Logsign

FREEDIVISION

Přehled funkcionalit systému Logsign

1. Obecné vlastnosti systému

Systém

- umožňuje shromažďování bezpečnostních údajů a jejich další analýzu,
- umožňuje detekci incidentů, poloautomatickou a automatickou reakci,
- slouží k hlídání souladu s příslušnými předpisy,
- je schopen obohacovat data o zpravodajské informace o hrozbách,
- umožňuje připojení neomezeného počtu zdrojů a uživatelů,
- není omezen počtem zpracovaných událostí za vteřinu (EPS),
- poskytuje možnosti reportingu - podávání zpráv,
- umožňuje používání funkcionalit a správu v jedné konzoli (na jedné obrazovce),
- poskytuje pokročilé funkce obohacování dat, reportování, analýzy, alarmu, správy událostí, detekce hrozeb, korelace, zpravodajství o hrozbách a reakce na incidenty,
- podporuje šifrovaný provoz pro správu,
- umožňuje správu prostřednictvím webového rozhraní,
- poskytuje integrovanou vzdálenou podporu výrobce.

2. Funkce pro sbírání dat

Systém

- je schopen shromažďovat data z více různých segmentů sítě současně a kombinovat je v jednom centrálním prostředí,
- podporuje sběr dat pomocí protokolů SYSLOG, SSH, SMB, API, FLOW, SFTP, WMI,
- umožňuje sbírat data přímo z tabulek v databázích Microsoft SQL, ORACLE, MY SQL, PostgreSQL, MangoDB a HanaDB,
- podporuje sběr logů z MS Windows prostředí pomocí NXLog agenta,
- je schopen shromažďovat data zapsaná databázemi Microsoft SQL a ORACLE do datové architektury operačních systémů Windows a Linux a textových prostředí,
- umožňuje integrace s aplikacemi, jako je Office 365, Microsoft Azure, a shromažďování dat prostřednictvím rozhraní API,
- umožňuje poskytovat vhodný rámec pro budoucí rozšíření a integraci s dalšími řešeními třetích stran a zařízeními internetu věcí,
- umožňuje vést záznamy o důležitých pracích a provedených změnách s možností zadávání dotazů a podávání zpráv týkajících se těchto prací/změn,
- umožňuje zahrnout a vyloučit určitá pole ze shromážděných nezpracovaných údajů,
- umožňuje provádět sběr dat s agentem nebo bez něj a také má možnost používat agenty třetích stran s globální platností,
- vede během procesu sběru dat odděleně zaznamenávané vytvořené údaje, čas jejich přijetí a čas jejich vytvoření,
- umožňuje provádět procesy dotazování a vykazování také podle času vytvoření dat,
- poskytuje tzv. vývojovou obrazovku “Vlastní zásuvný modul”, která v případě potřeby umožní uživateli vyvíjet nové zásuvné moduly ve formátech “CEF”, “Key-value” a “JSON”,
- je schopen shromážděná data vždy použít pro účely vizualizace,
- umožňuje použít všechny sloupce shromážděných dat v ovládacích panelech bez jakéhokoli omezení,
- je začleněn do systému “Geo Location”, který dokáže zobrazovat informace o zemi / poloze na základě IP v internetových datových záznamech, neustále tyto informace aktualizovat a zobrazovat je ve svých zprávách,
- je schopnost automaticky obohatit data shromážděná ze zdrojů spolu s hodnotami atributů Microsoft pomocí funkce ověřování LDAP,
- je schopen obohatit data z různých zdrojů pomocí funkce modifikátoru,
- je schopen obohatit údaje shromážděné ze zdrojů o údaje z globálních a místních zpravodajských služeb o kybernetických hrozbách,
- je schopen určit specifickou politiku správy dat pro každý integrovaný zdroj protokolů,
- podporuje filtrování, slučování a mapování stejných údajů během sběru dat.

3. Funkce pro analýzu dat

Systém

- umožňuje vyhledávat všechny sloupce patřící do všech datových formátů, které jsou v něm definovány pro aktuální data,
- umožňuje dotazovat se na data podle požadovaných parametrů,
- umožňuje provedené dotazy zaznamenat pro pozdější použití,
- podporuje pokročilý vyhledávací jazyk, který dokáže vyhledávat v aktuálních datech tak, že lze pro všechny názvy sloupců nebo hodnoty použít AND , OR , NOT , TO atd.,
- umožňuje vyhledávat pomocí logických kritérií, jako je seskupování v rámci určitých hodnot, udávání rozsahů v číselných hodnotách, rozsahů v hodnotách IP a používání parametrů,
- podporuje fulltextové vyhledávání, aby bylo umožněno vyhledávání nezávislé na sloupci a podrobné filtrování určitého slova,
- poskytuje předem nadefinovaná kritéria vyhledávání (tzv. Mini Queries),
- umožňuje dostupnost vyhledávacích kritérií také z modulů sestav a ovládacích panelů,
- je schopen provádět analýzu jednoho a více sloupců v rámci výsledků odpovídajících kritériím vyhledávání,
- je schopen vyfiltrovat 10 nejvyšších hodnot jako výsledek analýzy,
- umožňuje vyhledávat pomocí jednoduchých filtrů bez použití vyhledávacího jazyka,
- podporuje funkce vnitřního vyhledávání pro hlubší vyhledávání výsledků (Drill Down),
- podporuje automatické analýzy časového rozložení dat,
- je schopen navigovat uživatelské kroky při filtrování výsledků v rámci procesu vytváření analýzy,
- umožňuje převedení vyhledávacích kritérií do zobrazených sestav a ovládacích panelů (dashboard) pomocí průvodce procesy,
- umožňuje zkoumat raw data mezi podrobnými informacemi o datech.

4. Funkce pro detekci událostí

Systém

- umožňuje korelace záznamů o datech na základě shromážděných údajů,
- umožňuje zpracování záznamů o datech v souladu s pravidly stanovenými administrátorem, pokud jsou záznamy pořízené z různých zdrojů dat za určitou dobu,
- umožňuje zobrazení záznamů o datech na obrazovce správce a odeslání e-mailu/SMS v případě potřeby,
- je schopen automaticky analyzovat množství EPS a v případě nárůstu nebo poklesu anomálie ve stanovené míře informovat správce prostřednictvím SMS, e-mailu, Teams atd.
- poskytuje knihovnu hotových korelačních pravidel vhodných pro více než 500 parametrů MITRE ATT&CK a Cyber Kill Chain,
- umožňuje dopsat individuální korelační pravidla přímo v rámci konzole,
- podporuje neomezené množství přiřazovaných údajů,
- umožňuje údaje přiřadit k (N) různým úrovním dat z různých zdrojů a/nebo jejich struktur,
- podporuje automatické bodové hodnocení rizik pro alarmy, které se vyskytnou podle hodnot priority a spolehlivosti,
- podporuje manuální sledování analýzy dlouhodobých trendů prostřednictvím seznamů chování,
- podporuje proaktivní vyšetřování a vyhledávání hrozeb,
- je schopen analyzovat trendy a vypočítávat hodnoty výskytu požadovaných typů událostí v definovaných časových intervalech,
- je schopen generovat zvláštní alarm, pokud se nad těmito hodnotami vyskytne definovatelná hodnota odchylky, a to tak, že vezme průměr příslušných hodnot za definované období,
- umožňuje vytvoření libovolného počtu definic pro konektory,
- umožňuje označit techniky MITRE ATT&CK v individuálně vytvořených korelačních pravidlech,
- umožňuje definovat časový rámec události pro alerting, to znamená, ve kterých dnech a hodinách má být posílán alarm písemnou formou,
- podporuje pozastavení spuštěného alarmu na určitou dobu,

- umožňuje ztišení spuštěného alarmu na určitou dobu,
- je schopen generovat nový odlišný alarm na základě alespoň dvou odlišných výsledků korelace,
- umožňuje využít průvodce přípravou alarmu pro snadnou přípravu alarmu,
- umožňuje provést definici alarmu v závislosti na obsahu dat,
- umožňuje definovat alarm v závislosti na obsahu více než jedné informace v datech,
- umožňuje definovat pravidla při tvorbě alarmových pravidel v závislosti na výrazech jako “obsahuje, neobsahuje, je větší než, je menší než, začíná s, končí s”,
- umožňuje generovat alarmy z důvodu častého opakování určitých údajů,
- umožnuje odstupňovat alarmy podle jejich závažnosti,
- umožňuje nastavení různých stupňů závažnosti pro různé definice alarmu,
- uvádí u všech alarmů čas výskytu údajů, které alarm vyvolaly,
- umožňuje odeslat definované alarmy předem určeným osobám nebo skupinám jako varovnou zprávu e-mailem nebo formou SMS,
- generuje okamžitě alarm týkající se nedostupného softwaru nebo hardwaru, pokud dojde ke ztrátě přístupu k softwaru nebo hardwaru shromažďujícímu data,
- umožňuje každou událost, na základě které byl alarm vygenerován, zpětně do detailu prozkoumat a podat o ní detailní hlášení,
- je schopen vygenerovat historii alarmů pro zadanou skupinu alarmů za předpokladu, že má k dispozici dříve vygenerované reporty pro údaje o alarmech,
- je schopen zobrazit informace o raw datech, které vytvářejí alarm.

5. Funkce pro zpravodajské služby a služby sdílených kybernetických hrozeb

Systém

- podporuje přijímání a vyhodnocování informací z externích vstupů - z otevřených zdrojů OSINT, komerčních zdrojů, z jednotlivých odvětví a speciálně vytvořených informací o útocích,
- umožňuje skrývat sektorová pole s údaji typu IP adresa (Internet Protocol) souvisejících s kybernetickými zpravodajskými daty, URL (Uniform Resource Locator), FQDN (Fully Qualified Domain Name), digest souboru (hash), popis, datum vytvoření, skóre spolehlivosti, kód země zdroje nebo typ útoku,
- poskytuje rozhraní, které zajistí integraci s bezpečnostními produkty používanými pro detekci a reakci. Pomocí tohoto rozhraní mohou detekční a zásahové funkce fungovat automaticky.

6. Funkce pro reakce na incidenty

Systém

- podporuje funkce automatické a poloautomatické reakce,
- podporuje operace, jako je blokování bezpečnostních zařízení (firewall, EDR, NAC, DLP atd.) a jejich umístění do karantény v důsledku alarmů,
- umožňuje zakázání/povolení uživatele, přidání/odebrání do skupiny atd. v systémech identifikace (Active Directory, LDAP),
- umožňuje zasílat oznámení prostřednictvím oznamovacích systémů (sms, e-mail, teams),
- obsahuje vestavěnou funkci správy incidentů a díky ní umožňuje přidání forenzní analýzy a poznámek k jakémukoli případu, aby se urychlilo odhalování hrozeb a reakce na ně, a dále umožňuje nahlížení dalším spolupracovníkům, jimž je přidělen přístup.
- má vestavěné obrazovky s podrobnostmi o správě incidentů s možností interaktivní spolupráce přidělených osob a ukládání důkazů o každém jejich kroku,
- umožňuje také odesílání těchto údajů do ticketovacího systému prostřednictvím integrace s externím ticketovacím systémem,
- umožňuje provést akci ve více než jednom systému v důsledku poplachu/alarmu,
- je schopen se dotazovat integrovaných zdrojů kybernetického zpravodajství (VirusTotal, XForce, AbuseIPDB…) během poloautomatické reakce na incident, a také je schopen vizualizovat a předávat uživateli vygenerované výsledky,
- je schopen zajistit, aby byly při zásahu uživatele do událostí provedeny akce prostřednictvím bezpečnostních zařízení, jako je firewall, EDR, DLP, NAC atd.
- umožňuje retrospektivní analýzy nejvyšších trendů výskytu událostí pomocí obrazovky analýzy,
- podporuje proaktivní vyhledávání a vyšetřování hrozeb,
- umožňuje využívat integrace reakce na události ve více než jednom systému v důsledku kybernetického bezpečnostního incidentu,
- podporuje více než 200 metod reakce na události od nejméně 80 různých dodavatelů, které jsou předem definovány pro reakci na události v systému,
- umožňuje podrobnou analýzu pohybů akčního objektu (IP, uživatel, URL, Hash atd.) v rámci správy aktiv v systému,
- podporuje analýzy životního cyklu incidentu, jejichž kroky jsou provedeny v souladu s řízením procesů NIST,
- má předdefinované inteligentní reakce, které umožní rychle shromáždit forenzní údaje a zahájit cílená protiopatření v rámci procesu řízení incidentu,
- je schopen vykazovat výsledky životního cyklu incidentu, včetně doby detekce a reakce, a také je schopen vypočítat průměrnou dobu detekce a průměrnou dobu reakce pro všechny detekované/reagované události,
- umožňuje kategorizovat události/upozornění na různých úrovních, například kritické, vysoké, střední a nízké,
- je schopen nahlásit zapojení indikátorů ovlivňujících událost do různých událostí na stejné obrazovce, umožnit jejich podrobnou analýzu a vytvořit řetězce hrozeb pro objekt události,
- poskytuje údaje pro vyšetřování, které bezpečnostní analytik potřebuje pro každou událost, s rozsáhlými soubory dat indikátorů s bohatým obsahem,
- obsahuje více než 50 předdefinovaných dotazů pro vyhledávání hrozeb pro případné další vyšetřování,
- je schopen vizualizovat taktiky a techniky MITRE ATT&CK viditelně na obrazovce řízení incidentu a současně je schopen zobrazit maticovou obrazovku,
- umožňuje spravovat parametry (artefakty), ke kterým se objekt akce vztahuje.

7. Funkce pro vizualizaci dat, reporting a dodržování právních předpisů

Systém

- umožňuje zobrazit na obrazovce pro správu údaje o součástech celého systému na jednom panelu nebo na různých kartách na stejné obrazovce,
- umožňuje sledovat součásti systému prostřednictvím navržené obrazovky pro správu systému (například procesor, paměť, diskový vstup/výstup, kapacita disku),
- je schopen generovat reporty ve stanovených formátech (PDF, XLS, HTML) z dat a pravidla pro tyto zprávy uchovávat pro opakované použití,
- umožňuje při vyhledávání dat zadat rozsah dat nebo určité období,
- umožňuje využít průvodce pro snadnou přípravu reportu,
- je schopen vytvářet reporty podle obecných standardů v oblasti informatiky (ISO 27001, PCI, SOX, GLBA, KVKK atd.).
- umožňuje filtrovat podle definovaných skupin sestav a na obrazovce správce zobrazit údaje pocházející ze skupiny sestav určené v sestavě. V případě potřeby lze příslušný report přenést do počítače.
- umožňuje určit, který obsah se v sestavě zobrazí a také je schopen přidávat a odebírat sloupce,
- umožňuje přidat jakýkoli sloupec v rámci datových formátů definovaných v systému jako sloupec,
- je schopen určit podle jedné nebo více oblastí kritéria hodnocení, která se mají v reportu použít,
- je schopen provádět matematické a statistické výpočty na základě aktuálních dat,
- je schopen provádět výpočty, jako jsou seskupení hodnot, součty číselných údajů, časové rozložení hodnot, počet jedinečných hodnot. Např: Výpočet šířky pásma využívané IP adresou, počet spojení, která navazuje, různé porty, které používá, a počet různých IP adres, ke kterým přistupuje,
  umožňuje upravovat frekvenci generování reportu denně nebo týdně, měsíčně, a to včetně upřesnění času.
- umožňuje uživateli určit pracovní dobu reportu,
- je schopen vytvořit speciální návrhy dashboardů kombinací požadovaných zpráv a grafických widgetů a ukládat je pro pozdější použití.

8. Funkce pro řízení přístupu na základě rolí (RBAC)

Systém

- umožňuje omezení přístupu uživatelů na základě připojeného zdroje logů,
- poskytuje správci možnost definovat oprávnění uživatelů k přístupu k jednotlivým nabídkám funkcionalit a modulům na základě uživatelských rolí,
- umožňuje využít granulární nastavení přístupu uživatele vzhledem k vymáhání principu nejnižších privilegií (PoLP),
- podporuje řízení přístupu na základě rolí (RBAC) pro uživatelské účty. Všechny moduly systému a funkce v něm musí být autorizovány na základě definování oprávnění uživatelů,
- umožňuje provádět autorizaci v systému pouze oprávněnému správci,
- umožňuje provedení autorizace a omezení přístupu k reportům, dashboardům a kategoriím alarmů podle typu integrace, na základě atributů: rozsah IP (IP range), seznam schválených IP adres (whitelist), subnetů, uživatelských rolí,
- podporuje integraci s řešením LDAP nebo lokálním Active Directory pro autorizaci přístupu,
- je schopen používat metodu dvojúrovňového ověřování (2FA) pro autorizaci přístupu,
- je schopen definovat bezpečnostní politiky přístupu (komplexita hesla, délka session, IP pro přístup do GUI atd.).

9. Funkce pro ukládání dat

Systém

- podporuje kompresní funkce tak, že shromážděná data jsou po zpracování komprimována a uložena ve formátu gz nebo bz,
- umožňuje kdykoli změnit používaný algoritmus řízení,
- uživateli automaticky zobrazí příslušný záznam bez jakéhokoli provozního zatížení v případech, kdy je třeba provést operace s komprimovanými daty,
- podporuje proces komprese dat a umožňuje nastavit úroveň kompresního poměru,
- podporuje v rámci procesu archivace označování aktiv na základě datumu,
- umožňuje na požádání ukládat zaznamenaná data do různých diskových oblastí a automaticky je z těchto různých diskových oblastí vyvolávat do systému a provádět s nimi všechny operace,
- ukládá data v souborovém systému pomocí podepsaného digitálního certifikátu spolu s časovým razítkem a informacemi o hashi,
- zajišťuje kontrolu integrity při exportu archivovaných dat pomocí podepsaných dat (signed data),
- umožňuje nastavení doby uchovávání horkých (hot/live), studených (archived) a již podepsaných dat (signed data),
- umožňuje rozhodovat, která data budou uchovávána, archivována či „dropnuta“ na základě politik,
- umožňuje přenášet uložená data prostřednictvím FTP, rsync atd. a různými způsoby je odesílat do jiného místa určení pro účely zálohování. Tato nastavení je možné provést prostřednictvím webového rozhraní.

FREEDIVISION

Provozovna a korespondenční adresa
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

www.freedivision.com
+420 220 972 426