Logsign

K čemu slouží SIEM?

Obsah

1. Úvod

1.1 Co je to SIEM?

Moderní hrozby se neustále vyvíjejí, pokud jde o jejich složitost a sofistikovanost. Bezpečnostní tým neví, čemu bude čelit příště. S rostoucím počtem koncových zařízení a rostoucí závislostí na cloudových službách, se rozšiřuje plocha potenciálního útoku. Kombinace všech těchto faktorů ztěžuje bezpečnostním týmům sledování událostí v podnikové síti.

Organizace instalují řadu bezpečnostních zařízení a softwaru, aby odhalily neobvyklé chování a identifikovaly bezpečnostní incidenty. Ty však pracují izolovaně, takže jsou při odhalování pokročilých hrozeb neúčinné. Útočníci využívají arzenál nástrojů k plánování a provedení útoku i pokročilé techniky , které jim pomáhají vyhnout se detekci. Navíc se stále častěji objevuje tendence útočníků provádět distribuované útoky na více systémů namísto toho, aby se zaměřili na konkrétní systém.

Zde přichází ke slovu systém správy bezpečnostních informací a událostí (SIEM), který pomáhá bezpečnostnímu týmu shromažďovat a analyzovat logovací data, nebo-li logy, v reálném čase. Společnost Gartner uvádí všeobecně uznávanou definici systému SIEM jako “technologii, která poskytuje detekci hrozeb, dodržování předpisů a řízení bezpečnostních incidentů prostřednictvím sběru a analýzy (v reálném čase i v minulosti) bezpečnostních událostí, jakož i široké škály dalších zdrojů událostí a kontextových dat”.

1.2 Jak funguje systém SIEM?

Řešení SIEM shromažďuje logy a události z různých součástí podnikové sítě. Po normalizaci dat využívá informace o hrozbách, vestavěná pravidla a pokročilé analytické funkce k odhalování bezpečnostních incidentů v reálném čase. Jinými slovy, SIEM nabízí ucelený pohled na informační bezpečnost organizace z jednoho pohledu. V závislosti na své architektuře rozděluje upozornění, nebo-li alerty, do různých kategorií, jako je malware, neúspěšná přihlášení, úspěšná přihlášení a další potenciálně škodlivé aktivity.

Kombinuje dvě technologie: Správa bezpečnostních informací (SIM) a Správa bezpečnostních událostí (SEM). V moderních řešeních SIEM je obtížné tyto dvě složky oddělit. SIM se primárně stará o sběr logů ze všech dotupných zdrojů a generuje požadované reporty, zatímco SEM provádí monitorování podnikových systémů v reálném čase za účelem detekce hrozeb a korelace událostí.

Když řešení SIEM identifikuje potenciální hrozbu, generuje alerty, které informují bezpečnostní tým. Na základě předem definovaných pravidel může mít upozornění, nebo-li alert, nízkou, střední nebo vysokou prioritu. Pokud například uživatelský účet uživatele X vygeneruje deset pokusů o přihlášení během pěti minut, lze to považovat za podezřelou aktivitu. Nejpravděpodobnějším vysvětlením však je, že uživatel X zapomněl své heslo a nemůže se přihlásit. Předpokládejme, že stejný uživatelský účet zaznamená za stejnou dobu 200 pokusů o přihlášení. V takovém případě řešení SIEM označí tento případ jako incident s vysokou závažností, protože se s největší pravděpodobností jedná o útok hrubou silou , tzv. bruteforce.

1.3 Proč potřebujete SIEM?

Moderní řešení SIEM poskytují robustní metodu detekce hrozeb, generování zpráv a dlouhodobé analýzy bezpečnostních logů. Škálovatelná řešení SIEM rostou s obchodními požadavky organizace a přinášejí maximální m o ž n o u návratnost investic (ROI). Řešení SIEM podporuje bezpečnostní tým v rychlejší reakci n a potenciální bezpečnostní incident i tím, že automatizuje zdlouhavou práci s ruční analýzou logů z různých zdrojů. Bezpečnostní tým se tak může zaměřit na alerty s vysokým rizikem a významným dopadem. Například jediné upozornění vygenerované antivirovým řešením nemusí vzbudit dostatečnou pozornost. Pokud však firewall organizace detekuje neobvyklý provoz ve stejnou dobu jako upozornění antivirového řešení, může to svědčit o probíhajícím bezpečnostním incidentu. Tuto korelaci umožňuje právě SIEM.

Mezi výhody řešení SIEM patří:

- → Zvýšení efektivity bezpečnostního týmu a smysluplné využití času.
- → Zabraňuje tomu, aby se potenciální bezpečnostní hrozby staly rozsáhlými bezpečnostními incidenty.
- → Snižuje celkové výdaje na zabezpečení.
- → Poskytuje lepší systém pro podávání zpráv, analýzu logů a uchovávání dat.
- → Minimalizuje dopad narušení bezpečnosti.

2. Případy použití SIEM

Řešení pro správu bezpečnostních informací a událostí (SIEM) shromažďují data ve formě událostí a logů z celé podnikové sítě.

Pomáhají bezpečnostnímu týmu odhalovat bezpečnostní incidenty a reagovat na ně a zároveň generovat zprávy o nich často i v podobě hlášení k prokázání shody (Compliance), což z řešení SIEM činí důležitou součást podnikové bezpečnostní strategie.

Následující podkapitoly se zabývají běžnými případy použití SIEM, od tradičních až po pokročilé funkce.

Novodobé hrozby se neustále vyvíjejí, co se týče složitosti a sofistikovanosti. Bezpečnostní tým neví, čemu bude čelit příště. S rostoucím počtem koncových zařízení a rostoucí závislostí na cloudových službách se rozšiřuje potenciální plocha pro útoky. S ohledem na všechny tyto faktory je pro bezpečnostní týmy obtížné sledovat události, které se odehrávají v podnikové síti.

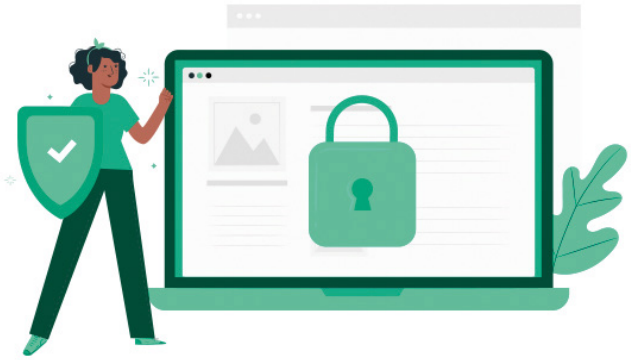
2.1 Exfiltrace dat

Exfiltrací dat se rozumí neoprávněný přenos dat, a to buď manuálně uživatelem nebo útočníkem, nebo automaticky pomocí malwaru. Jde o manuální přenos, kdy uživatel přenáší organizační data na fyzické zařízení nebo přes internet. Naproti tomu o automatický přenos se jedná v případě, kdy je počítačový systém infikován malwarem. Bez ohledu na velikost organizace představuje exfiltrace dat závažný problém.

SIEM disponují pokročilými Řešení SIEM odhaluje události exfiltrace dat pomocí pečlivého sledování síťového provozu, aby identifikovalo přenos dat ve velkých objemech, a může monitorovat logy e-mailových serverů, aby identifikovalo e-maily odeslané nedůvěryhodným příjemcům. Může generovat alert, pokud se příjemce jeví jako škodlivý nebo neznámý. Vzhledem k tomu, že řešení SIEM provádějí korelaci dat z více systémů, mohou také odhalit boční pohyb a nechtěné zvýšení oprávnění.

2.2 Útoky nultého dne

Přestože výrobci pravidelně vydávají záplaty a aktualizace svých produktů a služeb, často existují zranitelnosti, které nejsou veřejně známé. Když útočníci zneužijí tuto konkrétní podmnožinu zranitelností, označuje se to jako útok nultého dne. Tradiční bezpečnostní nástroje, jako je zařízení IDS/IPS nebo antivirový/antimalwarový software, obvykle nedokážou takové útoky odhalit, protože jejich signatury ještě nebyly zaznamenány. Pomocí monitorování IT infrastruktury organizace v reálném čase může řešení SIEM upozornit bezpečnostní tým, jakmile zjistí neobvyklé chování. Útok nultého dne může být zaměřen prakticky na jakýkoli zdroj dat, ale řešení možnostmi vyšetřování, které umožňuje bezpečnostnímu týmu vyhledávat konkrétní datové body nebo pomocí analýzy dat identifikovat vzorce útoku nultého dne.



2.3 Vzdálený přístup z podezřelého místa

Vzdálený přístup se stal pro organizace během pandemie a po ní klíčovým. Obchodní jednotky organizace a umístění zaměstnanců v konkrétních zemích by měly odpovídat přihlášením přes VPN, ale útočníci z jiných regionů se mohou pokusit přihlásit i z jiných vzdálených míst.

Řešení SIEM jsou vybavena vestavěnými korelačními pravidly pro detekci anomálií týkajících se vzdáleného přístupu. Pomocí databáze IP adres přiřazených k zeměpisným lokalitám poskytuje řešení SIEM kontextové informace o poloze až na úroveň města. Dále díky sledování přihlašovacích údajů do podnikové sítě rychle generuje alerty pro bezpečnostní tým, když zjistí vzdálený přístup z podezřelé lokality nebo souběžná přihlášení do VPN. Některá řešení SIEM mohou umožnit vedení bílé nebo černé listiny zemí pro určení přístupu do podnikové sítě.

2.4 Zvýšení oprávnění

Když útočníci proniknou do podnikové sítě, pokusí se provést zvýšení oprávnění, aby zvýšili úroveň oprávnění spojenou s napadeným účtem. Ideálním cílem je provést vertikální eskalaci oprávnění pro získání systémových oprávnění na úrovni správce. (Horizontální eskalace oprávnění umožňuje útočníkům získat přístup pouze k ostatním uživatelským účtům na stejné úrovni přístupu.) Moderní řešení SIEM využívají analýzu chování uživatelů a entit (UEBA) k určení základní linie normálního chování, aby řešení SIEM mohlo snadno odhalit takové abnormální chování.

2.5 Útoky hrubou silou (brute-force)

Útoky hrubou silou jsou známé již od přelomu století a k prolomení hesla se používá jednoduchá metoda pokusomyl. Útočník k úspěšnému uhodnutí hesla používá k o m b i n a c i abeced, číslic a speciálních znaků a může také využít slovníková slova a běžně používaná slova pro zvýšení úspěšnosti. Úspěšný útok hrubou silou vede k tomu, že ú t o č n í k získá přístup k uživatelským přihlašovacím údajům, které může použít ke krádeži citlivých informací, jako je duševní vlastnictví, obchodní tajemství a osobní údaje. Mnoho řešení SIEM je vybaveno vestavěnými pravidly, která vytvářejí upozornění na podezřelé zdrojové IP adresy, které překročí práh odmítnutých/neplatných pokusů o přihlášení.v daném čase. Pokročilá pravidla SIEM mohou zahrnovat identifikaci neúspěšných pokusů o přihlášení v daném časovém období a blokování kompromitovaných účtů.

2.6 Útoky v prostředí PowerShell

Tradiční útoky malwaru zahrnují spuštění škodlivého kódu v cílovém systému, ale útoky malwaru bez souborů využívají vestavěné nástroje systému Windows, například PowerShell. Vzhledem k tomu, že útok zahrnuje legitimní programy, může být náročné jej odhalit a zakázání prostředí PowerShell není řešením. Pro organizace má tato situace dalekosáhlé důsledky v podobě rozsáhlého šíření sad pro zneužití.

Řešení SIEM dokáže analyzovat příchozí logy a odhalit škodlivou aktivitu, přičemž v případě útoků prostřednictvím prostředí PowerShell platforma vyhledává v logovacích datech pocházejících z e systémů Windows specifická ID událostí a jejich charakteristiky. Například, při detekci bočního pohybu bude řešení SIEM hledat vzdálenou správu systému Windows (WinRM) spolu s příkazem PowerShell Enter-PSSession.

2.7 Boční Pohyb

Poté, co útočník získá počáteční přístup do podnikové sítě, bude se snažit dostat hlouběji do jejího nitra, aby získal přístup k citlivým datům a kritickým prostředkům. Počáteční narušení může být výsledkem infekce malwarem nebo phishingového útoku, po kterém se útočník může vydávat za skutečného uživatele, aby nebyl odhalen. Boční pohyb se obecně vyskytuje u pokročilých kybernetických útoků, kdy je cílem útočníka způsobit co největší škody. Krádež pověření, zvýšení oprávnění a získání přístupu k citlivým informacím jsou klasické indikátory bočního pohybu.

Na rozdíl od tradičních bodových řešení, která pracují izolovaně, mají řešení SIEM komplexní přehled o událostech v celé podnikové síti. Díky logům přicházejícím z různých systémů a zařízení může snadno odhalit techniky používané při bočním pohybu pomocí monitorování v reálném čase a analýzy chování, které poskytují kontextuální důkazy.

2.8 Hrozby ze strany zasvěcených osob

Hrozby zevnitř jsou jednou z hlavních příčin narušení bezpečnosti, protože obvykle zůstávají nepovšimnuty. Hrozby zevnitř se neomezují pouze na krádež dat zaměstnancem. Může k nim dojít i neúmyslně, například ztrátou notebooku nebo úložné jednotky nebo odesláním emailu na nesprávnou poštovní adresu.

Řešení SIEM mají více mechanismů pro odhalování vnitřních hrozeb. Řešení SIEM odhaluje abnormální chování uživatelů analýzou doby přihlášení, frekvence přihlašování a běžně používaných zdrojů a využívá kanály pro sledování hrozeb (TI) v korelaci se síťovým provozem, aby bylo možné určit, kde se používá řídicí a kontrolní centrum. Mezi další příznaky, které vyvolávají alerty, patří neočekávané šifrování dat, přesun velkého množství dat z jednoho zdroje do druhého a boční pohyb.

2.9 Detekce malwaru

Malware označuje jakýkoli škodlivý program, který má za cíl poškodit systém nebo získat neoprávněný přístup, takže jde o jakýsi souhrnný pojem, který zahrnuje viry, trojské koně, červy, spyware, ransomware a adware. V průběhu let způsobilo mnoho významných rodin malwaru a jejich variant značné škody podnikům po celém světě, například Stuxnet a WannaCry.

Malware se obvykle šíří prostřednictvím stažených souborů, příloh e-mailů a webových stránek s freewarem. Moderní řešení SIEM provádějí nepřetržité monitorování podnikových systémů za účelem odhalení škodlivých souborů se známými hashi. Při odhalování malwaru se spoléhají na historická data a zdroje informací o hrozbách. Řešení SIEM nové generace využívají techniky založené na signaturách a vzorcích útoků a dovedou také vytvářet hypotézy na základě analýzy chování pro vyšetřování.

2.10 Neoprávněný přístup ke sdíleným složkám

V tradičním nastavení vytváří sdílený souborový systém síťové úložiště a umožňuje přístup k úložišti více počítačovým systémům. Systém hierarchických práv organizace může určovat rozsah přístupu uděleného jednotlivcům. V dnešní době se ke sdílení úložného prostoru stále častěji využívají cloudové služby.

Řešení SIEM shromažďují autentizační záznamy z různých systémů a služeb a odhalují tak případy převzetí účtu. Řešení SIEM nové generace jdou ještě o krok dále a využívají korelační pravidla a analýzu chování k identifikaci anomálních aktivit a odhalení neoprávněného přístupu ke sdíleným složkám.

2.11 Nadměrné aktivity na webu

Každý den se přes síť odesílá množství požadavků a odpovědí - požadavky na připojení k databázi, přístupy na webové stránky, stahování souborů, data pro videokonference atd. S rostoucí velikostí sítě roste i počet požadavků a odpovědí.

Řešení SIEM snižuje zátěž bezpečnostního týmu tím, že filtruje nepotřebné síťové události. Pomocí vestavěných korelačních pravidel a informací o hrozbách generuje SIEM nové generace upozornění na indikátory, jako je nadměrné množství databázových připojení, připojení k bráně firewall z jednoho zdroje a nadměrné množství odchozích připojení. Alerty jsou doprovázeny kontextovými informacemi, což umožňuje bezpečnostnímu týmu rychle se rozhodnout a přijmout opatření.