

Ing. Lukáš Příbyl, CEO
AXENTA a.s.
pribyl@axenta.cz



Stavba a zkušenosti s provozem SOC

Agenda

» Vstupy

ZoKB & GDPR

Lidé

» SOC

LM + SIEM

PIM - PAM

Lidé

» SOC 2.0

Contextual Security

Workbench & Analytics

Kdo jsme / víme jak na to

Reference

O₂ IT Services



Řízení letového provozu
České republiky



GoodData®



Jihomoravský kraj

€ DanubePay



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



KB



Česká průmyslová
zdravotní pojišťovna



MINISTERSTVO OBRANY
ČESKÉ REPUBLIKY

di:Sig

ČEPS, a.s.

NOVARTIS



orange™



ČEZ



ČEPRO



Banka

ČMSS



Na těchto základech můžete stavět



MONETA

MONEY
BANK



PRAHA
MĚSTSKÁ ČÁST



ČESKÁ
POJIŠŤOVNA

Allianz



O₂

Vstupy

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



- » EU občani **celosvětově**
- » Data Protection Officer
28.000+ v Evropě
- » Nahlásit do **72** hodin
- » Právo „být zapomenut“
- » Chránit a **Monitorovat** všechnu aktivitu s osobními údaji
- » Pokuty **do výše 4% obrátu nebo €20M**



» Dostupnost

školy

» Čas

zaškolení



» Kvalita
vědomosti

» Cena
Kurzy

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

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 (CSIRT)

» Log Management

Archivace, vyhledávání

» SIEM

Korelace + Reporting + Dashboardy

» Tickety

Service Desk / Help Desk

» Procesy

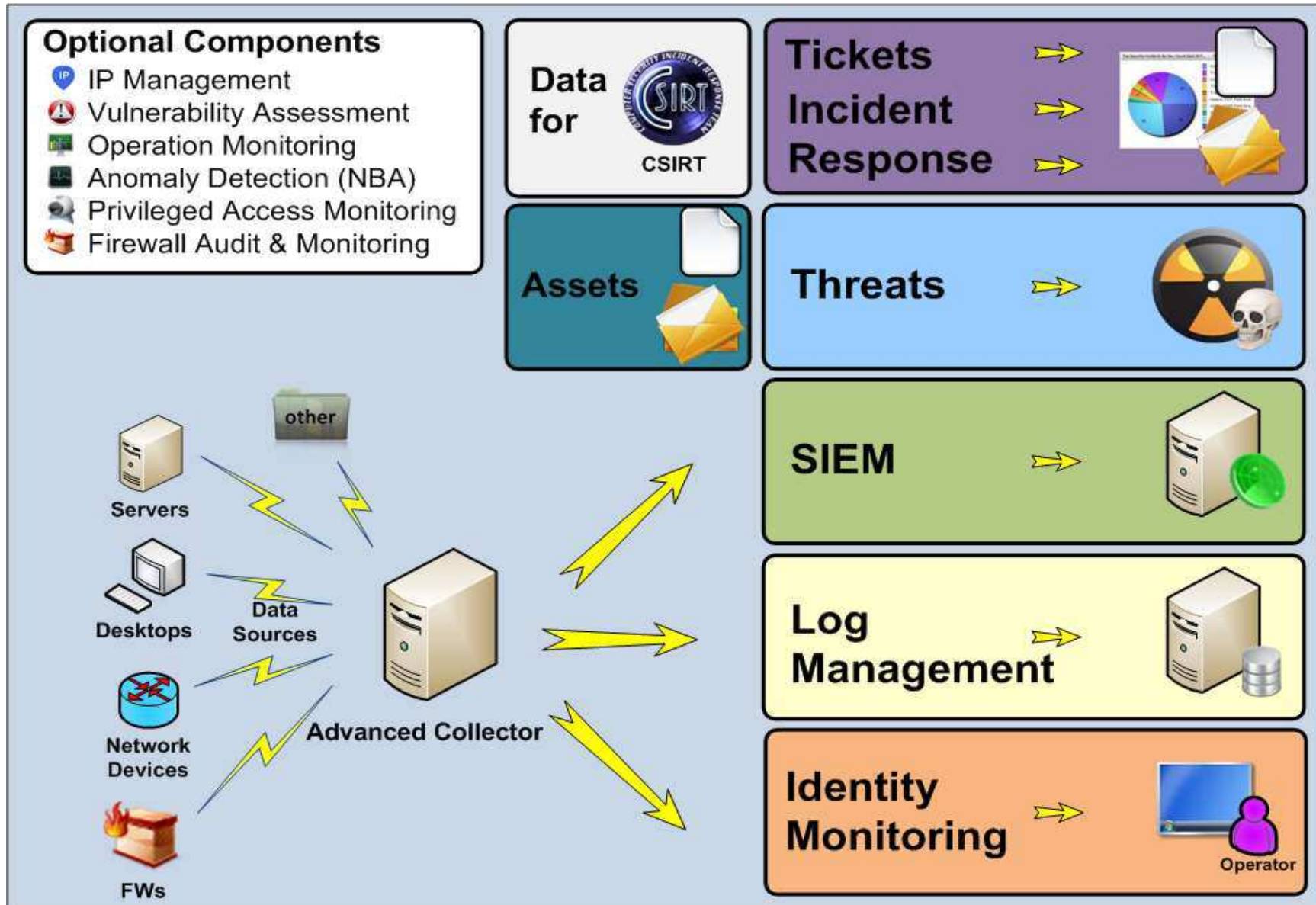
Interní předpisy a postupy

» Assety

IP plány, CMDB, kategorizace



AXENTA Advanced SOC



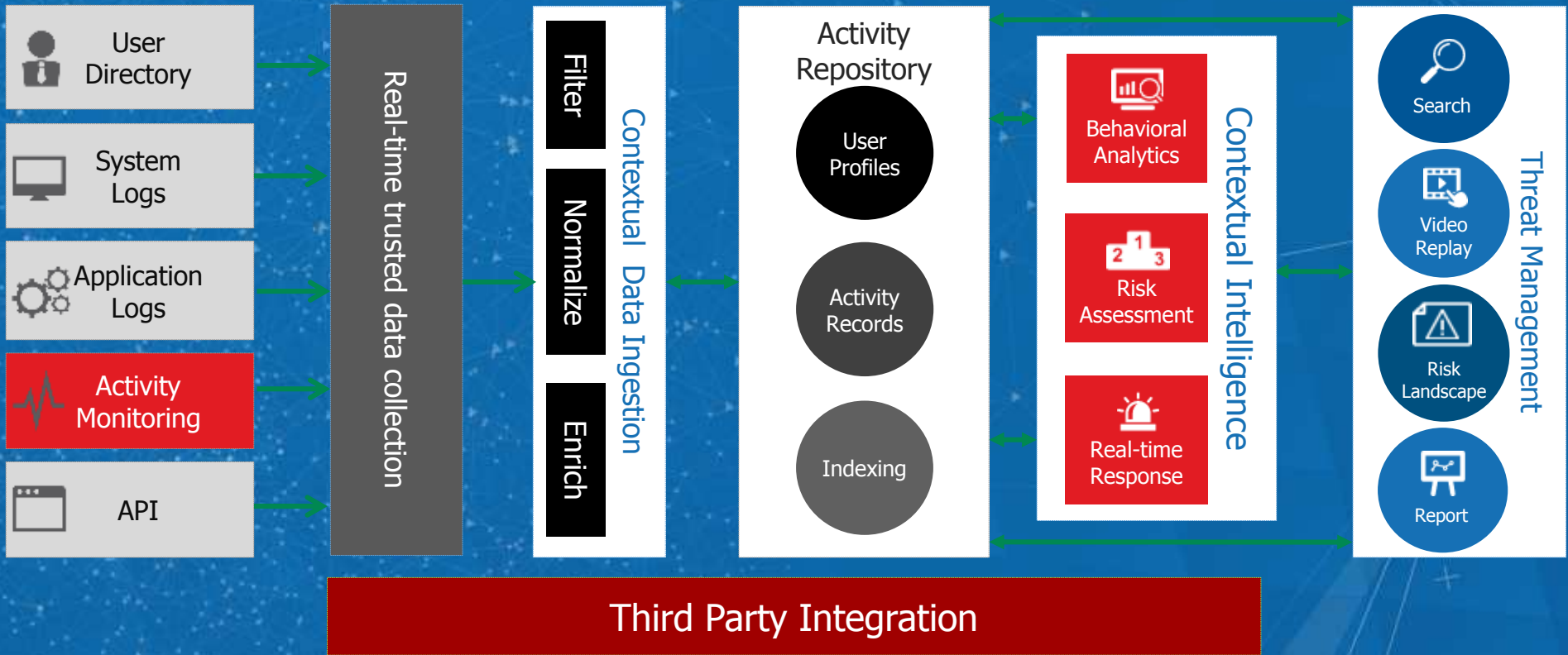
SOC 2.0

Analytics - Future of Security Monitoring

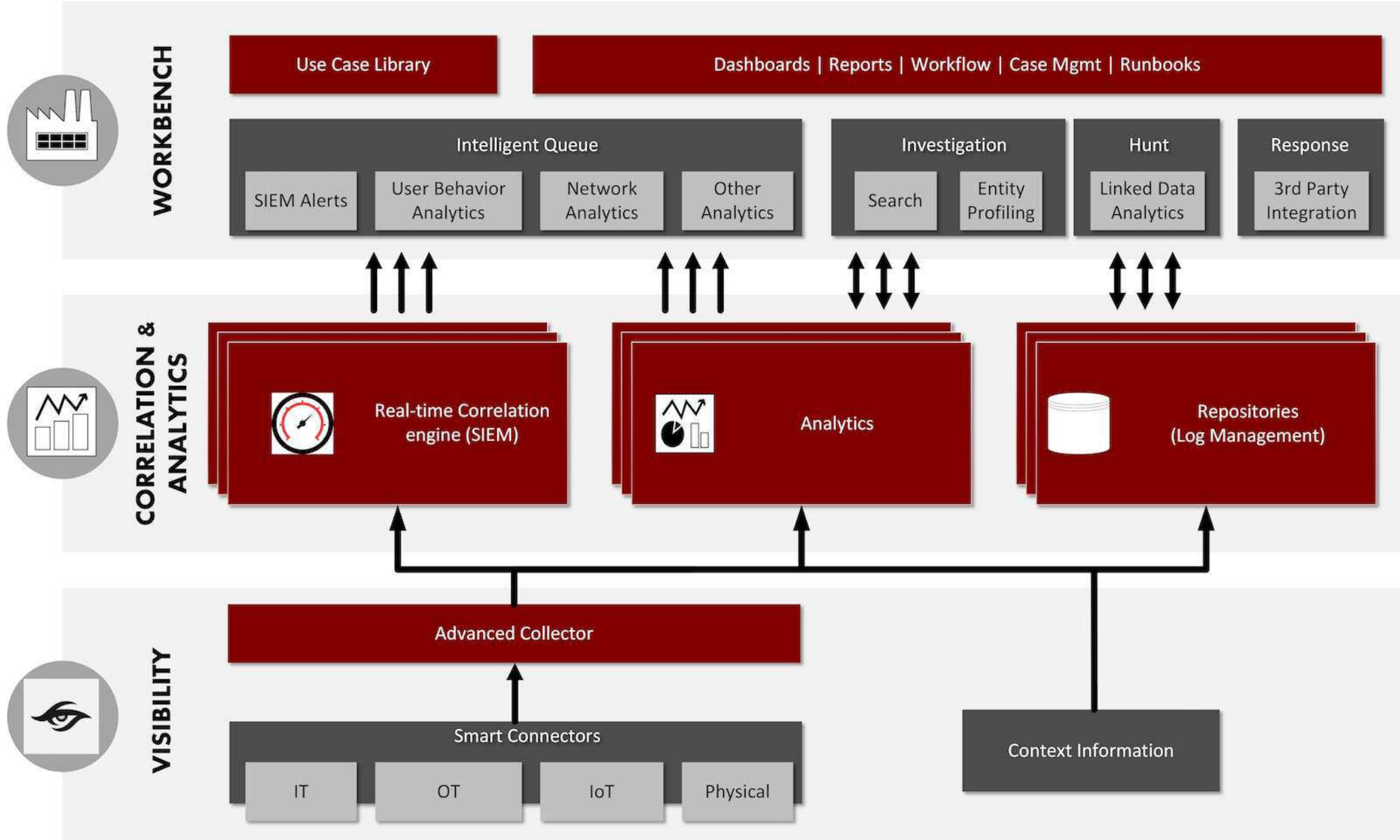
The Contextual Security Intelligence Platform



BALABIT
CONTEXTUAL SECURITY INTELLIGENCE



SOC 2.0 – Analytics + Workbench



Thank you

Security Analytics

