
# ČO JE TO SOC A PREČO SOC

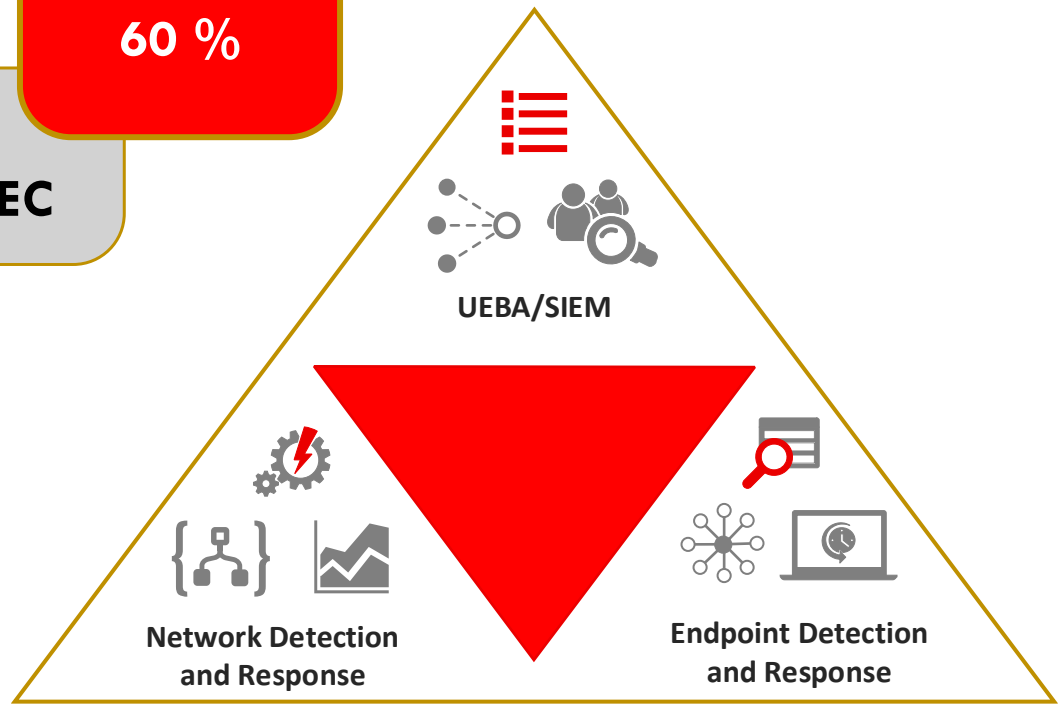
*Peter Jankovský, CTO & Security Architect, AXENTA*

UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™ & SME KONFERENCIE

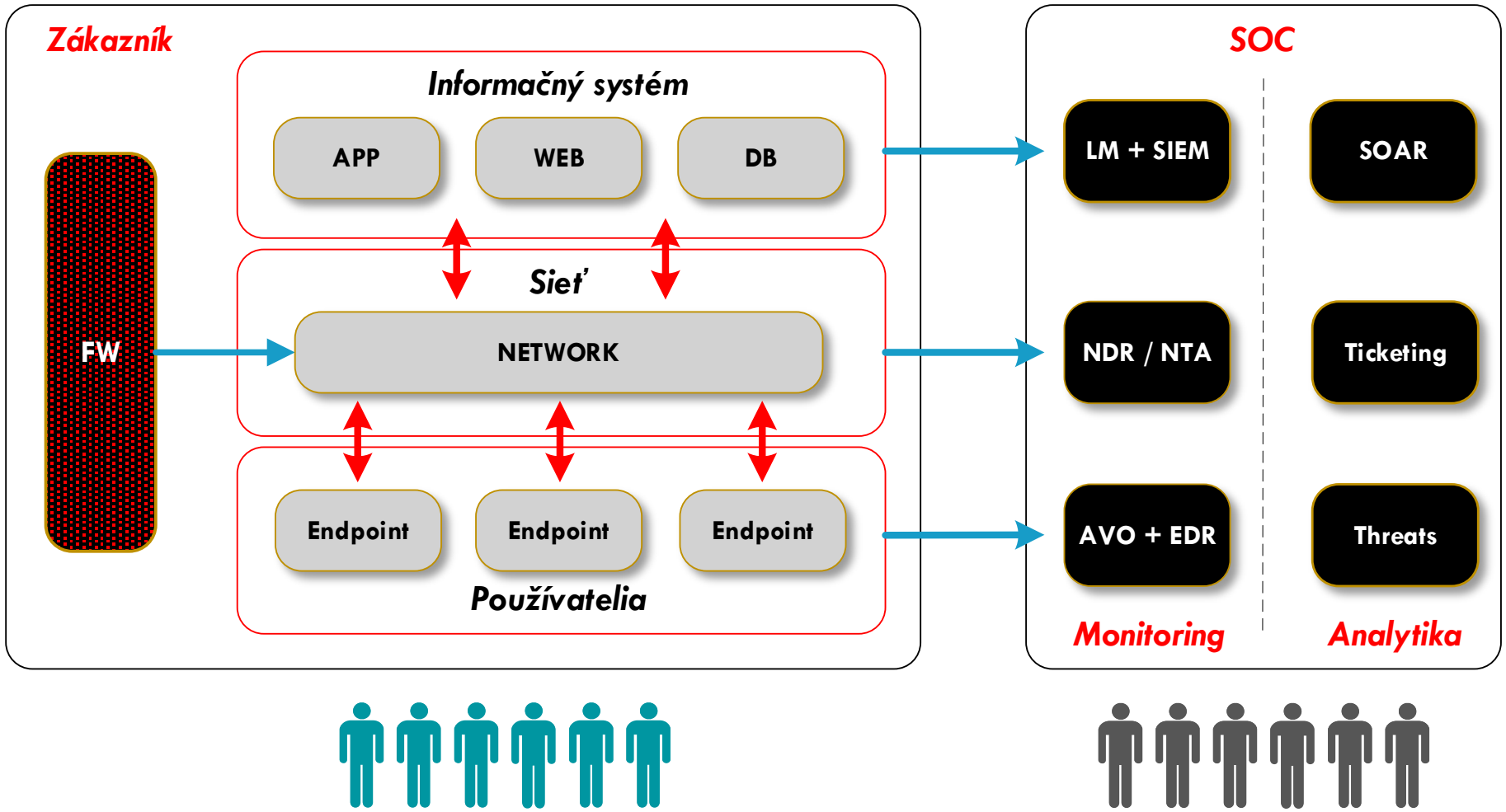
# Kto je útočník *(v roku 2021)*

**BEZPEČNOSTNÝ INCIDENT**

- **HACKER/útok** — 40 %
- **INTERNÝ ZAMESTNANEC** — 60 %



# Dokonalá bezpečnosť / Proti čomu a čím sa chrániť



# Čo je to SOC? A hlavne čo nie je SOC!

## Security Operation Center

Bezpečnostné Prevádzkové Centrum

## SOC vs Managed Security Services

Externé a Interné penetračné testy

FW konfigurácia

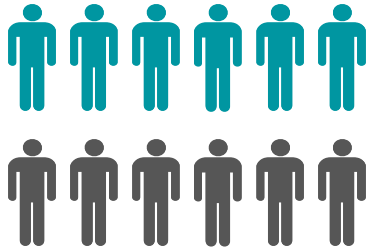
WAF, NAC, DLP...

## SOC -> Incident Response <-> CSIRT

Riešenie incidentov

CSIRT tím = forenzné šetrenie + informácie

Incident Response = náprava

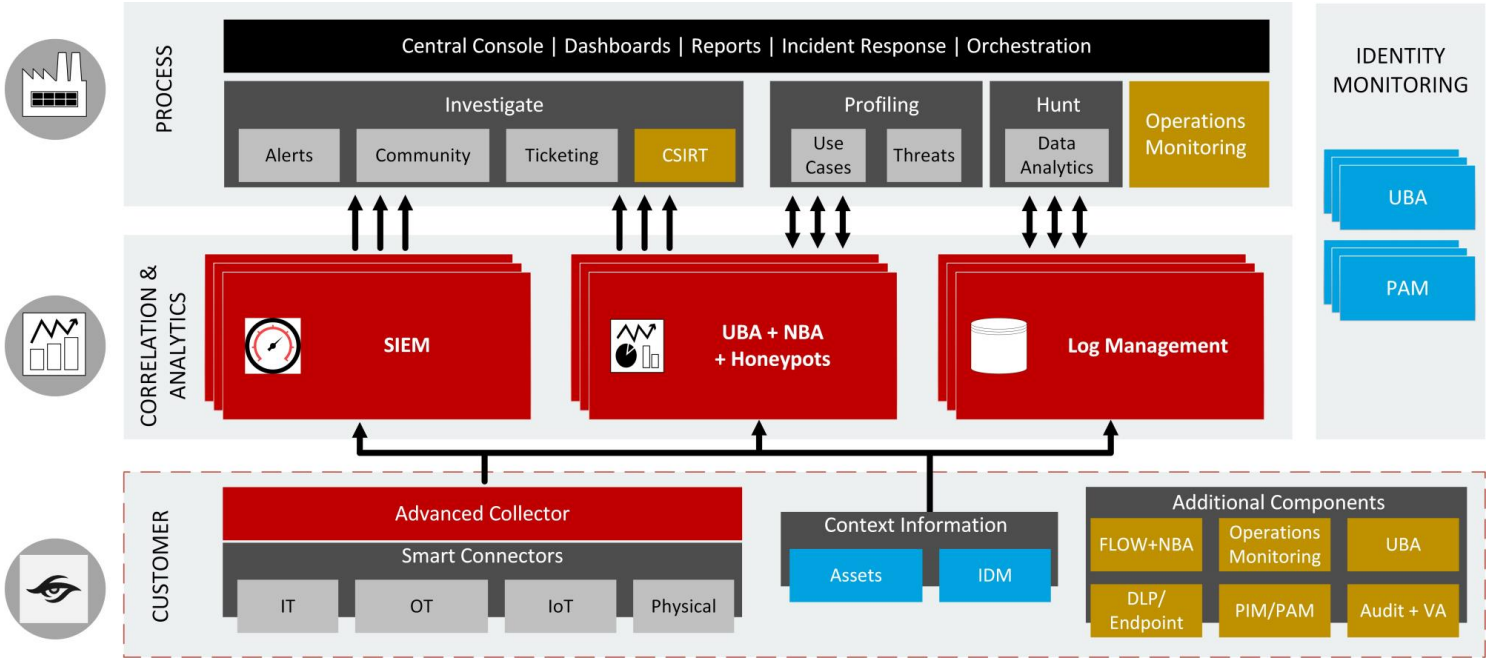


# Cyber SOC

*Intelligence-driven*

*Full-cyberchain*

*Time & cost-effective*




## Software

Event Management, SIEM, NDR, EDR, VA,

SOAR, Ticketing, Dashboardy

## Analytika

Hunting Unknown Unknowns

Reporting/KPI

Threats Exchange/MISP

Threats Intelligence

Vulnerability Management

Runbooks

## Ľudia

## Procesy

Incident Response, konzultácie, tvorba obsahu, vzdelávanie

CSIRT, Incident Forensics, Purple team

https://cybersoc.sk


https://www.itsec-nn.com/hierarchie-potreb-v-kyberbezpecnosti-1-cast/

# Slides pre diskusiu

# SOC mýty / Ľudia vs technológie

## Search and Hunt

- L1 = 0
- L2 = 10
- L3 = 2
- bez SIEM/EDR/NBA

## SOC

- L1 = 6
- L2 = 2
- L3 = 1
- so SIEM/EDR/NBA

***Reálne v TCO na 5 rokov = +30%***

# Interné/Externé náklady na SOC

## SOC 24/7

- 6x L1
- 2x L2
- 1x L3
- 1x SOC Manager

## SLA/podpora

- 5MD/mesačne
- 5-8 technológií

## IT/Incident Response

- CISO
- 2x IT špecialista
- 2x OT špecialista

Príklad --- **500** EPS, 8/5 (ľudia), TCO 5 rokov

- LM, SIEM, SOC ako služba = **3 000 EUR**/mesiac
- Hybridný model = **5 800 EUR**/mesiac
  - *LM, SIEM on premise, SOC ako služba*

# Otázky

- Náklady na ľudí v detaile – čo to teda znamená mať SOC z pohľadu ľudských zdrojov
- SOC nie je potreba, stačí auditná stopa a „Hunting“
- Kde zobrať ľudí  - úloha štátu, stredné školy, akčný plán