OPZ pre LMS/SIEM (kombinované riešenie)

1 Funkčné požiadavky

- LMS musí byť schopný zhromažďovať logové dáta z rôznych zdrojov, vrátane operačných systémov, sieťových zariadení, serverov a aplikácií.
- LMS musí byť schopný ukladať a spravovať logové záznamy na centrálnom sieťovom úložisku. To zahŕňa dostatočnú kapacitu pre dlhodobé uchovávanie logov a rôzne mechanizmy kompresie a archivácie.
- LMS musí byť schopný fungovať ako distribuované riešenie.
- LMS musí poskytovať funkcie indexovania a vyhľadávania, ktoré umožňujú efektívne vyhľadávanie a filtrovanie logových záznamov podľa rôznych kritérií, ako sú časové údaje, udalosti, identifikátory používateľov a ďalšie.
- LMS musí poskytovať nástroje a funkcie pre analýzu logových dát. Tieto nástroje môžu zahŕňať vytváranie prehľadov, generovanie štatistík, detekciu anomálií, identifikáciu trendov a ďalšie analytické funkcie.
- LMS musí byť schopný vytvárať upozornenia a spravovať incidenty na základe definovaných pravidiel a vzorov.
- LMS musí byť schopný integrácie s rôznymi bezpečnostnými nástrojmi, ako sú systémy IDS/IPS, NGFW alebo SIEM systémy.
- LMS musí poskytovať funkcie auditu a sledovania, ktoré zabezpečujú, že prístup k logovým záznamom a operáciám sú riadené a zdokumentované.
- LMS musí mať užívateľsky prívetivé rozhranie pre konfiguráciu a správu logovacích politík, filtrov, upozornení a ďalších nastavení. Taktiež by mal poskytovať správu užívateľských prístupov a oprávnení.
- LMS musí poskytovať možnosti generovania prehľadných správ a vizualizácií logových dát.
- SIEM musí byť schopný zberu a normalizácie logových dát z rôznych zdrojov, ako sú endpointy, aplikácie, sieťové zariadenia, bezpečnostné zariadenia, databázy a ďalšie.
- SIEM musí byť schopný detekcie abnormálnych vzorcov správania a indikátorov kompromitácie (IOC) na základe analýzy logových dát.
- SIEM musí ponúkať pokročilé analytické funkcie, ako je detekcia anomálií, správanie založené na pravidlách a strojové učenie pre identifikáciu potenciálnych hrozieb.
- SIEM musí umožňovať tvorbu vlastných korelačných pravidiel (Use Cases).
- SIEM musí mať schopnosť spracovať a evidovať bezpečnostné incidenty v rámci jedného systému.
- SIEM musí mať možnosť klasifikácie a prioritizácie incidentov, priradenie zodpovednosti a sledovanie ich postupu.
- SIEM musí mať schopnosť sledovať bezpečnostné udalosti v reálnom čase a generovať notifikácie o kritických incidentoch alebo výnimočných udalostiach.
- SIEM musí mať možnosť upozornení a notifikácií prostredníctvom e-mailu, SMS, mobilných aplikácií alebo iných kanálov.
- SIEM musí mať možnosť vizualizácie, prehľadného zobrazenia logových dát a bezpečnostných udalostí vo forme grafov, tabuliek, dashboardov a správ.

- SIEM musí mať schopnosť generovať štatistické a analytické prehľady pre monitorovanie stavu bezpečnosti.
- SIEM musí mať možnosť integrácie s ďalšími bezpečnostnými nástrojmi a systémami, ako sú IDS/IPS, antivírusové programy, správa identít a prístupov (IAM), ticketing systémy a ďalšie.
- SIEM musí mať schopnosť generovať auditné stopy a záznamy o činnostiach v rámci SIEM systému pre overenie dodržiavania bezpečnostných noriem a regulácií.
- SIEM musí mať možnosť vytvorenia komplexných auditných správ a sledovanie zmien v logových dátach.
- SIEM musí mať schopnosť spracovať a analyzovať veľké objemy logových dát a bezpečnostných udalostí.
- SIEM musí zabezpečiť vysoká dostupnosť a výkon systému, aby zabezpečil efektívne spracovanie a detekciu hrozieb v reálnom čase.
- SIEM by mal mať aj funkcionalitu sieťovej sondy bez použitia externých IDS/IPS.
- LMS/SIEM musí byť prevádzkovaný na samostatnom dedikovanom hardvéri (logická časť [server] a diskové pole oddelene) neodporúčame prevádzku vo virtualizovanom prostredí.
- LMS/SIEM musí byť modulárny a škálovateľný a musí podporovať rôzne prevádzkové modely (standalone, collector / processor, collector / processor / storage, collector / processor / storage / archive atď.).

2 Bezpečnostné požiadavky

- LMS/SIEM musí poskytovať mechanizmy prístupovej kontroly, ktoré zabezpečujú, že len oprávnené osoby majú prístup k logovým dátam. To zahŕňa autentifikáciu, autorizáciu a revíziu prístupových práv.
- Dáta uložené v LMS/SIEM, musia byť šifrované. Tým sa zabezpečuje, že sú chránené pred neoprávneným prístupom počas uloženia.
- LMS/SIEM musí byť umiestnené v zabezpečenom prostredí s obmedzeným prístupom. Zálohovanie a obnova dát musia byť tiež zahrnuté, aby sa minimalizovala strata údajov v prípade havárie alebo iných incidentov.
- LMS/SIEM musí byť vybavené mechanizmami monitorovania a detekcie hrozieb. Tieto mechanizmy by mali upozorniť na neobvyklé aktivity, pokusy o neoprávnený prístup alebo iné bezpečnostné incidenty týkajúce sa uložených dát.

3 Výkonnostné požiadavky

- Predpokladaný objem EPS (súbežne spracované logy) je minimálne 500 s potenciálom nárastu až na 2000
- Všetky časti dodávanej zákazky musia byť nové technologicky vyspelé produkty - aktuálne ponúkané na trhu, testované a schválené kompetentnými slovenskými alebo zahraničnými autoritami. Zároveň musia byť prispôsobené na pracovné a bezpečnostné prostredie i technické normy Slovenskej republiky.