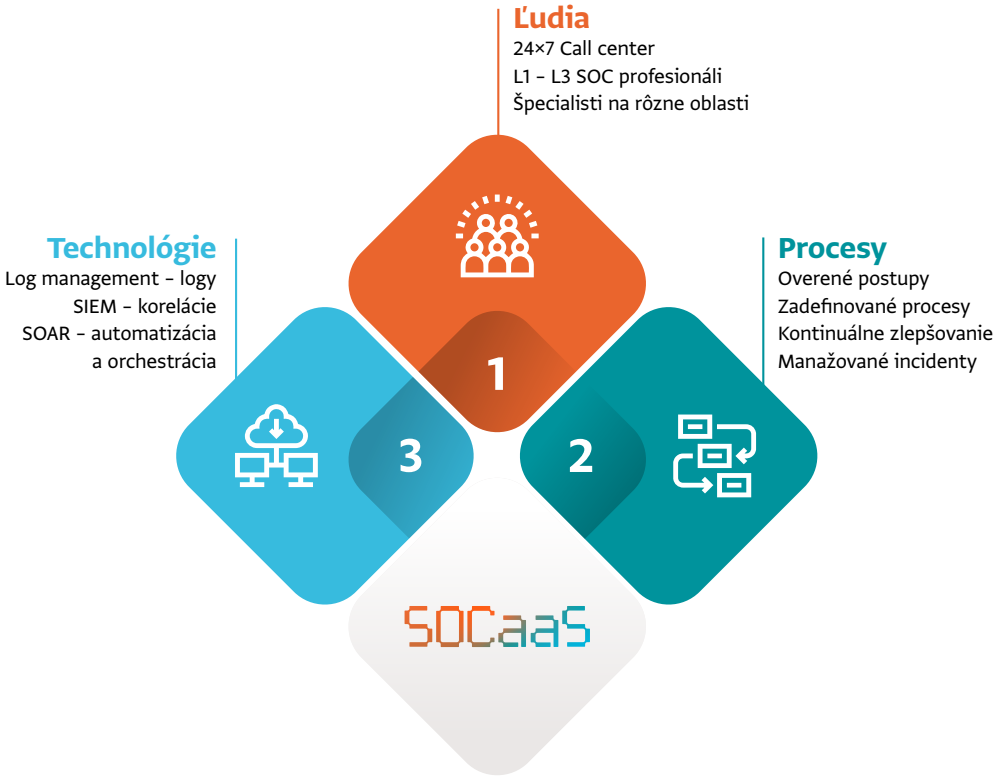
Alanata

SOCaaS

Čo je to SOCaaS (Security Operation Center as a service)?

SOCaaS predstavuje službu nepretržitého bezpečnostného dohľadu nad sieťou a infraštruktúrou zákazníka **kombináciou nasadených bezpečnostných technológií a poskytovaných proaktívnych a reaktívnych služieb bezpečnostnými špecialistami**. Čiže je to kombinácia nasadenej technológie a ľudských zdrojov vykonávajúcich bezpečnostný dohľad vrátane analýzy udalostí, ich vyšetrovania a reakcie na ne. Základ technológie bezpečnostného monitoringu tvorí systém SIEM (Security Information and Event Management) s Log managementom a SOAR (Security Orchestration, Automation and Response). Služby bezpečnostného monitoringu sú zabezpečované bezpečnostnými špecialistami na rôznych úrovniach.

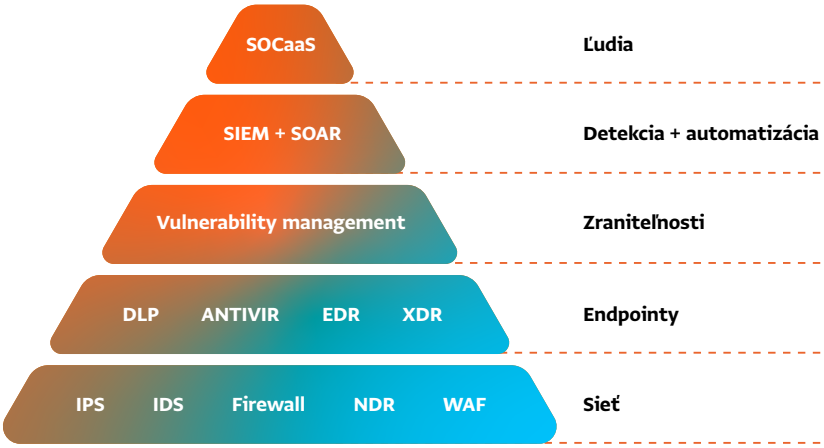


Možnosti nasadenia služby:

- on-premise riešenie SIEM, nad ktorým sú poskytované služby Alanata SOCaaS
- poskytovanie SIEM ako služby v rámci Alanata SOCaaS
- hybridné riešenia na mieru zákazníka, v rámci ktorého je možná integrácia SIEM zákazníka na Alanata SOCaaS

Základné parametre služby:

- 24x7 monitoring a detekcia hrozieb
- 8x5 / 24x7 bezpečnostný dohľad
- 24x7 Call Centrum (CC)
- on-line ticketing a reporting
- analýza správania sa používateľov (UBA)
- Threat Intelligence (TI)
- nastavenie úrovne služieb na mieru zákazníka



Aké prínosy má služba Alanata SOCaaS?

- **Ochrana infraštruktúry a údajov organizácie** = včasná detekcia hrozieb umožňujúca reagovať na hrozby ešte predtým, než spôsobia značné škody, a teda prevencia pred vznikom incidentov vedúcim k nedostupnosti infraštruktúry alebo k únikom či zničeniu údajov.
- **Rýchlejšia reakcia na bezpečnostné incidenty** = monitoring poskytuje aktuálne informácie o stave infraštruktúry a o prebiehajúcich incidentoch, čo znižuje reakčnú dobu.
- **Naplnenie zákonných požiadaviek** = organizácie, ktoré majú povinnosť monitorovať kybernetickú bezpečnosť zo zákona č. 69/2018 Z.z a v budúcnosti EÚ smernica NIS2.
- **Zvýšená viditeľnosť IT/OT prostredia** = zvýšená bezpečnosť.
- **Zvýšenie dôveryhodnosti voči klientom, zákazníkom a partnerom** tým, že ich dáta a služby ktoré využívajú, sú chránené.
- **Zníženie nákladov na FTE** voči in-house riešeniu pre dosiahnutie tých istých cieľov.

Ako dlho trvá nasadenie služby SOCaaS?

Pred spustením samotnej služby prebieha fáza tzv. onboardingu zákazníka. Táto doba je závislá najmä od množstva integrovaných systémov a komplikovanosti procesov, s ktorými bude musieť byť služba SOCaaS zintegrovaná. Spravidla sa táto doba pohybuje v rozmedzí dvoch týždňov až niekoľkých mesiacov. Dôležitou súčasťou fungovania služby SOCaaS je aj nastavenie procesov – workflowu pre jednotlivé pravidlá, nastavenie zodpovedností, definovanie reakcií pre jednotlivé situácie. Následne nastupuje pilotná prevádzka služby, počas ktorej už prebieha reálny bezpečnostný dohľad, počas ktorého sa vyladujú detekčné pravidlá, procesy, ako aj údaje zo zdrojových systémov. Tento proces trvá od niekoľkých týždňov až do dvoch mesiacov.

Licencovanie

SOCaaS ponúkame ako subscription licenčný model s mesačnými platbami, v ktorom sa zohľadňuje veľkosť a komplikovanosť infraštruktúry, rozsah, úroveň poskytovaných proaktívnych a reaktívnych služieb. Licenčný model je založený na počte produkčných serverov (fyzických aj virtuálnych), ktoré sa nachádzajú v dohľadovanej infraštruktúre (tzv. MVS) a nie na počte eventov za sekundu (EPS). Tento model poskytuje výhody najmä pre zákazníkov s veľkým počtom eventov (tzv EPS), ktoré zväčša generujú zariadenia ako firewally, IPS, DLP, pracovné stanice a kontajnerizované aplikácie.

Prečo ALANATA?

- Tím certifikovaných odborníkov s dlhoročnými skúsenosťami v oblasti informačnej a kybernetickej bezpečnosti.
- Bezpečnostní konzultanti s praxou s riešením legislatívnych požiadaviek v oblasti kybernetickej bezpečnosti, ITVS a GDPR.
- Možnosť využitia komplexných služieb a bezpečnostných riešení v oblasti informačnej a kybernetickej bezpečnosti.

Alanata a. s.
Krasovského 14
851 01 Bratislava

+421 2 502 67 111
info@alanata.sk
www.alanata.sk

Alanata
Technology Meets Business