

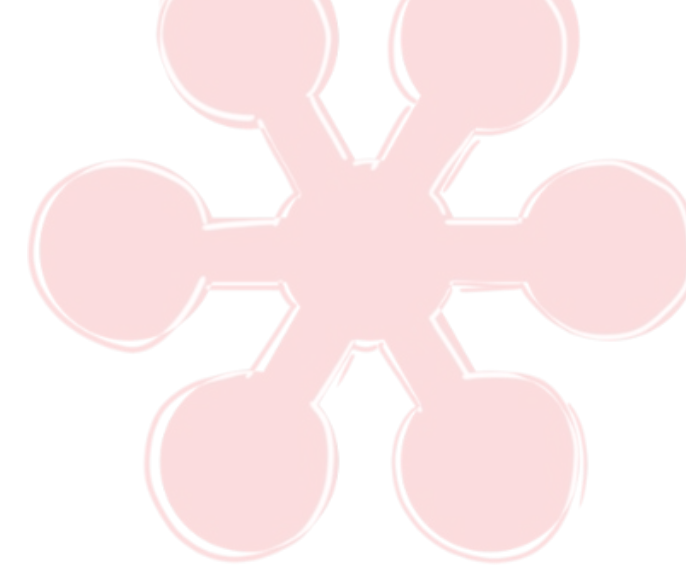
SOC: POSTAVIŤ, ZDIEĽAŤ, ALEBO KÚPIŤ?

Praktický rámec pre výber modelu monitoringu a reakcie na incidenty

RÝCHLA ANKETA

Aký model preferujete?

- A Vlastný SOC
- B Hybridný model
- C Externá služba



AGENDA

01

Prečo je to ťažké rozhodnutie

02

Čo vlastne SOC robí

03

Spektrum modelov

04

Rámec posúdenia: SIM3 + 2

05

Otázky, ktoré si položiť

06

Scenáre z praxe

07

Vývoj v čase

08

Zhrnutie a diskusia



1. PREČO JE TO ŤAŽKÉ

Monitoring a reakcia na incidenty nie sú len technologická otázka



TLAK ZO VŠETKÝCH STRÁN



24 h

na včasné varovanie o závažnom
incidente podľa ZoKB 69/2018



24/7

očakávaná dostupnosť monitoringu aj
reakcie



5–6 FTE

na jedno nepretržite obsadené miesto



SOC ≠ SIEM



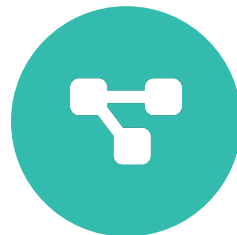
Organizácia

mandát, štruktúra, konštituencia



Ľudia

analytici, zmeny, rozvoj, rozhodovanie



Procesy

eskalácie, playbooky, komunikácia, hlásenie



Technológie

SIEM je len jedna z nich

2. ČO VLASTNE SOC ROBÍ

Skôr než začneme porovnávať



ČO (NE)ROBÍ SOC?



DETEKCIA

Zber a korelácia udalostí

Detection engineering

Threat hunting

Threat intelligence



REAKCIA

Triáž (L1)

Analýza (L2)

Reakcia a obnova (L3 / IR)

Forenzia, malvérová analýza...



RIADENIE

Reporting

Regulátorne hlásenie

Poučenie z incidentov

Školenia, konzultácie

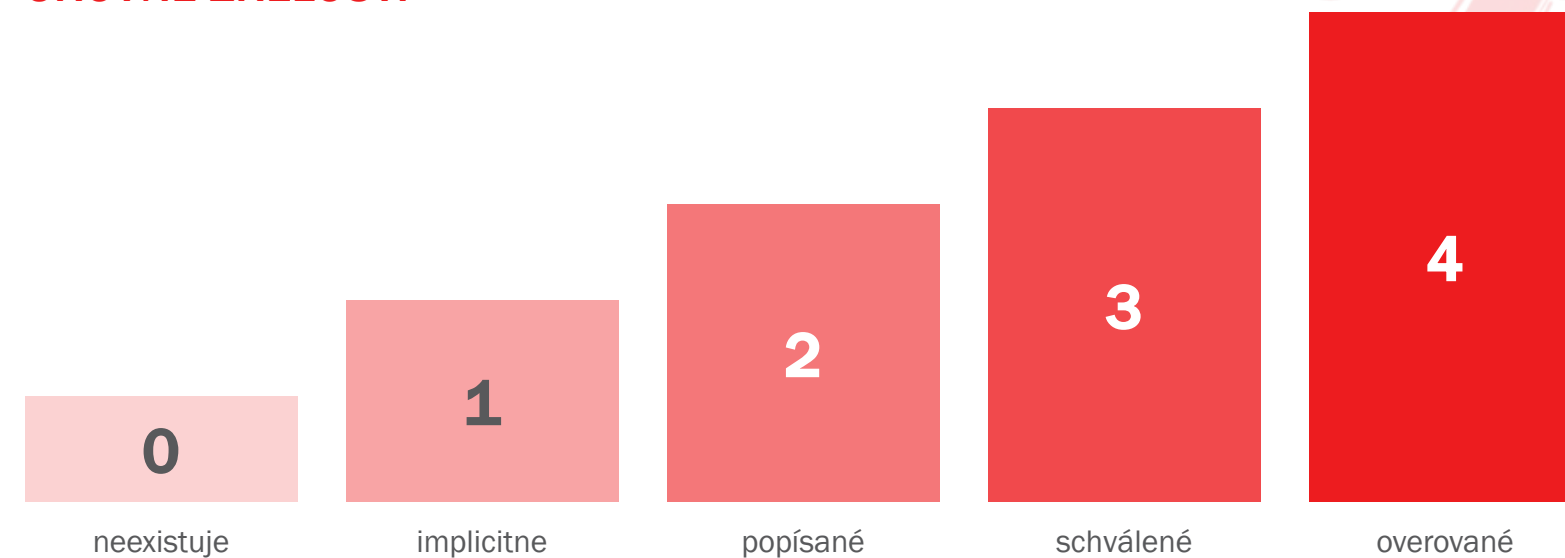


SIM3: MODEL, KTORÝ BUDEME POUŽÍVAŤ



Open CSIRT Foundation · Trusted Introducer · ENISA

ÚROVNE ZRELOSTI



3. SPEKTRUM MODELŮ

Od „všetko doma“ po „všetko externe“



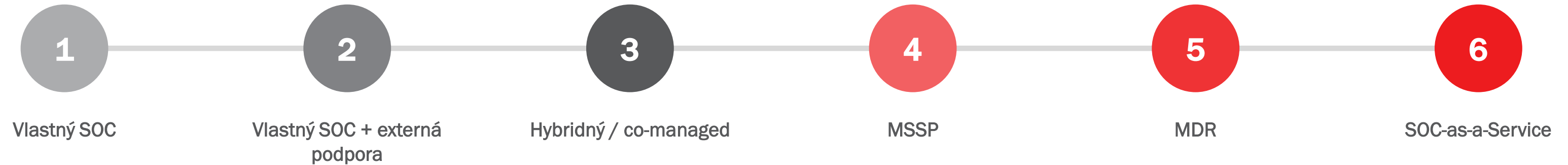
OS MODELOV, NIE ŠKATUĽKY

◀ VŠETKO DOMA

viac kontroly a know-how, viac nárokov

VŠETKO EXTERNE ▶

rýchlejší štart, viac závislosti



KEĎ JADRO ZOSTÁVA DOMA

1

Vlastný SOC

Všetko zabezpečuje vlastný tím.

+

Plná kontrola, know-how doma

-

Najvyššie nároky na ľudí a investície

2

Vlastný SOC + podpora

Interné jadro, nakúpené špecializácie (IR retainer, threat intel).

+

Expertíza bez stáleho úväzku

-

Vlastné 24/7 stále treba

3

Hybrid / co-managed

Rozdelené zodpovednosti, napr. L1 a noci externe.

+

Flexibilita a pokrytie 24/7

-

Kritické je jasné rozhranie

KEĎ VÝKON PREBERÁ PARTNER

4

MSSP

Poskytovateľ prevádzkuje FW, VPN a pod.) deteguje a upozorní.

+

Rýchly štart, nižšie náklady

-

Úzky scope, Reakcia zostáva na vás

5

MDR

Poskytovateľ deteguje aj aktívne zasiahne.

+

Kratší čas od detekcie po zásah

-

Právomoci a scope treba dohodnúť vopred,

6

SOC-as-a-Service

Kompletná prevádzka vrátane technológií.

+

Minimum prevádzkových starostí

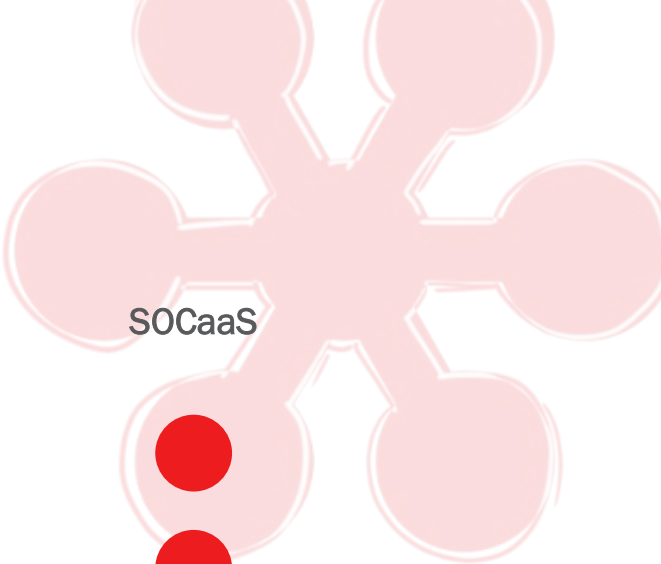
-

Závislosť a náročnejší exit

KTO ČO ROBÍ?

	Vlastný	+ podpora	Hybrid	MSSP	MDR	SOCaaS
Zber a detekcia	●	●	○	●	●	●
Triáž (L1)	●	●	●	●	●	●
Analýza (L2)	●	●	●	○	●	●
Zásah	●	○	○	●	●	●
Rozhodovanie	●	●	●	●	●	●
Regulatórne hlásenie	●	●	●	●	●	●

● interne ● externe ○ zdieľané



AKO VYZERÁ ZÁSAH V SOBOTU O 3:00 RÁNO?

MSSP



MDR



poskytovateľ

vy

SIM3 hodnotí mandát a autoritu explicitne. Dohodnite ich skôr, než ich budete potrebovať.



4. SIM3 + 2

Štyri oblasti zrelosti a dve otázky, ktoré SIM3 nekladie



SIM3 + 2



Ako dobre to vieme robiť?

úroveň zrelosti 0 až 4 podľa SIM3

Oplatí sa to?

mimo rozsahu SIM3



O

ORGANIZÁCIA

ČO HODNOTÍME

Mandát

Rozsah pôsobnosti

Autorita pri incidente

Popis a úroveň služieb

Pri outsourcingu nemizne. Presúva sa do zmluvy a SLA: mandát, rozsah, autorita, úroveň služieb.

KLÚČOVÁ OTÁZKA

Kto u nás rozhodne o odpojení produkčného systému o 3:00 ráno?





H

ĽUDIA

ČO HODNOTÍME

Pokrytie 24/7

Zručnosti a vzdelávanie

Odolnosť tímu

Nábor, lukuácia a vyhorenie

5–6 FTE

na **jedno** miesto obsadené 24/7, so zmenami, dovolenkami a chorobami

KLÚČOVÁ OTÁZKA

Vieme ľudí získať a udržať, nielen zaplatiť?





T

NÁSTROJE

ČO HODNOTÍME

SIEM / EDR / SOAR / log management / VM

Ticketing

Odolná komunikácia

Dáta a detekčné pravidlá

Pri externej službe: čie sú nástroje, kde sú dáta?

KLÚČOVÁ OTÁZKA

Komu patria dáta, pravidlá a playbooky, keď zmluva skončí?





P

PROCESY

ČO HODNOTÍME

Eskalácia

Riešenie incidentov

Regulatórne hlásenie

Poučenie z incidentov

PARTNER

VY

?

KLÚČOVÁ OTÁZKA

Kde presne sa proces odovzdáva a kto to kontroluje?



+2: EKONOMIKA A STRATÉGIA



EKONOMIKA

Vlastný SOC: mzdy, licencie, infraštruktúra, dáta, nábor

Služba: cenový model a dodatočné náklady

CapEx vs. OpEx, zdroje financovania

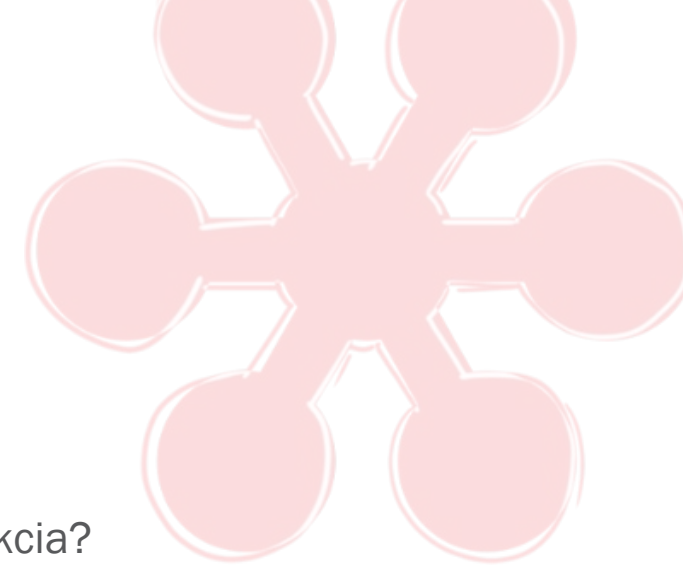


STRATÉGIA

Je bezpečnosť **klúčová kompetencia**, alebo podporná funkcia?

Kde chceme byť o **3 až 5 rokov**?

Máme potrebné **know-how** alebo je realistické ho **vybudovať**?



HODNOTIACA TABUĽKA

	0	1	2	3	4
O Organizácia					
H Ľudia					
T Nástroje					
P Procesy					
€ Rozpočet na vlastné kapacity					
S Ambícia budovať know-how					

Nízko

smer von: MDR alebo plne riadená služba

Vysoko

smer doma: vlastný SOC s cielenou podporou

5. SPRÁVNE OTÁZKY

Najprv sebe, potom poskytovateľovi





OTÁZKY PRE VÁS

- Čo chránime a pred čím?
- Kto rozhoduje počas incidentov a v akých lehotách?
- Ako sme pripravení technologicky?
- Aké máme schopnosti (budovať / riadiť partnera)?

6. SCENÁRE Z PRAXE

Rovnaký rámec, tri rôzne odpovede



TRI ORGANIZÁCIE, TRI ODPOVEDE



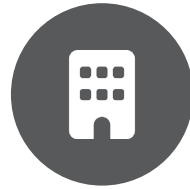
Menšia organizácia

bez vlastného bezpečnostného tímu

SOC-ako-služba

Doma zostáva:

aspoň 1 človek, ktorý službu riadi



Stredná regulovaná

s malým bezpečnostným tímom

Hybridný model

Doma zostáva:

analýza, rozhodovanie, hlásenie



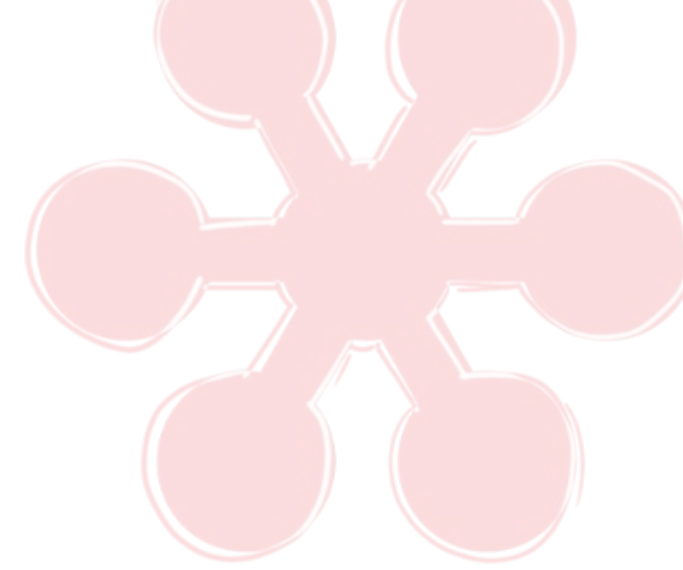
Veľká organizácia

so strategickou ambíciou

Vlastný SOC + podpora

Doma zostáva:

takmer všetko, IR a threat intel nakúpené



Takmer vždy doma ostáva organizácia (mandát, autorita) a časť procesov (eskalácia, hlásenie).



KOĽKO STOJÍ VLASTNÝ SOC?

0,7 – 1,1 mil. €

ročne za prevádzku 24/7

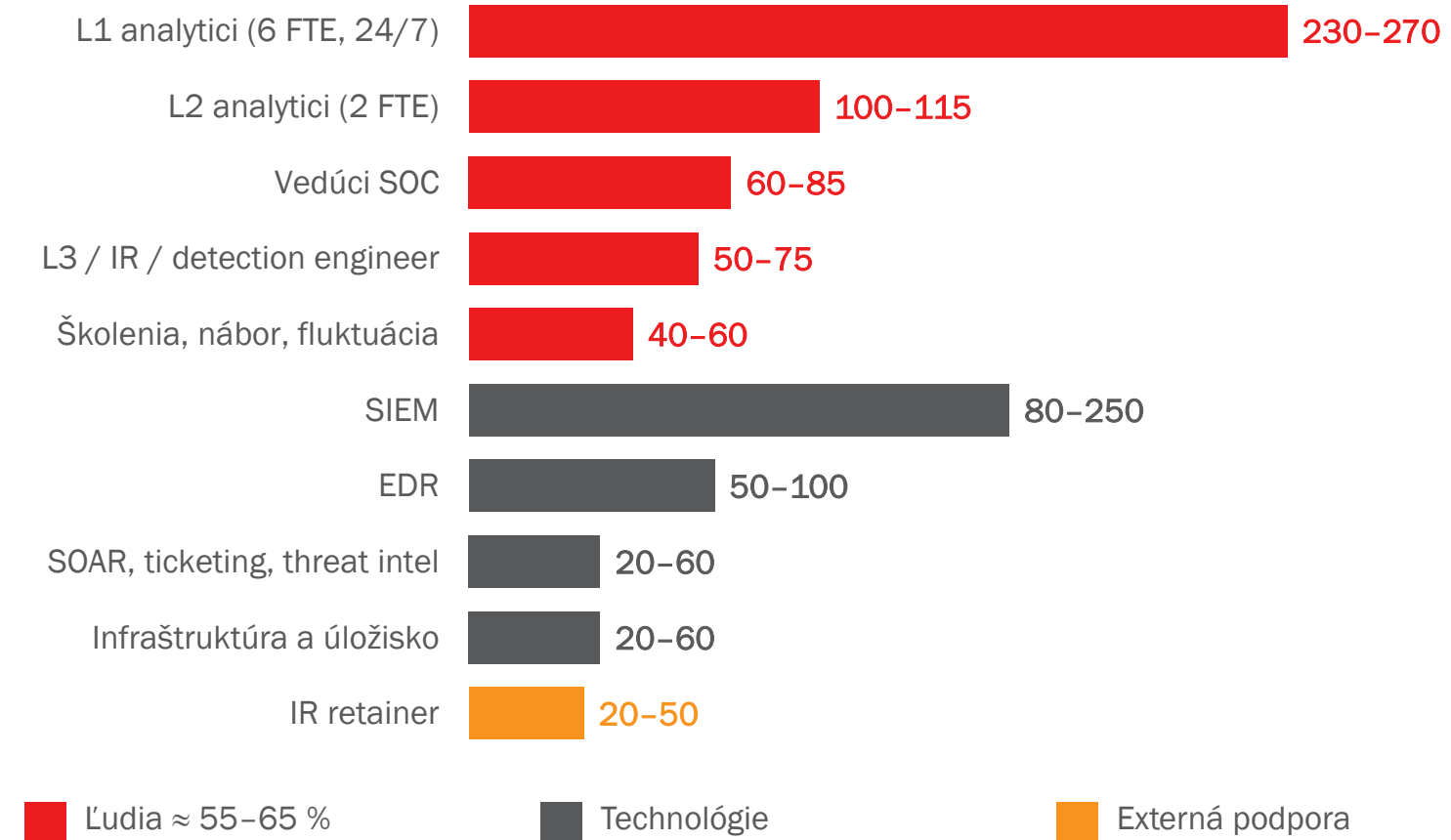
500 tis. € +

jednorazovo na vybudovanie

12+ mesiacov

do stabilnej prevádzky

ROČNÉ NÁKLADY V TIS. € orientačný odhad, bez DPH



7. PREFERENCIE V ČASE

Model nie je konečné rozhodnutie, ale bod na ceste



PRÍKLAD CESTY

Dnes

SOCaaS + interné riadenie

SIM3 O/P: 1

0 12 mesiacov

Hybrid, vlastná L2

SIM3 O/P: 2

0 36 mesiacov

Vlastný SOC + IR retainer

SIM3 O/P: 3

Ilustratívny príklad, cesta môže viesť aj opačným smerom.



Hodnoťte celý systém

vrátane rozhrania, nie každú stranu zvlášť



Exit plánujte od začiatku

dáta, pravidlá a znalosti musia byť prenositeľné

3 ODKAZY NA ZÁVER

1

Neexistuje univerzálne správny model.

Existuje model primeraný vašim potrebám a ambíciám.

2

Správne otázky > technológia.

SIM3 + 2 vám pomôže položiť ich systematicky.

3

Zodpovednosť nemožno outsourcovať.

Organizácia a rozhodovanie zostávajú doma.

? OTÁZKY A DISKUSIA





SOITRON*