

**ANECT**

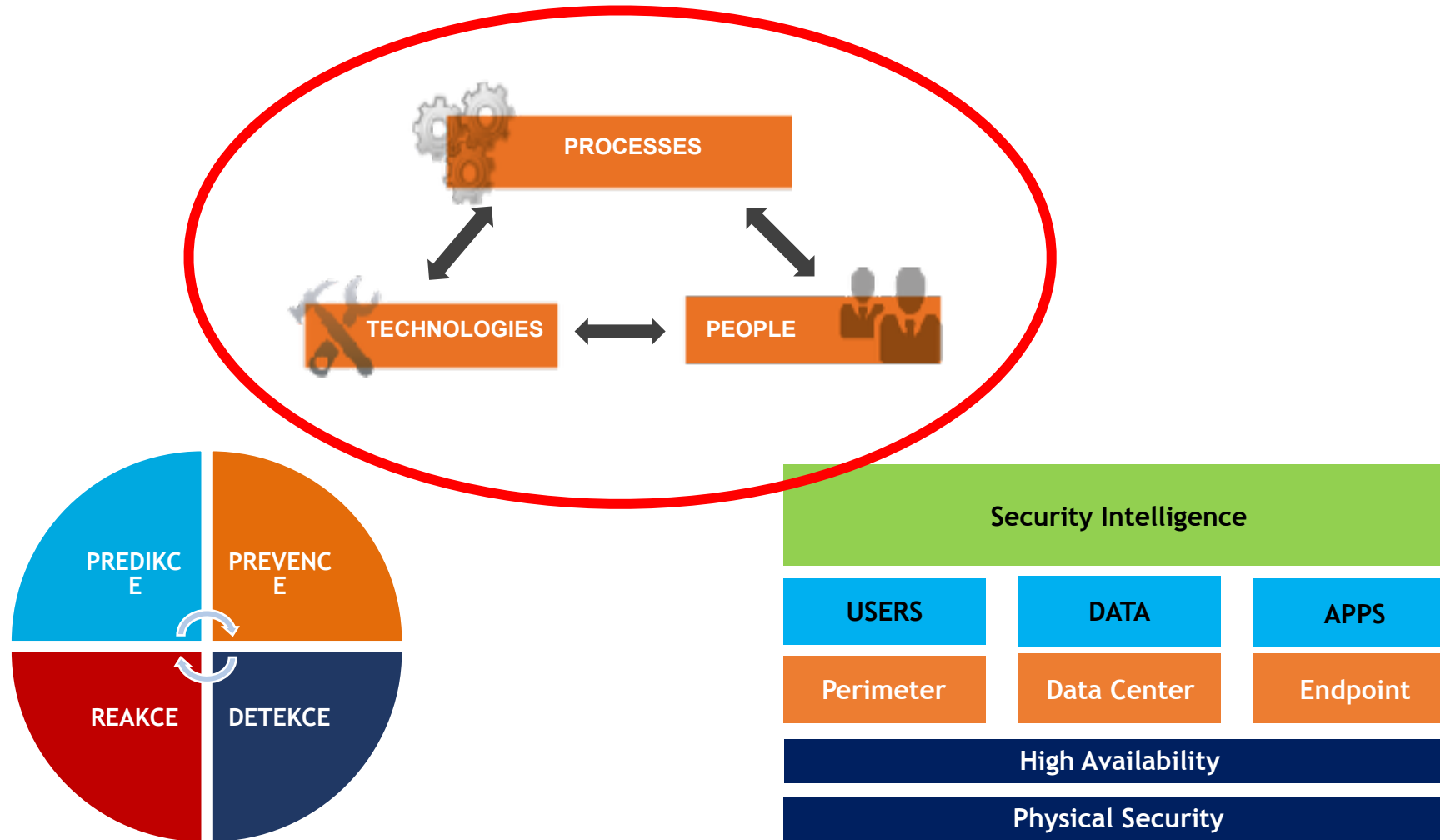
# SOCA

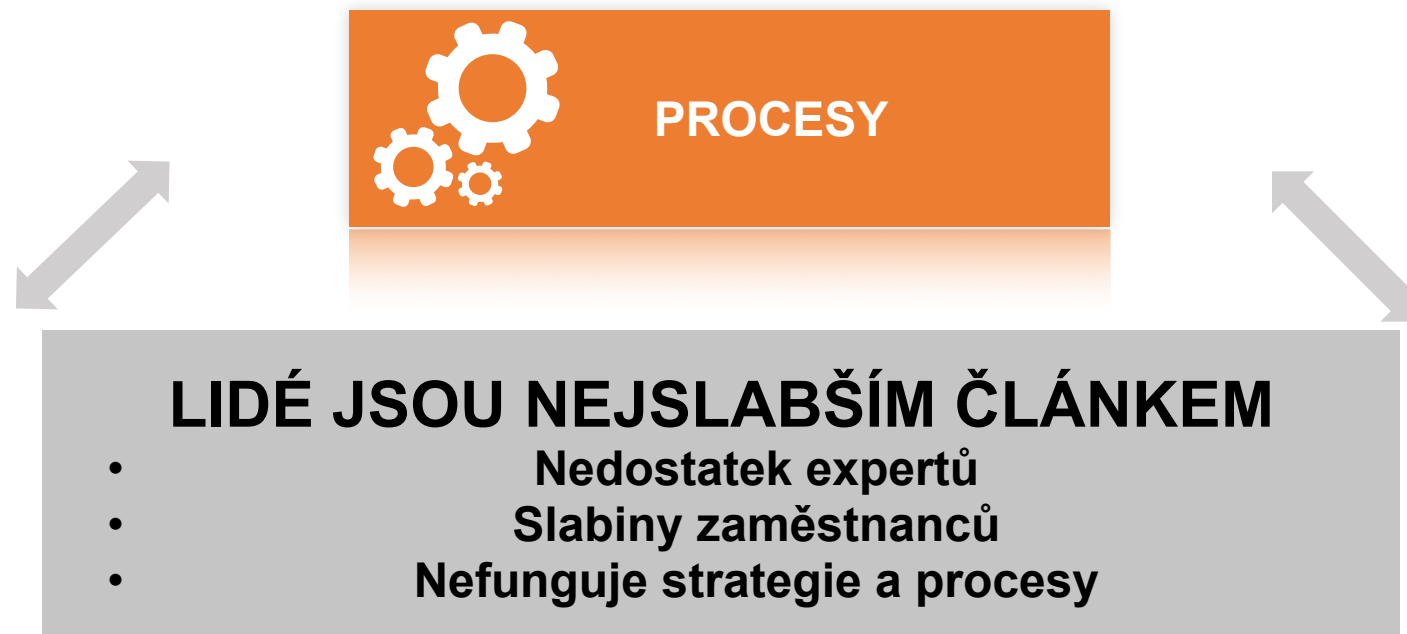
# BEZ LIDÍ TO NEPŮJDE

Ivan Svoboda, ANECT & SOCA

---









**PROCESY**

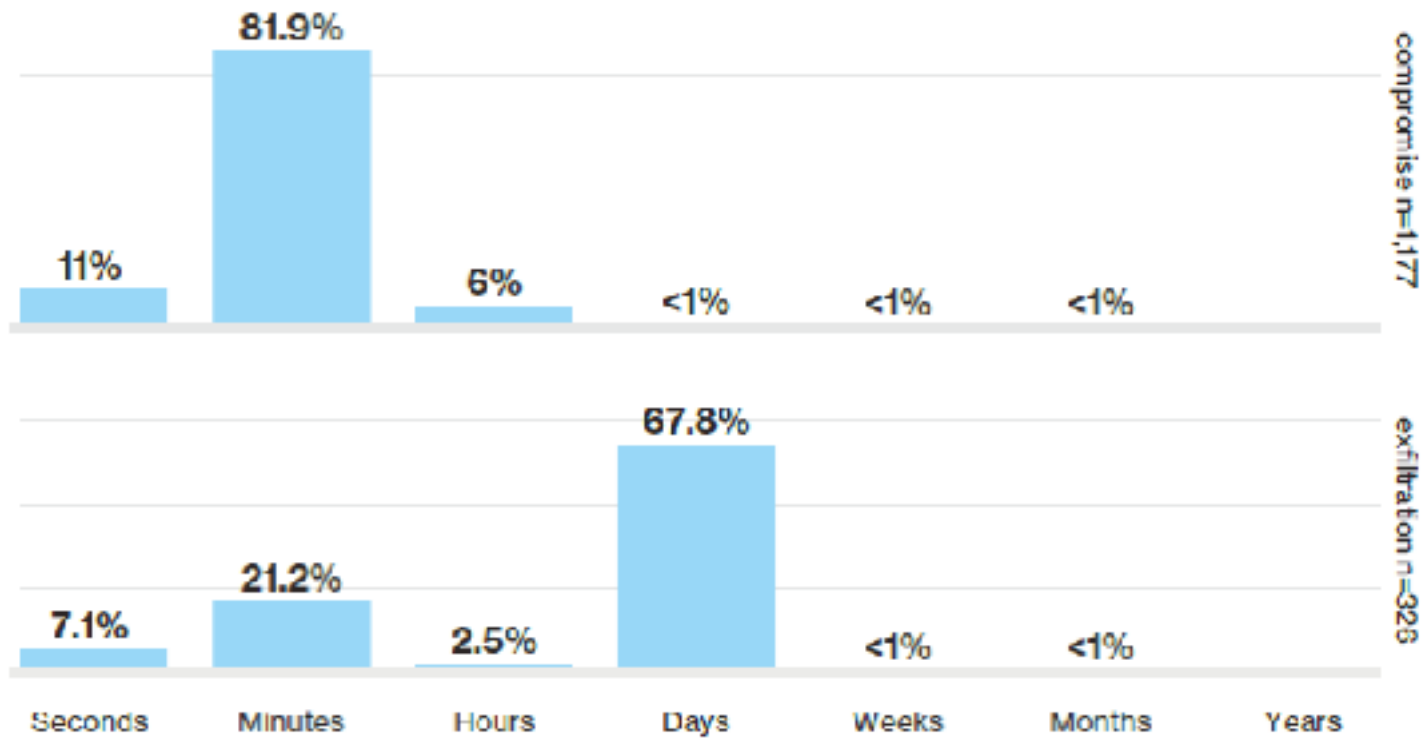
**SOC A**

**TECHNOLOGIE**



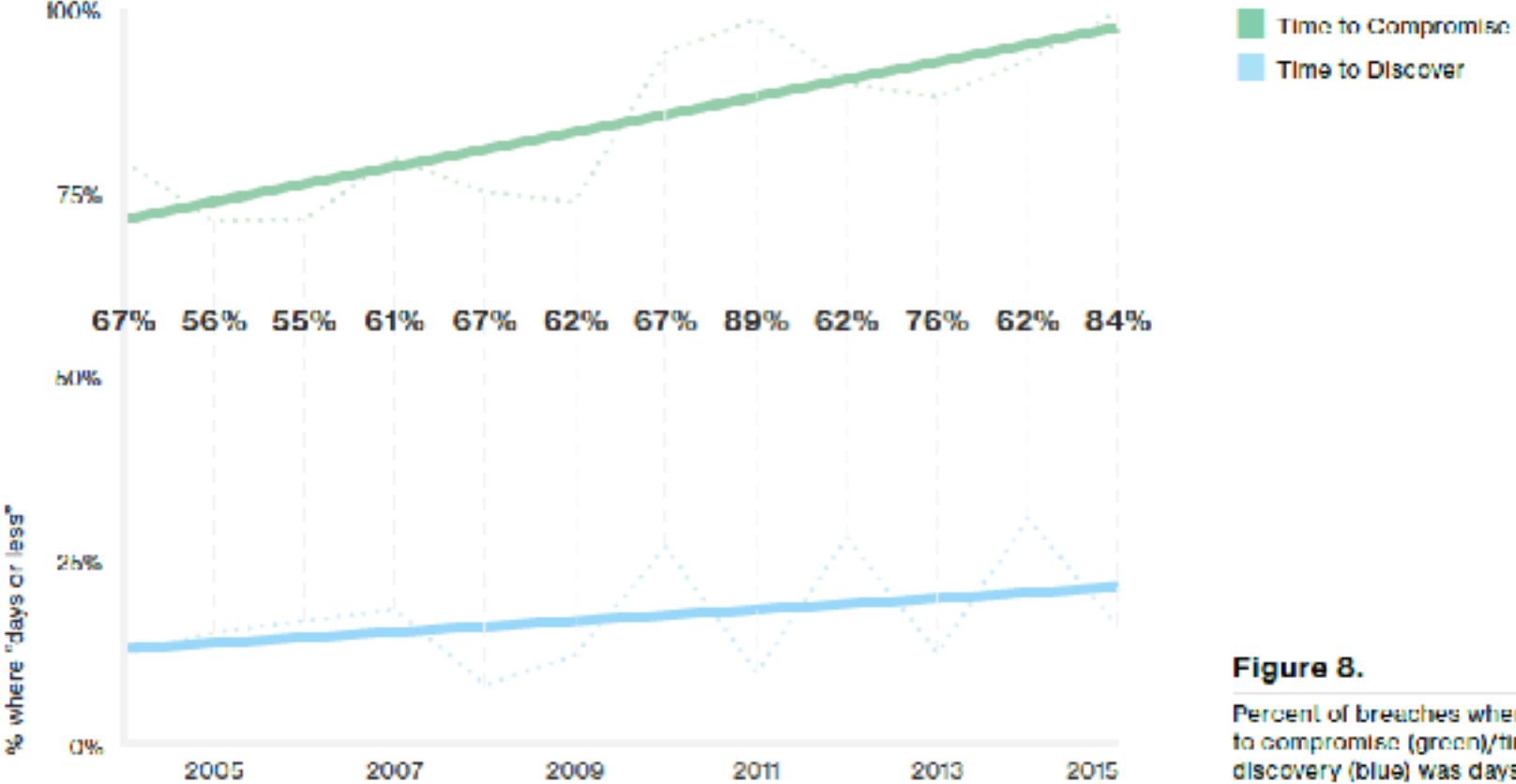
**LIDÉ**

# Statistiky



**Figure 7.**  
Time to compromise and exfiltration.

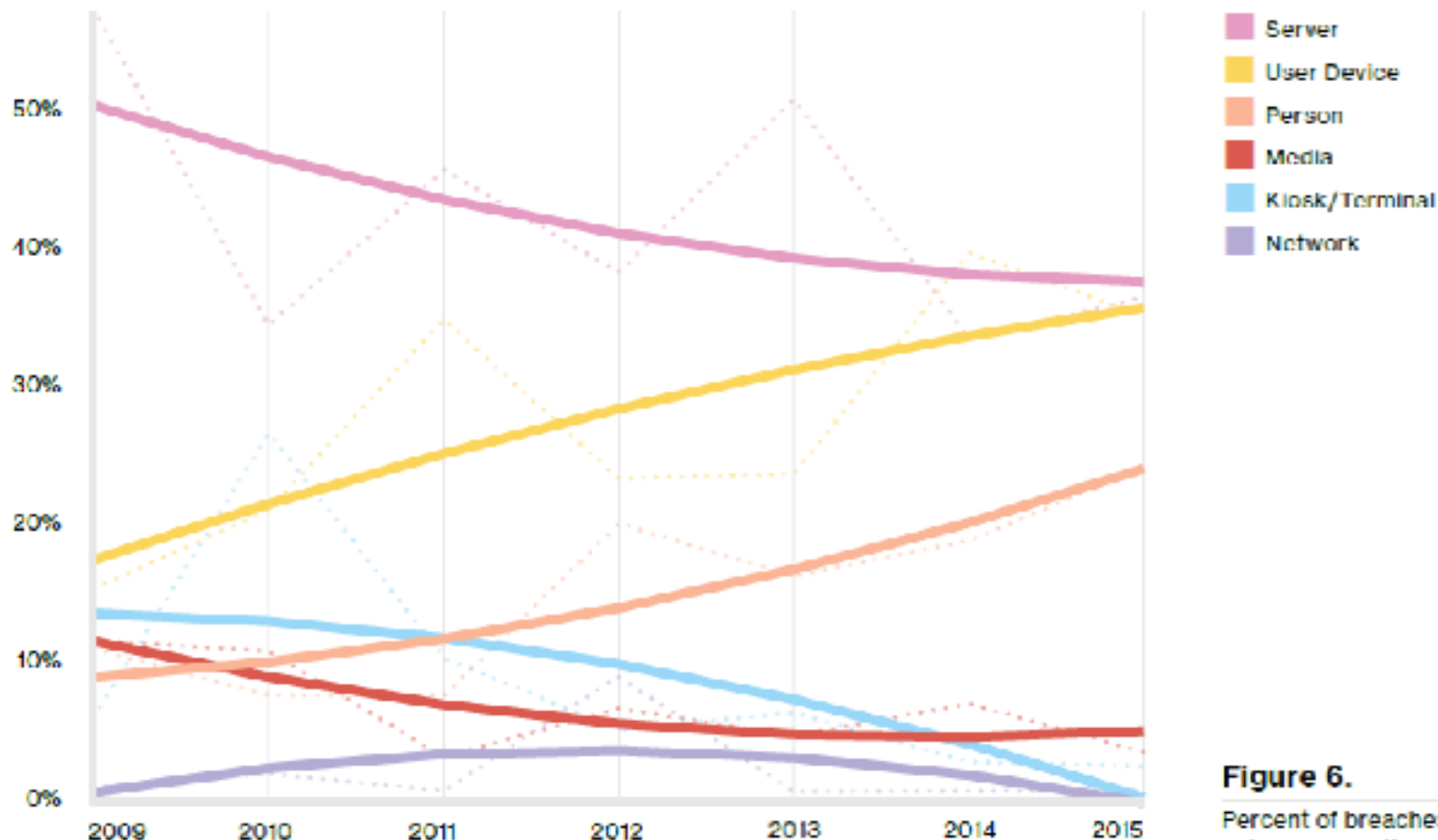
[http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2016](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2016)



**Figure 8.**  
Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

[http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2016](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2016)





**Figure 6.**  
Percent of breaches per asset category over time, (n=7,738)

[http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2016](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2016)

# Statistiky CSO / IDG: State of Cybercrime

- Phishing: 36%
- Ransomware: 17%
- Financial Fraud: 12%
- Cyber loss / damage: 70%
- IT Sec Budget: 11 M \$
- TTD (Time to Discover): 92 days



CSO / IDG: The 2017 State of Cybercrime Survey

# Typické scénáře

# Problémy a rizika (**A ŘEŠENÍ**)

## ■ Nové kybernetické hrozby a rizika

- Neznáte je? Neumíte je změřit?
- Neumíte je prioritizovat a řídit?

SCAN

ANALÝZA RIZIK

RISK MANAGEMENT

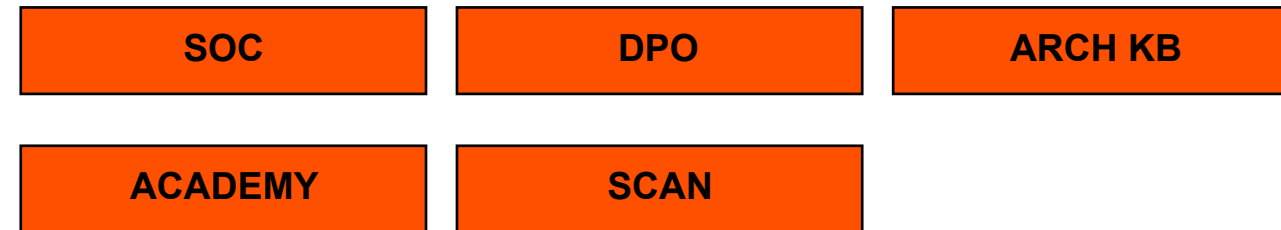
# Problémy a rizika (A ŘEŠENÍ)

- **Nové kybernetické hrozby a rizika**
- **Security technologie nepřináší efekt**
  - Chybí strategie?
  - Nejasná rizika?
  - Chybí procesy a strategie MDAR
  - Chybí lidé?



# Problémy a rizika (A ŘEŠENÍ)

- Nové kybernetické hrozby a rizika
- Security technologie nepřináší efekt
- Lidé jsou nejslabším článkem
  - Chybí experti?
  - Zaměstnanci jsou zranitelní?



# Problémy a rizika (A ŘEŠENÍ)

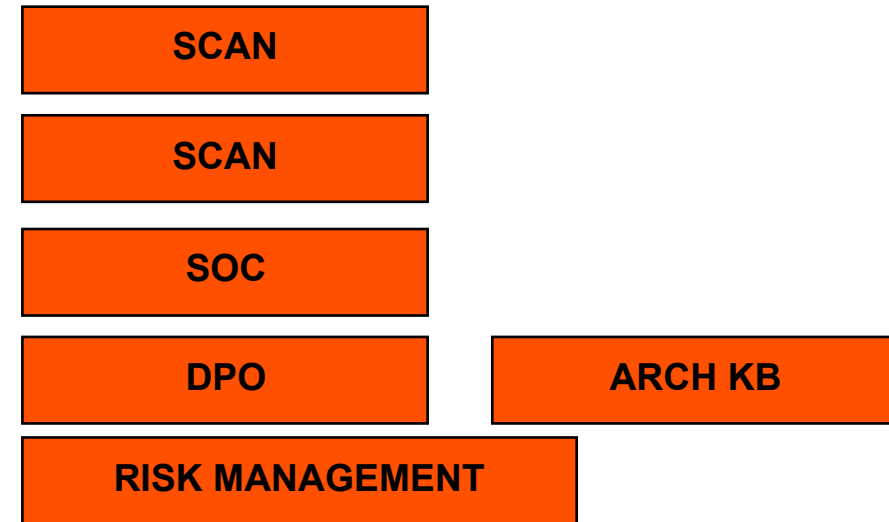
- Nové kybernetické hrozby a rizika
- Security technologie nepřináší efekt
- Lidé jsou nejslabším článkem
- Chybí vám technologie?
  - Neumíte prokázat jejich přínos?
  - Nemáte investice?

SCAN

MSP / TaaS

# Problémy a rizika (A ŘEŠENÍ)

- Nové kybernetické hrozby a rizika
- Security technologie nepřináší efekt
- Lidé jsou nejslabším článkem
- Chybí vám technologie?
- **Legislativa a standardy? (ZoKB, GDPR, ISO)**
  - Neznáte stav souladu?
  - Neznáte hrozby, aktiva, rizika, data?
  - Chybí vám incident management?
  - Chybí vám role?
  - Chybí vám řízení rizik?





# Problémy a rizika (**A ŘEŠENÍ**)

---

- Nové kybernetické hrozby a rizika
- Security technologie nepřináší efekt
- Lidé jsou nejslabším článkem
- Chybí vám technologie?
- Legislativa a standardy? (ZoKB, GDPR, ISO)
- **Bojíte se nových technologií?**
  - cloud, mobility, SDDC, ... ??

**SCAN**

**RISK MANAGEMENT**

# Problémy a rizika (A ŘEŠENÍ)

- Nové kybernetické hrozby a rizika
- Security technologie nepřináší efekt
- Lidé jsou nejslabším článkem
- Chybí vám technologie?
- Legislativa a standardy? (ZoKB, GDPR, ISO)
- Bojíte se nových technologií?
- **Chcete mít jistotu „pro případ požáru“?**
  - Jen výjimka
  - Trvalá ochrana

**INCIDENT RESPONSE**

**SOC / CSIRT**

# Problémy a rizika (A ŘEŠENÍ)

- **Nové kybernetické hrozby a rizika**
- **Security technologie nepřináší efekt**
- **Lidé jsou nejslabším článkem**
- **Chybí vám technologie?**
- **Legislativa a standardy? (ZoKB, GDPR, ISO)**
- **Bojíte se nových technologií?**
- **Chcete mít jistotu „pro případ požáru“?**

SCAN

RISK  
MANAGEMENT

DPO

ARCH KB

ACADEMY

SOC / CSIRT



**SCANY**

**S O C A**

## Změříme COKOLIV

AKTIVA ?

HROZBY ?

ZRANITELNOSTI ?

RIZIKA ?

IT ARCHITEKTURA ?

PROCESY ?

SOULAD ?

DETEKCE & REAKCE ?



**Změříme COKOLIV**

**KDEKOLIV**

**AKTIVA ?**

**HROZBY ?**

**ZRANITELNOSTI ?**

**RIZIKA ?**

**IT ARCHITEKTURA ?**

**PROCESY ?**

**SOULAD ?**

**DETEKCE & REAKCE ?**



Změříme COKOLIV

KDEKOLIV

RŮZNÝMI METODAMI

AKTIVA ?

HROZBY ?

ZRANITELNOSTI ?

RIZIKA ?

IT ARCHITEKTURA ?

PROCESY ?

SOULAD ?

DETEKCE & REAKCE ?

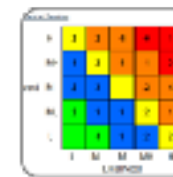


ANALÝZA

AUDIT / POSOUZENÍ

SCAN / TECHNICKÁ INVENTURA

PENETRAČNÍ TEST



# Znáte stav Vašich sítí a systémů?

**ODHALÍME, CO VÁS OHROŽUJE**

**ZMĚŘÍME STAV RIZIK A  
BEZPEČNOSTI**

**ZMĚŘÍME PŘÍNOSY NÁSTROJŮ**

**HROZBY A RIZIKA,  
KTERÁ NEZNÁTE / NEVIDÍTE,  
VÁS MOHOU VÁŽNĚ POŠKODIT**

**ZNÁTE VŠECHNY ZÁVAŽNÉ  
HROZBY A RIZIKA?**

**JAKOU MÁTE JISTOTU,  
ŽE JSTE V BEZPEČÍ?**





Using the following name and the highest score of each student, rank the students.

Name	Score	Rank
John	85	1
Jane	78	2
Bob	92	3
Alice	88	4
Charlie	75	5
Diana	82	6
Eve	90	7
Frank	70	8
Grace	87	9
Henry	79	10
Ivy	84	11
Jack	91	12
Karen	76	13
Liam	83	14
Mia	89	15
Noah	77	16
Olivia	86	17
Peter	93	18
Quinn	74	19
Rachel	81	20



# DPO

# SOCA

# Kdo potřebuje DPO službu?

## Kdo musí zřídit DPO:

- orgán veřejné moci / veřejný subjekt
- rozsáhlé pravidelné a systematické monitorování
- rozsáhlé zpracování zvláštních kategorií údajů

## Kdo chce zřídit „DPO“

- „někdo“ ty činnosti vykonávat musí

## Nedostatek lidských zdrojů

- Znalosti, zkušenosti, kvalifikace
- Dostupnost a spolehlivost

### Článek 37

Jmenování pověřence pro ochranu osobních údajů

1. Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:

- a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
- b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo
- c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10

# DPO: varianty služby

## DPO Mandatory

### Činnost pověřence v rámci služby

Ombudsman pro subjekty údajů

Poradenství v rámci organizace

Konzultace v případě porušení zabezpečení

Prověřování právního souladu zpracování

Zvyšování povědomí zaměstnanců

Posudek k posouzení vlivu

Komunikace s dozorovým úřadem

Pravidelný audit souladu se zákonnými požadavky

Reporting činností

## DPO Options

### Činnost pověřence v rámci služby

Vedení záznamů o činnostech zpracování včetně SW

Příprava posouzení vlivu

Konzultace záměrné a standardní ochrany

Komunikace v případě porušení zabezpečení

Konzultace k obsluze subjektů údajů

Konzultace k souhlasům se zpracováním osobních údajů

Konzultace ke komunikaci se subjekty údajů

Revize smluv se zpracovateli

Konzultace k předávání do třetích zemí

Konzultace k ustanovení společných správců

Vytvoření a údržba závazných podnikových pravidel

Vzdělávání zaměstnanců

Jiné činnosti v oblasti GDPR a bezpečnosti

## DPO Support



# RISK MANAGEMENT

# SOCA

# RISK MANAGEMENT

## Co to je?

- komplexní služba řízení rizik zahrnující všechny potřebné **metodiky, nástroje i lidské zdroje**

## Kdo potřebuje řídit rizika?

- GDPR
- ZoKB
- ISO 27000 (ISMS)
- Další typy rizik

## Přínosy

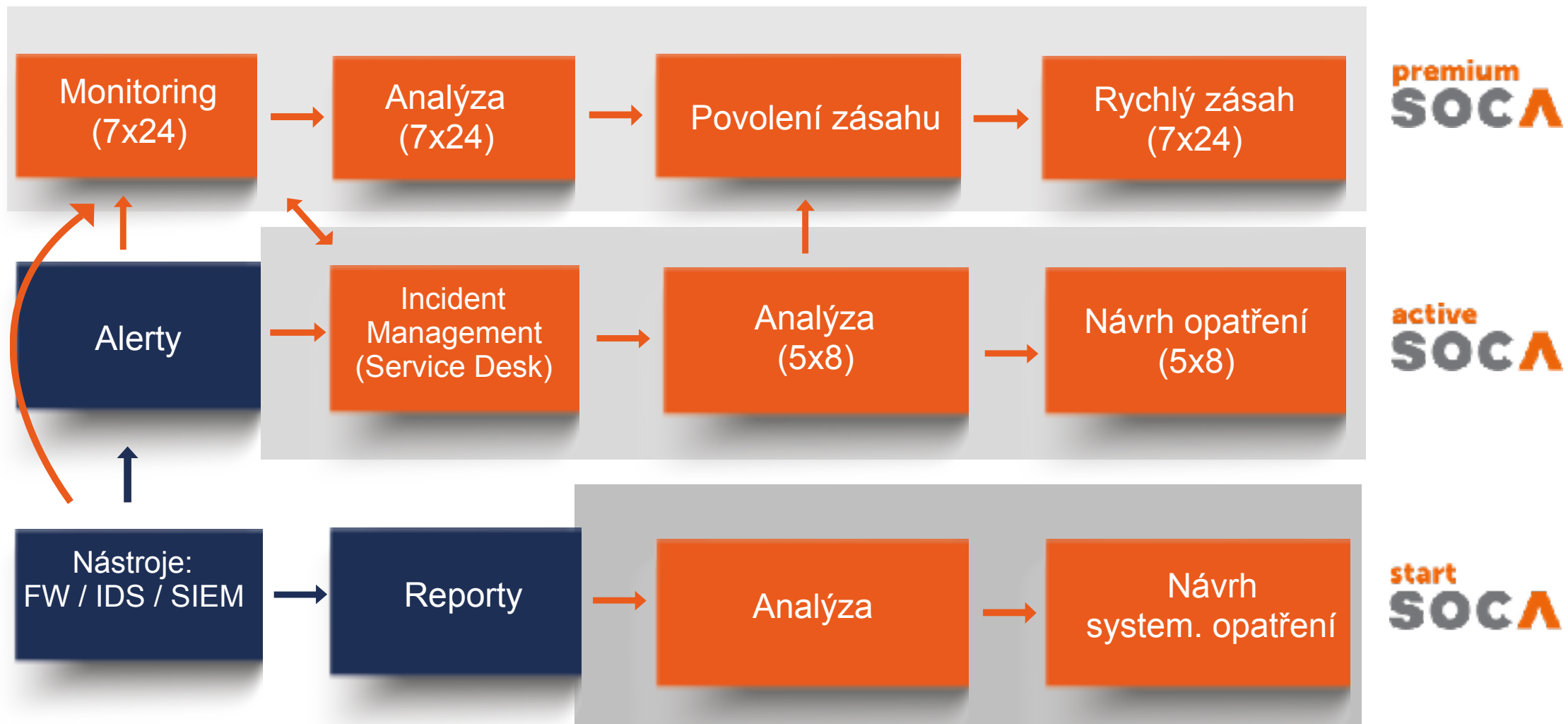
- Řada metodik podle účelu
- Nejen služba, ale i zavedení procesu
- Sofistikovaný nástroj v ceně
- Průběžně aktualizovaný pohled





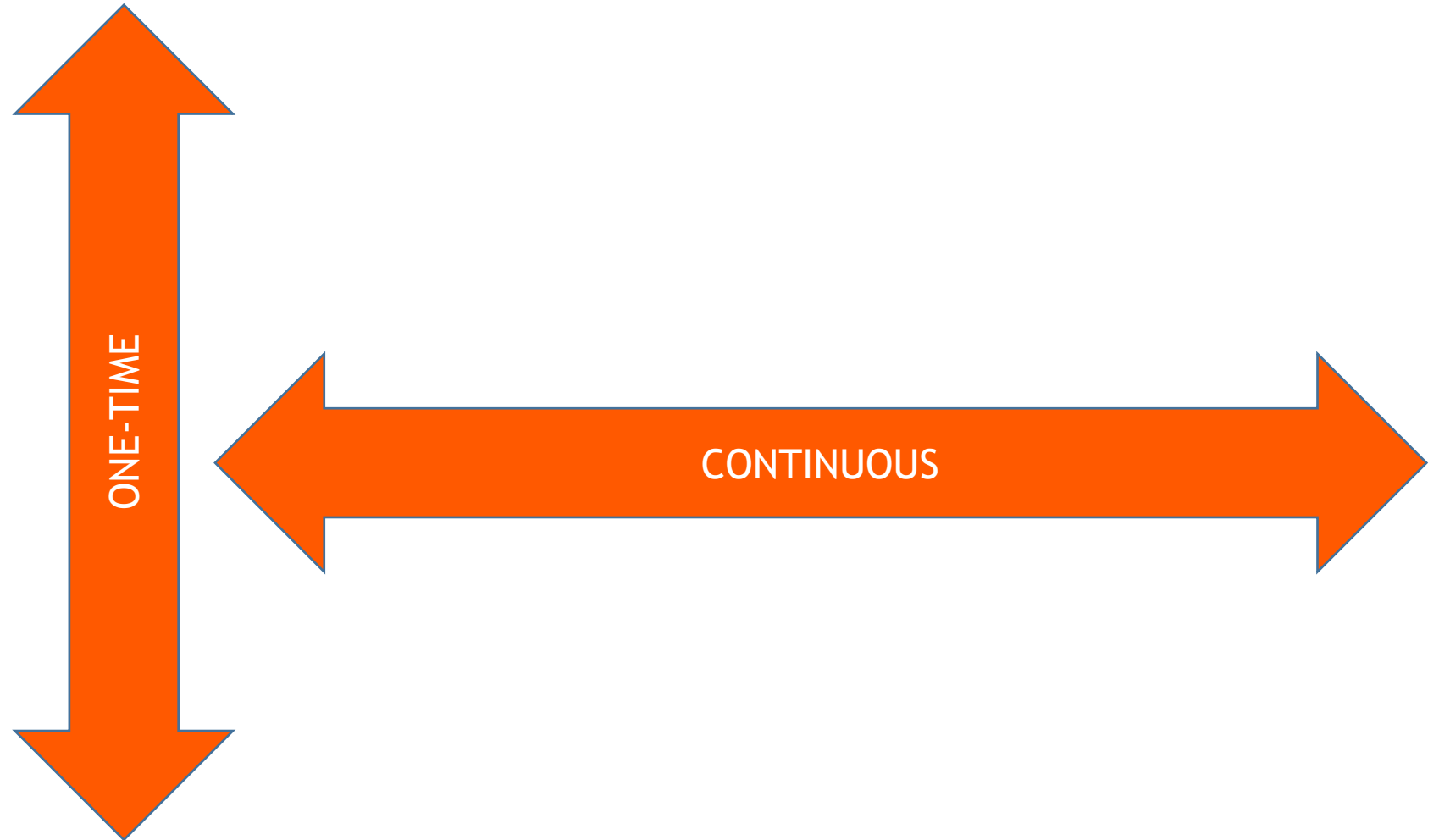
# SOC / CSIRT

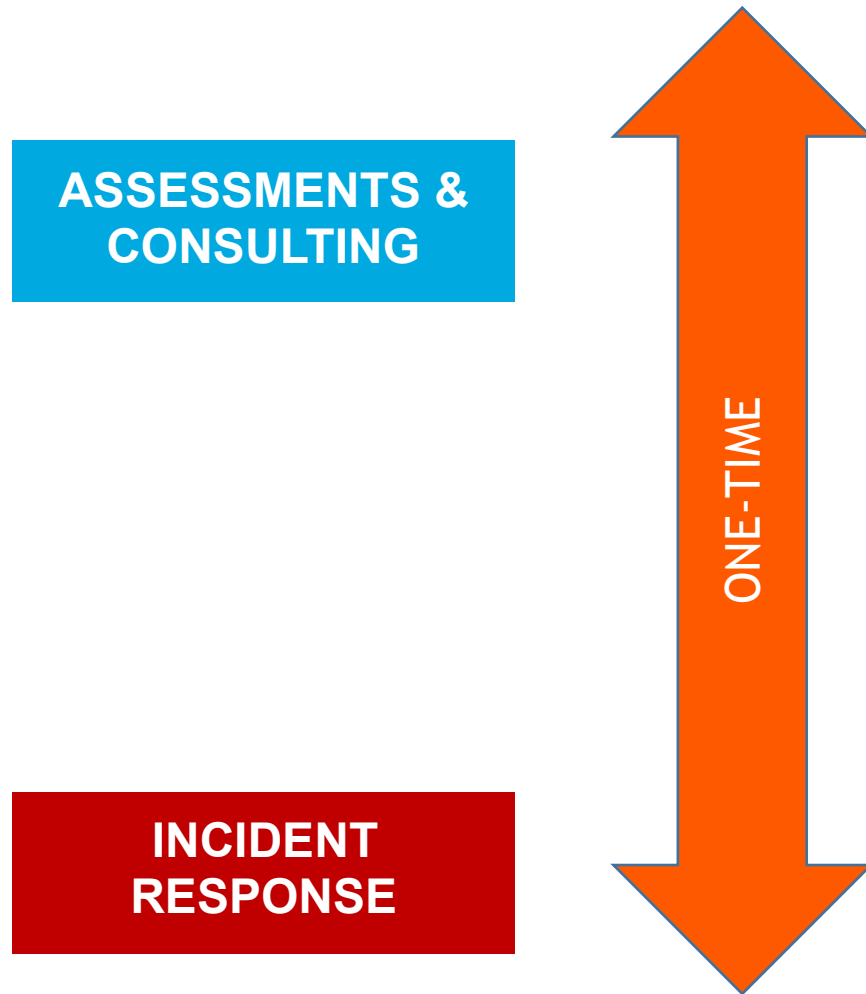
# SOC A



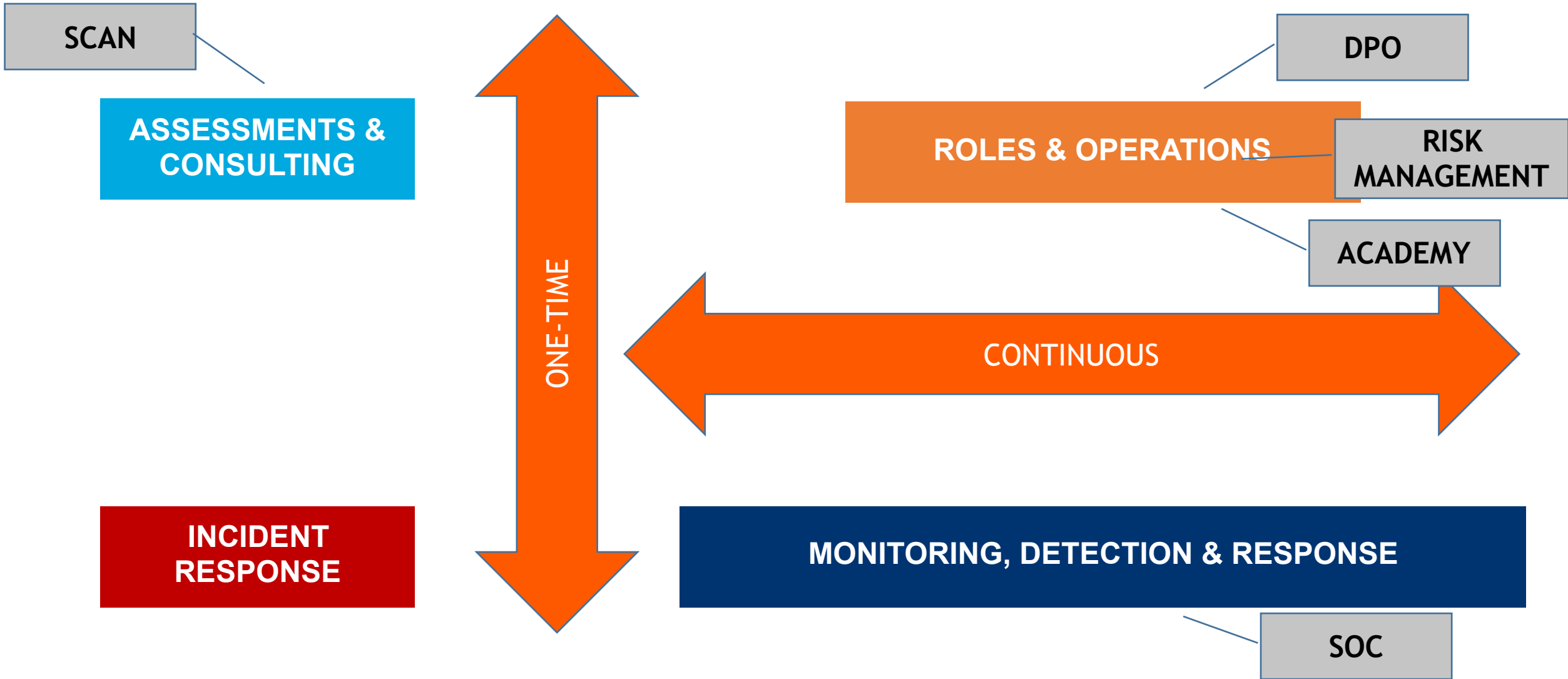
**SOCA: portfolio služeb**













---

Potřebujete pomoc se **zákony a standardy**?

---

Chcete zjistit, co vám **konkrétně** hrozí ?

---

Potřebujete technologie, **procesy, role**, lidi ?

---

Chcete **trvale** vidět, rozumět a reagovat ?



SOCA

SOC powered by ANECT

