



# NECHTE ÚŘAD FUNGOVAT!

Petr Stoklasa  
cybersecurity impresario

IT pro praxi, 9.11.2023, Ostrava

## Základní premisy

- Ohrožení infrastruktur provozujících informační systémy, které jsou kritické a významné nejen ve státní a veřejné správě a ve smyslu ZoKB narůstá nebývalým tempem,
- ukážeme si, jak je možné s využitím externalizace profesionálních služeb a současných technologií těmto výzvám účinně čelit,
- dotkneme se krátce technologického pozadí těchto služeb.

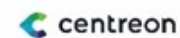
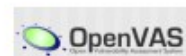
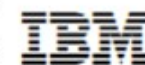
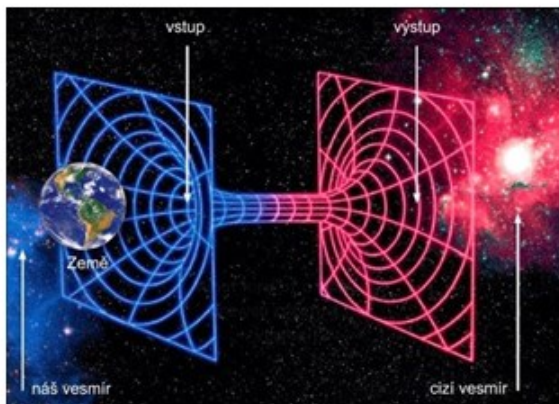
# Jak získat IT profesionály do úřadu

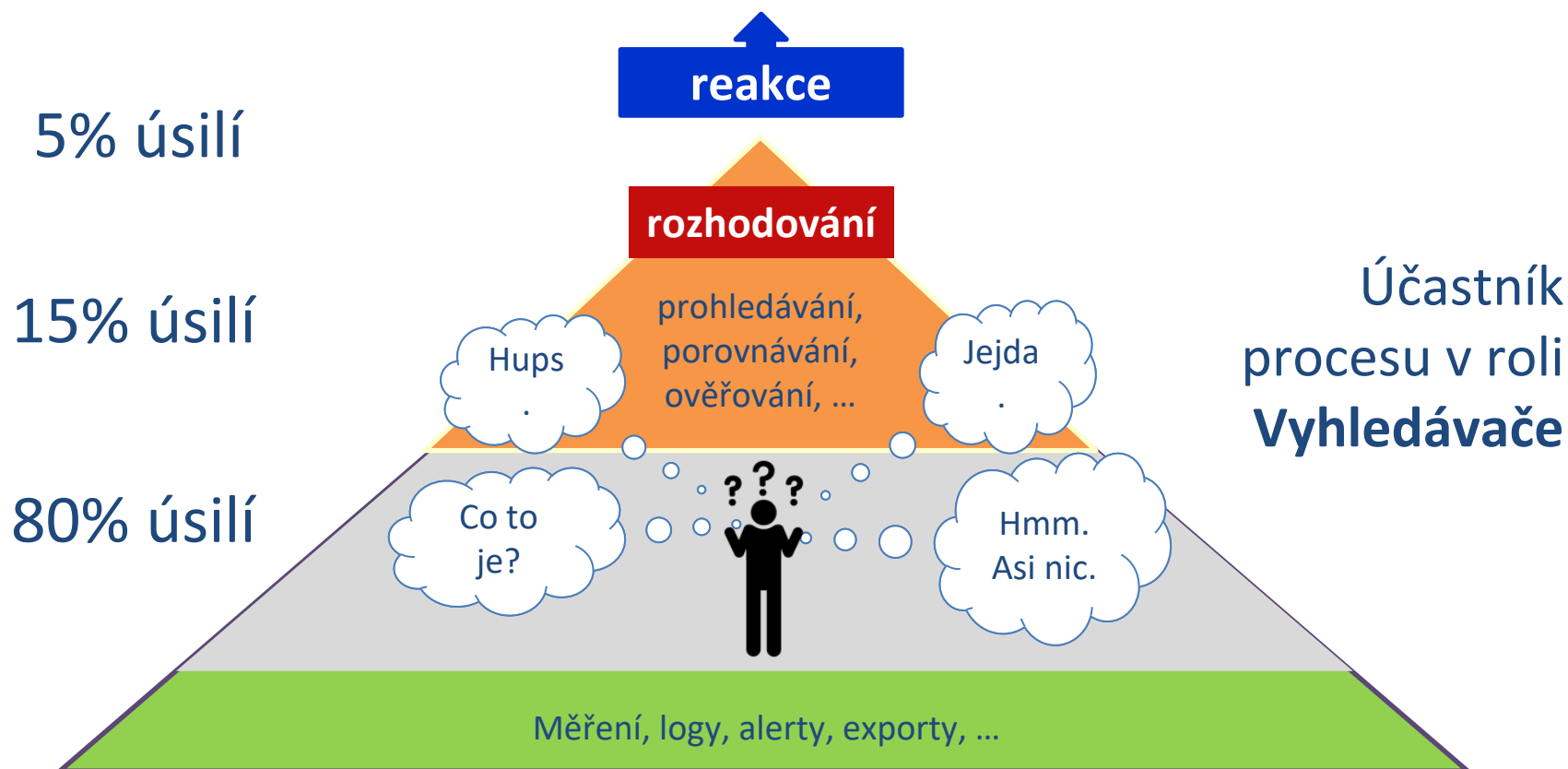
## za cenu, kterou si můžete dovolit?

- co byste řekli
- ...na to, kdybychom toto téma nyní opustili a věnovali se příjemnějším?
- To bychom patrně dopadli jako např. MV, ŘSD, MHMP a další.
- A protože to si my dovolit nemůžeme, musíme uvažovat co s tím...

### Východiska:

- máme omezené zdroje,
- nemáme dostatek lidí,
- bojiště je stále složitější a rozsáhlejší,
- náš protivník má zdroje neomezené a profesionálů přebytek.

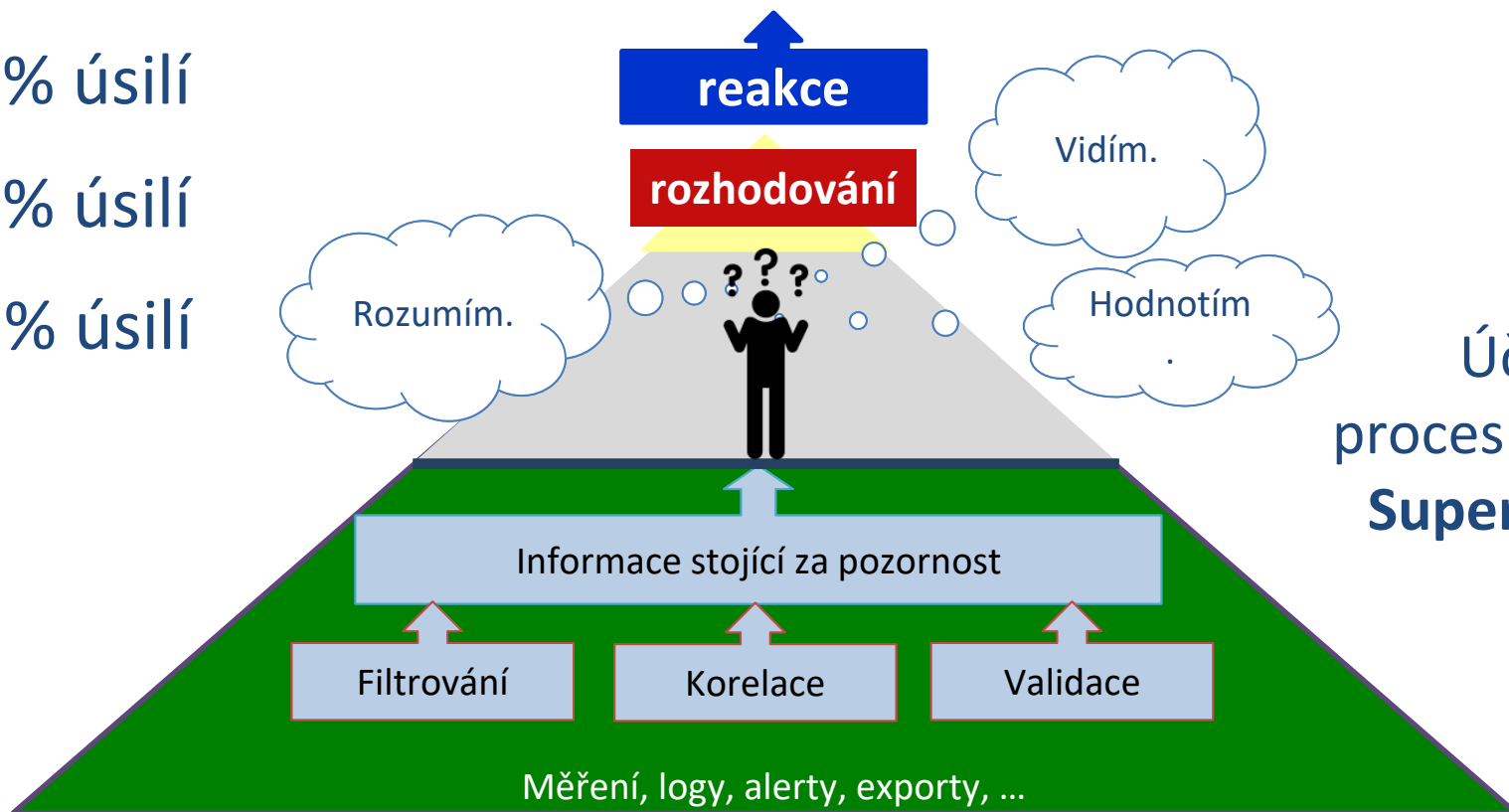




70% úsilí

15% úsilí

15% úsilí



Účastník  
procesu v roli  
**Supervisora**

# Security Operation Center

Tým osob

Procesy

Nástroje

Analytik

Operátor

Člen CERT

Manažer  
SOC

Incident  
Response

Config.  
Management

Deploy  
management

SIEM

Log  
management

Flow  
monitoring

Vulnerability  
management

Asset  
assessment

## Primární účel

Sběr dat

Analyzování

Detekce  
anomálií

Reakce na  
incidenty

Oprava/  
Vyléčení

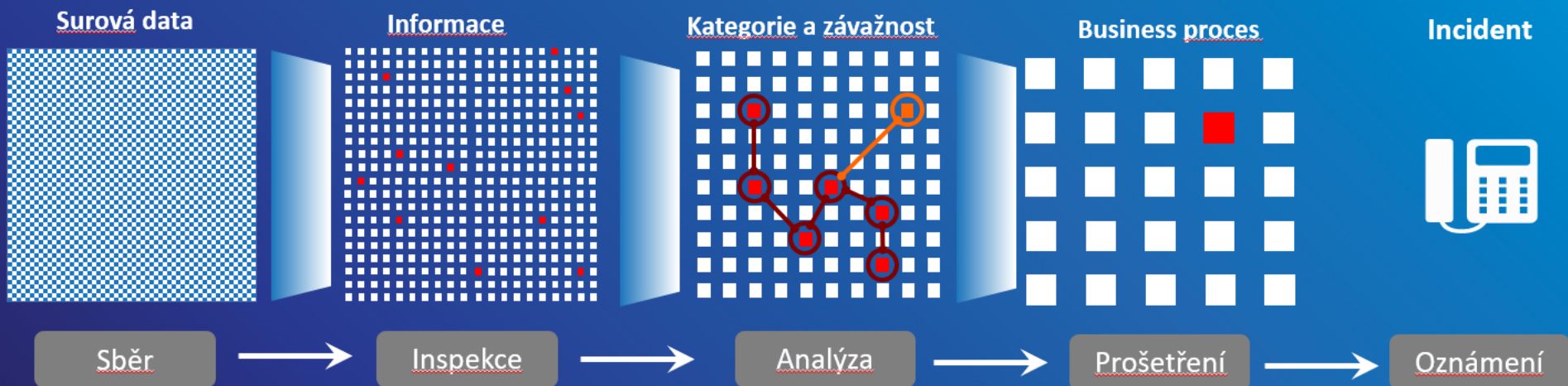
Reportování

## Primární cíle

Předcházení výskytům kybernetických  
incidentů

Předcházení provozním výpadkům

1. Z neviditelných dat tvoříme **Parsingem** a **Filtrováním** viditelné informace.
2. Viditelné informace přes **Inspekci** vkládáme do kategorií.
3. **Analýzou** kategorií stanovujeme kořenovou příčinu nebo následky.
4. **Prošetřením** kořenové příčiny **Oznamujeme** kompetentní osobě relevantní nález.



**Ze surových dat vytvořit zpravodajské informace a ty využít k prevenci a obraně!**

## Funkčnost

Zajistit **funkčnost** infrastruktury v celém jejím spektru.

## Nastavení a Harmonizace

**Nastavit správně provozní prostředí**, pravidelně jej optimalizovat.

## Prevence

Vědět v každém okamžiku o dění i kontextu. Umět **předcházet nežádoucím stavům**.

## Analýza, Reakce a Interpretace

Poznat falešné poplachy, **správně interpretovat** různé stavy infrastruktury a rychle odstínit její ohrožení. Poskytnout **srozumitelný a použitelný** reporting.

**POZOR NA (NIKOLIV LACINÉ) NAPODOBENINY!**

## Nejdůležitější vlastnosti

- Pokud možno co nejvíce jednotná technologická platforma
- **Automatizace**
  - Implementace,
  - provozu,
  - řešení.

## Nejdůležitější součásti/vlastnosti podvozku

- Nepřetržitý monitoring
  - provozu sítě, animozit v provozu,
  - chování uživatelů a jejich pracovních nástrojů,
  - chování administrátorů,
  - byznysových aplikací,
  - kondice infrastruktury.
- Sběr a ukládání provozních dat
- Automatizace
  - vyhodnocování,
  - signalizace a **reakce!**
- PROVÁZANOST na technologické úrovni



The screenshot shows a web security dashboard with a table of security events. The table has columns for Action, Time, Destination, Source, Security, Severity, and More. The events listed are:

Action	Time	Destination	Source	Security	Severity	More
Blocked	08 Jun 2023 09:11:12	www.skylink.cz	Russian Federation - RU	Geo-Blocking	High	
Blocked	08 Jun 2023 09:10:17	www.skylink.cz	Czech Republic (Czechia) - CZ	Tunnel Module HTTP RFC Violation	High	
Reported	08 Jun 2023 09:09:02	www.skylink.cz	United States of America - US	Allowed File Extension URL Access Violation	High	
Blocked	08 Jun 2023 09:08:34	www.skylink.sk	Slovakia - SK	Tunnel Module HTTP RFC Violation	High	
Blocked	08 Jun 2023 09:08:32	www.skylink.cz	Czech Republic (Czechia) - CZ	Tunnel Module HTTP RFC Violation	High	
Blocked	08 Jun 2023 09:07:58	www.skylink.cz	Iraq - IQ	Geo-Blocking	High	
Blocked	08 Jun 2023 09:07:13	www.skylink.cz	Egypt - EG	Geo-Blocking	High	
Blocked	08 Jun 2023 09:07:13	www.skylink.cz	Egypt - EG	Geo-Blocking	High	



**„Pro svět bez kybernetických hrozeb,  
pro mír všem aplikacím,  
pro svobodný přístup k informacím“.**

**Děkuji za pozornost**