Ing. Lukáš Přibyl, CEO
AXENTA a.s.
+420 724 256 695
pribyl@axenta.cz

Co je to SOC?

Agenda

- SOC - víme jak na to
- SOC - Co to je a co to není
  - SOC vs Incident Response
  - SOC vs Kybernetický zákon
  - SOC vs MSS
- Z čeho složit SOC
  - Vlastní SOC
  - SOC jako služba

Reference

DanubePay

MINISTERSTVO OBRANY
ČESKÉ REPUBLIKY

KB

ČEZ

PPF Banka

O2

SOC

Co je to SOC? **A hlavně co není SOC!**

» Security Operation Center

Bezpečnostní Provozní Centrum

» SOC & Managed Security Services

Externí a Interní penetrační testy

FW konfigurace

WAF, NAC, DLP...

» SOC -> Incident Response C

Řešení incidentů

CSIRT tým

» SOC & Kybernetický zákon

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

SOC -> Incident Response (CSIRT)

- **Log Management**
  Archivace, vyhledávaní
- **SIEM**
  Korelace + Reporting + Dashboardy
- **Tickety**
  Service Desk / Help Desk
- **Procesy**
  Interní předpisy a postupy
- **Assety**
  IP plány, CMDB, kategorizace

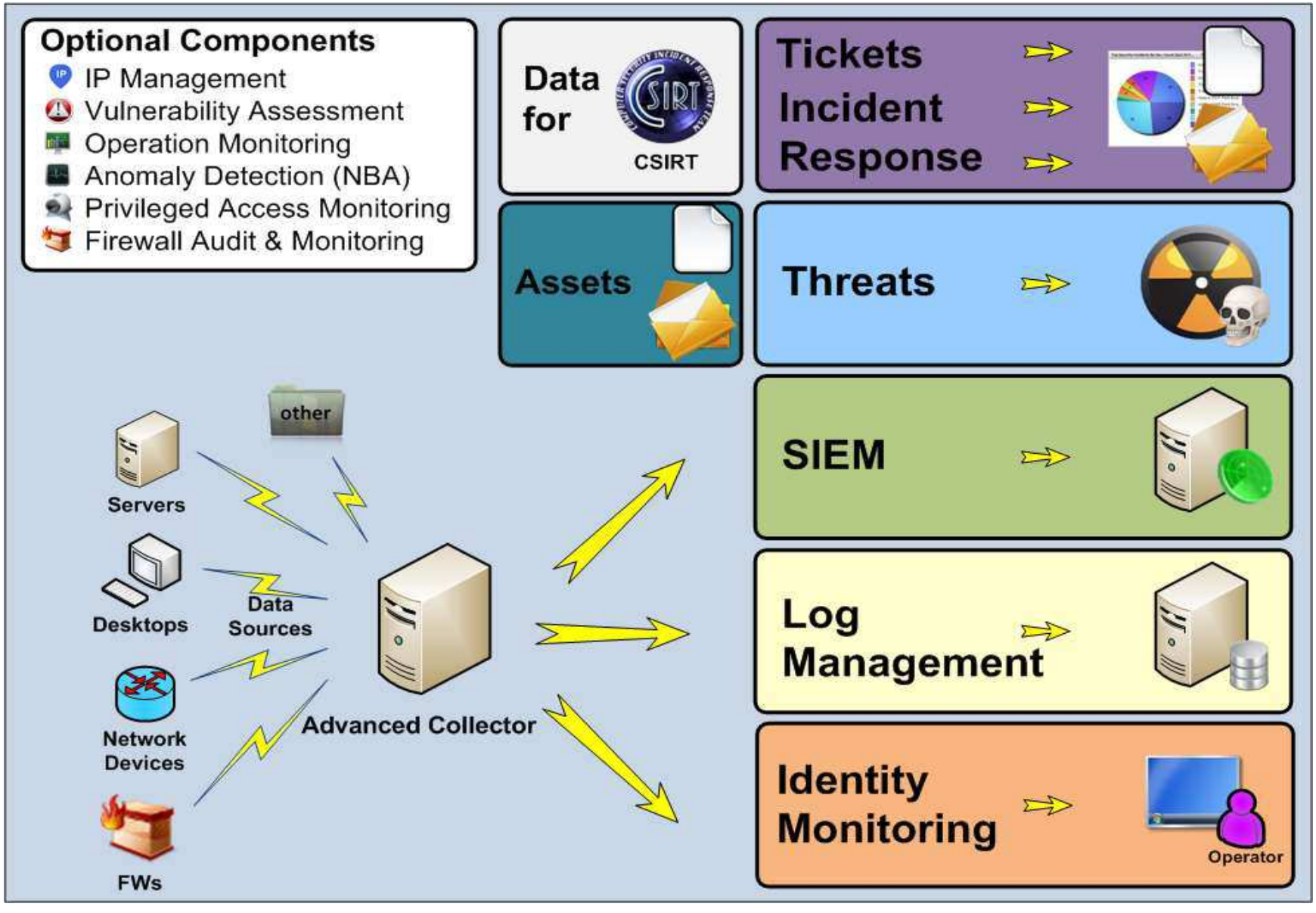
SOC & Kybernetický zákon

- 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.

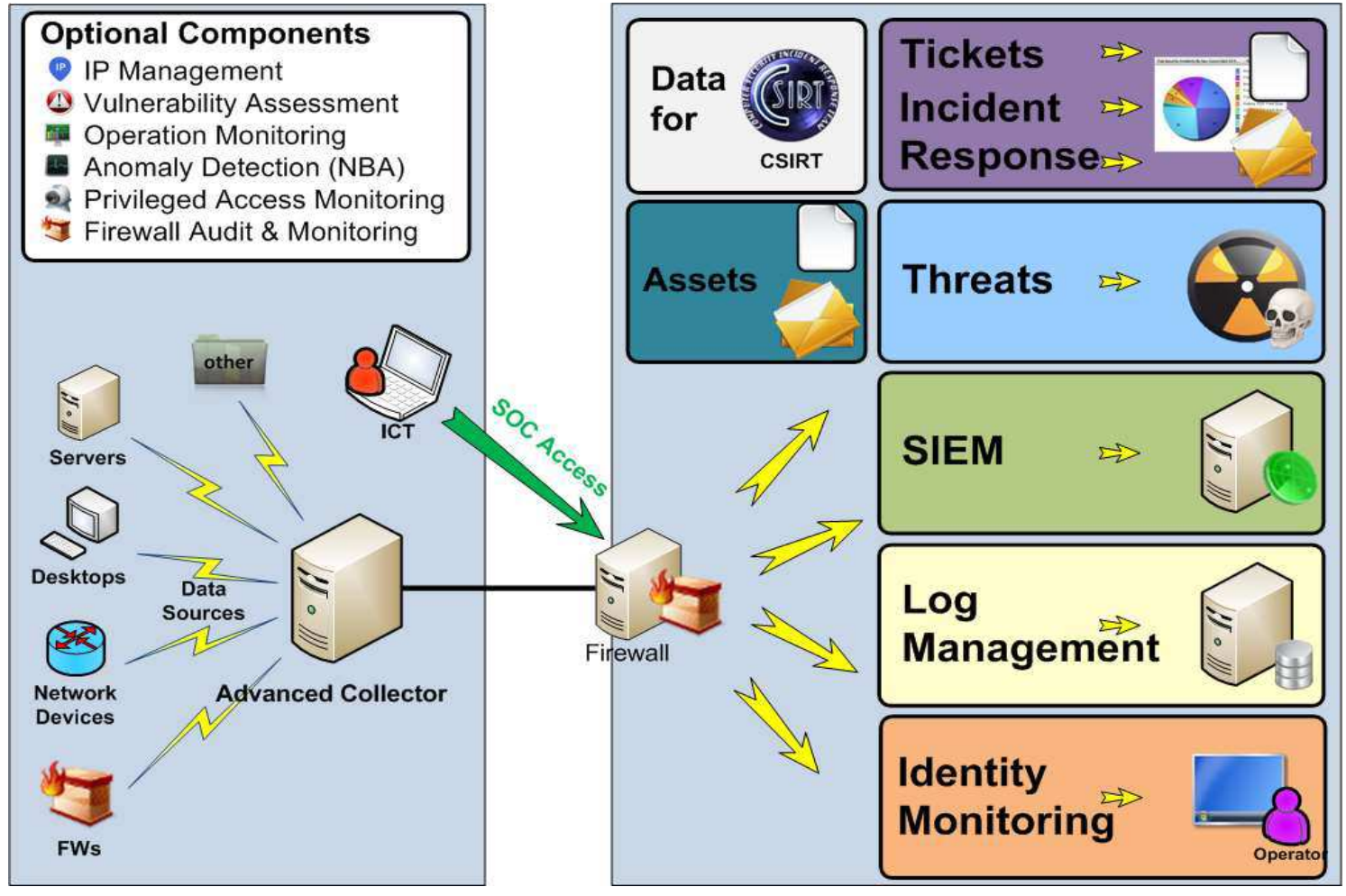
Příklad SOCu

AXENTA Advanced SOC

AXENTA Advanced SOC



AXENTA Advanced SOC service



10/5 nebo 24/7
operátor + analytik +
administrátor
SOC + CSiRT

Diskuse