Managed SOC v praxi, přínosy a limity outsourcingu

Maroš Barabas, Ph.D.; ARICOMA

13. – 15. října 2026

ISACA
Czech Republic Chapter

Hlavné problémy MSP SOC

- Výber dodávateľa
- Riadenie kvality služby
- Vstupy a zdroje
- Reakcia na incidenty
- Deformácia cenového modelu
- Udržateľnosť rozvoja
- Spolupráca oddelení
- Exit stratégia

ISACA
Czech Republic Chapter

Výber dodávateľa

Definícia služieb SOC/MDR

Definícia L1, L2 a L3	➢ 3x L1 a 1x L2/3
Interpretácia 24x7	➢ Smeny vs. on-call (L1 alebo L3?)
Referencie na SOC služby	➢ Anonymizované referencie (NDA) Nereflektujú kvalitu
CV a kvalifikácia	➢ Bait & Switch L1 spravidla nemá certifikácie L3 takmer neexistuje Kto sú kľúčoví ľudia SOC?
Úroveň požiadaviek	➢ „*Monitoring udalostí a riešenie incidentov*“
SLA	➢ Pickup Time MTTA a MTTD

ISACA Czech Republic Chapter

Riadenie kvality služby

Definícia SLA

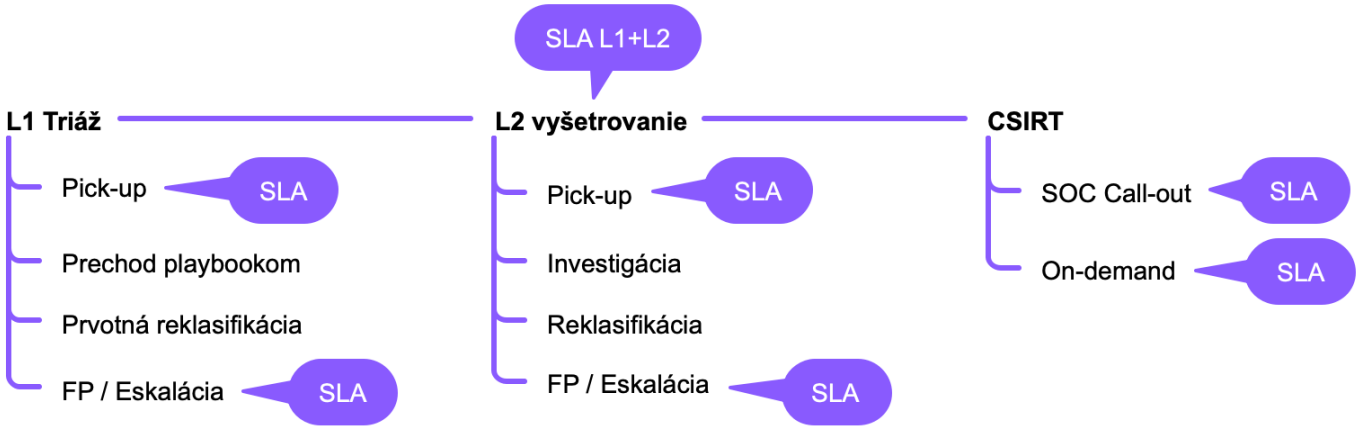
SLA: **Meriam dobu reakcie na kritické incidenty**

- Meriam? Alebo meria dodávateľ?
- Meriame dobu reakcie človeka alebo automatu?
- Chceme merať reakciu?
- Reaguje SOC na incidenty?
- Dokážeme klasifikovať vstupné udalosti?
- Kto určuje prioritu udalostí?

ISACA Czech Republic Chapter

Riadenie kvality služby

Definícia SLA



ISACA Czech Republic Chapter

Riadenie kvality služby

Očakávania od dodávateľa

- Meranie na strane zákazníka, nie dodávateľa
- Existencia investigatívnych playbookov
- Skúsenosti s riadením závažných incidentov
- Tréningy (table-top, red-teaming) CSIRT
- Doloženie pokrytia MITRE-ATT&CK

ISACA
Czech Republic Chapter

Vstupy a zdroje

Kto platí zdroje na rozvoj?
Kto je vlastník know-how?
Kto stanovuje klasifikáciu?

Zákazník

- Business požiadavky
- Baseline normálnej prevádzky
- Inventár aktív

Dodávateľ

- Use-cases
- Playbooky
- Zdroje
- Detekčné pravidlá

Generické a OOB pravidlá
Use-cases z katalógu dodávateľa bez väzby na riziká
Chýbajúci business kontext
Cenový model ticho formuje kvalitu detekcie

ISACA Czech Republic Chapter

Reakcia na incidenty

Kto má zodpovednosť konať?

- Kto nesie zodpovednosť za vykonanú akciu?
- Máme zavedené interné SLA odpovedajúce SLA SOC?
- Koho potrebujeme v krízovom manažmente?
- Ako definujeme a vyhodnocujeme dopad reakcie na incident?
- Ako definujeme povolené reakcie v špecifických situáciách?

SOC bez testovania reakcie je prepojovacia ústredňa

ISACA Czech Republic Chapter

Deformácia cenového modelu

Za čo platím keď chcem monitoring?

- **Paušál za GB/EPS/Incidenty** (platím objem)
  - Objem trestá rast telemetrie
  - SOC je v zajatí prevádzkovateľa technológie
- **Paušál za L1/L2 monitoring** (platím ľudí)
  - Neexistencia kvalitatívnych KPI vytvára minimálne úsilie
  - Únava z FP vedie k zníženiu citlivosti
  - Erózia služby na compliance monitoring

Rozvoj a kvalita SOC zvyčajne nie sú v cene služby.

Aké sú akceptačné kritériá služby?

ISACA Czech Republic Chapter

Rozvoj SOC

Definícia maturity SOC

- **Pračka na tikety** – majorita práce SOCu je čistenie FP, zvyšok reportuje
- **Compliance monitoring** – monitorujú a reportujú sa porušenia politík, investigácia prakticky neexistuje.
- **Prepojovacia ústredňa** – detekcia a investigácia prebieha, ale chýba kontext

- Maturita SOCu sa zvyšuje interne – MSP reaguje zvyšovaním skillov.
- Testy pripravenosti – napr. Red Teaming

80% nákladov do rozvoja SOC, 20% nákladov na monitoring

ISACA Czech Republic Chapter

Spolupráca oddelení

Viacerí externí i interní dodávatelia služieb

- Dodávateľ technológií vs. dodávateľ SOC
- Interné tímy a dostupnosť interných zdrojov
- Spolupráca spúšťačom, nie dobrou vôľou.
- Princíp modelovania procesov a mikro-služieb
- Existuje u vás BCP pre SOC?

EXIT stratégia

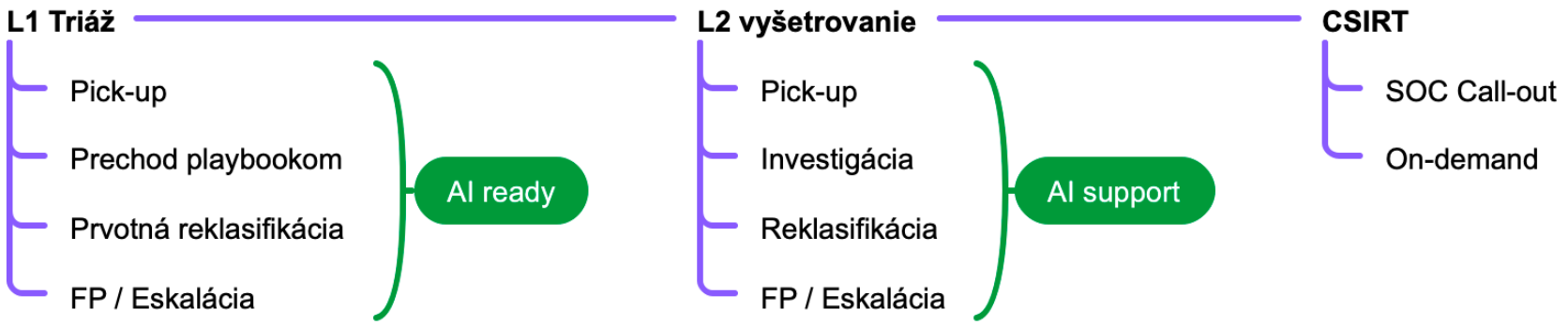
Dôvera, spoľahlivosť, hodnota dodávateľa alebo rast internej kompetencie

- **Čo mi nezostane?**
  - Znalosť prostredia u dodávateľa
  - Schopnosť retrospektívnej analýzy
  - Vzťahy
  - Know-how a vyladené use-cases a playbooky
- **Migrácia**
  - Trvá niekoľko mesiacov
  - Kto zaplatí súbeh 2 SOCov?

Exit plánujte v deň podpisu, nie v deň sklamania.
Aspoň raz by mal prebehnúť test.

ISACA Czech Republic Chapter

AI v SOC MSP



L1 agent u MSP alebo interne?

ISACA Czech Republic Chapter

Výzvy AI v SOC

- Závislosť na kvalite vstupov enormne rastie
- Znižuje sa citlivosť na hraničné situácie
- Agent potrebuje kontext, záznam predchádzajúcich rozhodnutí a jasne vymedzené oprávnenia.
- Riadenie dopadov zlých rozhodnutí – možnosť návratu
- Oprávnenie zásahu v špecifických situáciách

SOC ako MSP?

- ✓ Udržateľnosť ľudí vs. zaujímavé incidenty
- ✓ Skúsenosti z heterogénnych prostredí
- ✓ Interné TI by design
- ✓ Rýchlosť nábehu služby
- ✓ Predvídateľnosť nákladov
- ✓ Externý tlak na bezpečnosť a prevádzku
- x Vlastníctvo know-how
- x Zmeny u dodávateľa
- x Strety medzi dodávateľmi
- x Malá znalosť prostredia

Kontakt

Maroš Barabas, Ph.D.
ARICOMA
T: + 420 777 929 847
E: maros.barabas@aricoma.com

ISACA Czech Republic Chapter