Logsign

Migrace SIEM na Logsign

Migrace staršího systému SIEM na SIEM nové generace

Řešení SIM a SEM přišla na trh na přelomu století a tato první řešení SIEM byla složitá, obtížně konfigurovatelná a náročná na škálování. Tyto problémy urychlily vývoj řešení SIEM, která jsou flexibilní, pokročilá, založená na analýze a jednoduše škálovatelná. Pro moderní řešení SIEM nyní zajišťuje sběr logů z různých zdrojů jednoduchou operací a organizace má mnoho možností, jak tato data ukládat. Hlavní bitva spočívá v přeměně těchto dat na využitelnou inteligenci.

Organizace, které se spoléhají na starší řešení SIEM, často zjišťují, že jejich SIEM je statické povahy. Postrádá dostatečné korelační funkce a je poměrně komplikovaný, takže se potýká s problémy při podpoře časově náročných šetření. S nástupem technologie cloud computingu a modelu poskytování služeb SaaS se objevila řešení SIEM nové generace, která jsou nyní schopna pokrýt celý rozsah potenciálních hrozeb. Mezi běžně pozorované problémy starších systémů SIEM patří:

- Omezené možnosti detekce, vyšetřování a reakce na incidenty kvůli omezenému příjmu dat.
- Přebírání dat je zdlouhavý proces.
- Poměrně složitá obsluha, která vyžaduje kvalifikované zaměstnance.
- Generování velkého počtu falešně pozitivních a falešně negativních alertů.
- Neschopnost odhalit sofistikované hrozby, což vede ke zvýšení rizika.
- Nedostatečná škálovatelnost a přizpůsobivost potřebám podniku.
- Četné případy výpadků.
- Nedostatek funkcí pro integraci s jinými bezpečnostními nástroji.

Řešení SIEM nové generace jsou založena na analýze a umožňují organizacím monitorovat hrozby a reagovat na ně v reálném čase. Tato řešení SIEM se spoléhají na informace o hrozbách (TI), které umožňují pochopit rizika, jimž organizace čelí. Moderní řešení SIEM odstraňují omezení spočívající v nasazení řešení SIEM přímo v infrastruktuře zákazníka. Místo toho je lze nasadit v cloudové infrastruktuře nebo v hybridním prostředí. Řešení SIEM nové generace také přesahují rámec prosté korelace dat a nyní zahrnují specializované nástroje, které jsou schopny řešit hrozby prostřednictvím samotné platformy.