Čo je SIEM
(**S**ecurity **I**nformation and **E**vent **M**anagement)
a prečo je potrebný?

Súčasné siete a informačné systémy sú komplexnejšie ako kedykoľvek predtým. Generujú množstvo auditných/log záznamov, ktorých aktívne sledovanie a vyhodnocovanie v reálnom čase je čím ďalej tým zložitejšie. Ochrana sietí a informačných systémov musí byť nepretržitá. Je nevyhnutné, aby mali organizácie, ktoré sa snažia ochrániť svoje údaje a údaje klientov bezpečnostný monitoring IT prostredia. To isté platí o tých, ktorých úloha je zabezpečiť vlastný intelektuálny majetok a zamedziť výpadkom dôležitých systémov podporujúcich výrobné, riadiace alebo ďalšie podporné činnosti organizácie. Musia byť schopné rýchlo detegovať hrozby a adekvátne odpovedať na potenciálne útoky ešte predtým, ako sú útočníci schopní napáchať organizácii reálne škody.

SIEM absorbuje obrovský objem bezpečnostne relevantných údajov zo systémov naprieč celou organizáciou, vďaka čomu dokáže poskytnúť ucelený pohľad na aktivity či už on-premise, na virtualizačných platformách alebo v cloudovom prostredí. Počas zberu dát v reálnom čase aplikuje automatické procesy vyhodnocovania bezpečnostných udalostí, aby rýchlo a spoľahlivo detegoval a priorizoval hrozby. Na základe tohto spracovania vytvára záznamy o incidentoch, ktorých kontext obsahuje potrebné informácie umožňujúce bezpečnostným analytikom organizácie včas reagovať a obmedziť dopad plánovaného či prebiehajúceho útoku.

Aká je základná funkcionalita SIEM a pre koho je tento nástroj určený?

SIEM je v prvom rade monitorovací a auditný nástroj. Bezpečnostným IT tímom poskytuje centralizovaný pohľad na všetky relevantné bezpečnostné informácie z IT infraštruktúry v reálnom čase a vyhodnocuje rizikové bezpečnostné udalosti. Vo všeobecnosti technológia **SIEM** poskytuje najmä tieto činnosti:

- **Zber údajov a udalostí** – zber bezpečnostných a prevádzkových záznamov z rôznych zariadení nachádzajúcich sa v IT infraštruktúre organizácie.
- **Normalizácia zozbieraných údajov** – predspracovanie údajov za účelom zjednotenia rôznych formátov.
- **Korelácia** – posúdenie vzťahov medzi jednotlivými údajmi a udalosťami.
- **Log management** – uchovávanie log/auditných záznamov, ich komprimácia a indexácia.
- **Monitoring používateľov a jednotlivých častí IT infraštruktúry** – sledovanie neobvyklého správania sa používateľov a administrátorov, detekcia potenciálnych a reálnych bezpečnostných incidentov a neobvyklých aktivít voči pravidlám a/alebo minulému stavu.
- **Audit a reporting** – generovanie reportov o činnosti a bezpečnostnej kondícii IT infraštruktúry.

Okrem vyššie uvedených funkcionalít môže mať **SIEM** v závislosti od použitej technológie aj rôzne rozšírenia a nadstavby. Tie umožňujú vďaka využitiu umelej inteligencie presnejšie detegovať bezpečnostné udalosti a vykonávať aj forenzné analýzy.

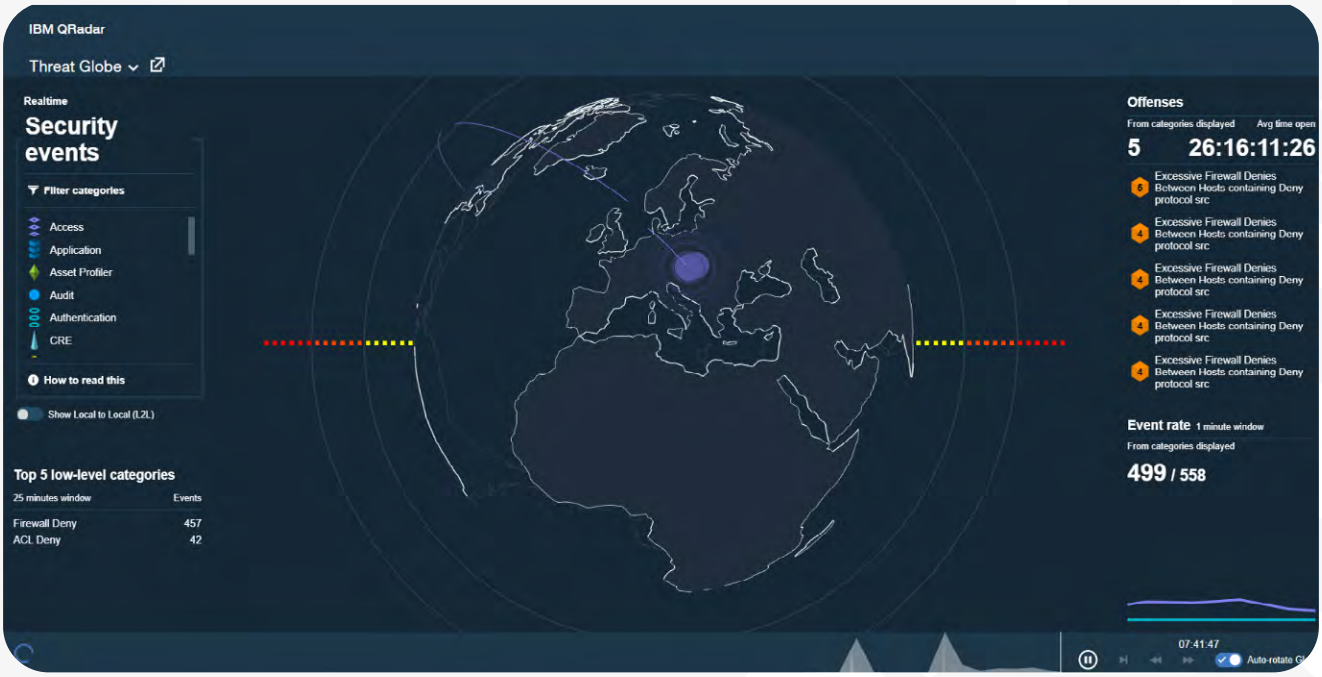
SIEM je nástroj, ktorý je možné implementovať do infraštruktúry organizácie akejkoľvek veľkosti a s akýmkoľvek zameraním. Bez automatizovanej detekcie, korelácie a vyhodnocovania bezpečnostných udalostí nie je žiadny bezpečnostný tím schopný zaistiť a garantovať bezpečnosť zverenej IT infraštruktúry.

Hlavné prínosy zavedenia SIEM

IT infraštruktúra organizácie pozostáva často z veľkého množstva sieťových prvkov, bezpečnostných technológií, serverov a aplikácií generujúcich veľké množstvo údajov. Tie sú zdrojom cenných informácií pre identifikáciu rôznych bezpečnostných hrozieb. Bez ďalšieho automatizovaného spracovania by však zostali tieto údaje často nevyužité a vzniknuté bezpečnostné hrozby nepovšimnuté.

Výhody implementácie SIEM pre organizáciu:

- schopnosť spracúvať veľké množstvo bezpečnostne relevantných údajov v reálnom čase a vzájomnú automatickú koreláciu týchto údajov,
- ucelený komplexný pohľad na bezpečnosť IT infraštruktúry organizácie,
- výrazné zníženie rizika prameniaceho z nedostatočného obrazu o tom, čo sa deje v rámci infraštruktúry z hľadiska bezpečnosti,
- možnosť forenznej analýzy udalostí z mnohých typov zariadení,
- centralizovaný nástroj na manažment bezpečnostných udalostí a na podporu reportingu bezpečnostným tímom, resp. na podporu manažmentu organizácie.



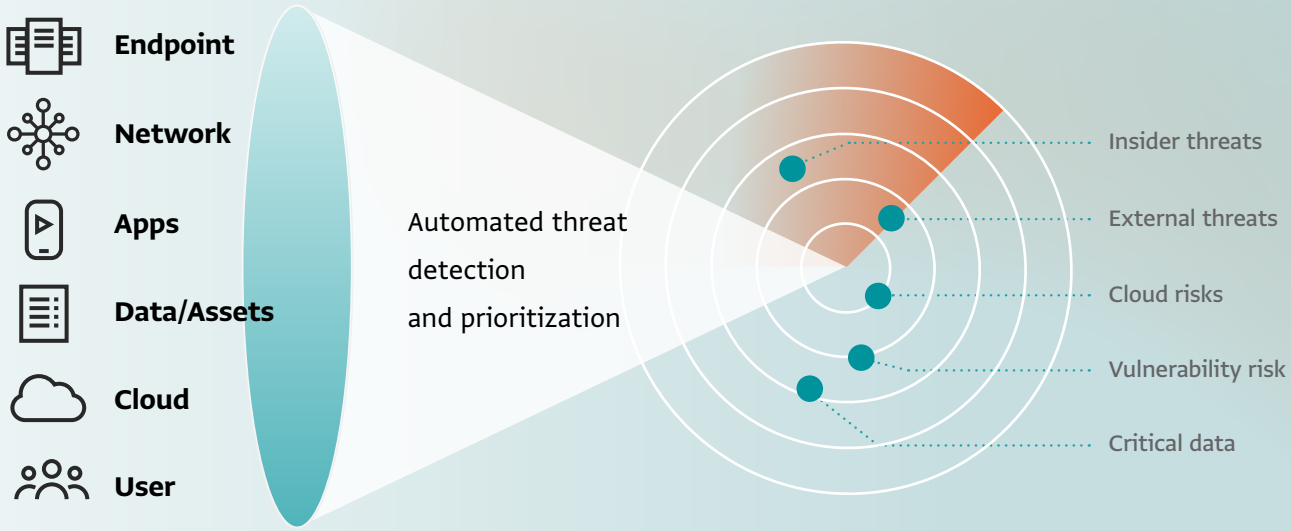
Aké údaje SIEM zbiera?

Aby SIEM identifikoval známe aj neznáme hrozby, automaticky zbiera, analyzuje a koreluje informácie o aktivitách z rôznych zdrojov, akými sú log súbory rôznych bezpečnostných technológií, udalosti, network flow data, aktivity používateľov a znalosti o bezpečnosti informačných systémov.

Súčasne je schopný zbierať a spracovávať aj informácie o existujúcich zraniteľnostiach jednotlivých prvkov IT infraštruktúry organizácie, ktoré boli identifikované napr. v organizácii implementovaným nástrojom na sken a správu zraniteľností.

SIEM štandardne zbiera napríklad nasledovné údaje:

- bezpečnostné udalosti z firewallov, VPN, IDS, IPS a databáz,
- sieťové udalosti zo switchov, routerov, serverov a ďalších zariadení,
- sieťové aktivity a komunikáciu až na úrovni Layer 7,
- aktivity v cloude, Informácie zo SaaS a IaaS prostredia, ako sú Office365, SalesForce.com, Amazon Web Services (AWS), Azure a Google Cloud,
- dáta o používateľoch a aktívach, teda informácie zo systémov na riadenie prístupov a identít,
- informácie zo skenerov zraniteľností,
- udalosti koncových zariadení, ako je Windows event Log, Sysmon a podobne,
- aplikačné logy, či už ide o štandardné ERP, alebo vlastné aplikácie,
- informácie o hrozbách, ako je napríklad IBM X-Force®.



- Real-time correlation and behavioral anomally detection
- Threat intelligence and vulnerability insight
- Machine learning, service and user profiling

Súlad s bezpečnostnými štandardmi a legislatívou

Implementácia **SIEM** a s tým súvisiaci log manažment sú základným predpokladom pre zabezpečenie súladu organizácií najmä s nasledovnými bezpečnostnými štandardmi a legislatívou:

- zabezpečenie zberu a vyhodnocovania kybernetických bezpečnostných incidentov a monitorovanie bezpečnosti sietí a IS v **zmysle zákona č. 69/2019 Z.z. o kybernetickej bezpečnosti a nadväzujúcich vyhlášok**,
- zaznamenávanie činnosti sietí a IS a ich používateľov (log manažment) a uchovávanie auditných/log záznamov v **zmysle zákona č. 69/2019 Z.z. o kybernetickej bezpečnosti a nadväzujúcich vyhlášok**,
- zabezpečenie ochrany osobných údajov spracúvaných v informačných systémoch v zmysle nariadenia **GDPR**, resp. **zákona č. 18/2018 Z.z. o ochrane osobných údajov**,
- zabezpečenie ochrany informačných systémov a technológií verejnej správy v zmysle požiadaviek **zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe**.

Zabezpečuje aj súlad s vybranými požiadavkami, ako napríklad Payment Card Industry Data Security Standard (PCI DSS), The Federal Information Security Management Act **(FISMA)**, Sarbanes-Oxley **(SOX)** a **ISO/IEC 27001** a **ISO/IEC 20000-1**.

O nástrojoch SIEM

Jedným zo **SIEM** riešení podporovaných spoločnosťou Alanata je bezpečnostná platforma QRadar® Security Intelligence od spoločnosti IBM, lídra v oblasti **SIEM** riešení.

Vyznačuje sa širokou podporou technológií, aplikácií a cloudových služieb, pokročilou úrovňou korelácie a detekcie bezpečnostných udalostí, ako aj možnosťou implementácie riešenia on-premise alebo v cloude.

Možnosti nasadenia SIEM

Technológia bezpečnostného monitoringu môže byť vo vašej organizácii implementovaná s ohľadom na aktuálne potreby, rozsah IT infraštruktúry a disponibilitu zamestnancov s dostatočnými technologickými a bezpečnostnými znalosťami na nasledovných úrovniach:

ON-PREMISE inštalácia SIEM:

- → všetky komponenty SIEM riešenia prevádzkujete na vlastných serveroch,
- → všetky údaje zostávajú v organizácii.

SIEM ako cloud služba:

- → nemusíte inštalovať žiadnu IT infraštruktúru, priamo si volíte, aké komponenty a aký výkon potrebujete pre pokrytie vašej IT infraštruktúry.

Poskytnutie SIEM v rámci bezpečnostného operačného centra (tzv. SOC):

- → riešenie je prevádzkované na infraštruktúre spoločnosti Alanata a v sledovanej infraštruktúre zákazníka sú umiestnené iba tzv. kolektory udalostí,
- → 24/7 dohľad nad SIEM – detekcia, analýza a vyhodnocovanie kybernetických bezpečnostných incidentov,
- → reakcia na incidenty SOC tímom.

Nasadenie SIEM ako log manažment nástroja:

- → riešenie, ktoré poskytuje zber a archiváciu logov a ich základné vyhodnotenie s možnosťou vyhľadávania, reportingu a exportu.

Čo je to SOC (Security operations center) a ako pomáha pri zlepšovaní kybernetickej bezpečnosti?

Ak **SIEM** vykonáva zber a vyhodnocovanie údajov podieľajúcich sa na tvorbe bezpečnostných udalostí, SOC zabezpečuje ich monitorovanie a reakciu na vzniknuté bezpečnostné upozornenia. Srdce SOCu tvoria ľudia, ktorí monitorujú prichádzajúce upozornenia, vyhodnocujú ich a reagujú na ne podľa dohodnutých procesov. Pri vyhodnocovaní im okrem skúseností pomáha široké spektrum nástrojov. Medzi najdôležitejšie nástroje SOCu patrí SIEM, rôzne threat inteligence platformy, nástroje na analýzu malwaru, knowledge base, ticketing systém a iné.

Základné funkcie SOCu:

- **Monitoring bezpečnostnej situácie:** SOC operátori monitorujú udalosti prostredníctvom jednotnej konzoly, do ktorej sú agregované všetky zdroje dát.
- **Detekcia hrozieb:** SIEM nástroj nepretržite deteguje hrozby prostredníctvom nastavených pravidiel. Operátor L1 sleduje konzolu s udalosťami.
- **Investigácia bezpečnostných upozornení:** Operátor L1 vykonáva triáž udalostí, analyzuje ich a validuje relevantnosť bezpečnostných incidentov.
- **Odpoveď na incidenty:** Eskalácia incidentov na vyššiu úroveň (L2/L3) alebo na zákazníka. Návrh protiopatrení alebo vykonanie nápravnej akcie.
- **Manažment a kontinuálne zlepšovanie:** Manažment bezpečnostných incidentov, neustále zlepšovanie detekcií a procesov.

SOC tvoria tri základné piliere: ľudia, procesy a technológie

Budovanie vlastného SOCu môže byť pre spoločnosti časovo a finančne náročné. Preto Alanata prišla so službou SOCaaS (SOC as a Service).

Výhody SOCaaS pre zákazníka

- → Rýchlosť nasadenia
- → Nepretržitý monitoring a detekcia
- → Kratšia reakčná doba
- → Optimalizácia ľudských zdrojov
- → Eliminácia únavy z upozornení (alert fatigue)

Pre koho je SOCaaS určený?

Služba SOCaaS je určená pre všetkých zákazníkov, ktorí nemajú dostatočné kapacity na vybudovanie vlastného SOCu v ktorejkoľvek oblasti troch pilieroch služby: ľudia, procesy a technológie. Tiež je určená pre spoločnosti, ktoré nedisponujú dostatočným know-how alebo potrebujú služby SOCu v krátkom čase.

Možnosti nasadenia SOCaaS

Pre zachovanie čo najvyššej kvality služby SOCu, odporúčame vybudovanie spolu so zakúpením SIEM riešenia od spoločnosti Alanata. Ak už vaša spoločnosť disponuje SIEM riešením, nie je to prekážka a je možné ho pripojiť do nášho SOCu.

Prečo Alanata?

Alanata vznikla spojením tých najskúsenejších expertov na slovenskom trhu informačných technológií. V súčasnosti spoločnosť zamestnáva viac ako 320 ľudí. Disponuje 30-ročnými skúsenosťami, ktoré nadobudli pri významných projektoch pre rôznych klientov: od malých a stredných podnikov, cez veľké spoločnosti a korporácie až po verejnú správu.

Kompetencie Alanata pokrývajú najvýznamnejšie technologické oblastí ako cloudové a infraštruktúrne riešenia, kybernetická a informačná bezpečnosť, management dát a umelá inteligencia, consulting, riešenia SAP, vývoj softvérových riešení na mieru, IT prevádzka a outsourcing, service management a monitoring.

Alanata a. s.
Krasovského 14
851 01 Bratislava

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

Alanata
Technology Meets Business