Axenta CyberSOC

Dávid Kosť, Lead Security Analyst

AXENTA

SOC

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, red teaming
FW konfigurace
WAF, NAC, DLP...

SOC -> Incident Response (CSIRT)

Řešení incidentů
CSIRT tým

SOC & Kybernetický zákon

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

SOC ≠ Incident Response

Log Management + SIEM

Auditní stopa, detekce, reporting, dashboardy

Tickety

Service Desk / Help Desk

Start Incident Response

Procesy a Lidé

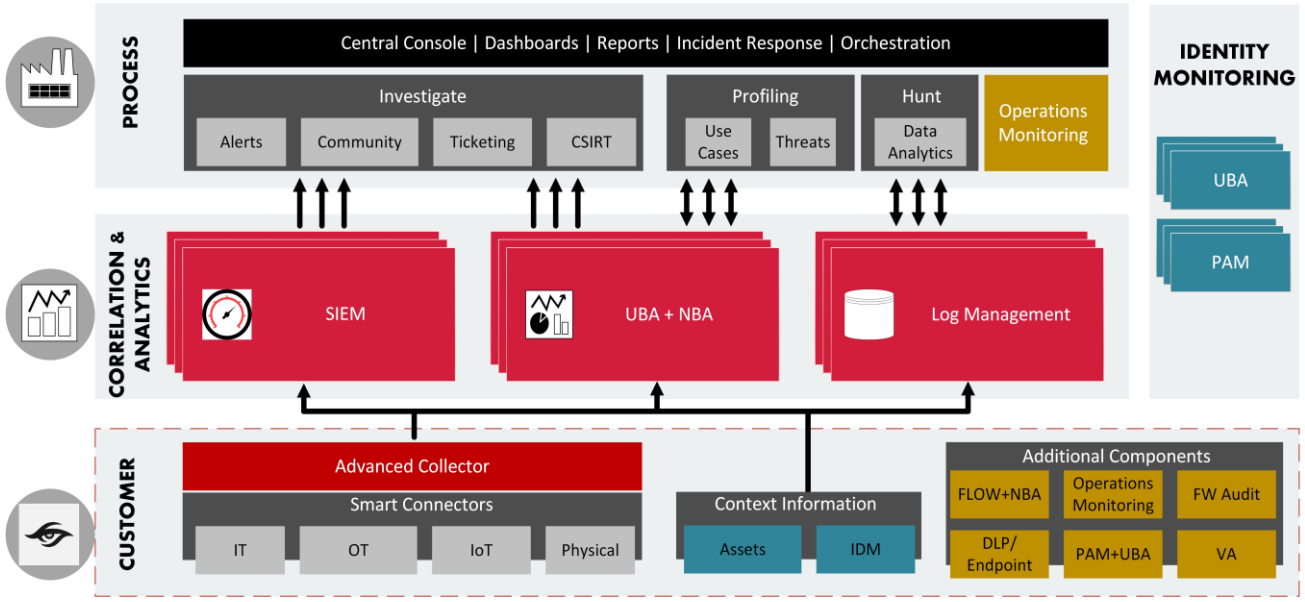
Interní předpisy a postupy

Provoz 24/7

Assety

IP plány, CMDB, vulnerability management

Cyber SOC



Software

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

Analytika

Threat Hunting
Reporting/KPI
Threat Intelligence

Lidé

Procesy

Incident Response, konzultácie, tvorba obsahu, vzdelávanie

AXENTA

Analytika

Trendy v 2019

IoT, kritická infraštruktúra a SCADA – LockerGoga ransomware

Bezpečnosť cloudových služieb

Hrozby novej generácie

Štátom podporované útoky

Trendy v 2019

Software supply chain útoky – ASUS ShadowHammer

Mobilné hrozby – Chamois botnet

GDPR a legislatíva – 230 000 € PL, 50 mil. € FR

Čo máme (pomerne) nové?

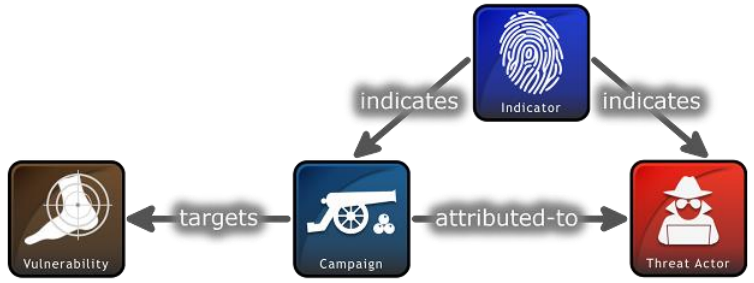
Threat Intelligence

6000+ organizations

Europe, US

IOT, ICT, SCADA

Human Integration and Correlation



Early warning system

Multi-honeypot platform

Docker based

20+ honeypots

ICS/SCADA support

CSIRT

TF-CSIRT
Trusted Introducer

11/2018 – **Listed**

02/2019 – **Accredited**

Q2/2019 – **Plný súlad s ZoKB ČR a SR**

CyberSOC R&D

- deep endpoint visibility
- automation (operations & IR support)
- advanced threat analytics

Ďakujem

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