Kľúčové pohľady

na kybernetickú bezpečnosť

Atos CYBER security

Tomáš Hlavsa, Atos IT Solutions and Services

ATOS – základní údaje

- **ATOS celosvětově**
- v 72 zemích světa
- 100 000 zaměstnanců
- tržby 11 mld. EUR
- zaměření na systémovou integraci, řízené služby, kybernetická bezpečnost

- **ATOS ČR**
- 310 zaměstnanců členěných ve 3 divizích
- Sídlo v Praze
- Pobočky v Brně, Vysokém Mýtě, Zlíně, Ostravě

- **ATOS SK**
- 320 zaměstnanců členěných ve 3 divizích
- Sídlo v Bratislavě
- Pobočky: Prievidza, Martin, Banska Bystrica, Kosice

Cyber Security - reference

NetFlow / SIEM /SOC implementace a support

od roku 2011
orientace na IBM security portfolio
zkušenosti s McAfee, RSA

Identity Access Management

Telekomunikace / Pojištění / Zdravotnictví
ATOS má 2 vlastní řešení

- DirX
- Evidian

Normy, zákony, regulace

Zákon o kybernetické bezpečnosti – ???/2016 Sb.

Norma pro systém řízení bezpečnosti informací - ISO 27001

Zákon o ochraně osobních údajů - 122/2013 Sb.

Hrozby? Reálné, nebo virtuální téma?

Kolik notebooků / tabletů / mobilních telefonů Vaše firma za poslední rok ztratila?

…….a více jistě co všechno na nich bylo?

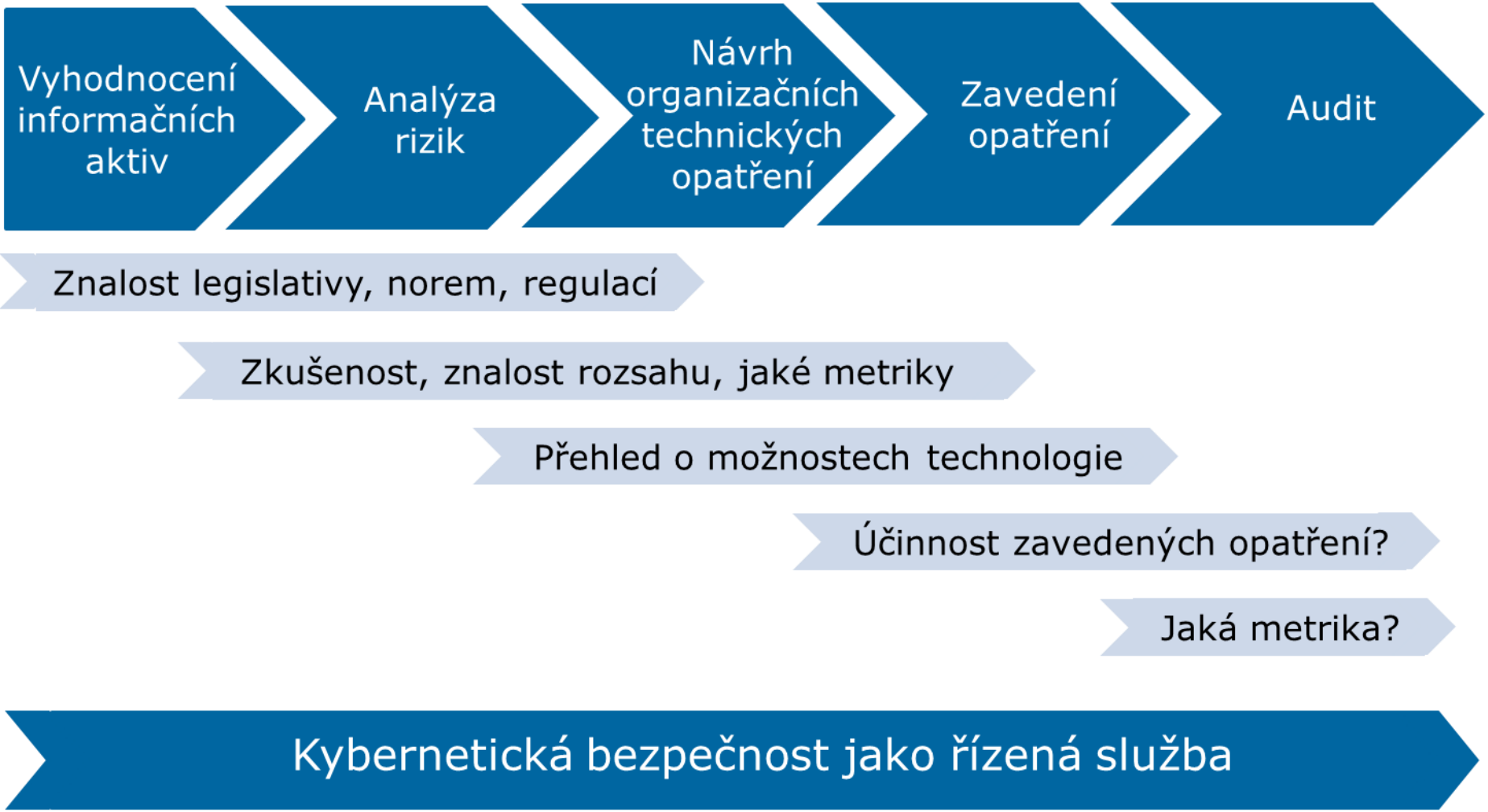
Evidujete USB flash disky? Máte na ně bezpečnostní politiku?

Kolik stojí hodina provozu Vaší firmy?

Kolik zakázek jste za poslední dobu „o chlup" prohráli?

Ne technologie, ale lidé a procesy

Co poskytujeme a v čem se odlišujeme



A co mi to přinese?

Ochrana informací
- Nebo máte snad ve firmě něco cennějšího?
- Ceníky, výkresy, finanční systém, HR systém…

Garance výkonu / dostupnosti

Na kolik si ceníte hodinu/den výpadek běhu Vaší organizace?

Snížení nákladů na IT
- Budujete si vlastní bezpečnostní oddělení ?
- Jak často obměňujete své bezpečnostní technologie?
- Nešlo by bezpečnostní dohled řešit službou?

Pojištění vůči kybernetickým hrozbám
- požární řád, směrnice
- evakuační plán
- povodňové plány

…..ohodnocení informačních aktiv -> Analýza rizik

Bavme se o penězích

Cyber security compliance jako **přidaná hodnota** Vaší organizace
ISO kvality má každý, ISO 27001 skoro každý, soulad se cyber zákonem bude výhodou…….minimálně vůči státní správě

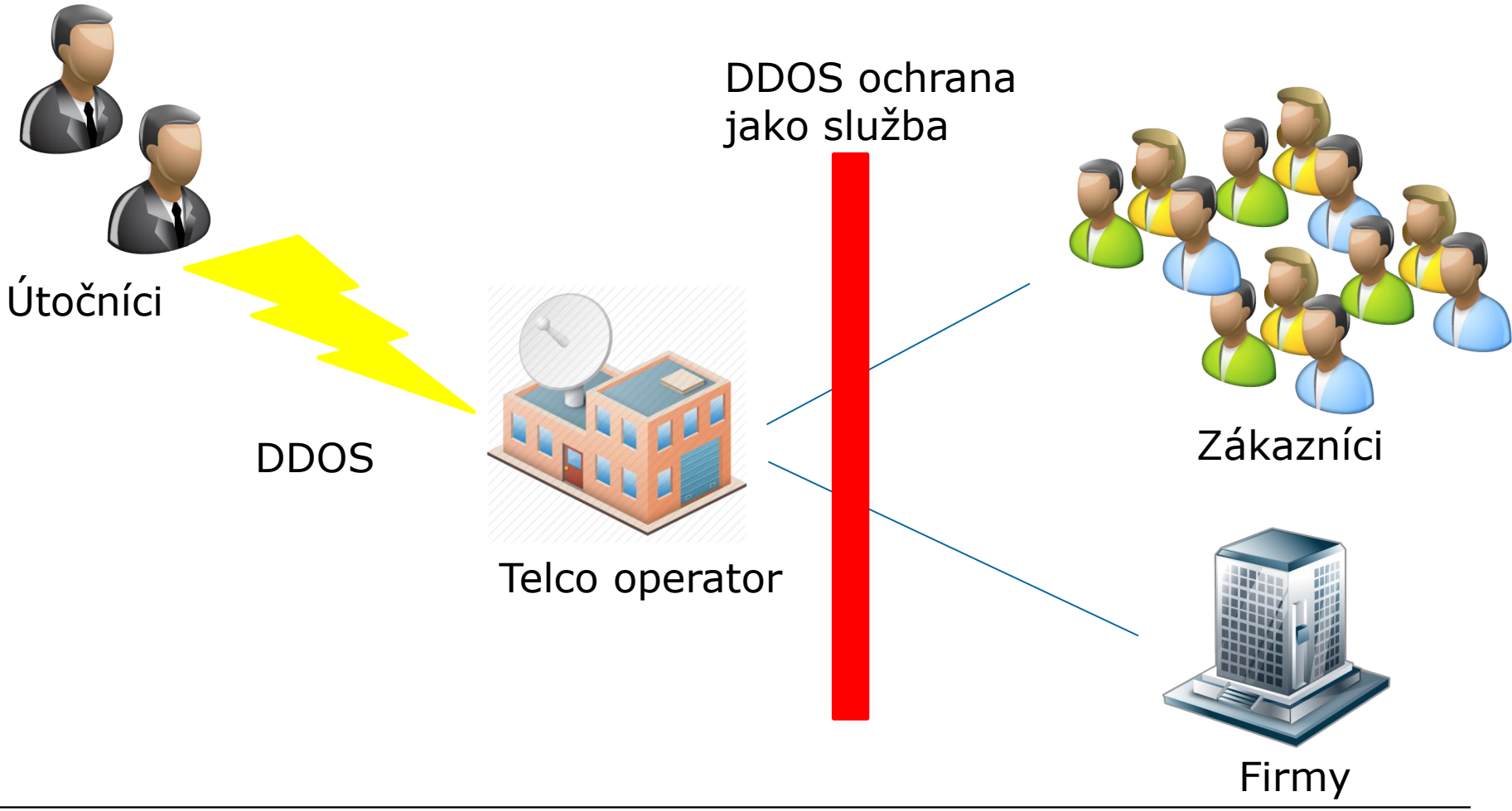
Vzdělávání zaměstnanců ohledně informačních rizik je nutná součást opatření. Proč z toho neučinit **zaměstnanecký benefit**.

Dodavatelé IT / síťových technologií / infrastruktury – mohou přeci řadu opatření vyřešit za Vás

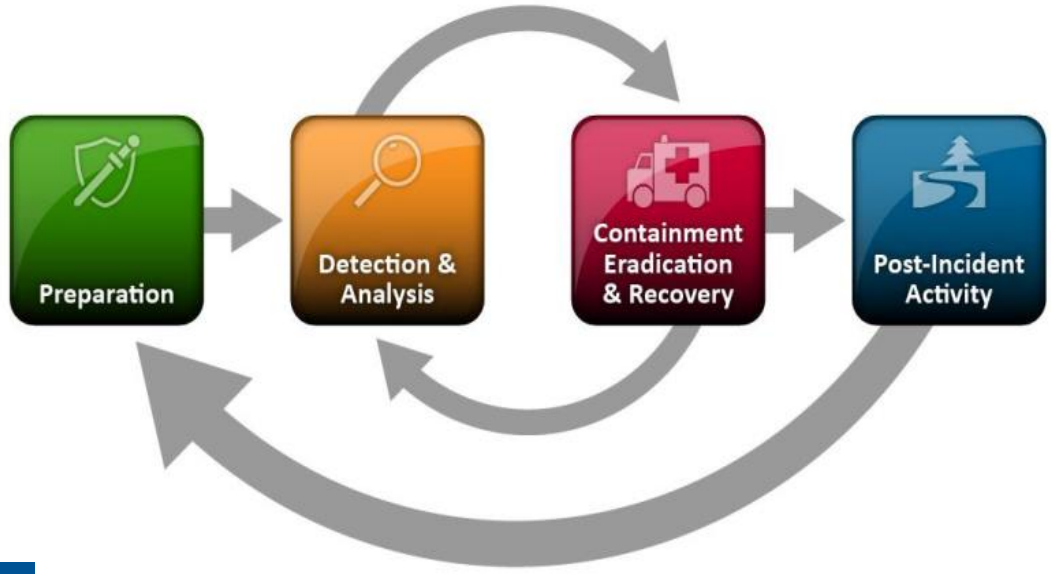
– síťové prvky mohou generovat netflow
- dodavatelé aplikací mohou upravit logy aby je Váš SIEM lépe parsoval
- dodavatelé firmwarů Vašich zařízení garantují jejich odolnost vůči penetračnímu testování?

Povinnost přetvořená do obchodní příležitosti

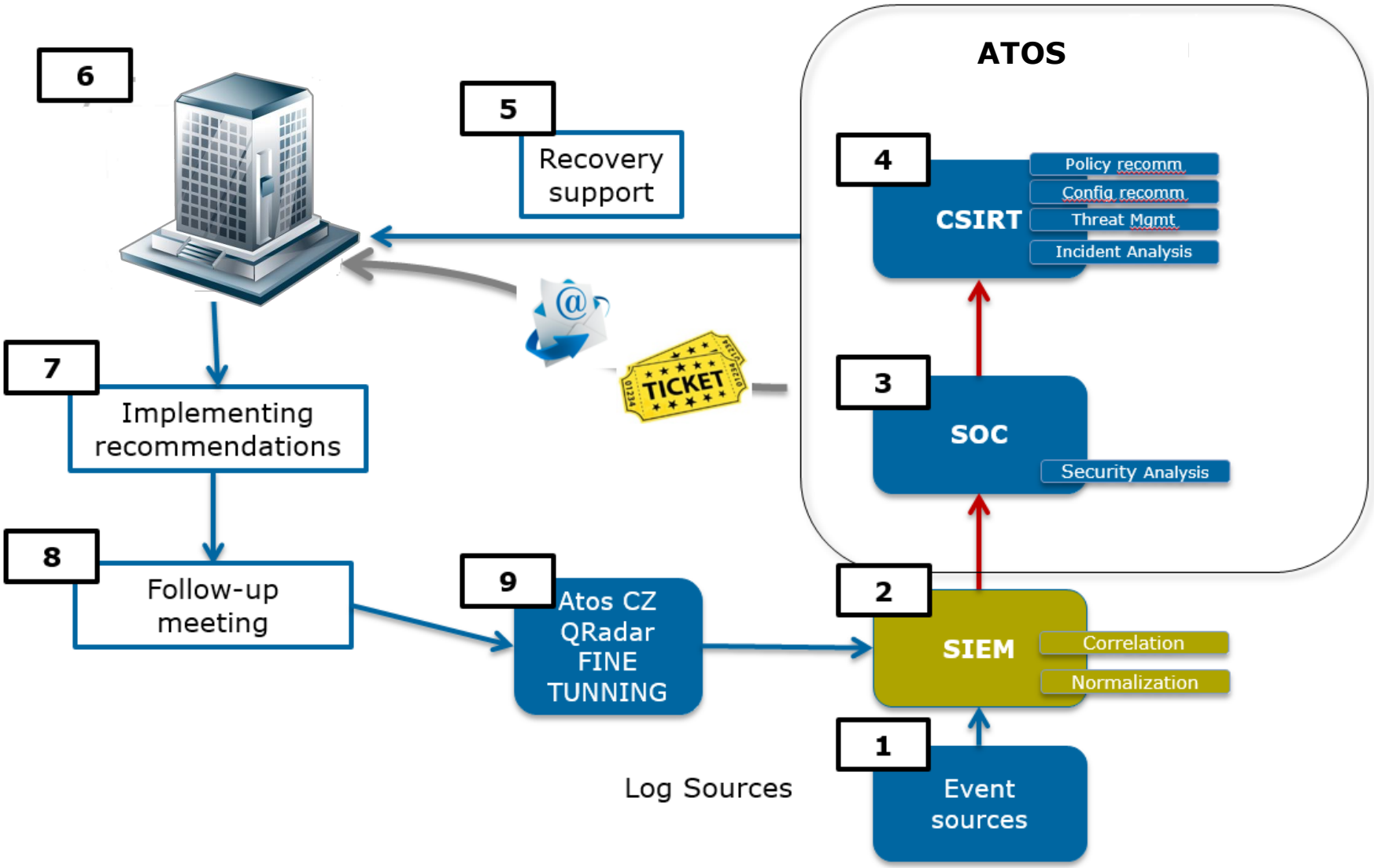
….. a to nejen pro komerční subjekty



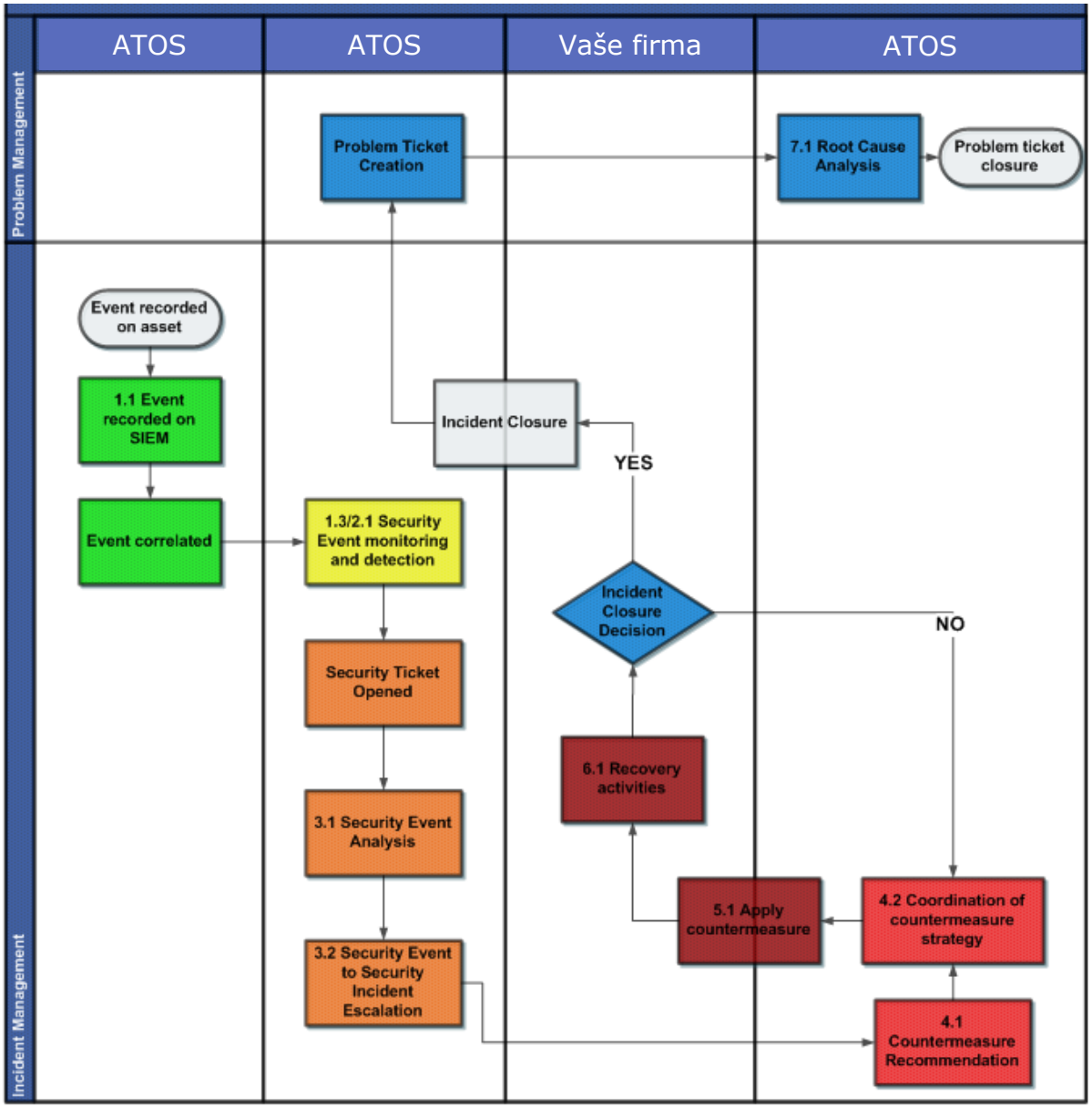
ATOS: V čem jsme dobří - metodika



V čem jsme dobří – metodika



V čem jsme dobří – metodika



Typické workflow řešení bezpečnostního incidentu

Každý incident je v souladu s Vaší bezpečnostní politikou zpracován dle daného SLA

Každý scénář má jasné přiřazení odpovědnosti

Security – Požadavky na lidský zdroje
Analytik cyber security

Atos CYBER security

- Zkušeností z obdobné pozice
- **Certifikace**

CompTIA Security+

- **Anglický jazyk**

B2 – Common European Framework of Reference for Languages

- **Sentinel Training**

NetIQ Sentinel

- **SIEM McAfee Training**

McAfee

- **QRadar Training**

IBM Radar

- **Other Security Trainings**

- ITIL Foundation

  - ✓ Event Mgmt
  - ✓ Incidnet Mgmt
  - ✓ Change Mgmt
  - ✓ Problem Mgmt
- Interní procesy organizace na zvládání incidentů

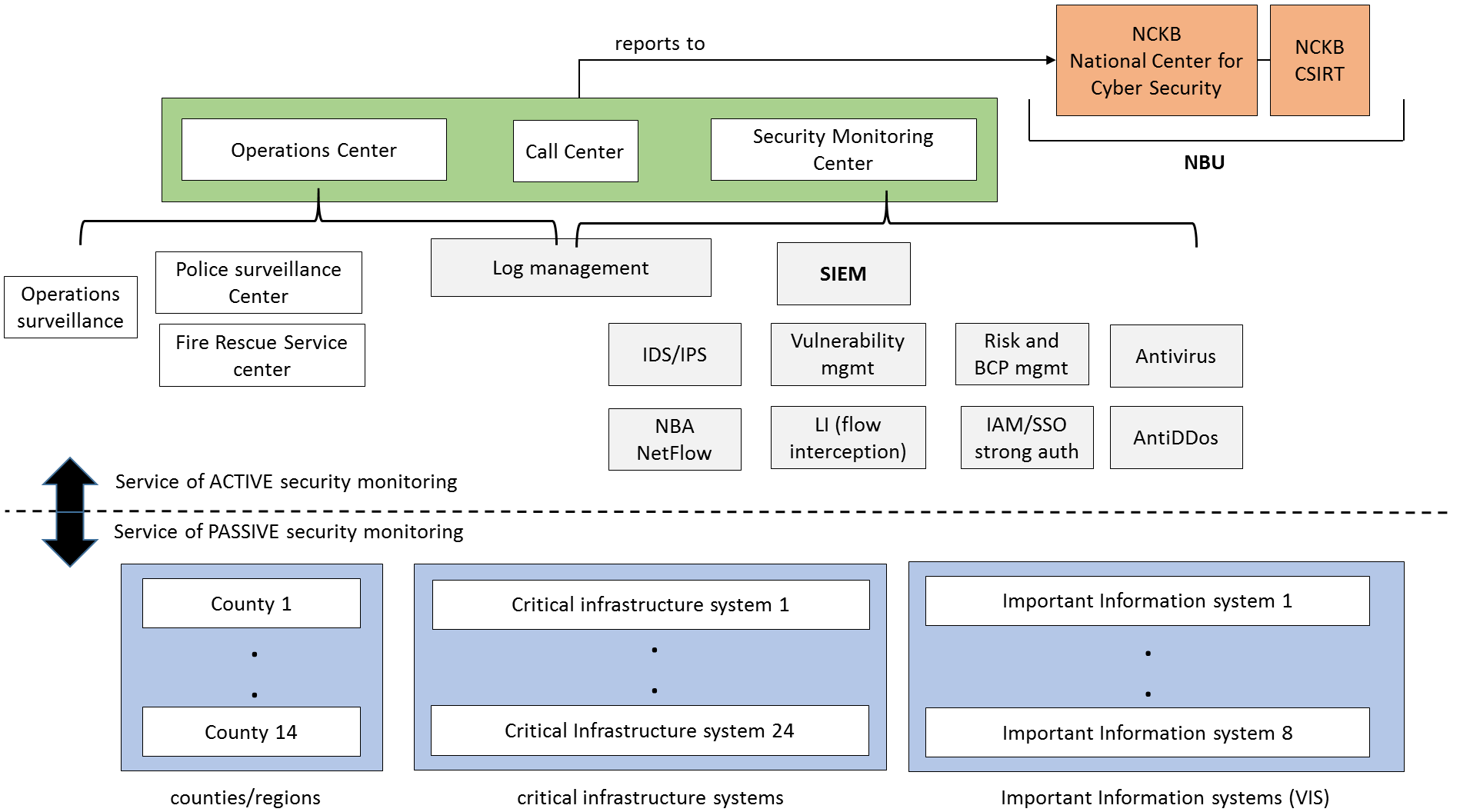
- Rozsah monitoringu
- Security Incident Response procedures
- CSIRT Incident Management
- Eskalační procedury

Management

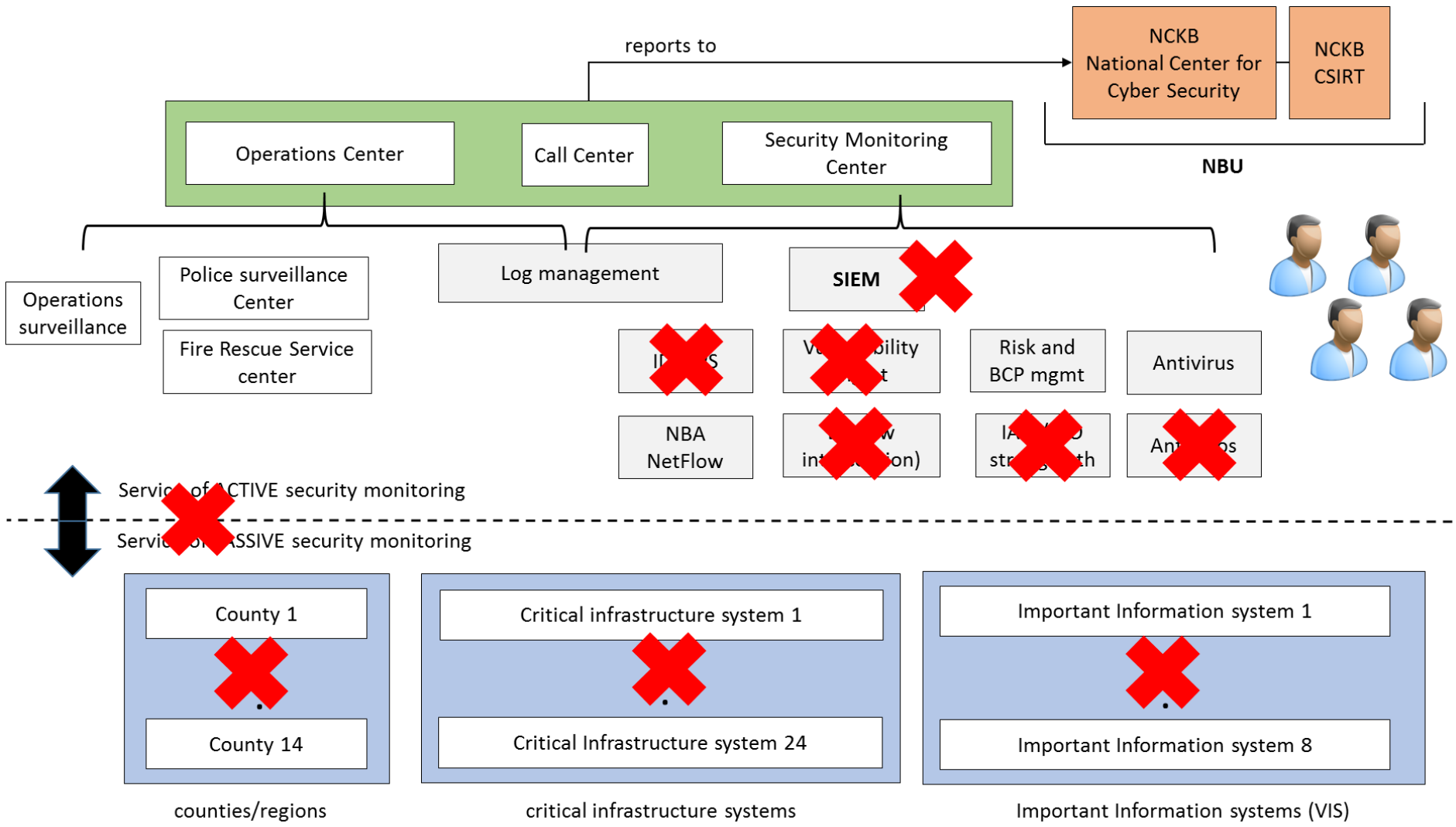
Technické znalosti → Nástroje → Pracovní náplň → Řešení incidentů

Atos

Jaký je na začátku plán



A po 2 letech.....


reports to
NCKB
National Center for
Cyber Security
NCKB
CSIRT
NBU
Operations Center
Call Center
Security Monitoring
Center
Operations
surveillance
Police surveillance
Center
Fire Rescue Service
center
Log management
SIEM
Risk and
BCP mgmt
Antivirus
NBA
NetFlow
ACTIVE security monitoring
PASSIVE security monitoring
County 1
County 14
Critical infrastructure system 1
Critical Infrastructure system 24
Important Information system 1
Important Information system 8
counties/regions
critical infrastructure systems
Important Information systems (VIS)

Nejnižší cena = nejvyšší TCO

13. Hodnoticí kritéria a způsob hodnocení nabídek

a. Základním hodnotícím kritériem pro hodnocení VZ je ve smyslu § 78 odst. 1 písm. b) ZVZ **nejnižší nabídková cena**.

b. Pro hodnocení nabídek je rozhodující **nejnižší celková nabídková cena v Kč včetně DPH.**

Způsob podání nabídky

Dodavatel podává nabídku elektronicky prostřednictvím e-tržiště.

Specifikace hodnotících kritérií a metody hodnocení

Základní hodnotící kritérium Nejnižší nabídková cena

Označení	Název dílčího hodnotícího kritéria	Váha v %
A	Nabídková cena	70%
B1	Požadavky na součinnost Zadavatele	5%
B2	Počet pracovních dní nutných pro první část implementace dle Přílohy 2 vzoru smlouvy	20%
B3	Počet pracovních dní nutných pro druhou část implementace dle Přílohy 2 vzoru smlouvy	5%

ATOS SOC – přijeďte se inspirovat

Referenční návštěva v ATOS Security Operations Center

14 – 15. 4. 2016, Bydgoszcz, Polsko

Agenda

DEN 1 – čtvrtek 14. 4. 2016

09:30	Zahájení - Představení Atos Big Data & Security Poland	*Marcin Lipinski, CEE Head of*
10:00	Atos Security Monitoring and Detection	*SOC (Maciej Glama)* *Vulnerability Management (* *AHPS service (Przemek Buko*
12.00	Oběd	
13.30	Prohlídka všech oddělení Security Operations Center	*Jakub Chmielewski*
14:30	TPS – Organizational Cyber Security –	
16:00	Atos Security Incident Response - CSIRT	*Piotr Chmylkowski*
16:45	Atos Security Prevention – Identity and Access Management	*Kamil Jarzembski*
18:00	Individuální konzultace s jednotlivými členy SOC týmu	

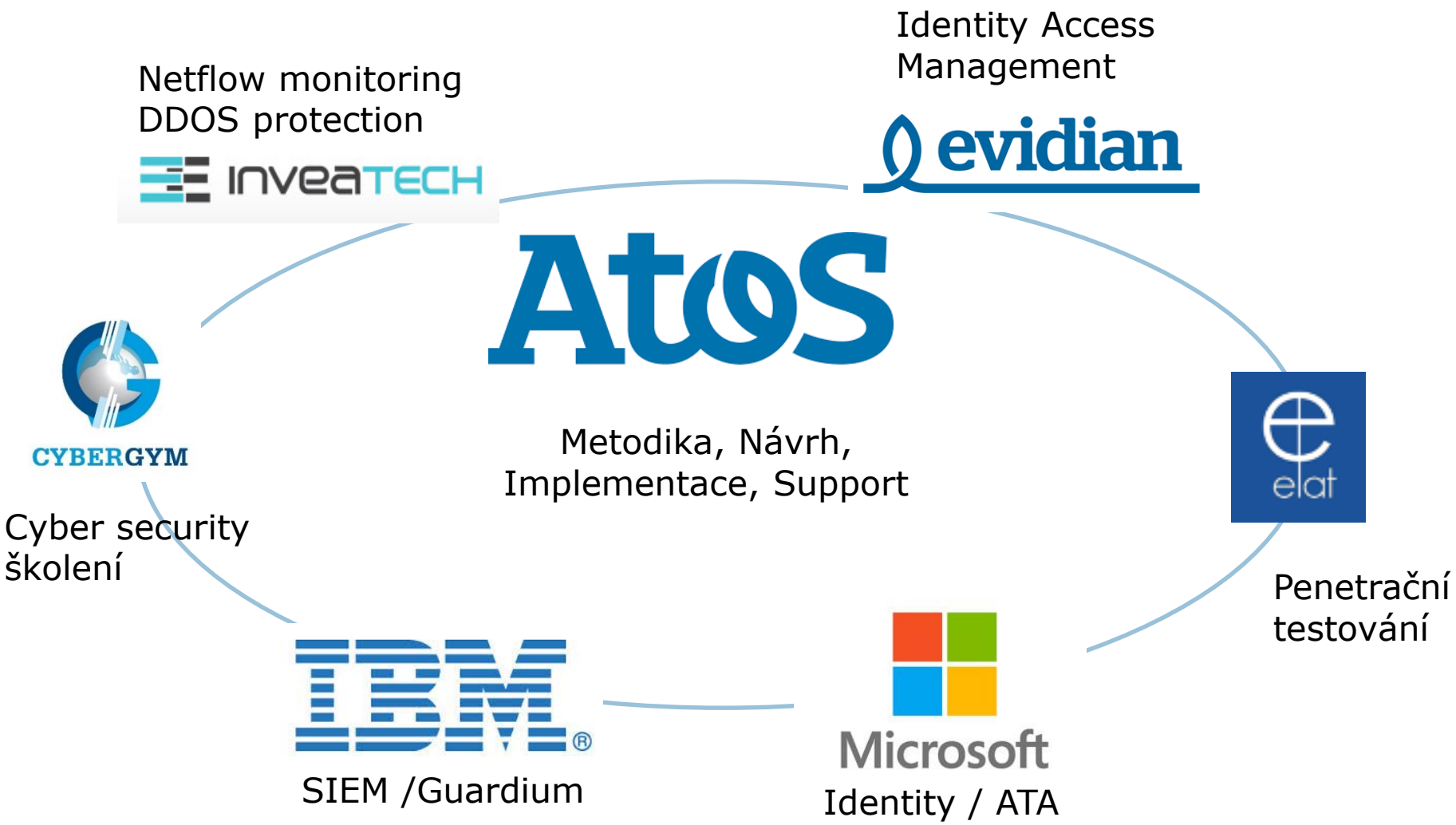
DEN 2 – pátek 15. 4. 2016

09:30	Atos Security Prevention – Endpoint perimeter protectio	*Rafal Grochowski*
10.15	CIC – National Cyber security challenge to country inter	
12.00	Individuální konzultace s jednotlivými členy SOC týmu	

Security Operations Center – služba nebo infrastruktura?

Dohledové bezpečnostní centrum jako služba?
Nebo si chcete vytvořit své vlastní centrum?

ATOS je Integrátor



Tomáš Hlavsa

tomas.hlavsa@atos.net

cz.atos.net