Kybernetická bezpečnost od A do Z

....aneb na co v Čechách zapomněli

Tomáš Hlavsa

Atos CYBER security

Your business technologists. Powering progress

ATOS – základní údaje

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

ATOS a jeho partneři

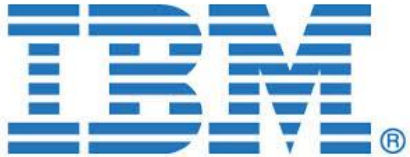
Netflow monitoring
DDOS protection

Identity Access
Management

Methodology, Implementation,
Support, Services

Cyber security
Training

Penetration
testing



SIEM
Security software vendor

Ne technologie, ale lidé a procesy

Co poskytujeme a v čem se odlišujeme

Vyhodnocení informačních aktiv → Analýza rizik → Návrh organizačních technických opatření → Zavedení opatření → Audit

- Znalost legislativy, norem, regulací
- Zkušenost, znalost rozsahu, jaké metriky
- Přehled o možnostech technologie
- Účinnost zavedených opatření?
- Jaká metrika?

Kybernetická bezpečnost jako řízená služba

Atos

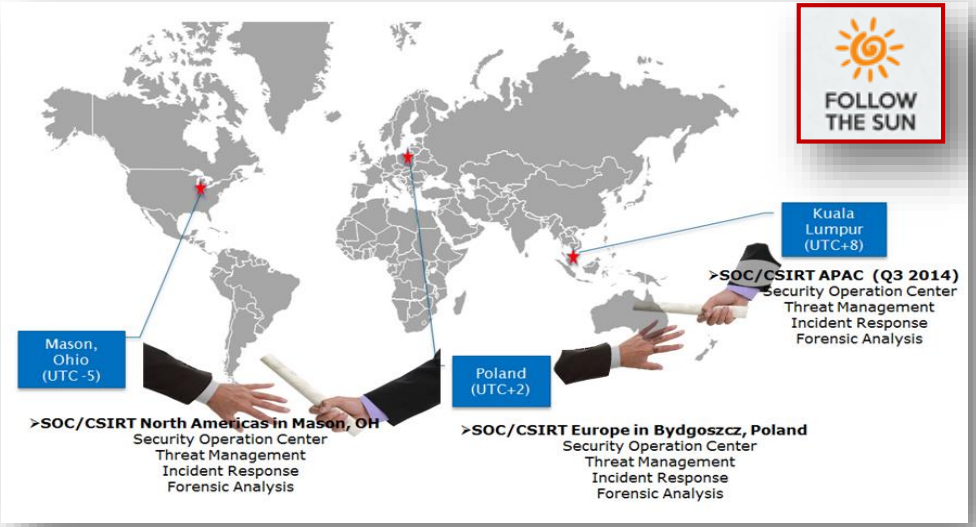
ATOS – 6 mezinárodních SOC center

FAKTA |

ATOS Poland | Bydgoszcz

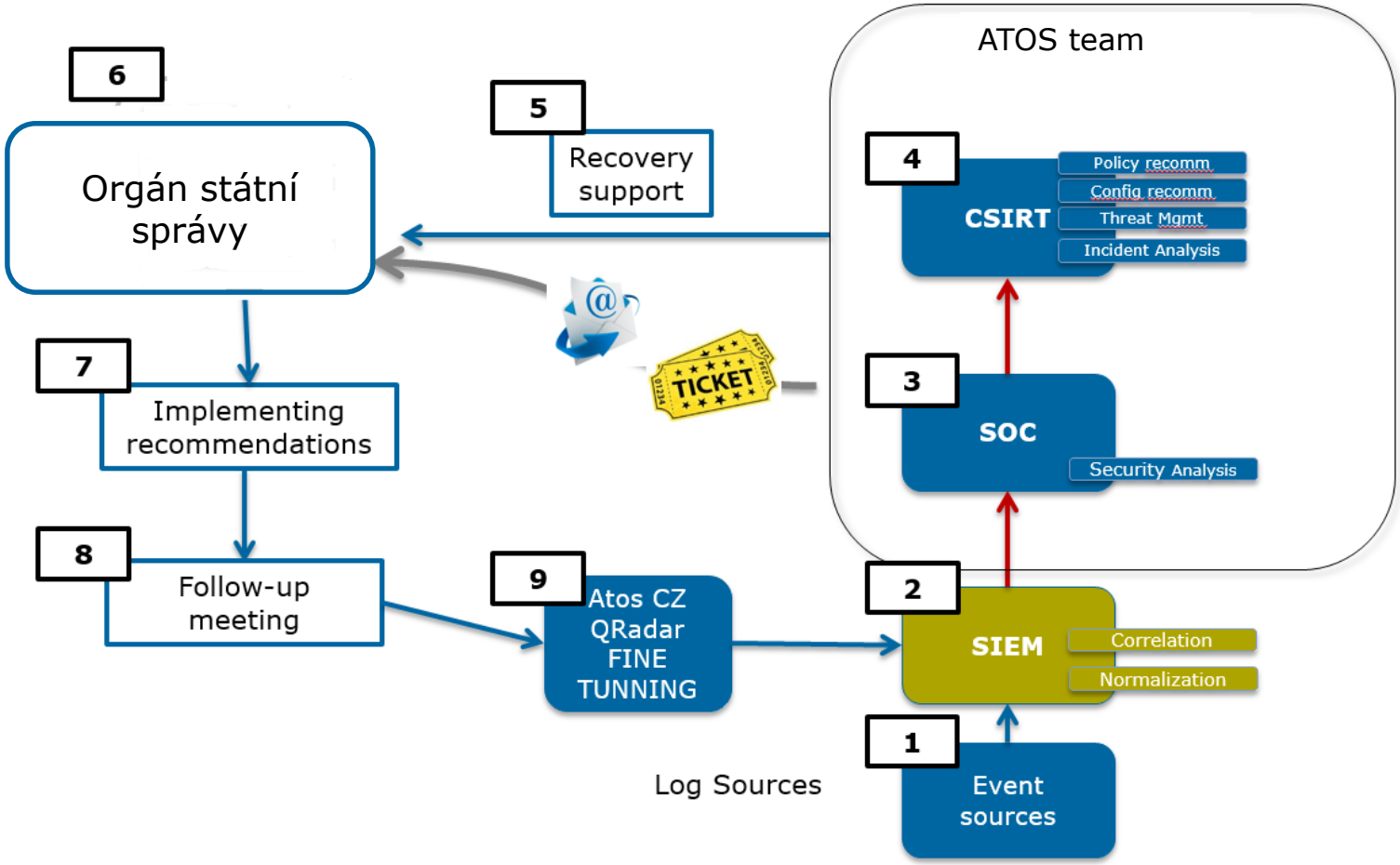
- **SOC centra v:**
  - **Polsku**
  - FRANCII
  - SPOJENÉM KRÁLOVSTVÍ
  - **SEVERNÍ AMERICE**
  - **MALAYSII**
  - INDII

*ATOS **GLOBAL** SOC – FOLLOW THE SUN

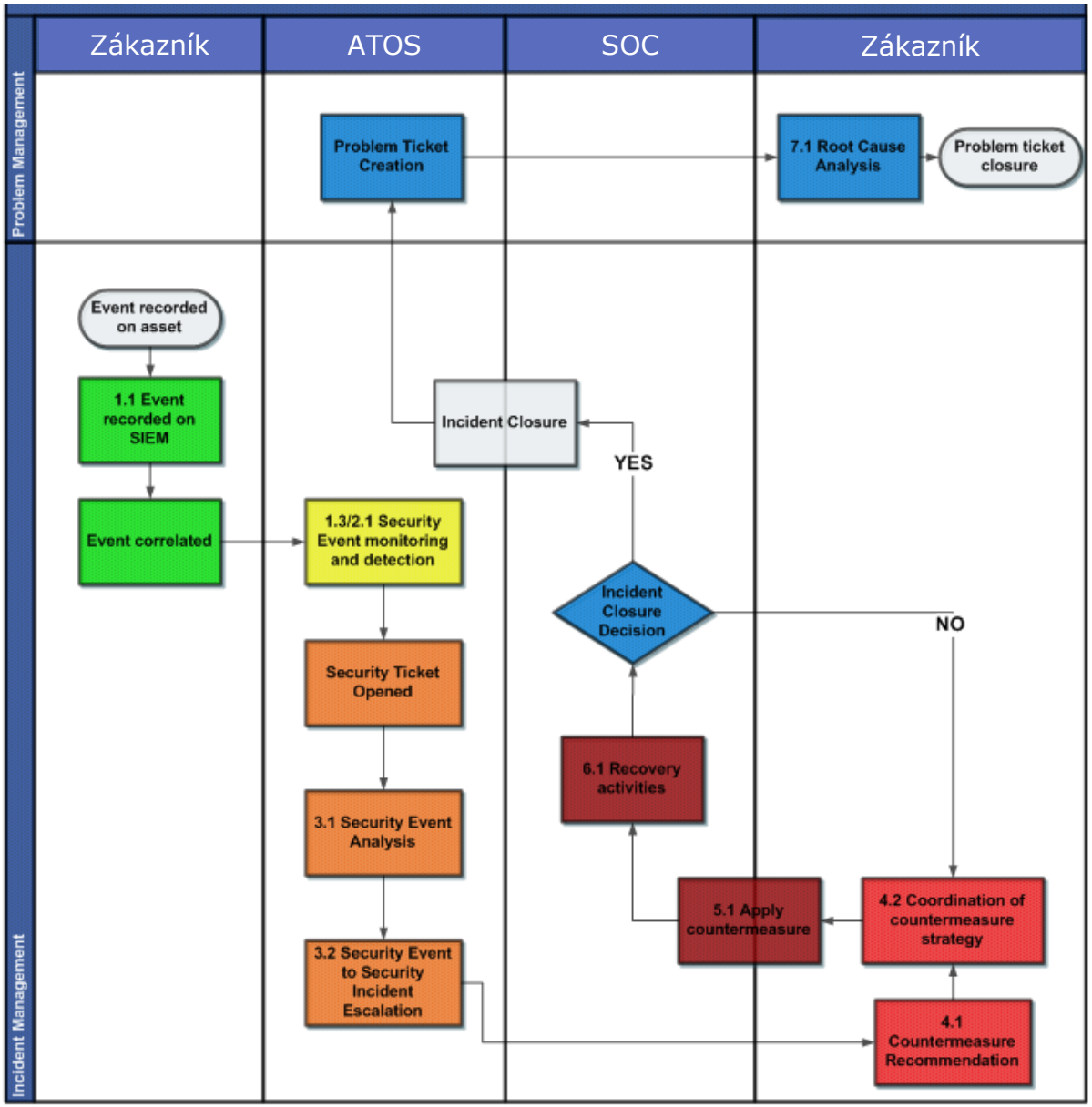


Typické Workflow

Workflow cyber incidentu (ticketu) poskytuje základní informaci o aktivitách provázejících každý incident. Detailní popis workflow ATOS dokumentuje v „Security Incident Response Procedure“, který musí být odsouhlasen Zákazníkem.



Workflow



Typické workflow řešení cyber incidentu

Každý bezpečnostní incident vychází ze scénáře, který má oporu v bezpečnostní politice Zákazníka.

Scénaře jsou „na míru“ každému zákazníkovi.

Jasné rozdělení odpovědnosti a návaznosti v komunikaci.

SLA v praxi

Solving		
Critical event/incident	**Medium priority event/incident**	**Low priority events/incidents**
2 hrs (response time*) / 4 hrs (solving)	**6 hrs (response time) / 8 hrs (solving)**	**2 MD (response time) / 14 hrs (solving)**
*Response time = pick up the incident and start to solve it, so called reaction time as usually defined in RFP		
Analysis		
Critical event/incident	**Medium priority event/incident**	**Low priority events/incidents**
3 MD (solving) /4 hrs (response time)	**6 MD (solving) /8 hrs (response time)**	**10 MD (solving) / 14 hrs (response time)**
Post-incident Activities		
Critical event/incident	**Medium priority event/incident**	**Low priority events/incidents**
1 MD After mitigation steps for alerts and their solving		

Security – Požadavky na lidský zdroje
Operátor cyber security

- **Certifikace**

CompTIA Security+

- **Znalost organizace a její bezpečnostní politiky**
- **Anglický jazyk**

B2 – Common European Framework of Reference for Languages

- **Ticketing systems**
- **Security Monitoring tools**

- ITIL Foundation

- ✓ Event Mgmt
- ✓ Incidnet Mgmt
- ✓ Change Mgmt
- ✓ Problem Mgmt

- Infrastructure monitoring
- Infrastructure Incident Response prodecury
- Eskalační procedury

Technické znalosti → Nástroje → Pracovní náplň → Řešení incidentů

Security – Požadavky na lidský zdroje
Analytik cyber security

- Zkušeností z obdobné pozice
- **Certifikace**
- **Anglický jazyk**

- **Sentinel Training**
- **SIEM McAfee Training**
- **QRadar Training**
- **Other Security Trainings**

- ITIL Foundation

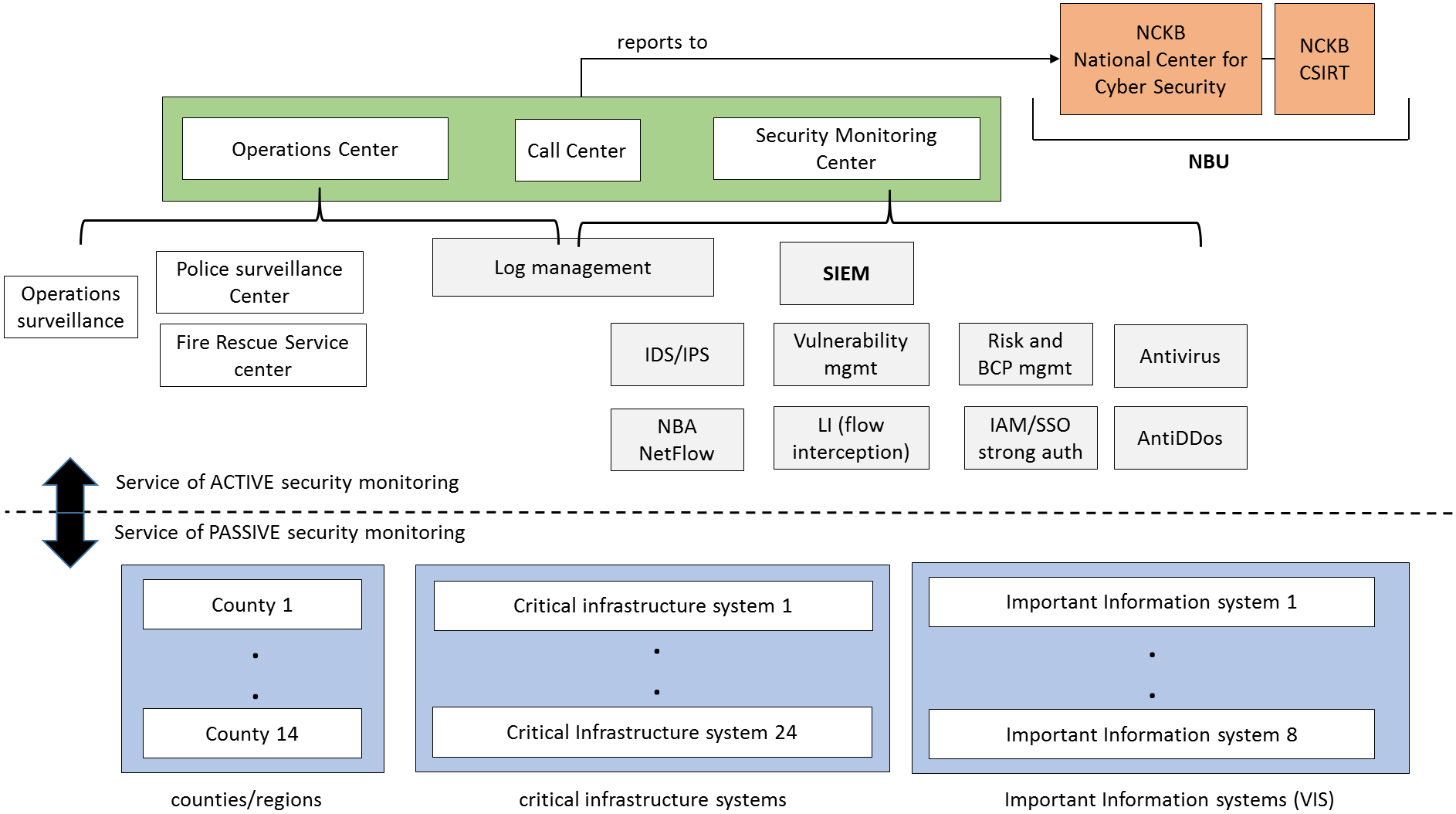
  - ✓ Event Mgmt
  - ✓ Incidnet Mgmt
  - ✓ Change Mgmt
  - ✓ Problem Mgmt
- Interní procesy organizace na zvládání incidentů

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

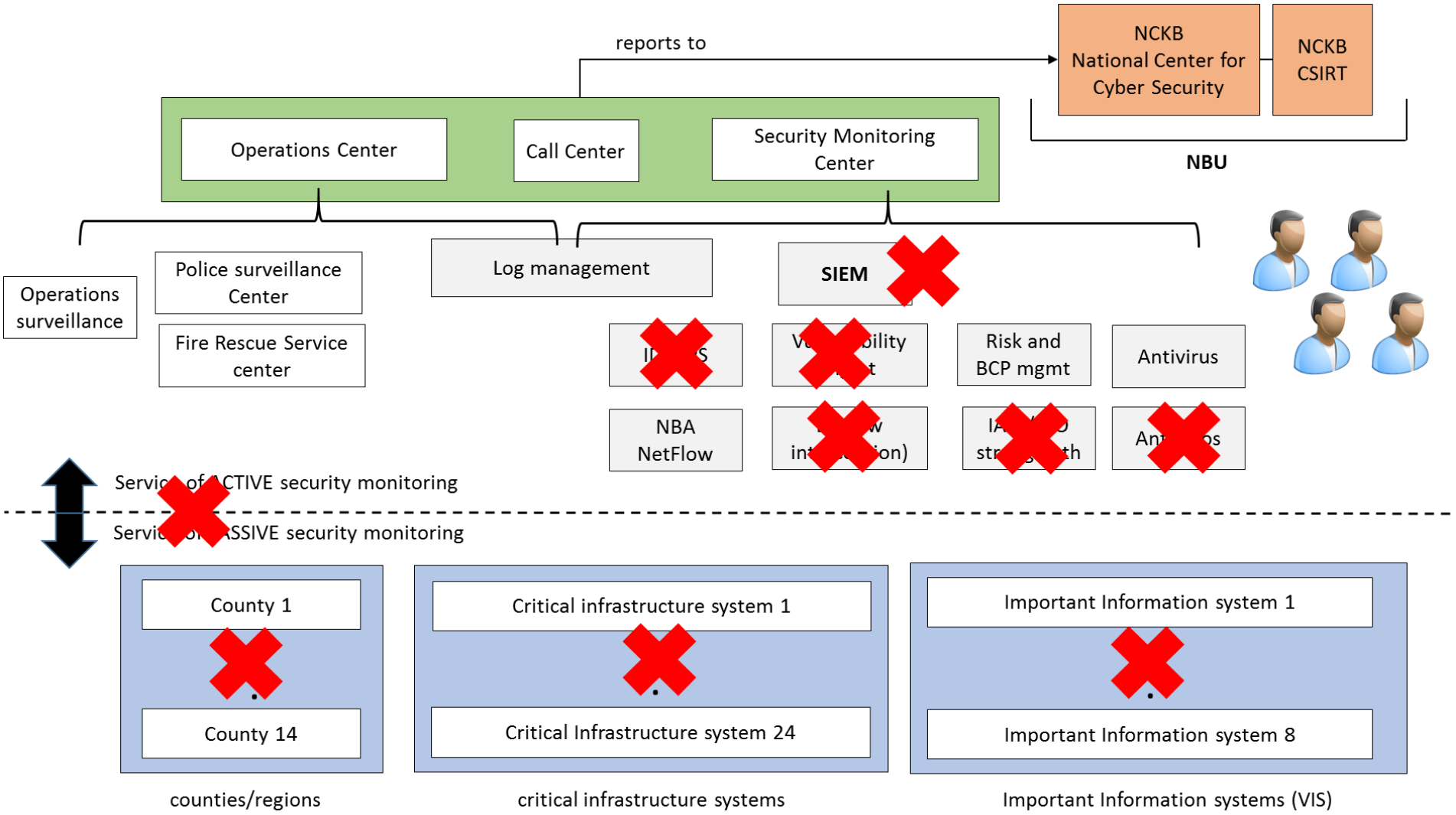
Management

Technické znalosti → Nástroje → Pracovní náplň → Řešení incidentů

Jaký je na začátku plán



A po 2 letech.....

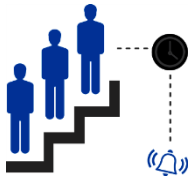

reports to
NCKB
National Center for
Cyber Security
NCKB
CSIRT
NBU
Operations Center
Call Center
Security Monitoring
Center
Operations
surveillance
Police surveillance
Center
Fire Rescue Service
center
Log management
SIEM
Risk and
BCP mgmt
Antivirus
NBA
NetFlow
ACTIVE security monitoring
PASSIVE security 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)

Jak se staví - SOC

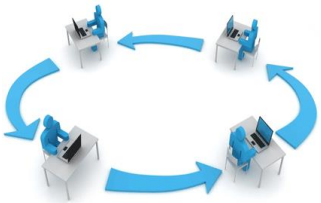
Security Operations Center 24/7/365

- ✓ **ITIL ALREADY IN ACTION**

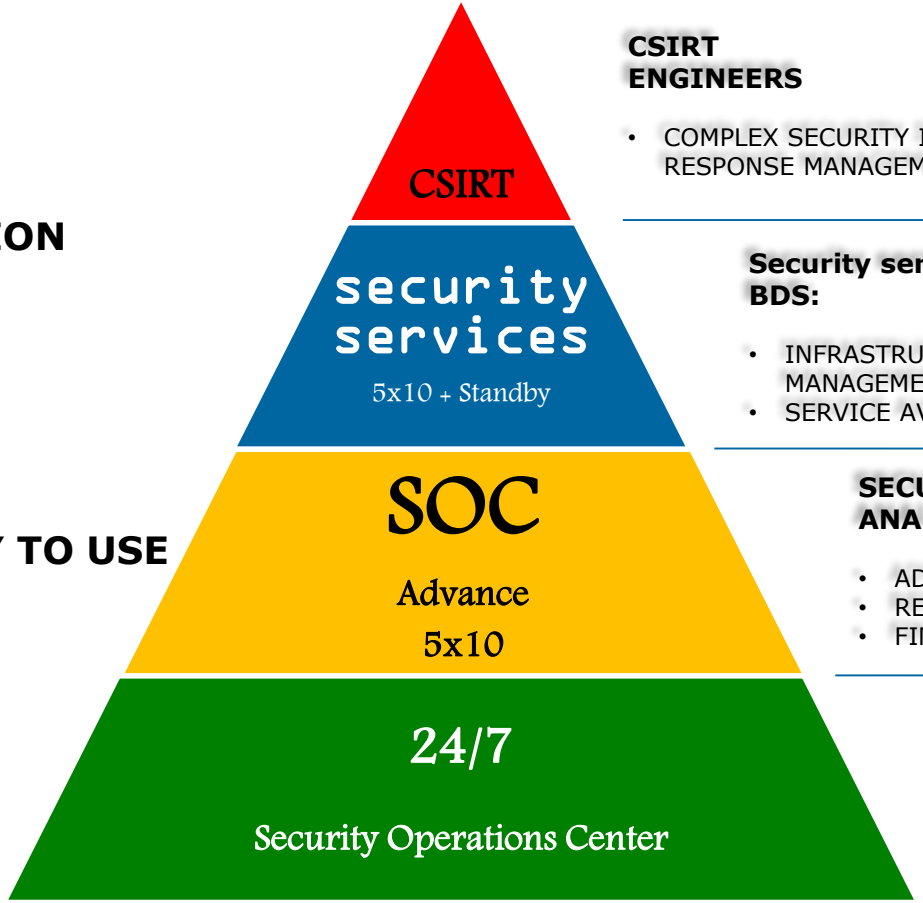
- ✓ **WORKING ESCALATION PROCEDURES**



- ✓ **WORKFLOWS READY TO USE**



- ✓ **DOCUMENTATION LIBRARY IN PLACE**



CSIRT ENGINEERS

- COMPLEX SECURITY INCIDENT RESPONSE MANAGEMENT

Security services from Atos BDS:

- INFRASTRUCTURE MANAGEMENT
- SERVICE AVAILABILITY

SECURITY ANALYSTS

- ADVANCE INVESTIGATION
- REPORTS
- FINE-TUNNING

SECURITY OPERATORS

- MONITORING SECURITY
- MONITORING AHPS INFRASTRUCTURE
- COMMUNICATION

Ne technologie, ale lidé a procesy

Co poskytujeme a v čem se odlišujeme

Vyhodnocení informačních aktiv → Analýza rizik → Návrh organizačních technických opatření → Zavedení opatření → Audit

- Znalost legislativy, norem, regulací
- Zkušenost, znalost rozsahu, jaké metriky
- Přehled o možnostech technologie
- Účinnost zavedených opatření?
- Jaká metrika?

Kybernetická bezpečnost jako řízená služba

Top ten safety and security guidelines

Atos

1 You are responsible for SECURITY

Atos implemented a security management system that encompasses information security, data protection, safety and physical security. All Atos assets (people, information incl. personal data, sites, materials, intellectual property) and the assets of our customers held in custody by Atos need to be protected by each of us (internal, external and third-parties). Therefore Atos has defined mandatory policies regarding security. You can obtain further information about these policies and on the roles and responsibilities in security by connecting to the SharePoint homepage, then clicking "Organization", "Support Functions" and "Group Security"*.

2 Always report security incidents

Security incidents (whether related to information security, data protection, safety, or physical security) must be reported as quickly as possible, in order to reduce possible damage to the Atos assets. See SharePoint, "Group Security"* and "How to report a security event or incident" for more information.

apply the appropriate protection. In addition, special attention must be paid by each of us when working with personal data (along with confidential and secret information), and must be strongly protected everywhere: during business trips/missions, at office, on removable devices, when spoken about in public or by phone, and not referred to in social media networks... Always consider the safest and most secure way!

5 Be careful with e-information (e-mails, Internet, etc.)

All kinds of virus programs can be attached to e-mails or downloaded from the Internet. Never open an e-mail that seems suspicious. Avoid the urge to read it – instead delete it! Surfing on the Internet, especially in social media, is not as anonymous and harmless as you might think. Don't download files from suspicious, dubious, or unauthorized sites as these may contain malware. Don't click on links to sites sent to you in an unsolicited e-mail - it may be a "phishing" trap.

6 Protect your data and devices (laptops, mobile devices...)

tant company information when you are out of your office. Never throw confidential papers/files in the collective baskets but in a locked bin or shredder in order to protect the information from any indiscretion.

8 Apply Atos sites security ruless

Know the site security measures (reminder: smoking is strictly forbidden inside all premises of Atos) and the site evacuation procedures in case of fire, bomb alert, flood, etc. and be prepared to apply them in case of need (regardless whether it is a real alarm or an exercise).

9 Respect access and controls in Atos sites

You hold one (or more) passes at various Atos premises. You must wear it visibly at all times. Everybody is responsible for his or her visitors. Visitors without proper clearance must be accompanied during their stay on premises at all times. Unescorted visitors are a serious violation of our safety and physical security policies. Do not hesitate to offer your assistance to an unescorted visitor.

ATOS SOC – přijďte 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

Kybernetická bezpečnosť pre verejnú správu

SEMINÁR – Štvrtok 2. Jún 2016

AGENDA:

08:30 – 09:00 *Registrácia účastníkov, občerstvenie*

09:00 – 09:15 Úvodné slovo, PPP + ATOS SK, Marian Duda

09:15 - 09:45 IBM Security Incident and Event Management (SIEM) – detekcia cyber security hrozieb, IBM CZ/SK, Juraj Porubčan

09:45 – 10: 30 Služby Security Operations Center (SOC) – budovanie/prevádzka špecializovaných IT Security pracovísk, ATOS SK, Marian Duda

10:30 – 10:45 prestávka na kávu

10:45 – 11:15 IBM Identity Access Management – správa identít a prístupov v IT prostredí, ATOS CZ, Ondřej Fišer / Miroslav Skokan

11:15 – 11:45 IBM Guardium – ochrana databáz, ATOS CZ, Petr Němec

11:45 – 12:30 IBM Netflow Monitoring - detekcia anomálií v komunikačných sieťach, Atos CZ, Security expert

12:30 – 13:30 prestávka na obed

13.30 – 14:00 IBM Security Threat Protection System (TPS), Atos CZ, Security expert

14.00 – 14.30 DDOS protection, ATOS, Security Expert

14.30 – 15:00 IBM Privilege Account management – monitoring privilegovaných užívateľov/administrátorov, Atos CZ, Ondrej Fiser

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%

Děkuji za pozornost

Tomas Hlavsa
tomas.hlavsa@atos.net
+420 604 290 196