Kybernetická bezpečnost ve státní správě

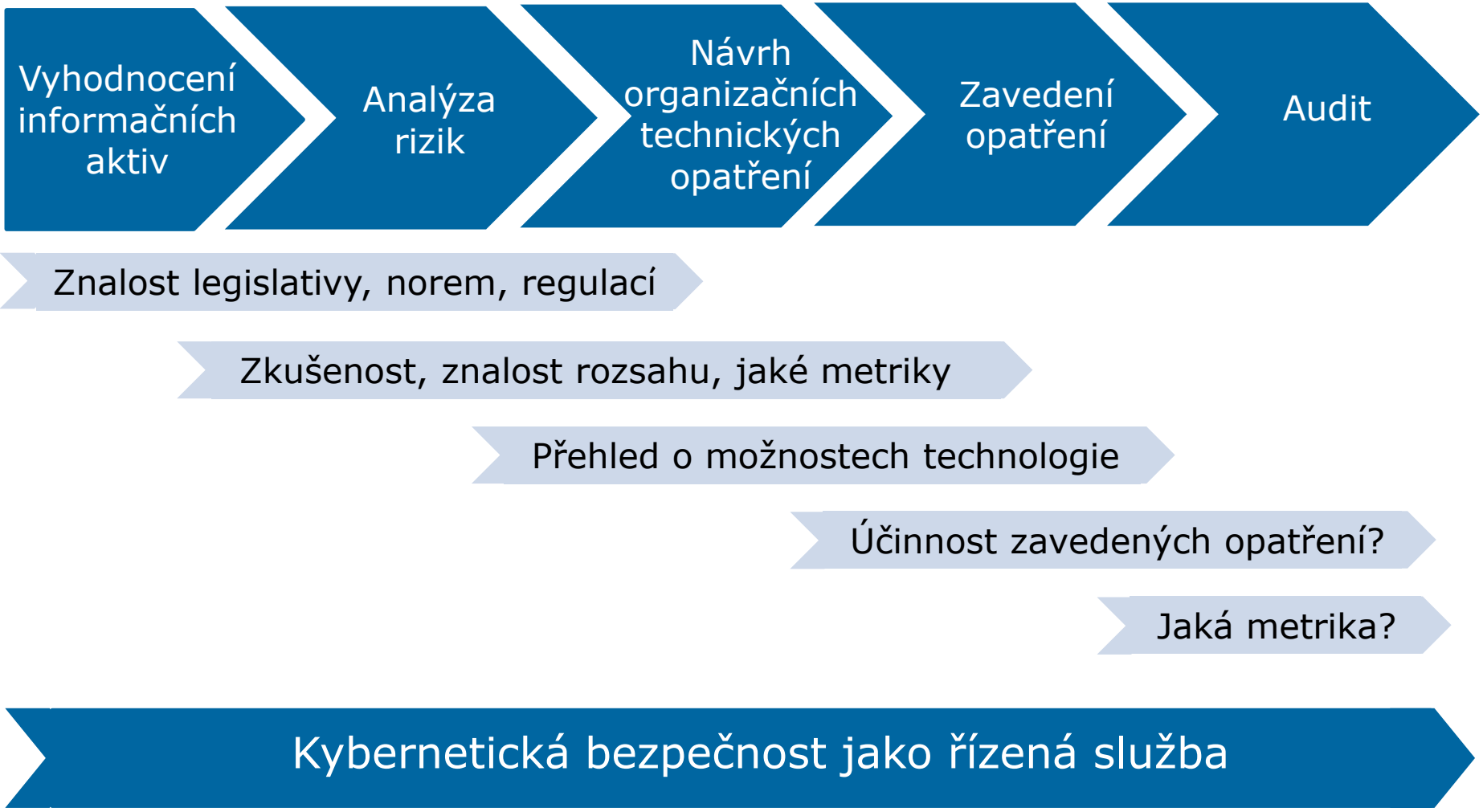
Tomáš Hlavsa

Atos CYBER security

Atos

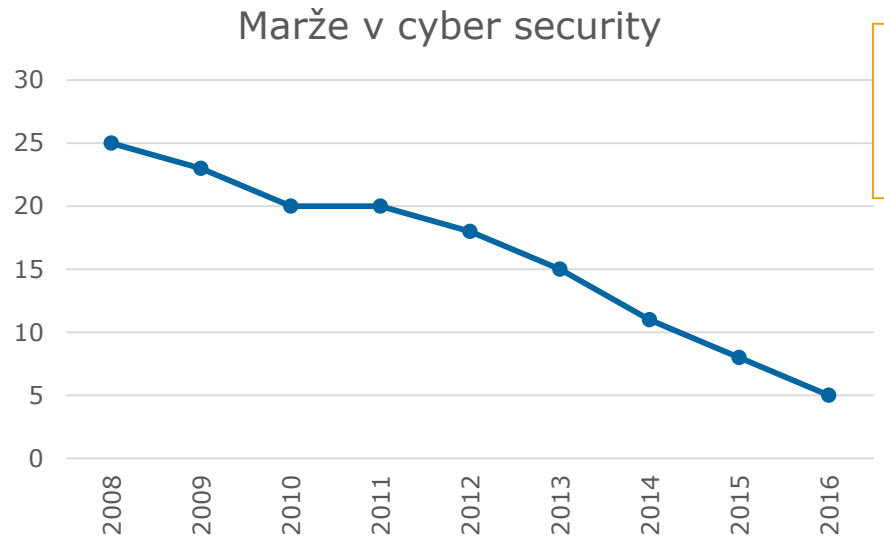
Investice do lidí x Investice do technologií

…… nezačínejte prosím technickým opatřením ……



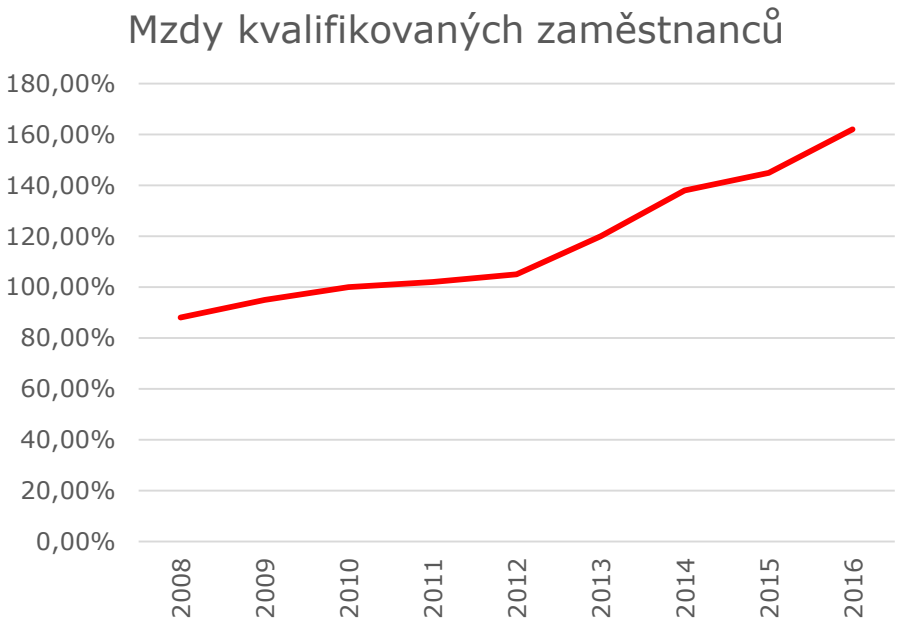
Pohled systémového integrátora

..... lépe již bylo .....



SIEM byl v roce 2011 „niche business“

…dnes je to komodita s <5% marží



Dnešní absolvent je o 60% dražší

než konzultant s praxí před 6ti lety

Nejnižší cena ? ….. a TCO na x let … a co kvalita? …..

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.**

Název	Outsourcing role specialisty na kybernetickou bezpečnost
Druh veřejné zakázky	
Druh plnění	Služby
Kriterium Nabídková cena	
Název	Nabídková cena
Váha	100,00
Absolutní omezení hodnot	

Způsob podání nabídky

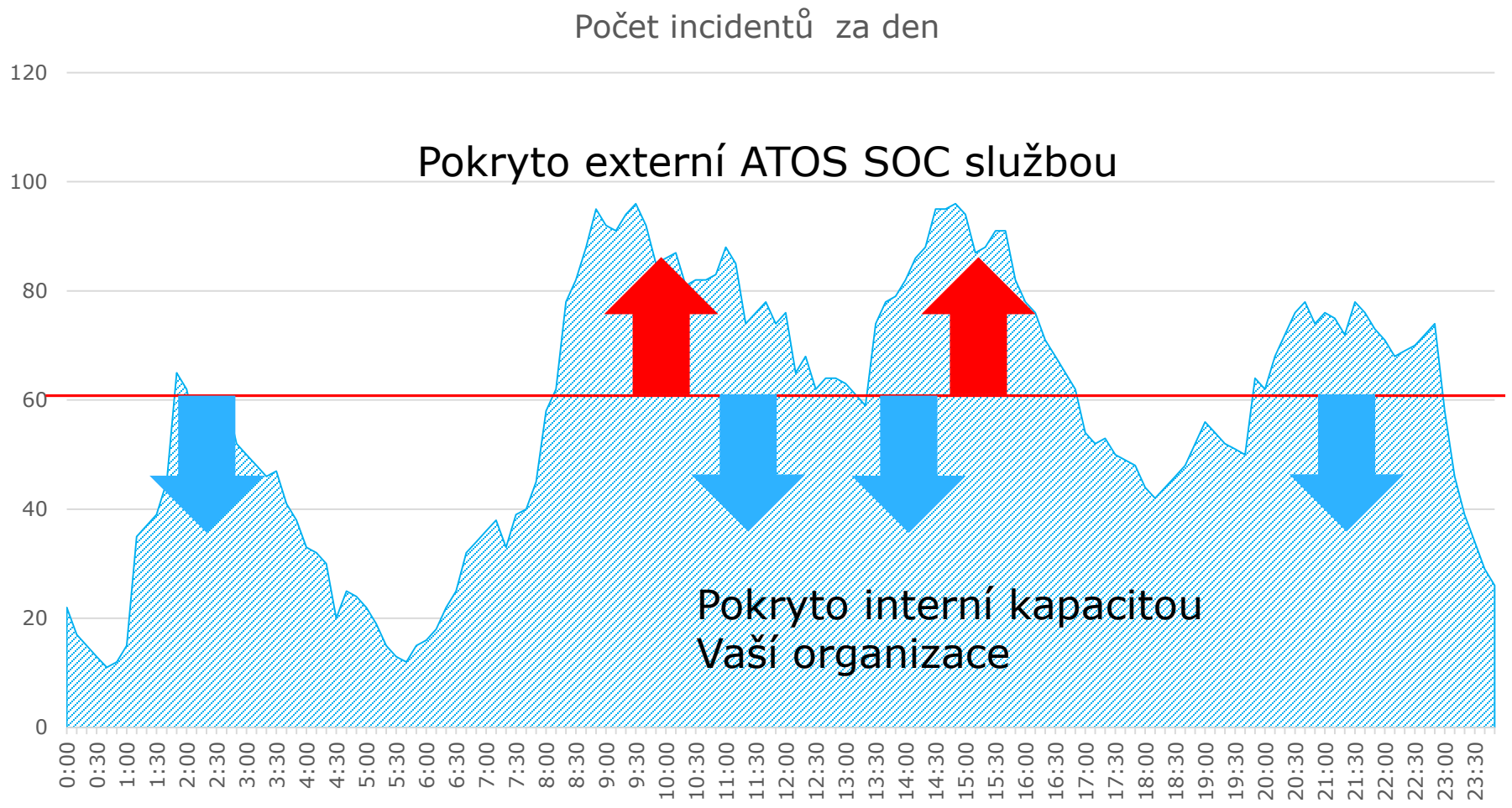
Dodavatel podává nabídku elektronicky pro

Specifikace hodnotících kritérií a metody hodnocení

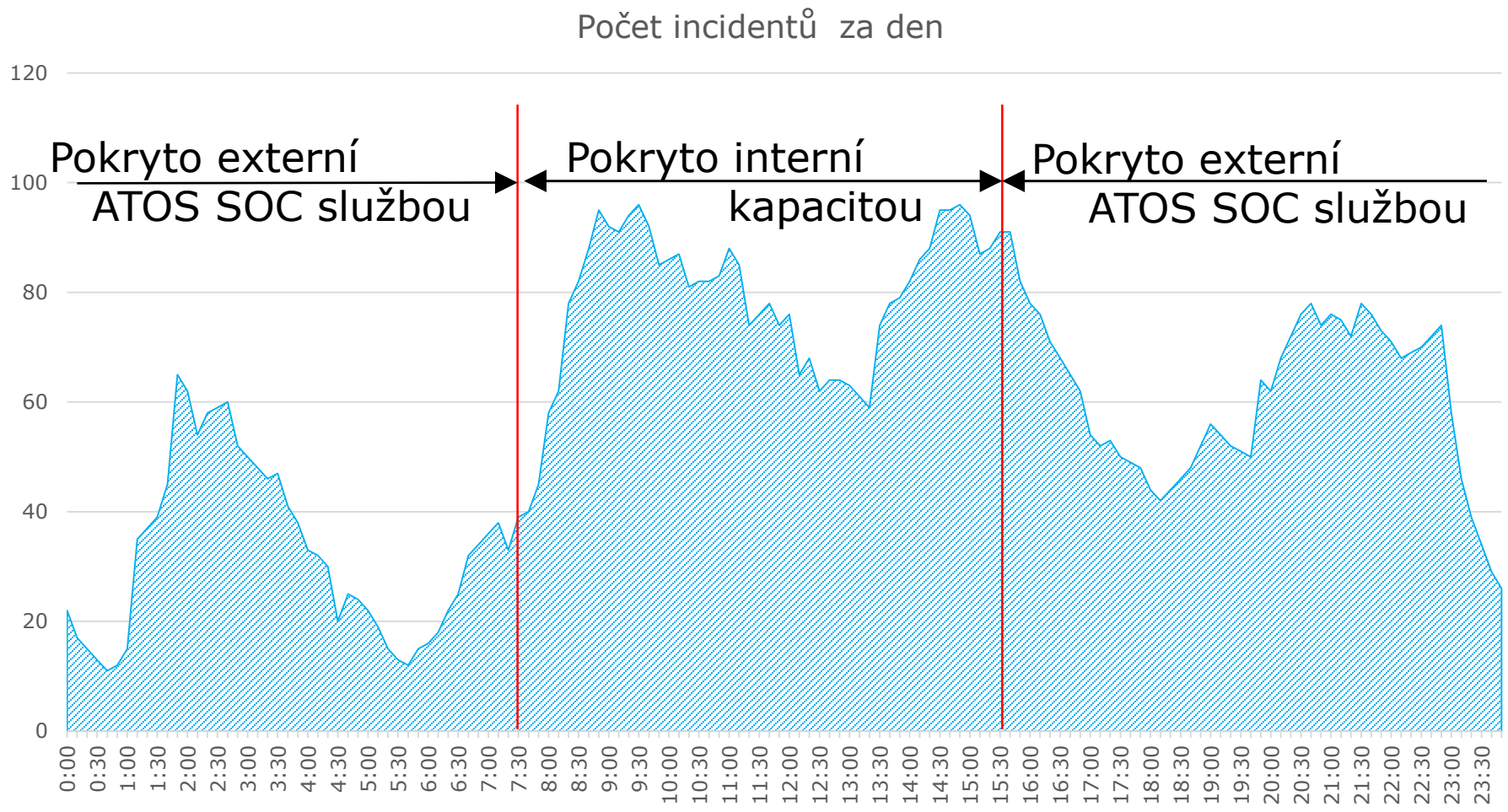
Základní hodnotící kritérium Nejnižší nabídková cena

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%

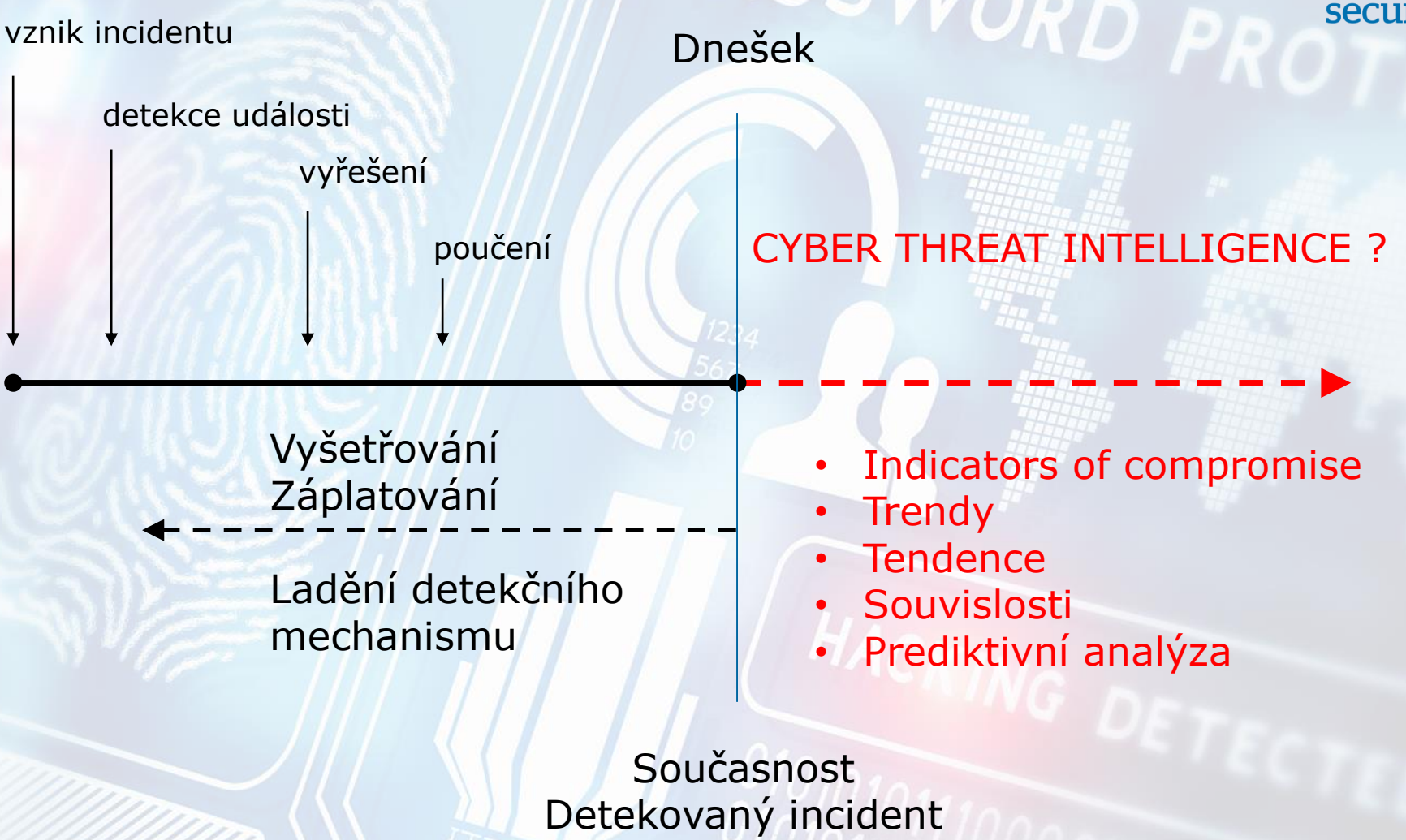
Pokryjete dnes incidenty vlastními silami?
…… a zítra?



Řešíte incidenty 24 x 7?
… a dovoláme se k Vám v sobotu dopoledne?



Příliš se díváme do minulosti



Co tedy ATOS odlišuje od desítek CYBER zaměřených firem?

Atos CYBER security

Schopnost přenosu zkušeností ze zahraničí

(Polsko, Izrael, Francie …….)

(SOC centra, informační zajištění Olympijských her ….)

Věda a výzkum

Bezpečnostní výzkum, H2020 ……

Vzdělávání

(eLearning, kontinuální vzdělávání …)

Síla největší evropské IT firmy

Kapacitní pokrytí,
expertiza, partnerská síť

Bezpečnostní řešení nejen v oblasti CYBER

Národní bezp. integrátor (Švýcarsko, Francie ….)

? Existuje vzájemně udržitelná spolupráce?

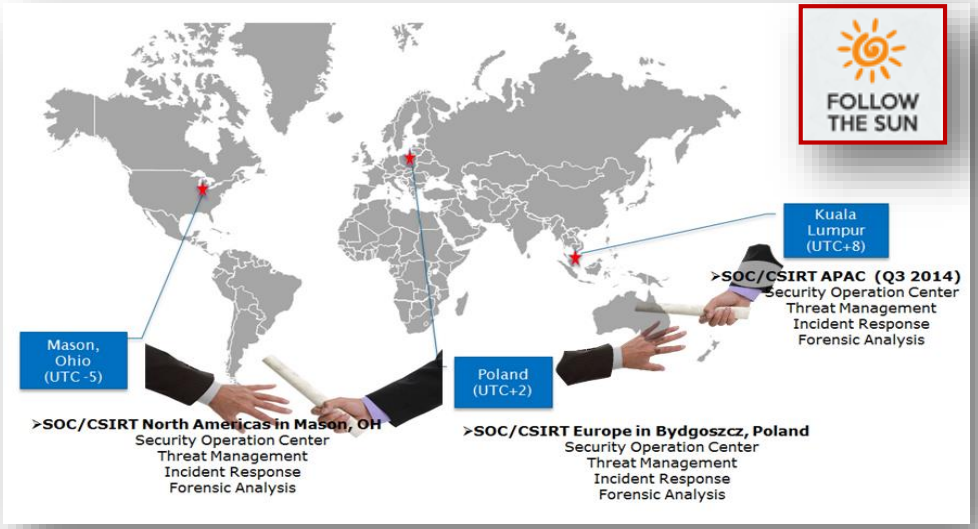
Atos

ATOS – mezinárodní SOC centra

ATOS Poland | Bydgoszcz

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

*ATOS **GLOBAL** SOC – FOLLOW THE SUN



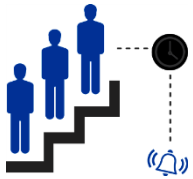
Jak se staví SOC – pár jsme jich už zvládli

.....Security Operations Center 24/7/365

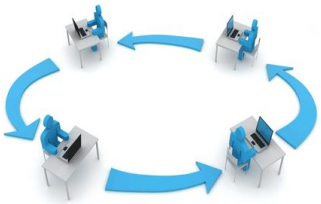
Atos CYBER security

- ✓ **ITIL ALREADY IN ACTION**

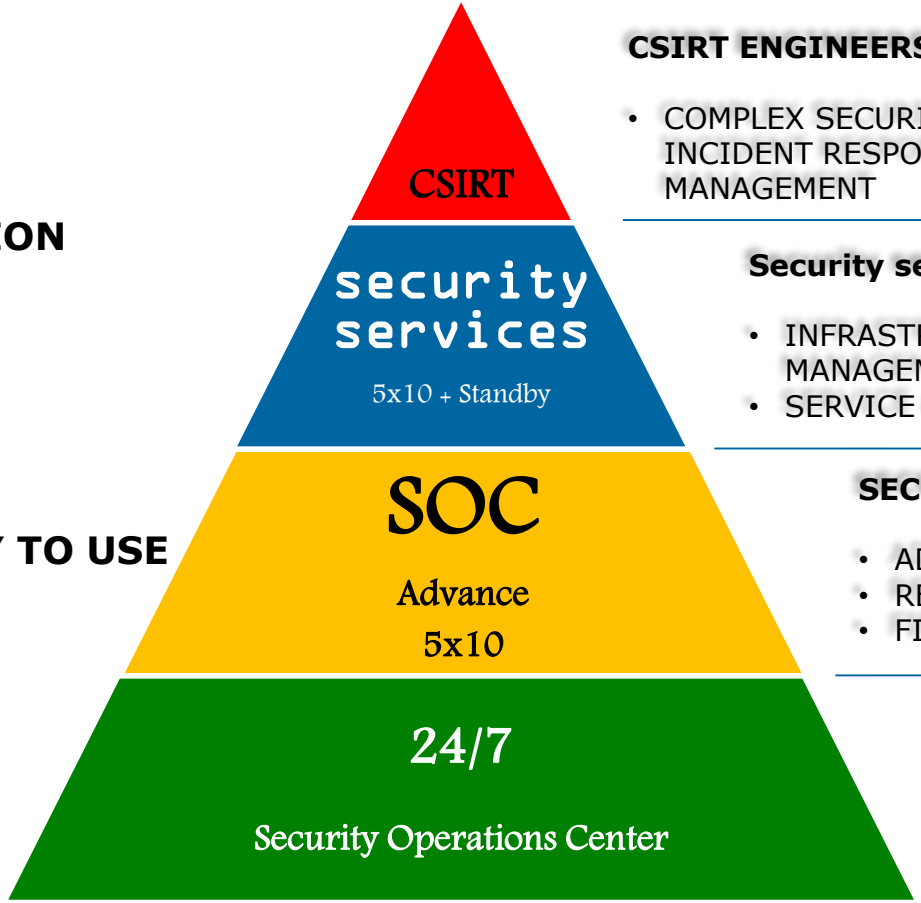
- ✓ **WORKING ESCALATION PROCEDURES**



- ✓ **WORKFLOWS READY TO USE**



- ✓ **DOCUMENTATION LIBRARY IN PLACE**



CSIRT ENGINEERS

- COMPLEX SECURITY INCIDENT RESPONSE MANAGEMENT

Security services from Atos

- INFRASTRUCTURE MANAGEMENT
- SERVICE AVAILABILITY

SECURITY ANALYSTS

- ADVANCE INVESTIGATION
- REPORTS
- FINE-TUNNING

SECURITY OPERATORS

- MONITORING SECURITY
- MONITORING AHPS INFRASTRUCTURE
- COMMUNICATION

Atos

Požadavky na Váš bezpečnostní tým?
.... vzdělání / praxe .....

Atos CYBER security

Technické znalosti

Zkušenosti z obdobné pozice

Certifikace

CompTIA Security+

Anglický jazyk

B2 – Common European Framework of Reference for Languages

Nástroje

Sentinel Training

NetIQ

NetIQ Sentinel

SIEM McAfee Training

McAfee

IBM Qradar Training

IBM Radar

Jiné podobné nástroje?

Pracovní náplň

ITIL Foundation

- Event Mgmt
- Incident mgmt
- Change mgmt
- Problem mgmt

Interní procesy organizace na zvládání incidentů

Řešení incidentů

Rozsah monitoringu

Security Incident Response proceduresv

CSIRT Incident Management

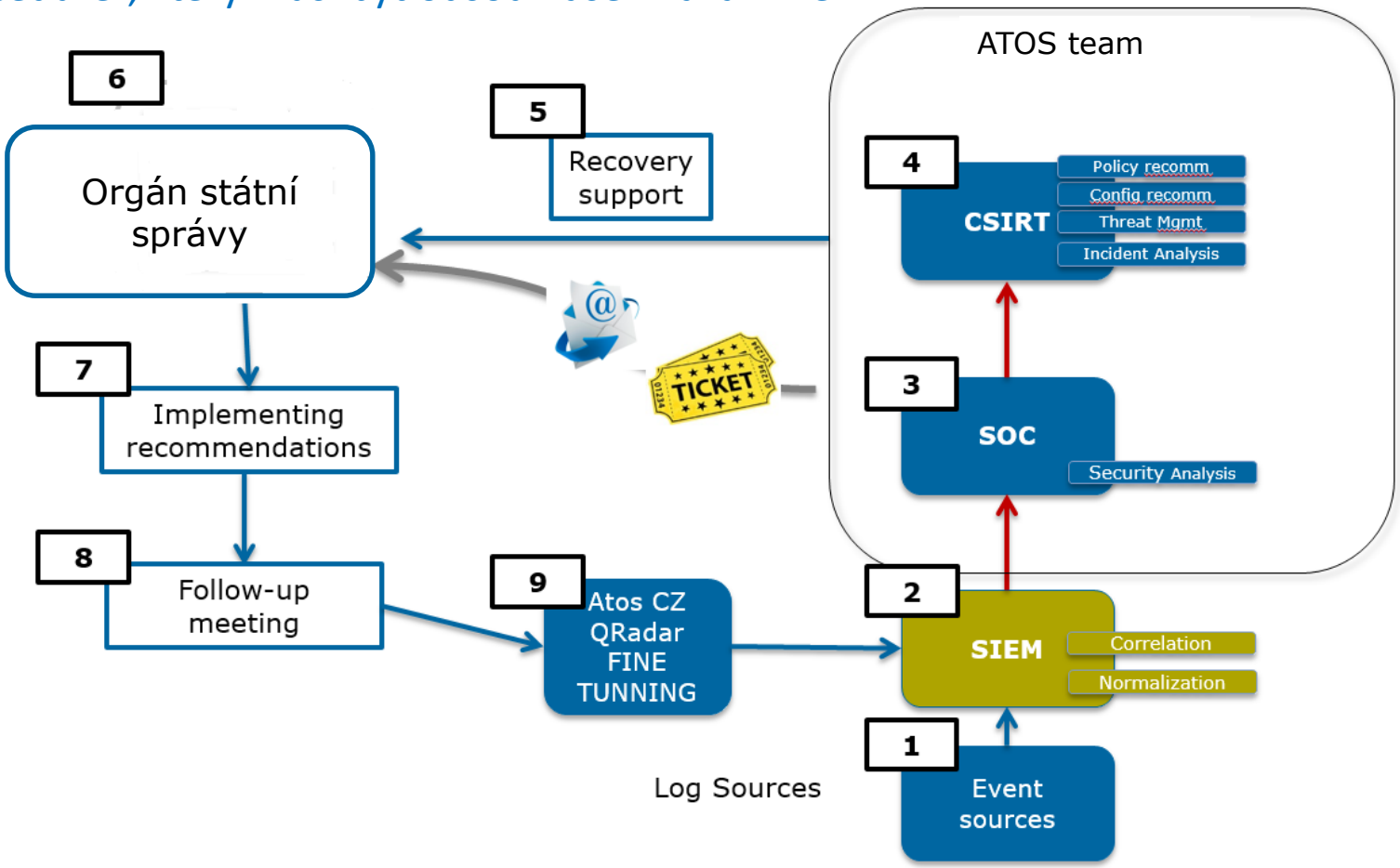
Eskalační procedury

Management

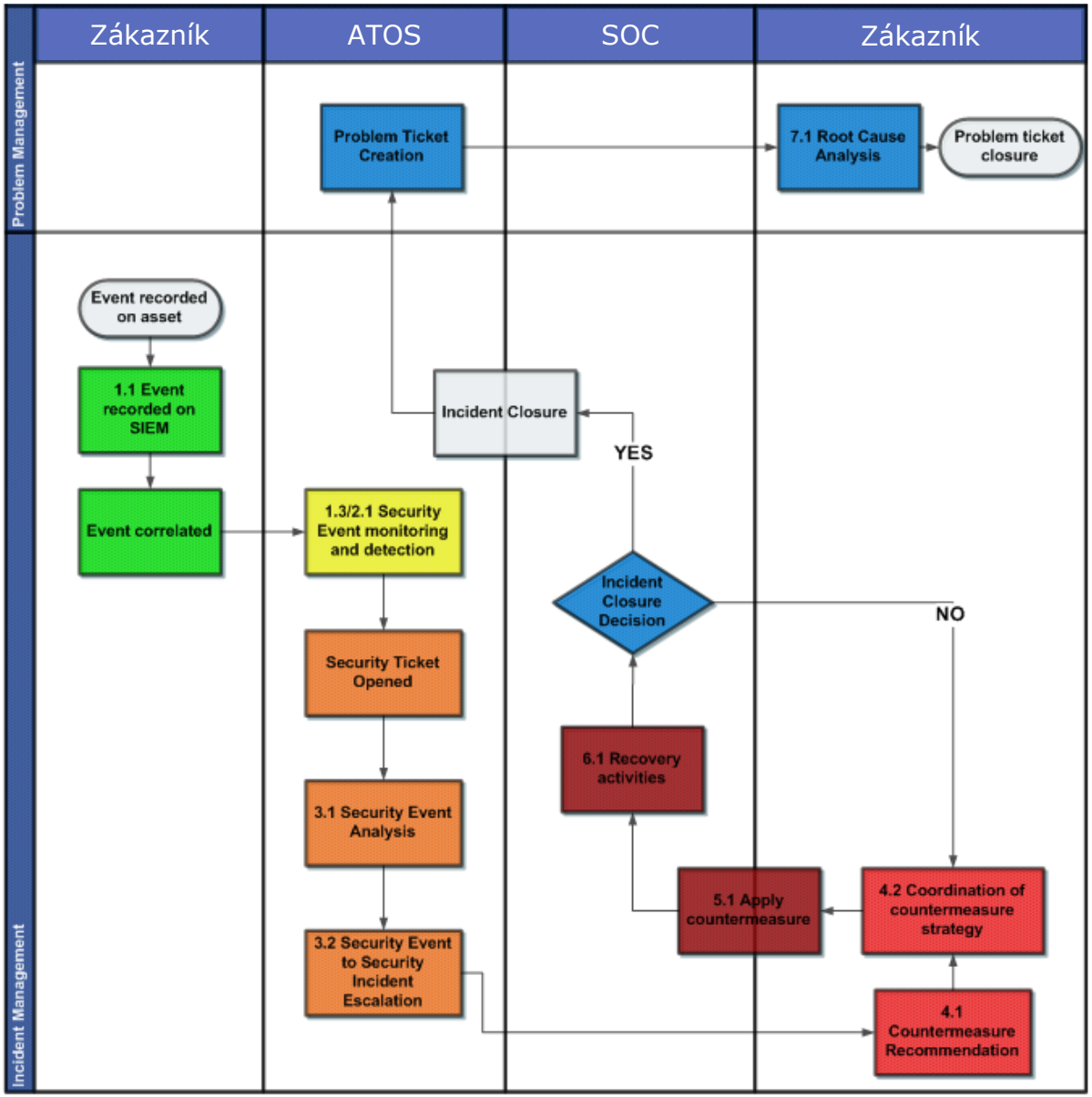
Atos

Když už incident nastane a je detekován

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



Workflow - Je u Vás jasně dáno kdo, má co na starosti?



Jasné rozdělení odpovědnosti a návazností v komunikaci.

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

Budování bezpečnostního povědomí

Atos CYBER security

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

Inspirujte se v našem SOC centru

….. pravidelné referenční návštěvy

Atos CYBER security

Referenční návštěva v ATOS Security Operations Center

Agenda

DEN 1

09:30	Zahájení - Představení Atos Big Data & Security Polan *Marcin Lipinski, CEE Hea*
10:00	Atos Security Monitoring and Detection *SOC (Maciej Glama)* *Vulnerability Managem* *AHPS service (Przemek*
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

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

Děkuji za pozornost

Trusted partner for your Digital Journey

Tomáš Hlavsa

tomas.Hlavsa@atos.net
604 290 196