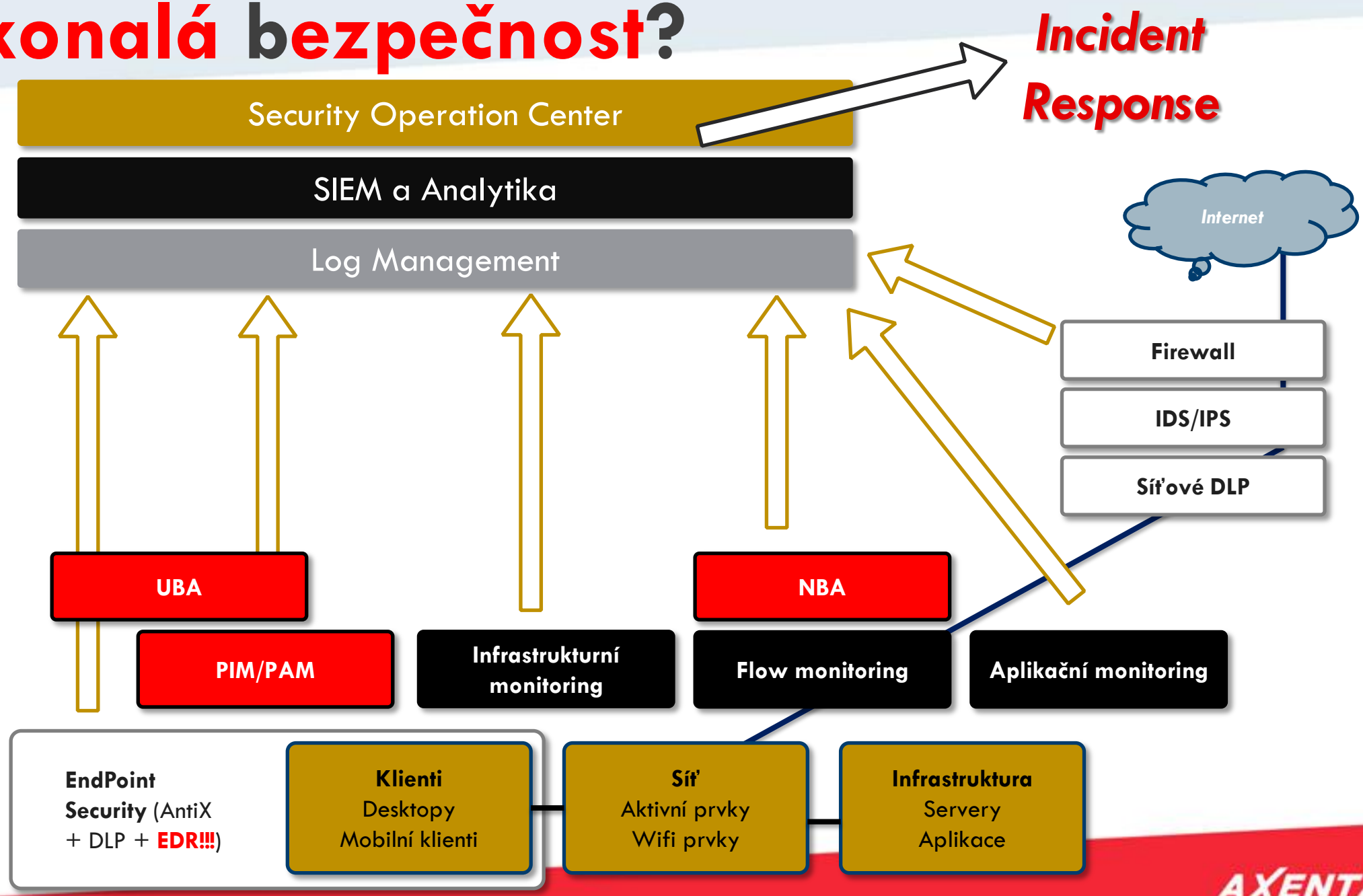
- ***GDPR***
- *Analýzy rizik, procesů a informací*
- ***Kybernetická bezpečnost***
- *Incident Response*
- *Školení*

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 a SOC 2.0 by AXENTA a.s.

Analytics - Future of Security Monitoring

AXENTA

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

AXENTA

Co je to SOC?

SW + HW

Log Management - auditní stopa
Detekce síťového provozu – vidět pohyby v síti
EDR – vidět činnosti na koncových zařízeních
SIEM - detekce, reporting, dashboardy
Další vstupy - IP plány, CMDB, zranitelnosti apod.

Procesy = Interní předpisy a postupy

Provoz 24/7
Runbooks
Service Desk / Help Desk
Ticketing

Lidé!!

Kontinuální vzdělávání, kultura bezpečnosti, atd.

Co je to SOC? A hlavně co není SOC!

Security Operation Center

Bezpečnostní Provozní Centrum

SOC *není* Managed Security Services

Externí a Interní penetrační testy

FW konfigurace

WAF, NAC, DLP...

SOC + Incident Response = CSIRT

Řešení incidentů

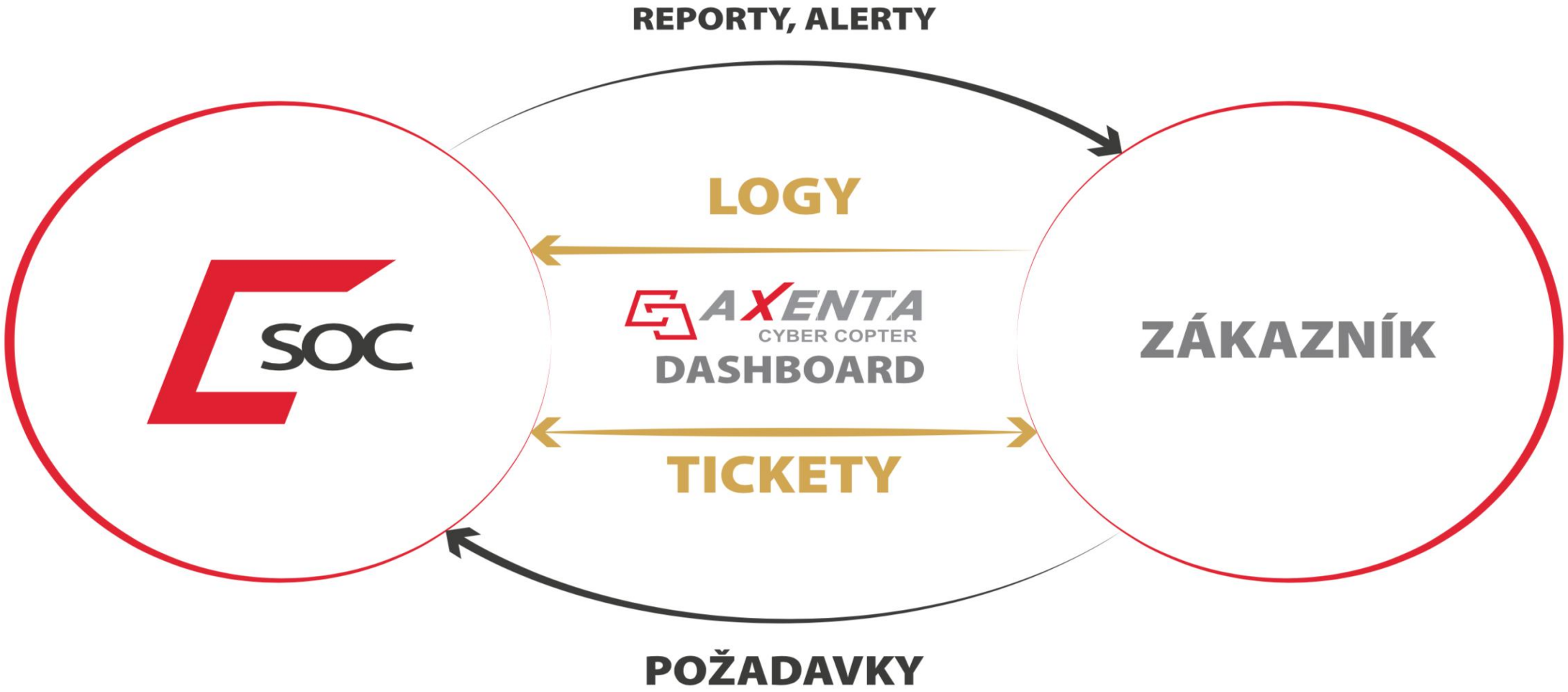
CSIRT tým pro forenzní šetření

SOC & ZoKB

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

AXENTA

Co je to „bezpečnostní dohled jako služba“?



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

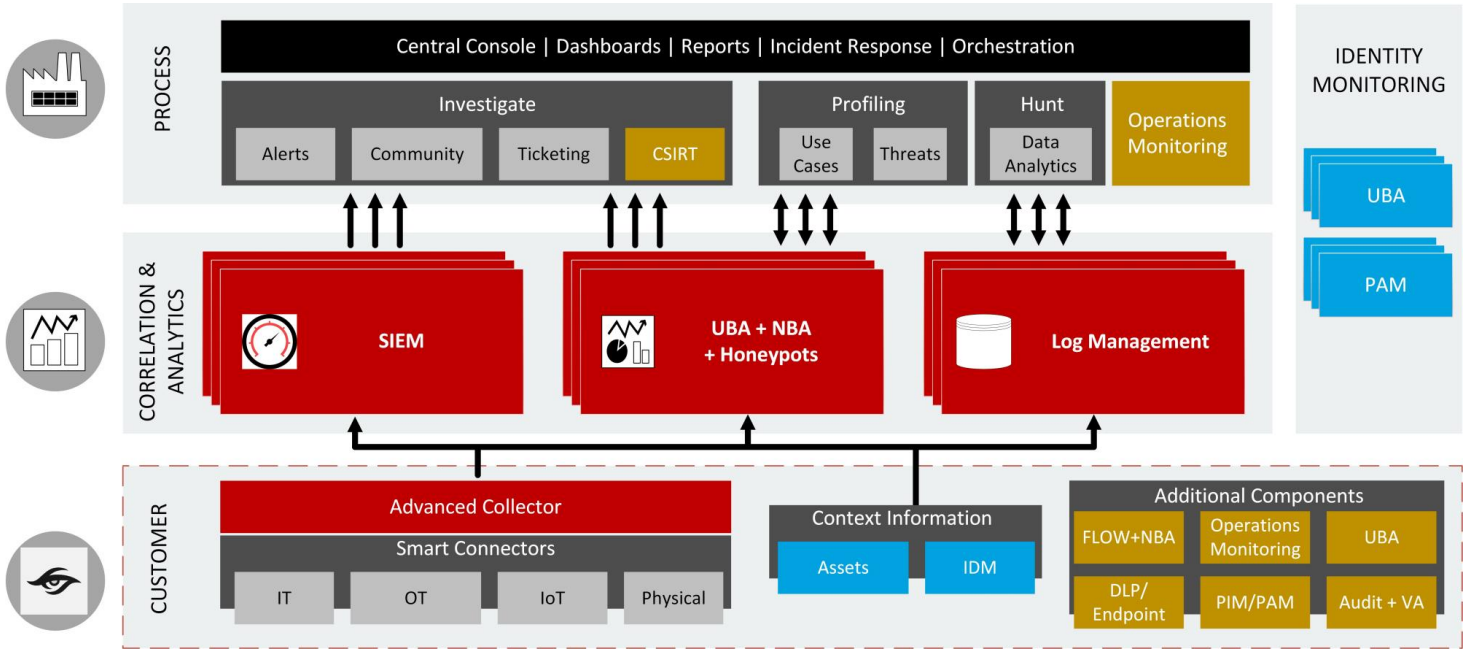
Network Behavior Analytics

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

Lidské zdroje

Team s fokusem na zákazníka

Procesy

Incident Response, konzultace, tvorba obsahu, vzdělávání
CSIRT

AXENTA

Děkuji

SIEM

Investigate

Security

User Behavior Anomaly

Continuous compliance

IT operations

Mobile Monitoring

Security Analytics

Storage

Log Management

Big Data

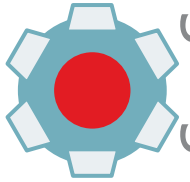
Workbench

managed cloud

in-house/legacy custom apps

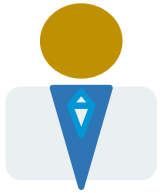
Apps

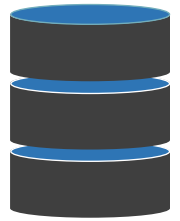
Applications



SaaS

Systems Monitoring





Virtual

Insider threats

Cloud security

350+ CEF partners

Contextual Security Intelligence

AXENTA