LOGmanager

> Centrální úložiště logů
> Dostupný SIEM

SPLŇUJE POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A GDPR

Proč potřebujeme log management?

V dnešním světě, který je zcela závislý na IT, každá organizace silně spoléhá na svou IT infrastrukturu. Jak firmy rostou, narůstá také jejich infrastruktura — i malá organizace může mít síť složenou ze stovek komponent: serverů, aplikací, databází, koncových bodů, IoT zařízení atd. A každá z těchto komponent s námi dokáže mluvit prostřednictvím strojových dat, která produkuje – informuje nás o změnách konfigurace, provozních stavech, aktivitách, diagnostice a o mnohém dalším. Mít ta správná data z logů je klíčové pro mnoho důležitých úkolů, jakými jsou monitoring, diagnostika, audit, forenzní analýzy, tvorba reportů, soulad s předpisy. Každého, kdo by chtěl zpracovávat data z logů, čekají **tyto výzvy**:

- ### Porozumění údajům z logů

Není žádná norma, jak by měla strojová data vypadat. Existují tucty nejrůznějších standardů, a přesto má každý výrobce svůj vlastní přístup. A co hůř, každá aktualizace systému může přinést změnu stávajícího formátu logů. Díky tomu je ruční zpracování logů velmi obtížné. Přizpůsobit se nejrůznějším formátům a jejich neustálým změnám je nezbytné.

- ### Mazání a změny

Starší logy jsou přepisovány novými, takže když je potřebujete, už tam nemusí být. A když dojde k narušení bezpečnosti, útočníci po sobě zaručeně zahladí stopy tím, že důležitá auditní data smažou nebo pozmění.

- ### Předpisy a regulace

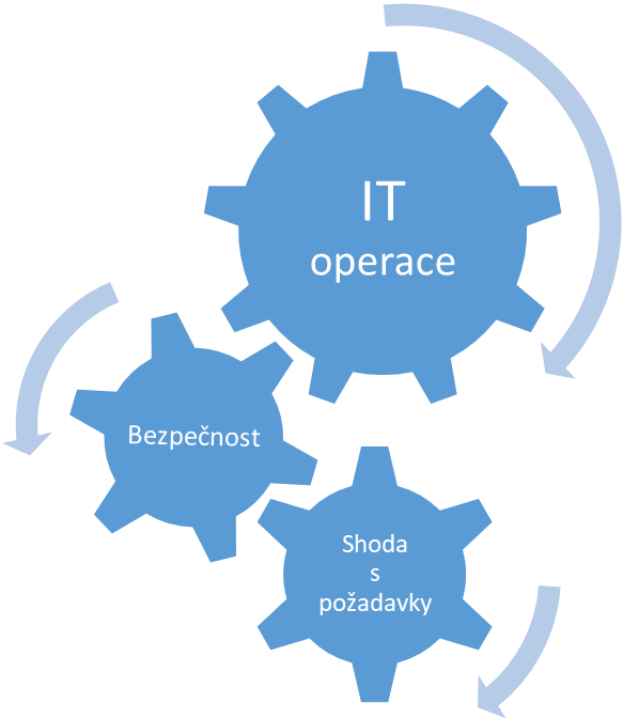
Mít vyřešený log management je klíčové pro dosažení souladu s nejrůznějšími standardy, předpisy a místně platnými zákony o kybernetické bezpečnosti.

- ### Nemožnost centrálního vyhledávání

Uchovávání logů v zařízení, které je samo produkuje, je činí obtížně dohledatelnými – což značně zpomaluje řešení IT a bezpečnostních incidentů. A jak všichni víme, čas jsou peníze.

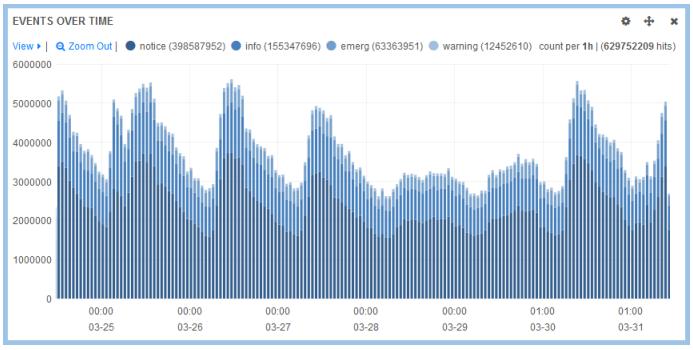
Vzhledem k výše uvedenému je jasné, že každá organizace potřebuje log management. Tradiční log managementy byly určeny speciálně pro potřeby velkých organizací. Výsledkem byl komplexní systém, který vyžaduje specializované znalosti a tým. Spolu s vysokou cenou to nutilo střední a menší společnosti používat open-source řešení. Jenže open-source řešení se většinou obtížně implementuje a udržuje, nebo mu chybí kritické funkce. Řešením je moderní log management.

Log management je pomocníkem ve všech důležitým oblastech IT.



Bez porozumění strojovým datům je v našich informacích vždy mezera. Log management je široce přijímaným řešením k zaplnění této mezery.

LOGmanager je moderní nástroj kategorie log managementu. Je určen pro organizace všech velikostí a jeho použití, údržba i implementace jsou snadné. Je vybaven všemi kritickými funkcionalitami pro správu logů. A s nejlepším poměrem ceny a užitné hodnoty na trhu díky hardwaru zahrnutému v ceně a bezlicenční politice.



I malé řešení pro správu logů si musí poradit s velkým objemem dat. Výkonný hardware a dostatečně velké úložiště jsou nutností, bez které nelze tak velké objemy dat efektivně zpracovávat.

Oblasti správy logů hodné Vaší pozornosti

IT operace

Kritický IT incident je středobodem dnešního IT světa, je nevyhnutelný stejně jako daně a smrt, protože dříve či později nastane. Nejprve, co je to kritický IT incident – je to stav, kdy je nefunkční business aplikace nebo infrastruktura na ní navázaná. Taková situace vyžaduje okamžitou reakci a IT tým organizace musí být schopen spolupracovat dle charakteru incidentu na rychlém odstranění závady. V souvislosti s tím jsou zažité dva pojmy – **MTTR a RCA** (Mean Time To Repair a Root Cause Analysis; volně přeloženo to znamená Střední doba k nápravě a Analýza příčin problému). Úkolem IT oddělení je, co nejdříve najít příčinu výpadku a odstranit ji, poté analyzovat, proč výpadek nastal včetně všech souvislostí, a určit opravné mechanizmy, aby ke stejnému nebo podobnému incidentu v budoucnu nemohlo dojít.

Sjednocení formátů a centralizace logů. Distribuce logů napříč různými systémy a zařízeními, rozdílná retence a jazyk logů mohou působit potíže. Různá zařízení mají různý přístup k managementu logů, zapisují je ve vlastním jazyce a mají různě velká lokální úložiště logů. Díky tomu mají i rozdílnou retenční dobu, po kterou jsou logy uchovávány. Když hledáte konkrétní záznam, protože potřebujete řešit provozní záležitost, musíte projít logy uložené na nejrůznějších zařízeních, pochopit, kde a jak v nich hledané informace naleznete v každém jednotlivém záznamu, a dlouze prohledávat. Zde má smysl nasadit centralizovaný systém managementu logů.

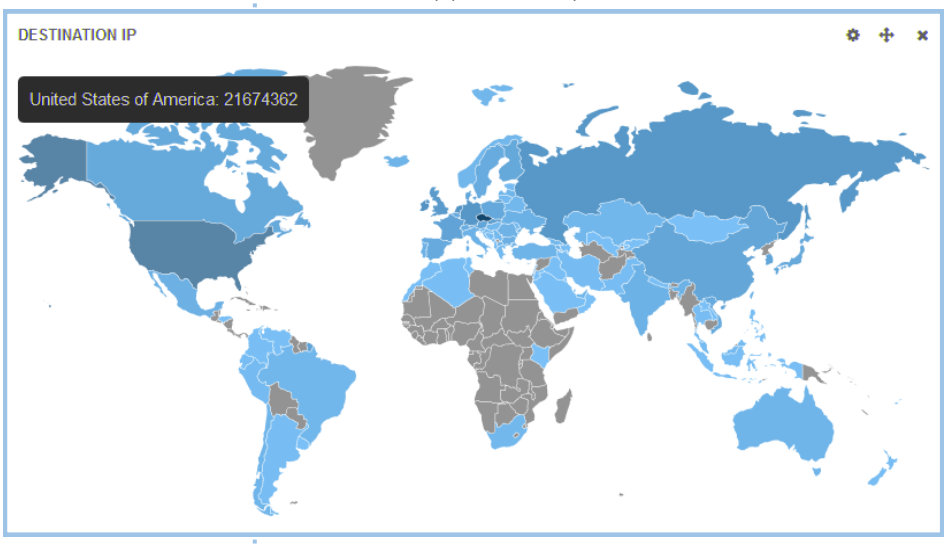
Centralizovaný systém jako je **LOGmanager** pohodlně sbírá logy ze všech zdrojů a ukládá je všechny na jedno místo. Navíc používá parsery k překladu logů do jednotného formátu, který je snadno pochopitelný a všechny údaje jsou vždy plně indexované pro rychlé prohledávání. Když pak potřebujete řešit nějakou provozní záležitost, stačí se obrátit na jediný zdroj informací – můžete si tam prohlížet logy generované infrastrukturou, bezpečnostními zařízeními, servery i aplikacemi. A to včetně těch, které se vinou IT incidentu již staly nedostupnými. Díky tomu můžete identifikovat možnou příčinu problému na jednom místě, rychle a efektivně.

Rychlá analýza dat díky centralizovaným logům. Díky centralizaci logů v nástroji na log management mohou IT operátoři rychle analyzovat informace z mnoha zdrojů, aniž by potřebovali administrátorský přístup ke všem z dotčených systémů. Logy uložené v LOGmanageru nemohou být smazány ani nijak modifikovány. Díky tomu jsou technici schopni i bez administrátorských oprávnění prohlížet logy z většiny interních provozních systémů a cloudových služeb. Analýza běžného provozu se tak stává samozřejmou součástí jejich práce a výsledky řešení provozních problémů mohou velmi rychle předávat svým nadřízeným.

Bezpečnost

V oblasti bezpečnosti je nejvýznamnější **ochrana logů před manipulací.** Dále možnost aktivně identifikovat potenciální bezpečnostní rizika, ladit konfigurace a sledovat provedené změny. Jakmile je nějaký záznam uložen v LOGmanageru, nemůže být vymazán ani jinak modifikován. Organizace, které se potýkají s bezpečnostními problémy, často zjistí, že útočník smazal všechny záznamy o škodlivé aktivitě v zařízeních a systémech, ke kterým se mu podařilo získat neoprávněný přístup. Pak může být velmi obtížné shromáždit podrobné údaje o útočníkových aktivitách a tyto údaje poskytnout pro detailní forenzní analýzu incidentu.

Nechte aktuální údaje o kybernetických hrozbách provázat s vlastními strojovými daty. Kybernetické hrozby se neustále vyvíjejí, a když o nich budete mít správné informace, může vám to usnadnit odhalení kybernetických incidentů a zahájit rychlé a cílené odpovědi. LOGmanager používá vlastní Reputační databázi vyvíjenou ve spolupráci s českým operátorem národní e-infrastruktury pro vědu, výzkum a vzdělávání - CESNET.



Proaktivní přístup

Log management vám umožní nastavit vlastní alerty, které budou detekovat určité události, jako třeba smazání kritických souborů. Moderní řešení by mělo zvládat i korelaci více událostí, což vám umožní detekovat posloupnost událostí a upozorňovat jen při dosažení definovaných prahových hodnot. Díky tomu může vaše organizace rychle reagovat na problém, jakmile nastane. LOGmanager sbírá informace o změnách implementovaných v jednotlivých systémech, což umožní snadno identifikovat, kdo změnu provedl a s jakým výsledkem. Můžete také sledovat neúspěšné pokusy o přihlášení do systémů, které obsahují citlivá data, pokusy testovat bezpečnostní pravidla v síti a tak dále.

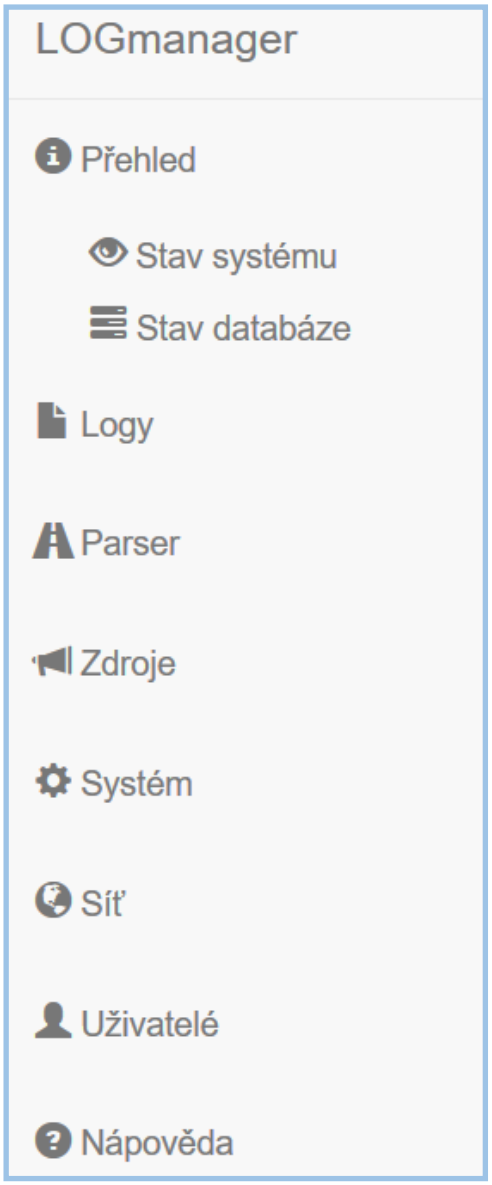
Soulad s předpisy

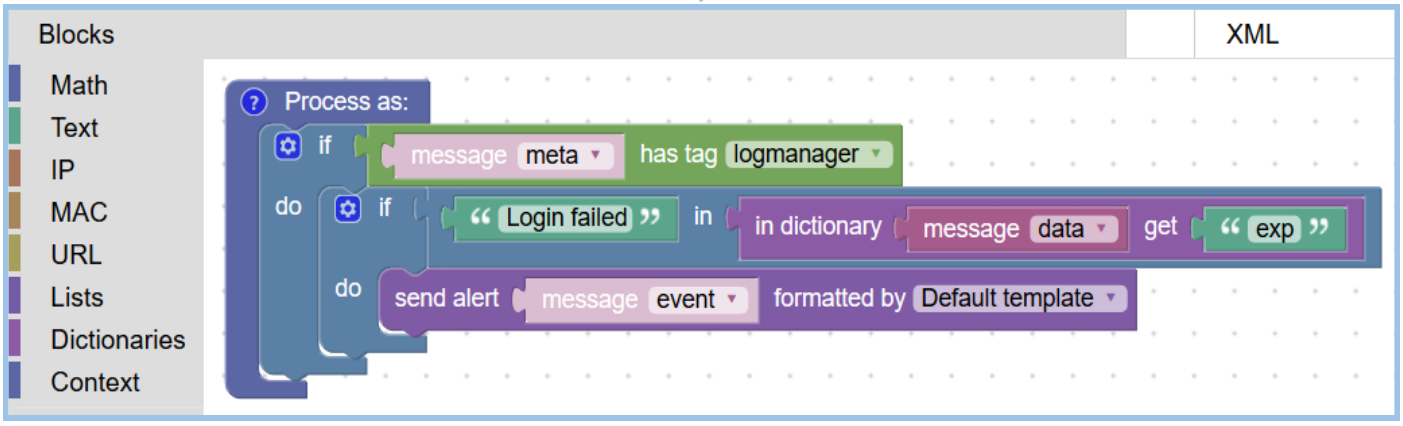
V oblasti souladu s předpisy čelíme mnohým výzvám. Organizace jsou povinny archivovat a analyzovat logy, zachytávat aktivity i dlouhodobě uchovávat logy z kritických systémů a zdrojů. **ZKB/VKB, GDPR, NIST CSF, PCI-DSS, ISO 27001:2013, NISD 2016/1148/EU, HIPPA?** Nezáleží na tom, které zákony či normy musí vaše organizace plnit; funkční log management je vždy součástí řešení.

Audity/Reporty – Když organizace provádí bezpečnostní audit, je nezbytné mít systém, který je schopen vytvářet reporty dle požadavků auditora. LOGmanager vám umožní vytvářet reporty nejen v grafické formě, ale i v PDF nebo CSV formátu, strukturované dle požadavků auditora. Můžete se vybrat kterýkoliv z logů uložených v databázi a zahrnout ho do reportu. Můžete dokonce exportovat soubory s miliony řádků, pokud potřebujete. LOGmanager navíc podporuje možnost přístupu do databáze logů přes REST-API, takže můžete zadávat strukturované dotazy přímo ze svého vlastního reportovacího nástroje.

Radikální jednoduchost

Nedostatek zdrojů dokáže zmařit i ty nejlepší projekty. Log management by neměl vyčerpat vaše interní lidské zdroje. Na log managementu jsou typicky ceněny hodnoty jako rychlá implementace, krátké zaškolení a jednoduché integrované rozhraní, které dokáže obsluhovat i operátor-junior.





Unikátní vlastností LOGmanageru je využití blokových schémat, zjednodušující operátorům bez znalosti programování život.

Často kladené otázky:

Log management nebo SIEM?

Mnozí IT specialisté prohlašují, že pro každou středně velkou společnost je SIEM nezbytností. My v LOGmanageru jsme jiného názoru. Nezapomínejte, že SIEM je zaměřen primárně na kybernetickou bezpečnost. Pokud nějaká společnost dosud nemá vlastní tým bezpečnosti IT, nebo je tento tým příliš malý, velká investice do SIEM je kontraproduktivní. Při omezených možnostech lidských zdrojů se nedostává času k učení se a obsluze komplexního SIEM produktu. Ten pak dříve či později končí nevyužit. Moderní log management dokáže nahradit řadu SIEM funkcionalit za cenu mnohem nižších nákladů i úsilí. Počínaje dynamickými dashboardy, připravenými a nastavitelnými alerty a korelacemi, přes reporty bezpečnostních událostí, aktuální údaje o kybernetických hrozbách, až po forenzní analýzy. A pokud společnost stále zvažuje SIEM, moderní log management řešení může výrazně snížit celkové náklady.

Zkrátka - log management v reálném čase sbírá/ukládá všechny logy, ale předává do SIEM jen ty, které souvisejí s bezpečností. Tento přístup zlepšuje celkovou funkčnost a snižuje počet logů přijatých do SIEM, čímž snižuje i náklady na SIEM licence.

Jaká strojová data máme sbírat?

Odpověď spočívá v pochopení hlavního účelu sběru strojových dat, který vedl k pořízení logmanagement nástroje. Jsou obvykle tři hlavní důvody – provozní, bezpečnostní a zákonné. Pravidlem je sbírat vše, co má hodnotu pro naplnění očekávaných požadavků pořízení nástroje. Nastavení každého zdroje dat by mělo být upraveno k naplnění účelu sběru. Je to ovšem soustavná činnost, protože nové systémy jsou průběžně přidávány a stávající modifikovány nebo odstraňovány. Je nutné neustále sledovat změny v IT infrastruktuře a zahrnout logování do systému managementu změn. Co se týče objemu dat, vždy je lepší sbírat co nejvíce informací a s co nejvíce detaily. Odfiltrování irelevantních dat je v LOGmanageru snadné. Můžeme použít příměr: se správným nástrojem je snadné najít jehlu v kupě sena; ale nemožné dohledat, pokud tam nebyla nikdy vložena. Proto jsou v dokumentaci LOGmanageru detailní návody, jak správně nakonfigurovat typická zdrojová zařízení (včetně nastavení auditních politik v prostředí Microsoft AD nebo Office365).

Jak dlouho máme uchovat strojová data?

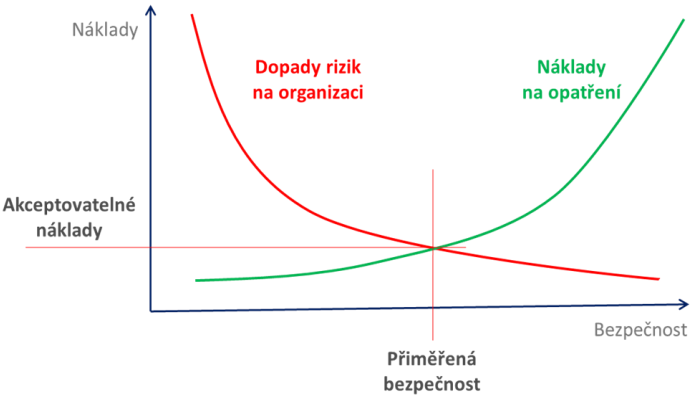
Zde je odpověď snadná. LOGmanager nabízí více než dostatečnou kapacitu rychle přístupného vnitřního úložiště. Takový přístup splňuje téměř jakýkoliv požadavek legislativy nebo nějaké uznávané autority. Navíc LOGmanager umožňuje automatické zálohování shromážděných denních dat na levné externí úložiště s virtuálně neomezenou dobou retence.

Je to drahé?

Odpověď je samozřejmě relativní, ale obecně je LOGmanager systémem bez skrytých nákladů. A co je nejdůležitější LOGmanager nepoužívá žádnou formu licencování. Vždy využívá maximální možný výkon hardwaru a dokonce je ještě výkonnější (díky unikátnímu subsystému vyrovnávací paměti). Ceny uvedené v ceníku zahrnují kompletní řešení včetně optimalizovaného hardwaru od prověřených výrobců. Aktualizace softwaru a technická podpora na první rok jsou zahrnuty v pořizovací ceně. Cena za prodloužení podpory je nastavena na 15% z ceny produktu.

Jak vybrat to správné řešení?

Ověřením, referencí a volbou vhodného poměru cena-výkon. Vyzkoušejte a otestujte si různá řešení. Pokud vás zaujal LOGmanager – kontaktujte některého z našich partnerů a vyžádejte si demo LOGmanager. Rozjeďte test ve vlastním prostředí. Berte v úvahu poměr ceny a užitné hodnoty každého z porovnávaných produktů jako celku. Nezapomeňte na cenu potřebného hardwaru a úložiště, instalaci, zaškolení, údržby hardwaru a pravidelnou aktualizaci.



Informace o výrobci a reference

LOGmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.