Co je to SOC a jak se staví?

Ing. Peter Jankovský, CTO
AXENTA a.s.
+420 724 952 661
jankovsky@axenta.cz

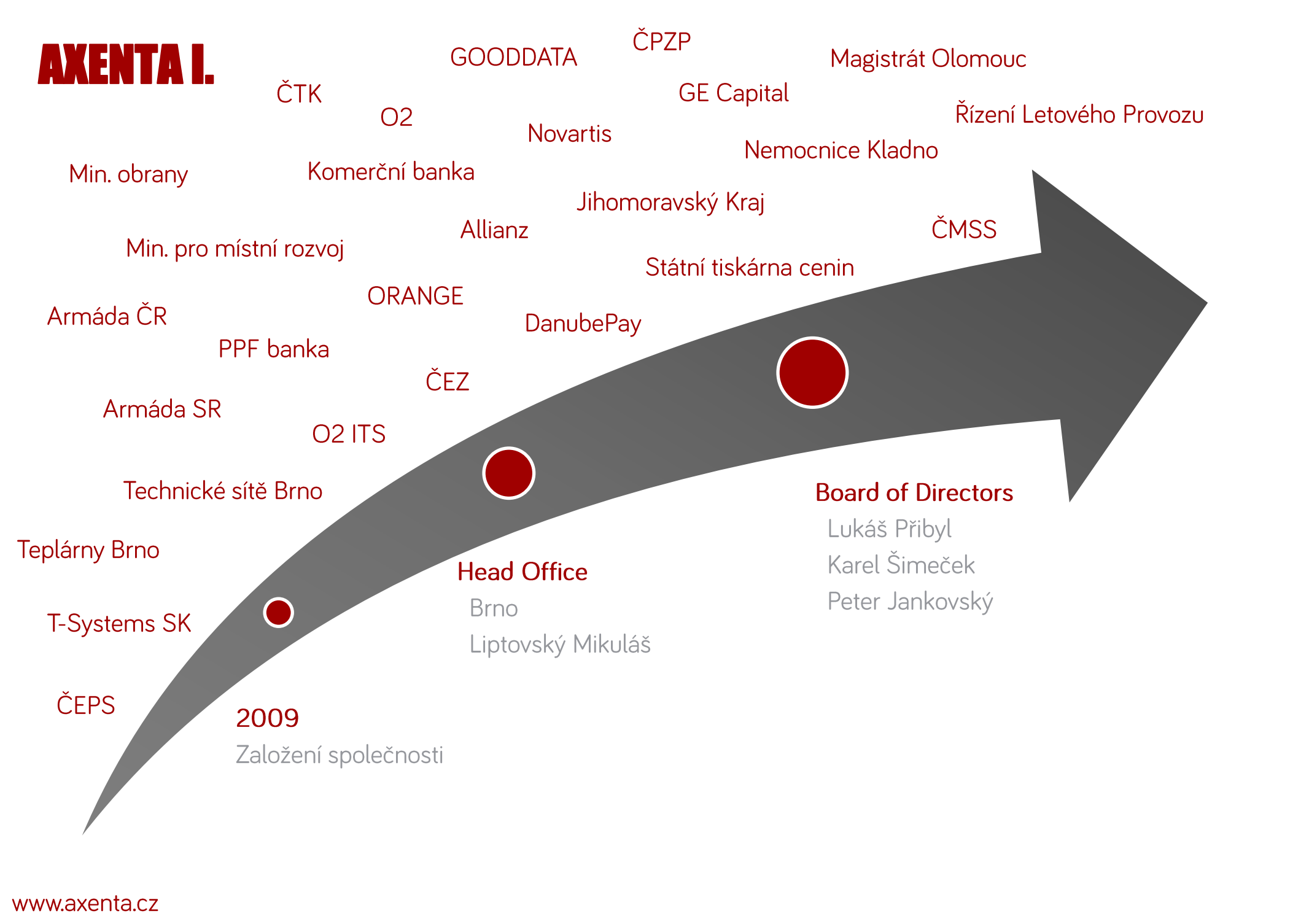
Agenda

- Kdo je AXENTA a proč víme jak na to?
- SOC – Co to je a co to není

  SOC // MSSP // Kybernetický zákon // Incident Response
- Z čeho složit SOC?
- Jak se staví SOC?

  Technologie // Lidé a Procesy // Úskalí

AXENTA I.



www.axenta.cz

AXENTA II.

Analýzy

- Bezpečnosti informací
- Rizik
- Procesů a informací
- Kybernetické bezpečnosti

Monitoring

- Provozní monitoring
- Aplikační monitoring
- Log Management
- Detekce Anomálií (NBA)
- SIEM
- Řízení privilegovaných přístupů (PIM/PAM)

ICT bezpečnost

- WAF
- Správa IP (ADDNET)
- Školení, uvědomovací kampaně
- Security Operation Center (SOC)

Reference // víme jak na to

Reference

O2 IT Services

Řízení letového provozu České republiky

DanubePay

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

KB

MINISTERSTVO OBRANY ČESKÉ REPUBLIKY

orange™

ČEPS, a.s.

PPF Banka

ČMSS

Na těchto základech můžete stavět

ČEZ

O2

ČESKÁ POJIŠŤOVNA

Allianz

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 (CSIRT)
  - Řešení incidentů
  - CSIRT tým
- SOC & Kybernetický zákon
  - +/- 85 požadavků, více než polovina požadavků mimo rámec SOC

SOC & Kybernetický zákon

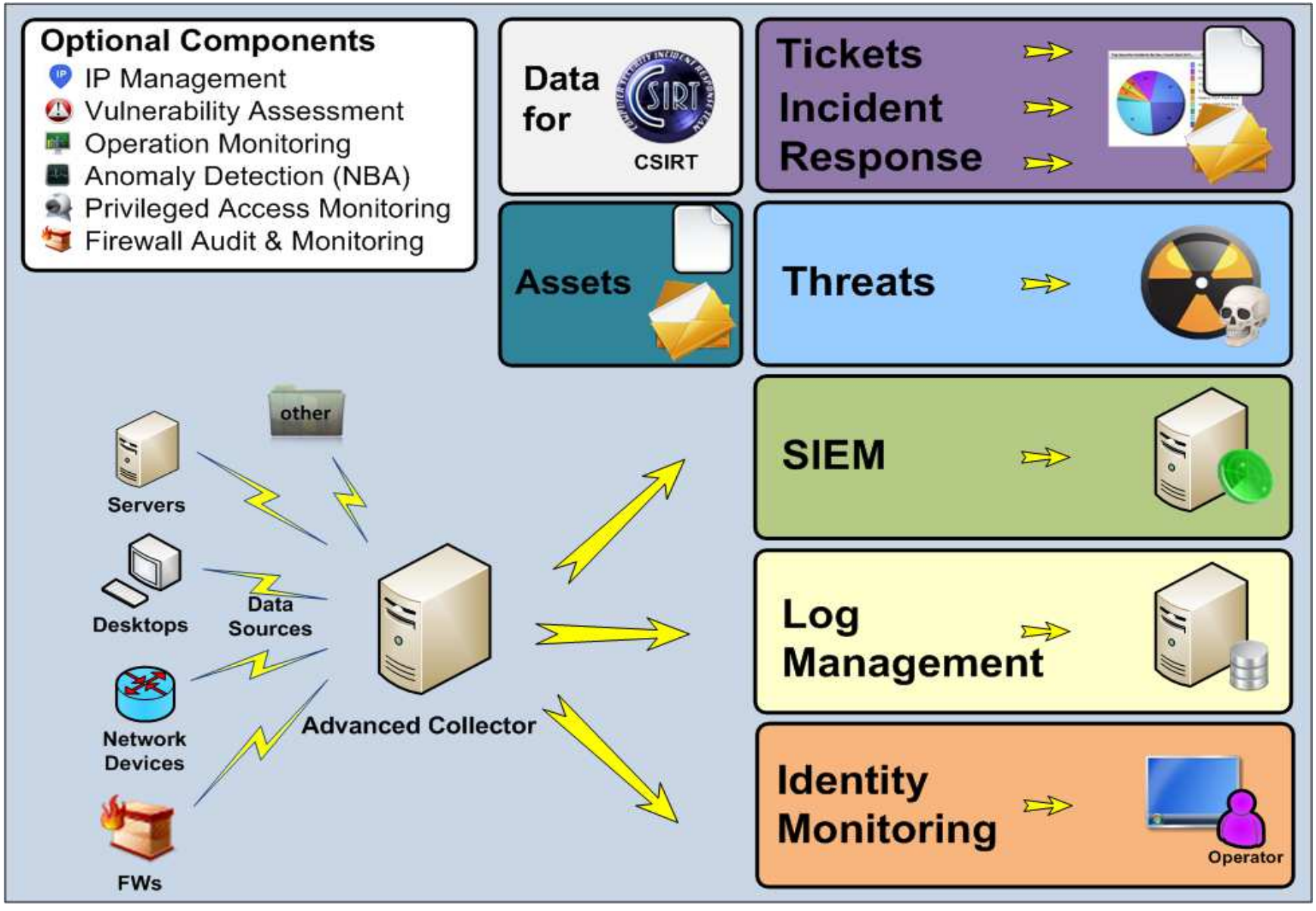
- Fyzická bezpečnost
- Ochrana integrity komunikačních sítí
- Ověřování identity uživatelů
- Řízení přístupových oprávnění
- Ochrana před škodlivým kódem
- Zaznamenávání činností
- **Detekce kybernetických bezpečnostních událostí**
- **Sběr a vyhodnocení kybernetických bezpečnostních událostí**
- Aplikační bezpečnost
- Kryptografické prostředky
- Ostatní technologie podporující org. a tech. opatření

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

Z čeho složit SOC

AXENTA Advanced SOC



Jak se staví SOC

Solidní základy SOC

Prostory

- Serverovna
- Office

Technologie

- HW + Virtualizace + Storage
- OS, Infrastruktura (LDAP, DNS, CA, Dokumenty/Share, Webserver)
- Vysoká dostupnost
- Monitoring

Škálovatelnost

- Horizontálně // Vertikálně
- Časově
- Business model
- Rozvoj

Solidní řešení SOC

Lidé a Role

- Operátor // Analytik
- Manažer // Architekt
- Administrátor

Procesy

- Incident Response
- Workflow a Ticketing
- Configuration Management // CMDB + Assety
- Metriky // SLA
- Podpora a Provoz

Technologie

- PIM/PAM?
- SIEM // Multitenant // Hrozby
- LM // oddělené LOGSTORE + TSA + Šifrování + Podpis
- Kolektor // TLS + Komprese + Cache

Děkuji