

Budujeme **SOC** – Best practice

Ing. Karel Šimeček, Ph.D.

+420 724 042 686

simecek@axenta.cz

SOC – je součástí skutečných SIEM řešení



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

DanubePay



MINISTERSTVO OBRANY
ČESKÉ REPUBLIKY



KB



ČEZ

PPF

Banka

O₂



Co je SOC?

Co je to SOC? **A hlavně, co není SOC!**

Security Operation Center

Tým osob

Nástroj

Analytik

Operátor

Člen CERT

Manažer

SIEM

Log
management

Network IDS/
IPS

Vulnerability

Primární účel

Analyzování

Detekce

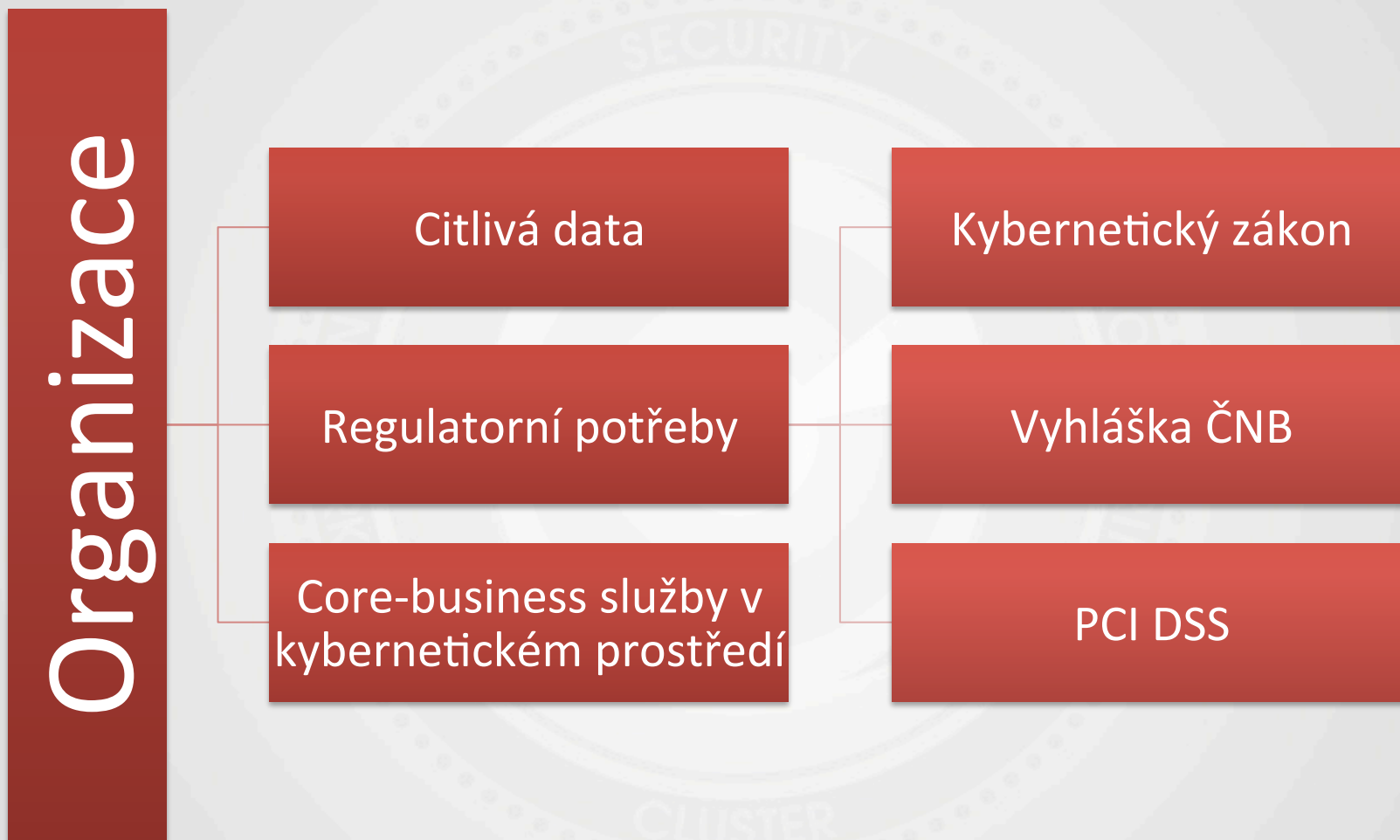
Reakce

Reportování

Primární cíl

Předcházení výskytům kybernetických incidentů

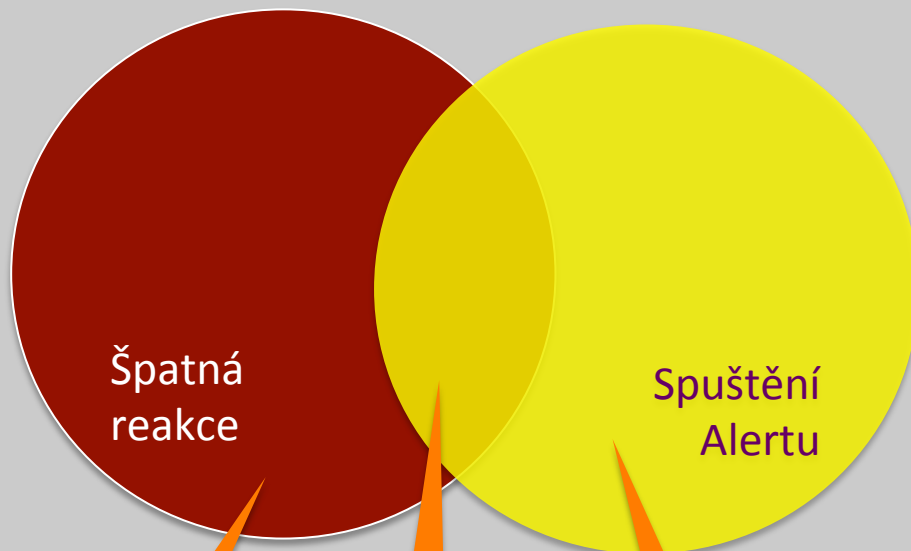
Kde je potřeba SOC?



Kybernetický zákon ustavuje **+/- 85** požadavků. **Více než polovina** požadavků **mimo rámec SOC !!!!**

Stavba SOC

Prostor možných akcí



False
negatives

True
positives

False
positives

True
negatives

Kvalita reakce

False negatives (nedetekovaný problém)

False positives (falešný poplach)

True negatives (nehlášená událost)

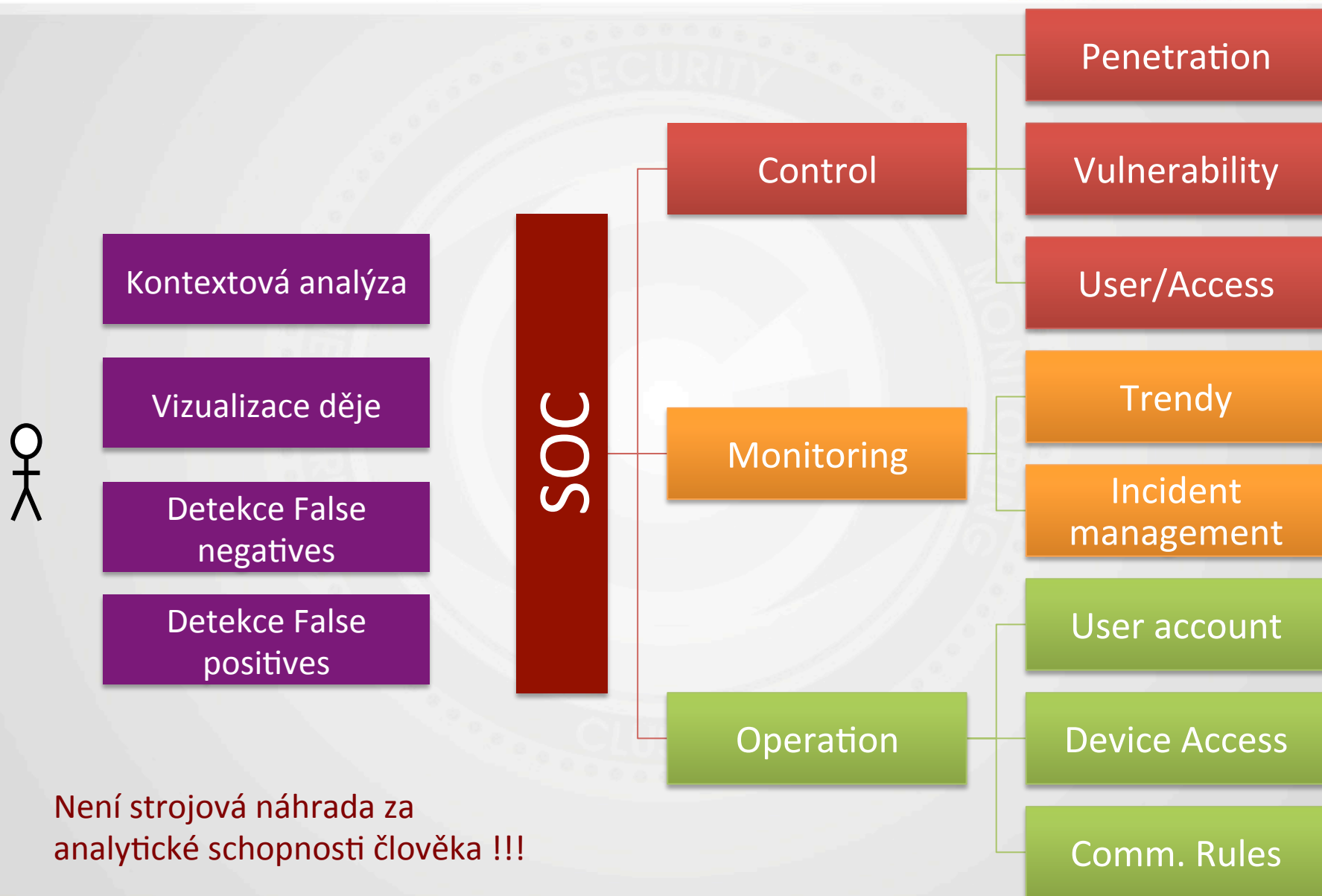
True positives (detekovaný problém)

Rychlost reakce

Zpoždění reakce mezi výskytem a informováním o provozním problému

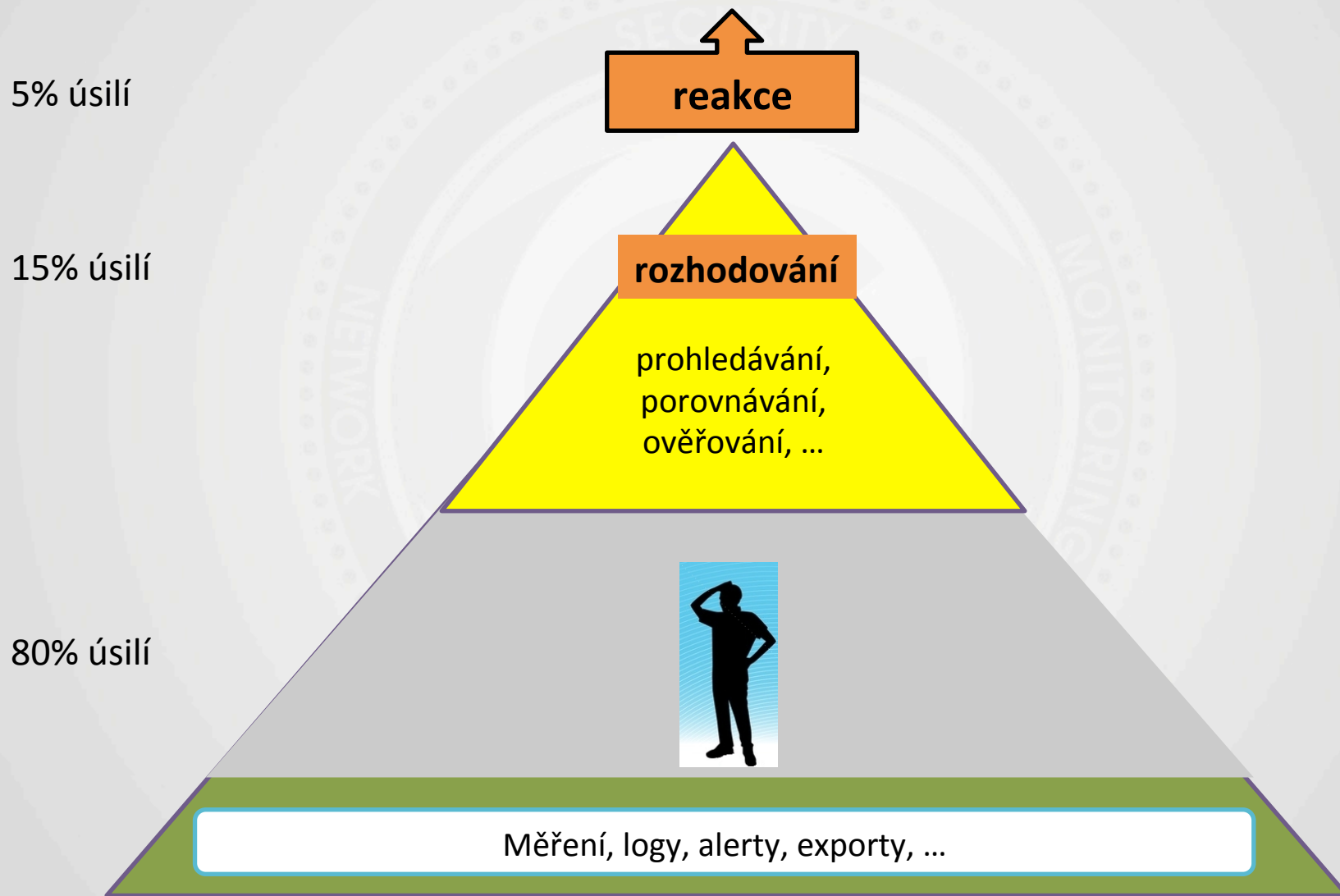
- Kladné (zpoždění)
- Real-time
- Záporné (proaktivita)

Činnosti SOC





Uživatel SOC v roli Vyhledávače



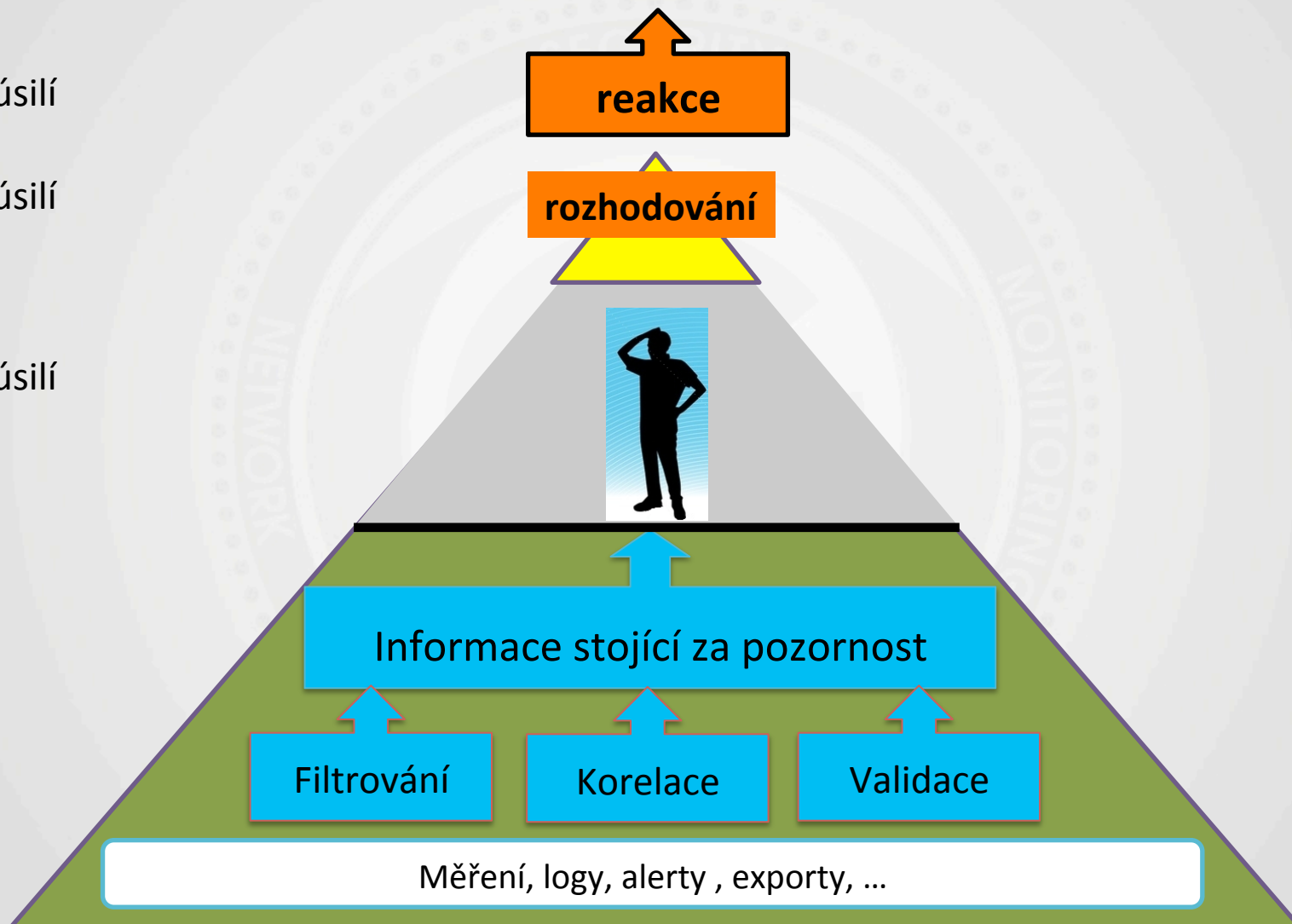
70% úsilí

reakce

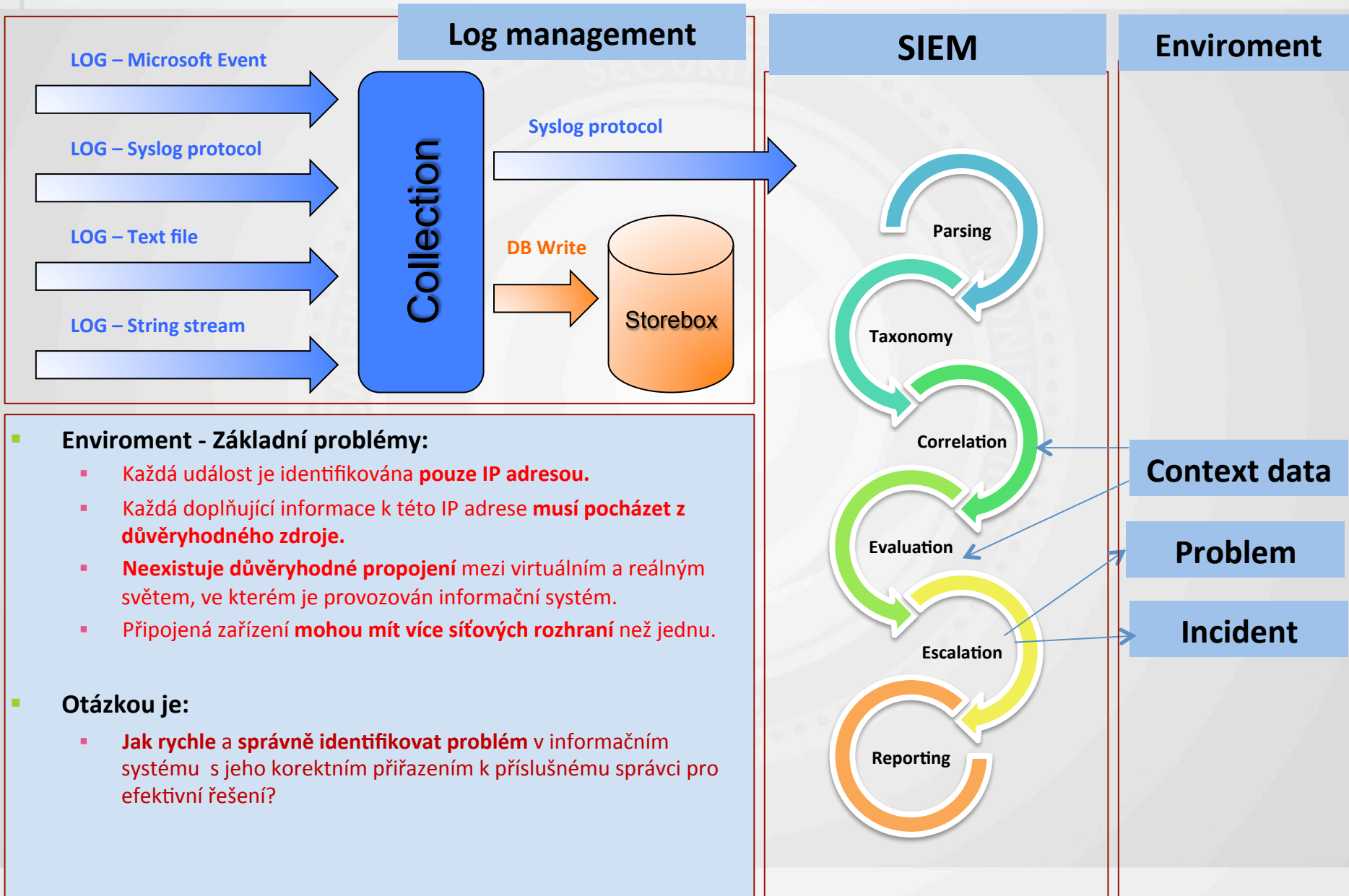
15% úsilí

rozhodování

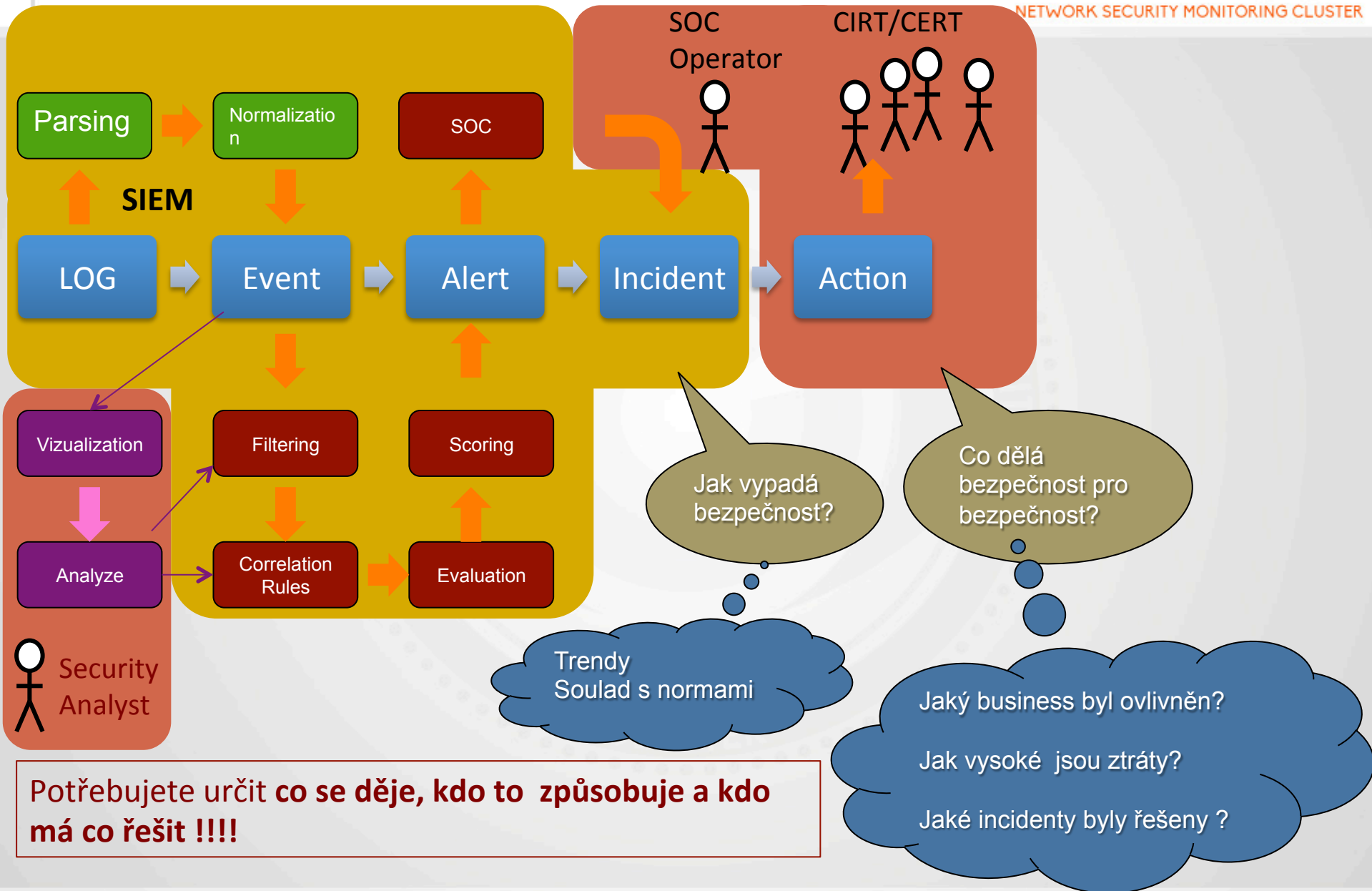
15% úsilí



Jak se provozuje SOC? 1 díl - Nástroj



Jak se provozuje SOC? 2 díl – Tým osob



Provoz SOC

Cena Software

- Licence
- Support
- Servisní smlouvy

Cena hardware

- Servery
- Storage

Cena implementace

- Instalace
- Konfigurace
- Školení obsluhy
- Školení provozu
- Školení analýzy

Vlastnit, Pečovat, Užívat

Cena služby

- Model reakce (8x5, 10x5, 24x7)
- Support napojení na SOC
- Servisní smlouvy

Cena správy aktiv

- Zranitelnosti
- Hrozby
- Knowledge base (Co mám udělat?)

Cena implementace

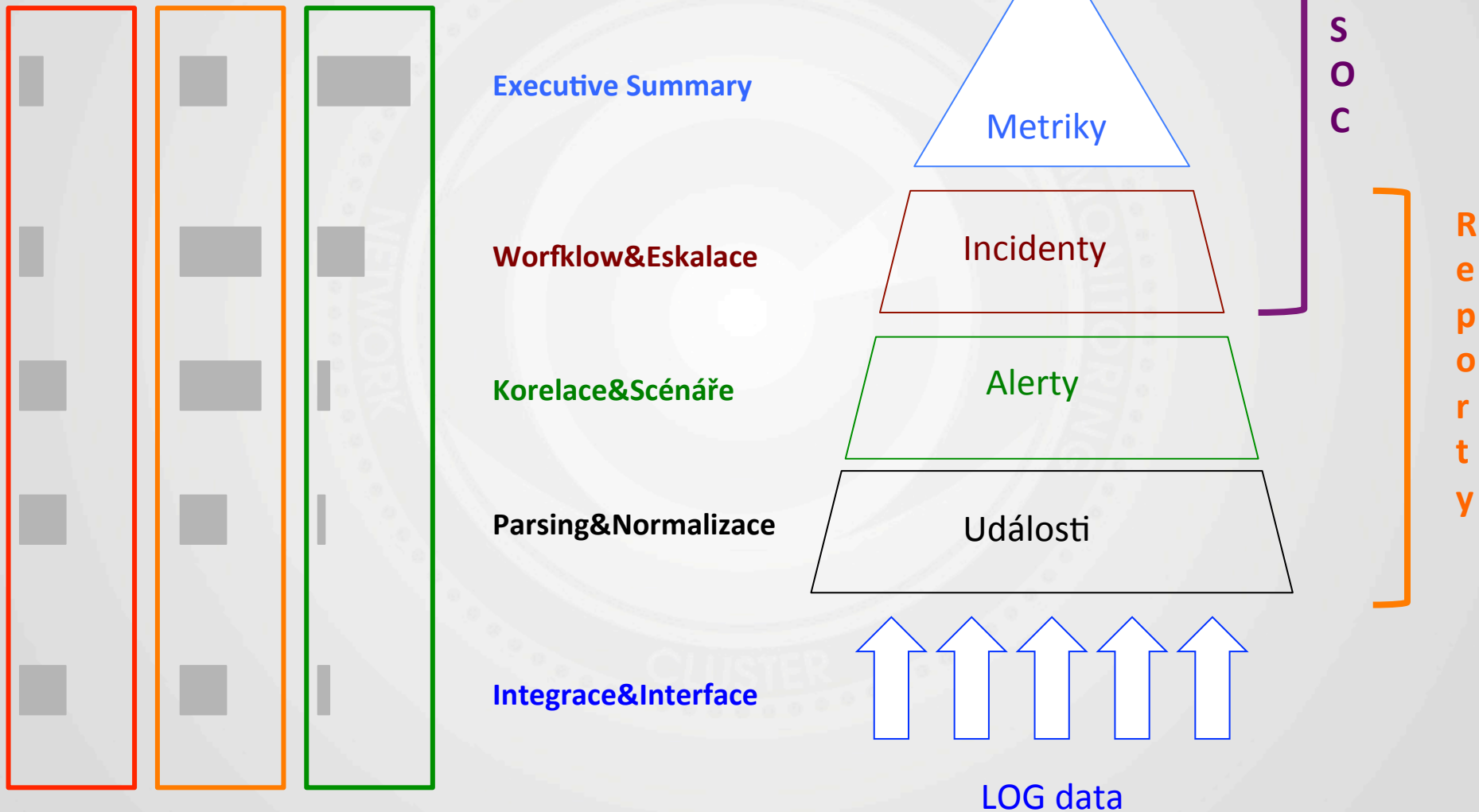
- Instalace
- Školení provozu
- Školení analýzy

Užívat, Reagovat, Zlepšovat se

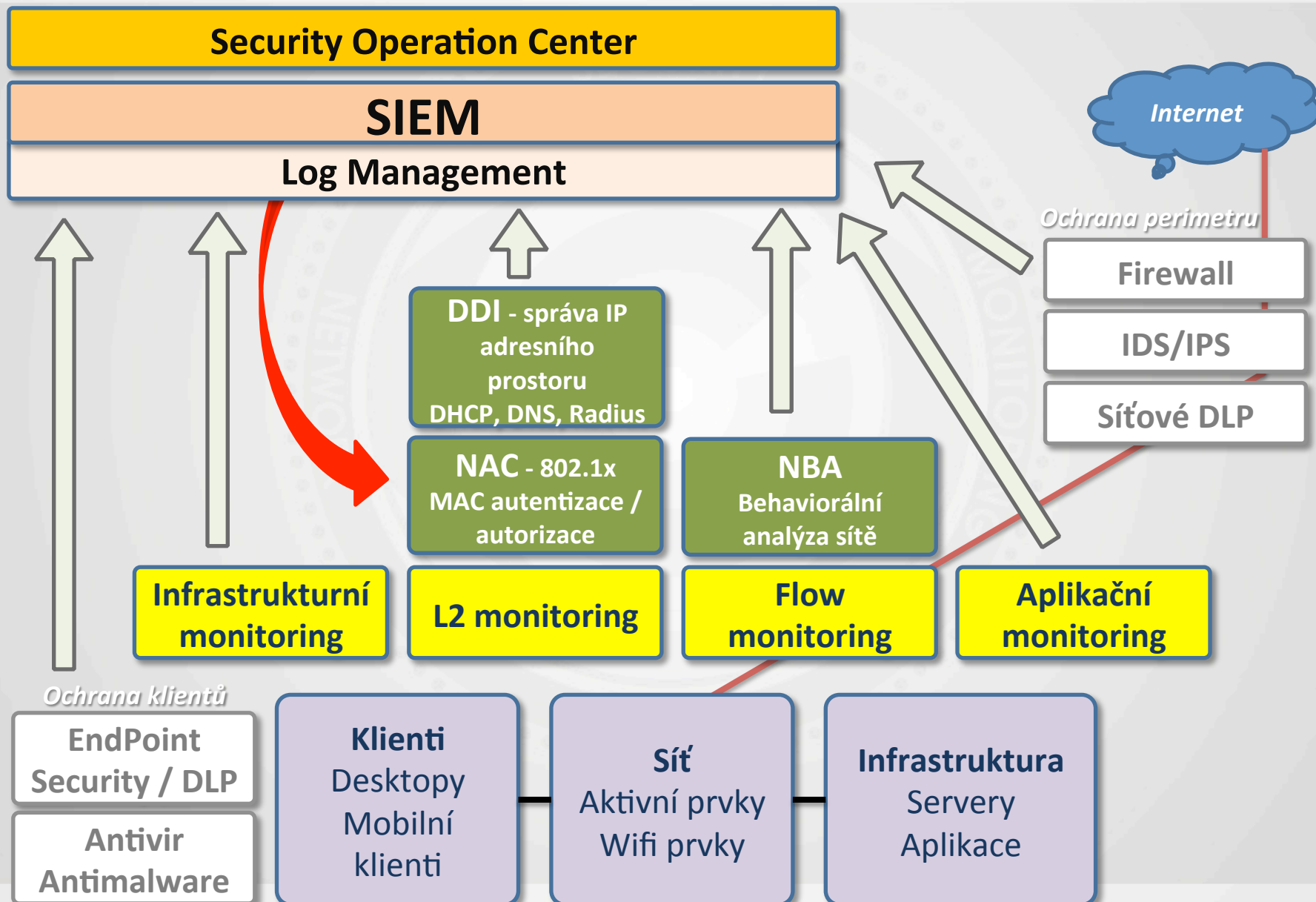
Implementace SOC

Implementační součinnost

Výrobce Dodavatel Zákazník



Principiální koncept SOC



Jak se staví SOC jako systém?

4. Zpřesnění

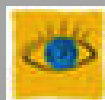
Variable Components



AddNet



FlowMon



Nessus



Firemon



APM



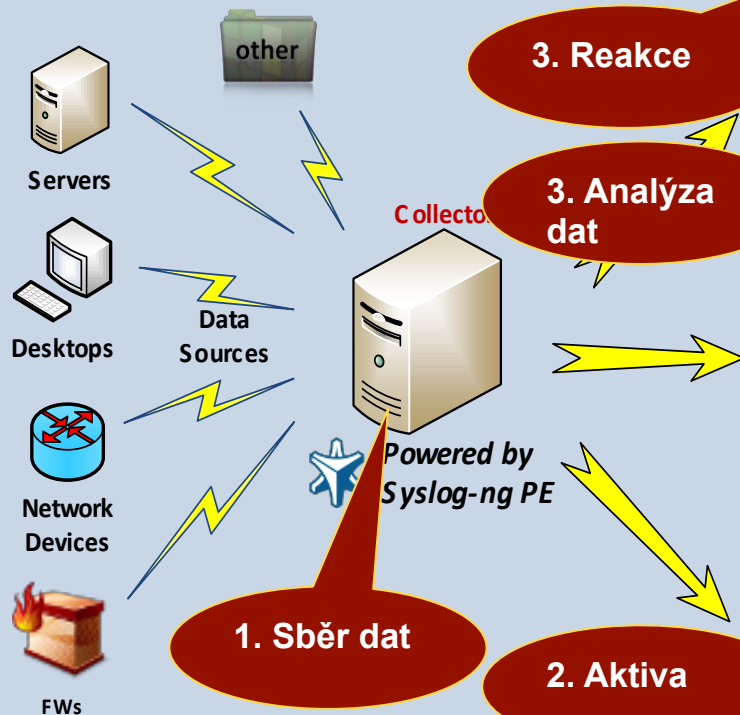
Centreon



SCB



SEC



2. Akiva

Assets

Data for



CSIRT

Tickets

Dashboards

Reporting



SIEM



Logs
Archive



Identity
Monitoring



Operator

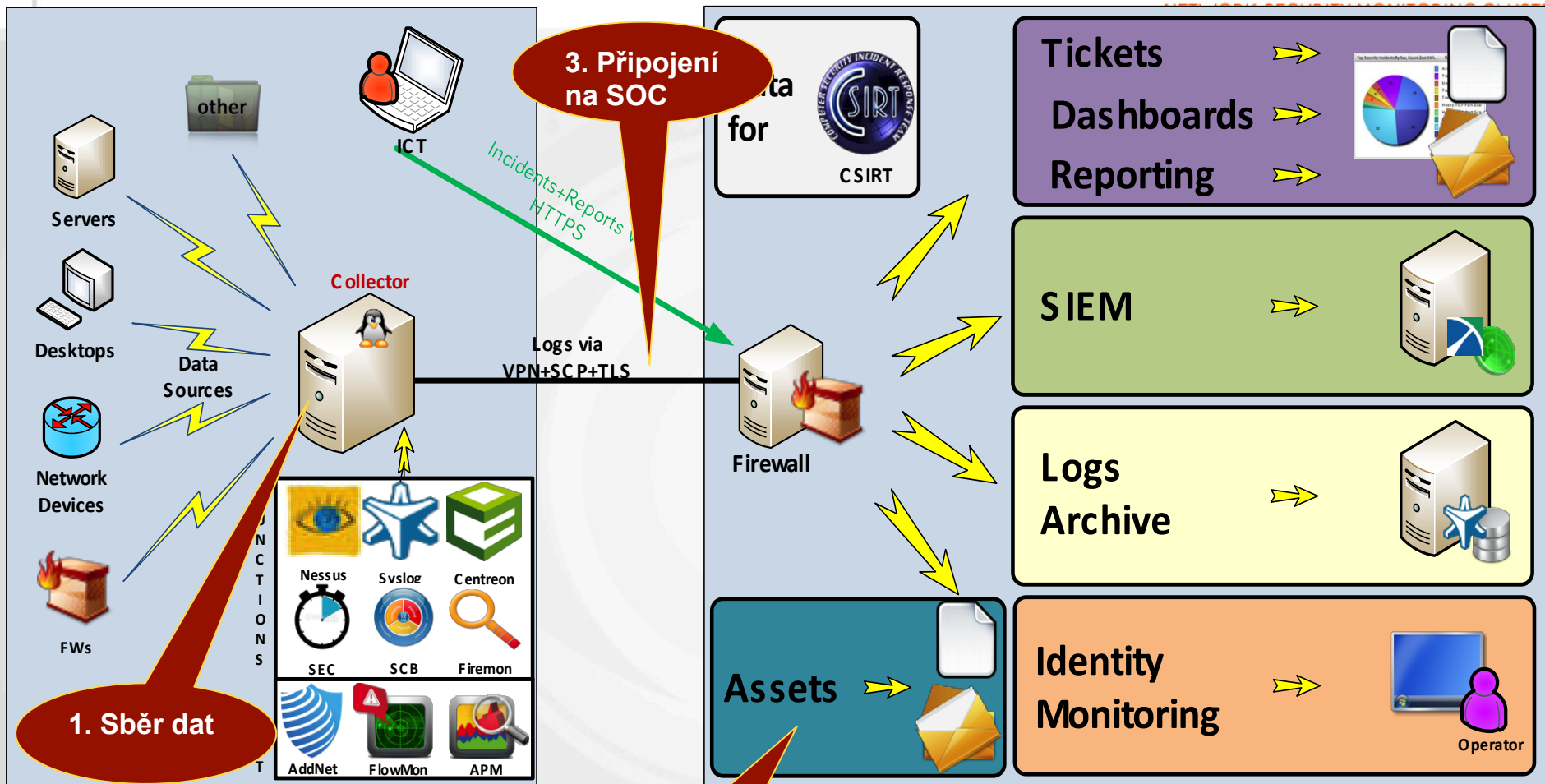
3. Reakce

3. Analýza
dat

1. Sběr dat

2. Akiva

Jak se staví SOC jako služba?



2. Aktiva

10/5 nebo 24/7

operátor + analytik + auditor

SOC + CSiRT

rychlost reakce = *schopnost detekce + nové korelační metody*

Shrnutí

Log management

Řeším sběr,
vyhledávání a
archivaci log dat

LM Centralize
Reporting
Data
Retention

Flow a NBA

Řeším, *které
anomalie mne
zajímají*
(analyzovat, řešit)
a *které anomalie
mne trápí* (řešit,
eliminovat)

FLOW Centralize
Reporting
Automatic
Detection

SIEM

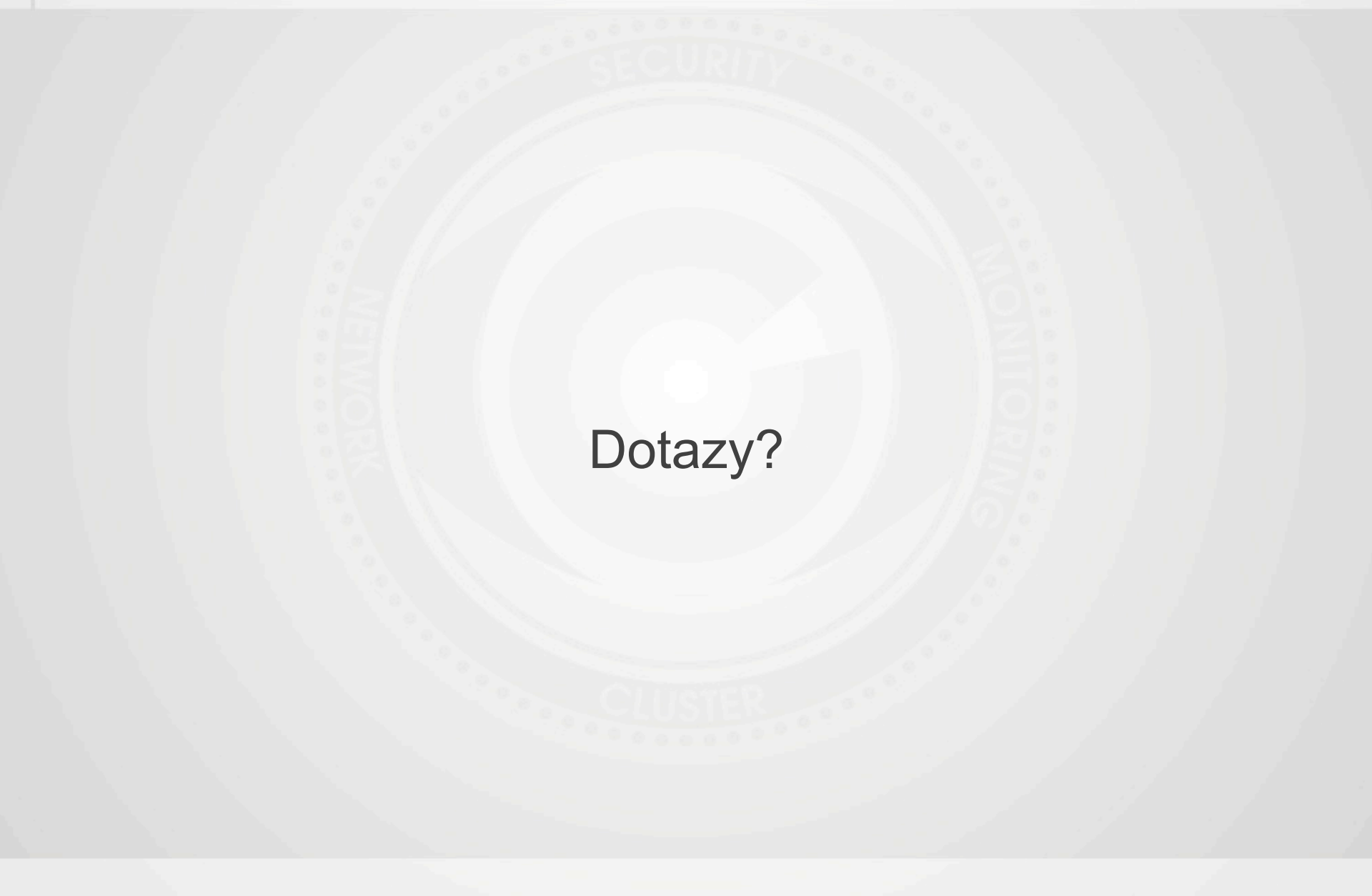
Řeším
*komplexní
prostředí s
cílem zajistit
Incident
Response*

SIEM Centralize
Reporting
Automatic
Incident
Response

SOC

Řeším workflow
problémů,
incidentů,
kontext dat a
kooperaci
zvládání
následků

SOC Kooperace v
Incident
Response
Aktualizace aktiv
Aktualizace
hrozeb



Dotazy?