Logsign

Kritéria výběru SIEM

Obsah

Kritéria hodnocení

Škálovatelnost a architektura pro velká data

S růstem organizace narůstá i počet logovacích dat, nebo-li logů. Zatímco mnoho organizací plánuje rozšíření infrastruktury s dostatečným předstihem před novými požadavky uživatelů, stejně nemohou 100% předvídat, jaké množství logů bude jejich podniková síť v budoucnu generovat. Moderní řešení SIEM postavené na architektuře velkých dat může růst spolu s organizací ve všech možných směrech, podle počtu zařízení, zdrojů logů, velikosti dat, výpočetního výkonu a efektivity, a pomáhá tak zajistit budoucnost organizace.

Agregace dat

Řešení SIEM by mělo být schopno zpracovávat logy ze všech podnikových systémů, včetně bezpečnostních zařízení, firewallů, VPN, IPS/IDS, e-mailových serverů, FTP serverů, bran a antivirových/anti-malwarových produktů. Pokud nástroj SIEM není kompatibilní se stávajícím nastavením infrastruktury, neměl by být součástí vaší bezpečnostní strategie.

Nativní podpora by měla zahrnovat minimálně logy operačního systému, logy připojení k databázi, systémové logy a logy cloudových služeb. Některá řešení SIEM nové generace mohou umožnit bezpečnostním týmům vyvinout ruční kód pro zpracování logů z unikátního zdroje.

Korelace a upozornění (alerty)

Starší řešení SIEM identifikují většinu bezpečnostních událostí z různých zařízení, ale mají minimální nebo zanedbatelnou schopnost určit mezi nimi korelaci. Moderní řešení SIEM využívají korelaci, aby poskytla širší kontext a pomohla bezpečnostnímu týmu zaměřit se na vysoce riziková upozornění, která mohou mít významný dopad. Tato řešení SIEM jsou vybavena vestavěnými korelačními pravidly pro identifikaci hrozby, zranitelnosti nebo probíhajícího bezpečnostního incident. Pro každou korelaci je určují posloupnost událostí, jež indikují anomálii nebo odchylku od očekávaného chování sítě. Při výběru řešení SIEM bychom tedy měli hledat takového dodavatele, jehož tým se skládá z bezpečnostních expertů s rozsáhlými znalostmi a zkušenostmi v dané oblasti.

Analýza zabezpečení

Bezpečnostní analytika pomáhá bezpečnostním týmům provádět proaktivní pokročilé vyšetřování, místo aby se omezovaly na čekání, až korelační pravidla spustí alert. Ručně definovaná korelační pravidla vyžadují specializovaný tým, který by prováděl průběžné úpravy a aktualizace, což není vzhledem k rychlému vývoji hrozeb reálné. Analýza zabezpečení využívá algoritmy strojového učení, které pomáhají řešení SIEM identifikovat vzory útoků a nové hrozby bez předchozích signatur, pravidel nebo vzorů. Aby techniky strojového učení mohly pracovat efektivně, potřebují k analýze obrovské množství testovacích dat v omezeném čase, takže je pro tyto účely nezbytná architektura velkých dat, která napomáhá zpracování a urychluje předávání poznatků a opatření bezpečnostnímu týmu.

Analýza chování uživatelů a sítě

Řešení SIEM poskytuje bezpečnostnímu týmu komplexní přehled o činnosti uživatelů spolu s kontextovými údaji a vytváří upozornění na známé hrozby a změny chování. Řešení SIEM nové generace také poskytují přehled o hrozbách pro uživatele a sítě, které by často zůstaly nepovšimnuty. Analýza chování je podporována technologiemi umělé inteligence (AI) a strojového učení (ML), které zkracují průměrnou dobu detekce (MTTD) a průměrnou dobu reakce (MTTR).

Pokročilá detekce hrozeb

Moderní řešení SIEM by se mělo umět přizpůsobit neustále se vyvíjejícímu prostředí hrozeb. Této schopnosti je dosaženo kombinací analýzy chování, monitorování sítě, detekce koncových bodů a informačních kanálů o hrozbách. Pokročilá detekce hrozeb však nespočívá pouze v odhalení hrozby.
Měla by také poskytovat informace, jako je rozsah hrozby, pohyb v síti a možnosti řešení hrozby.

Starší systémy SIEM mají zabudované statické vyhledávací dotazy, které vedou k vysokému počtu falešných pozitivních výsledků. V důsledku toho bezpečnostní týmy často neodhalí hrozby. Naproti tomu řešení SIEM nové generace umožňují bezpečnostnímu týmu spouštět vlastní vyhledávací dotazy pro detekci hrozeb a indikátorů ohrožení (IOC) a přizpůsobovat alerty konkrétním obchodním požadavkům.

Zpravodajství o hrozbách (Threat Intelligence)

Mnohé služby zpravodajství o hrozbách poskytují informace o taktikách, technikách a postupech (TTP), indikátorech kompromitace IOC a další kontextové informace o hrozbách a bezpečnostních incidentech a nyní tyto informace využívá i nová generace SIEM ke zlepšení detekce.

Pokud například počítačový systém komunikuje s externí IP adresou, může řešení SIEM nové generace rychle zjistit, zda je cílová IP adresa dříve známým C&C serverem používaným pro škodlivé aktivity. Moderní SIEM shromažďuje relevantní data o incidentech z různých zdrojů, aby pomohl bezpečnostnímu týmu analyzovat dopad bezpečnostního incidentu, a kombinací příchozích logů se zpravodajskými informacemi o hrozbách může zkrátit dobu detekce.

Vyhledávání a forenzní vyšetřování

Tradiční řešení SIEM shromažďují pouze omezené množství logů a mají omezené možnosti vyhledávání, které pak omezují bezpečnostní tým. Moderní řešení SIEM umožňují týmu vytvářet vlastní vyhledávací dotazy a umožňují bezpečnostnímu týmu prozkoumat logy a zjistit další podrobnosti související s bezpečnostním incidentem.

Některá řešení SIEM mohou bezpečnostnímu týmu pomoci tím, že zobrazí vizuální časovou osu vývoje situace pro konkrétní incident.

Dodržování předpisů

Řešení SIEM jsou velmi zdatná při plnění povinností týkajících se dodržování předpisů a řešení SIEM nové generace jsou ještě o krok dál, protože nabízejí vysoce přizpůsobitelné reporty. Ty lze klasifikovat pomocí různých kategorií specifických pro oborové předpisy a normy.

Pokud řešení SIEM neobsahuje vestavěné reporty pro daný předpis nebo normu, lze je přizpůsobit pomocí přizpůsobitelných reportů.

SOC Automatizace

Řešení SIEM se stává základem bezpečnostního operačního centra (SOC). Řešení SIEM nové generace automatizují procesy SOC a umožňují bezpečnostnímu týmu soustředit se na kritická a vysoce riziková upozornění. Generování alertů a vytváření tiketů, shromažďování kontextových údajů pro alerty, poskytování informací pro zmírnění a vytváření zpráv o zmírňujících opatřeních jsou některé z procesů, které by měl moderní SIEM automatizovat. U alertů s nízkým rizikem by navíc bezpečnostní tým měl mít možnost definovat pravidla pro zmírnění, aby se akce na omezení rizik prováděly automaticky.

Dashboardy a reporty

Ovládací panely SIEM pomáhají vizualizovat stav zabezpečení organizace. Řešení SIEM může být vybaveno řadou dashboardů pro různé účely, které by měly být přizpůsobitelné. Pokud jde o reporty, sada vestavěných reportů pomáhá při počátečním nastavení a provozu řešení SIEM, ale s rozšiřováním obchodních operací a změnou bezpečnostních požadavků by organizace měla mít možnost přizpůsobit i tyto reporty. Před výběrem řešení SIEM by měla organizace prozkoumat nabízené možnosti přizpůsobení, protože ty mohou pomoci výrazně zefektivnit každodenní provoz.

Automatizovaná odezva

Ruční reakce na alerty s nízkým rizikem mohou být časově náročné a zvyšují pravděpodobnost únavy a frustrace, v důsledku čehož může bezpečnostní tým přehlédnout i kritický alert. Řešení SIEM nové generace umožňují bezpečnostním týmům definovat automatické reakce na běžně detekované alerty. Například pokud se uživatel nemohl přihlásit ani po 10 pokusech provedených během 10 minut, může dojít k zablokování uživatelského účtu a vydání upozornění bezpečnostnímu týmu, který následně rozhodne, zda má blokování pokračovat.

Retence dat

Řešení SIEM nové generace vyžadují rozsáhlé datové zdroje pro základní algoritmus strojového učení. Řešení SIEM by mělo být schopno ukládat historická data v průběhu času, aniž by to ovlivnilo jeho integritu nebo možnosti zpracování dat. Historická data pomáhají platformám SIEM správně předpovídat, minimalizují počet falešně pozitivních alertů a pomáhají bezpečnostním týmům rychleji a efektivněji vystopovat zdroj narušení. Některé jurisdikce mohou také vyžadovat, aby organizace uchovávala své informace související s bezpečností po určitou d o b u .

Odolnost vůči poruchám

Odolnost proti poruchám označuje schopnost systému pokračovat v činnosti i v případě, že dojde k poruše jedné nebo více jeho dílčích součástí. Moderní systémy SIEM musí být odolné vůči poruchám, aby bylo zajištěno, že v celé architektuře backendu neexistuje jediný bod selhání (SPOF), a aby byla zajištěna kontinuita provozu a vysoká dostupnost.

Před výběrem řešení SIEM by se měl bezpečnostní tým snažit porozumět základní architektuře dodavatele SIEM.