LOGmanager

> Centrální úložiště logů
> Dostupný SIEM

SPĹŇUJE POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A GDPR

Prečo potrebujete log manažment?

V dnešnom svete, ktorý je úplne závislý od IT, sa každá organizácia maximálne spolieha na svoju IT infraštruktúru. Ako firmy rastú, narastá aj ich infraštruktúra — aj malá organizácia môže mať sieť zloženú zo stoviek komponentov: serverov, aplikácií, databáz, koncových bodov, IoT zariadení atď. Každý z týchto komponentov s nami dokáže komunikovať prostredníctvom strojových dát, ktoré produkuje – informuje nás o zmenách konfigurácie, prevádzkových stavoch, aktivitách, diagnostike a o mnohom ďalšom. Mať tie správne dáta z logov je kľúčové pre mnoho dôležitých úloh, akými sú prevádzka, monitoring, diagnostika, audit, forenzné analýzy, tvorba reportov, súlad s predpismi a zákonmi. Každého, kto by chcel spracovávať dáta z logov, čakajú **nasledovné výzvy:**

- ### Pochopenie údajov z logov

Neexistuje norma, ako by mali strojové dáta vyzerať. Máme tucty najrôznejších štandardov, no napriek tomu má každý výrobca svoj vlastný prístup. Čo je horšie, každá aktualizácia systému môže priniesť zmenu aktuálneho formátu logov. Preto je ručné spracovanie logov časovo náročné. Prispôsobovať sa najrôznejším formátom a neustálym zmenám je nevyhnutné.

- ### Mazanie a zmeny

Staršie logy sa prepisujú novými, to znamená, že ak práve nejaké logy potrebujete, nemusíte ich už nájsť. Ak by došlo k narušeniu bezpečnosti, útočníci po sebe zaručene zahladia stopy tak, že ich okamžite zmažú/prepíšu, čím vám znemožnia akúkoľvek ďalšiu forenznú analýzu.

- ### Predpisy

Mať vyriešený manažment logov je kľúčové na dosiahnutie súladu s najrôznejšími štandardmi, predpismi a miestne platnými zákonmi (napr. o kybernetickej bezpečnosti, o ochrane osobných údajov, telekomunikačný zákon, bankový atď.).

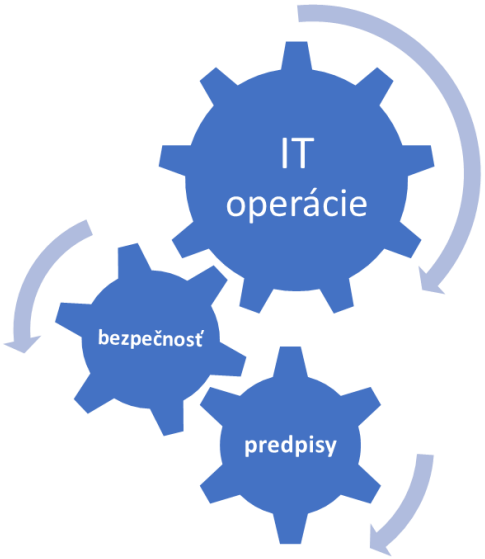
- ### Nemožnosť centrálneho vyhľadávania

Uchovávanie logov v zariadení, ktoré ich samo produkuje, ich robí ťažko dohľadateľnými – čo značne spomaľuje riešenia incidentov. A ako všetci vieme, čas sú peniaze.

Vzhľadom na vyššie uvedené skutočnosti je jasné, že každá organizácia potrebuje zabezpečiť manažment logov. Tradičné log manažmenty boli určené špeciálne na potreby veľkých organizácií. Výsledkom bol komplexný systém, ktorý si vyžaduje špecializované znalosti a veľký tím vyškolených ľudí.

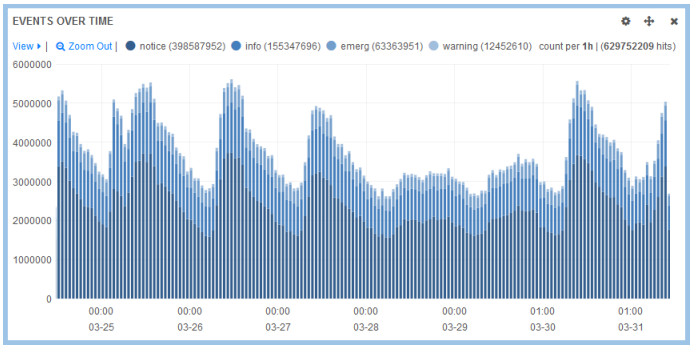
Spolu s vysokou cenou to nútilo stredné a menšie spoločnosti používať open-source riešenie. Nevýhodou open-source riešení je, že sa väčšinou ťažko implementujú a udržujú, zle sa s nimi pracuje alebo im chýbajú kritické funkcie. Riešením je moderný systém na manažment logov.

Logmanažment je pomocníkom vo všetkých oblastiach IT



Bez pochopenia strojových dát je v našich informáciách vždy medzera. Log manažment je široko prijímané riešenie na zaplnenie tejto medzery.

LOGmanager je určený pre malé až stredné organizácie a jeho používanie, údržba aj implementácia sú jednoduché. Je vybavený všetkými kritickými funkcionalitami na správu logov s najlepším pomerom ceny a úžitkovej hodnoty na trhu vďaka hardvéru zahrnutému v cene a bezlicenčnej politike.



Aj malé zariadenie na manažment logov si musí poradiť s veľkým objemom dát. Rýchle spracovanie a dostatočne veľké úložisko sú nevyhnutnosť, bez ktorej sa veľké objemy dát nedajú spracovávať.

Oblasti správy logov hodné Vašej pozornosti

IT operácia

Kritický IT incident je stredobodom dnešného IT sveta, je istý rovnako ako dane a smrť, pretože skôr či neskôr sa mu nevyhneme. Čo je to kritický IT incident? Je to stav, keď nefunguje business aplikácia alebo infraštruktúra na ňu naviazaná. Takáto situácia si vyžaduje okamžitú reakciu a IT tím organizácie musí byť schopný spolupracovať podľa charakteru incidentu na rýchlom odstránení chyby. V súvislosti s tým sú zažité dva pojmy – **MTTR a RCA** (Mean Time To Repair a Root Cause Analysis; voľne preložené to znamená Stredný čas potrebný na nápravu a Analýza príčin problému). Úlohou IT oddelenia je čo najskôr nájsť príčinu výpadku a odstrániť ju, potom analyzovať, prečo výpadok nastal vrátane všetkých súvislostí a nastaviť nápravné mechanizmy, aby k rovnakému alebo podobnému incidentu v budúcnosti nedošlo.

Zjednotenie formátov a centralizácia logov. Distribúcia logov naprieč rôznymi systémami a zariadeniami, rozdielna retencia a jazyk logov môžu spôsobovať problémy. Rôzne zariadenia majú rôzny prístup k manažmentu logov, zapisujú ich vo vlastnom jazyku a majú rôzne veľké lokálne úložisko logov. Preto majú i rozdielnu retenčnú dobu, počas ktorej sa logy uchovávajú. Keď hľadáte konkrétny záznam, pretože potrebujete riešiť prevádzkovú záležitosť, musíte prejsť logy uložené na najrôznejších zariadeniach, pochopiť, kde v nich hľadané informácie nájdete, a prehľadávať, a prehľadávať. Tu má zmysel nasadiť centralizovaný systém manažmentu logov.

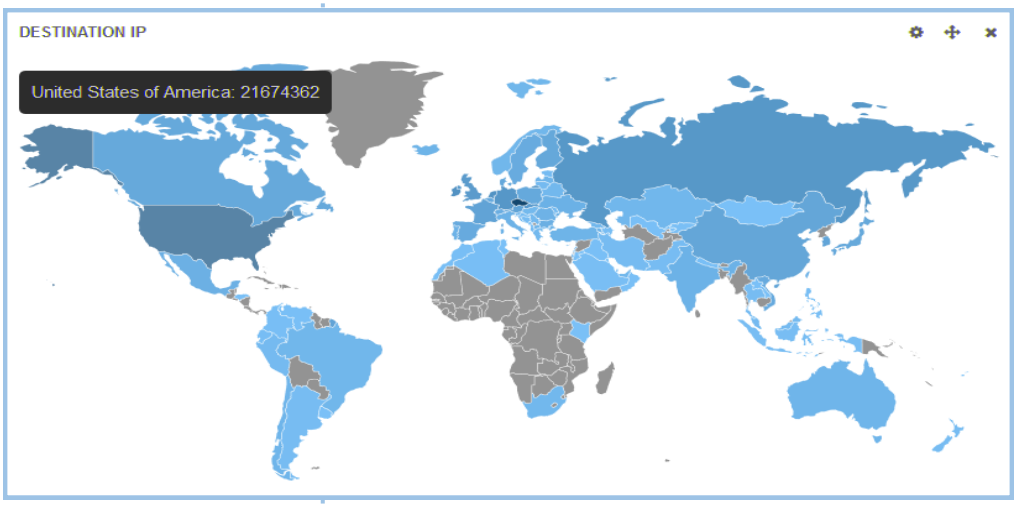
Centralizovaný systém, ako je **LOGmanager**, pohodlne zbiera logy zo všetkých zariadení a ukladá ich na jedno miesto. Navyše používa parsery na prekladanie logov do jednotného formátu, ktorý je ľahko pochopiteľný, a všetky údaje sa dajú ľahko indexovať na rýchle prehľadávanie. Keď neskôr potrebujete riešiť prevádzkové záležitosti, stačí sa obrátiť na jediný zdroj informácií – môžete si prehliadať logy generované infraštruktúrou, bezpečnostnými zariadeniami, servermi aj aplikáciami, ktoré sa stali nedostupnými, a môžete identifikovať príčinu problému rýchlo a efektívne.

Rýchla analýza dát vďaka centralizovaným logom. Vďaka centralizácii logov v LOGmanageri môžu IT operátori rýchlo analyzovať informácie z mnohých zdrojov bez toho, aby potrebovali administrátorský prístup ku každému z dotyčných systémov. Logy uložené v LOGmanageri nemôžu byť zmazané ani nijako modifikované. Vďaka tomu sú technici schopní i bez nutnosti administrátorských oprávnení prezerať logy z prevádzkových systémov, aj keď k týmto systémom nemajú prístupové práva. Analýza bežnej prevádzky sa tak stáva samozrejmou súčasťou ich práce a požiadavky na riešenia prevádzkových problémov môžu rovno posúvať svojim nadriadeným.

Bezpečnosť

V oblasti bezpečnosti je najvýznamnejšia **ochrana logov pred manipuláciou** a možnosť proaktívne identifikovať potenciálne bezpečnostné riziká, ladiť konfigurácie a sledovať vykonané zmeny. Len čo je nejaký záznam uložený v LOGmanageri, nemôže byť vymazaný ani nijako modifikovaný. Organizácie, ktoré sa stretávajú s bezpečnostnými problémami, často zisťujú, že útočník zmazal alebo zmenil všetky záznamy o škodlivej aktivite vo všetkých zariadeniach a systémoch, ku ktorým sa mu podarilo získať neoprávnený prístup. Môže byť potom veľmi zložité zistiť podrobné údaje o útočníkových aktivitách a tieto údaje poskytnúť na detailnú forenznú analýzu incidentu.

Nechajte **aktuálne údaje o kybernetických hrozbách** interagovať s vlastnými strojovými dátami. Kybernetické hrozby sa neustále vyvíjajú a keď o nich budete mať správne informácie, môže vám to uľahčiť predpovedanie kybernetických incidentov a rýchlu a cielenú odpoveď. LOGmanager používa vlastnú Reputačnú databázu vyvíjanú v spolupráci s českým operátorom národnej e-infraštruktúry – CESNET.



Proaktivny prístup

Log manažment vám umožní nastaviť vlastné upozornenia, ktoré budú detegovať určité udalosti ako napríklad zmazanie kritických súborov. Moderné zariadenia by mali zvládať aj koreláciu viacerých udalostí, čo umožní detegovať sériu udalostí a posielať upozornenia len pri dosiahnutí definovanej prahovej hodnoty. Vďaka okamžitému zasielaniu upozornení môže vaša organizácia rýchlo reagovať na problém, ktorý nastane. LOGmanager zbiera informácie o zmenách implementovaných v jednotlivých systémoch, čo vám umožní ľahko identifikovať, kto zmenu urobil a s akým výsledkom. Môžete taktiež sledovať neúspešné pokusy o prihlásenie do systémov, ktoré obsahujú citlivé dáta, pokusy testovať bezpečnostné pravidlá v sieti a tak ďalej.

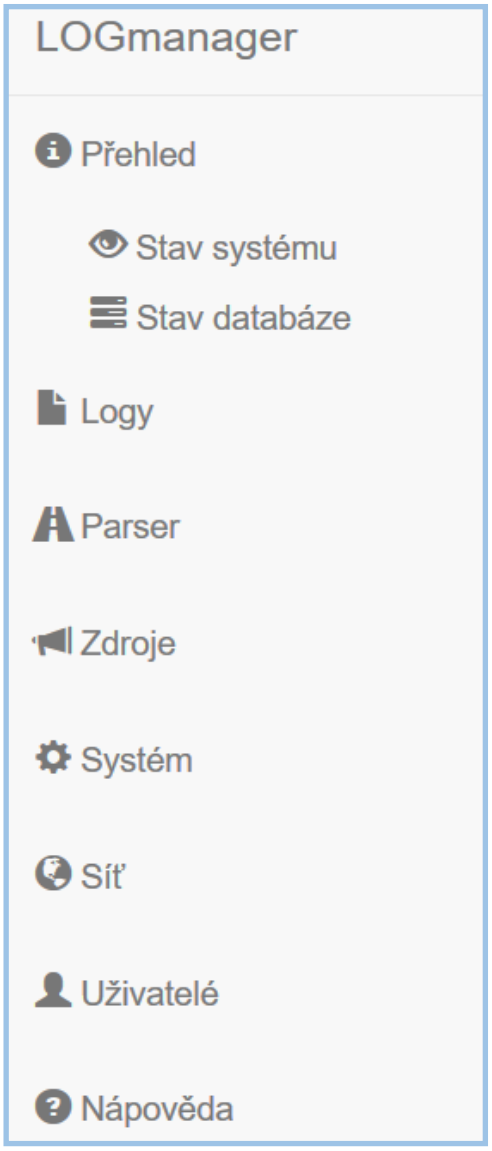
Súlad s predpismi

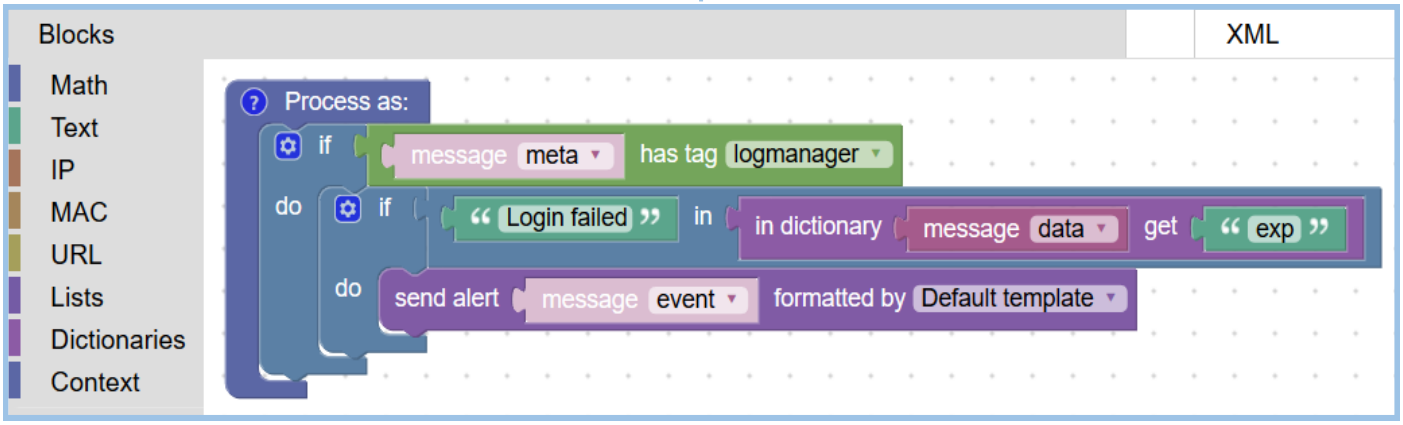
V oblasti súladu s predpismi čelíme mnohým výzvam. Organizácie sú povinné archivovať a analyzovať logy, zachytávať aktivity i dlhodobo uchovávať logy z kritických systémov a zdrojov. **ZKB/VKB, GDPR, NIST CSF, PCI-DSS, ISO 27001:2013, NISD 2016/1148/EU, HIPPA** – nezáleží na tom, ktoré zákony či normy musí vaša organizácia plniť, správny manažment logov je vždy súčasťou riešenia.

Audity/Reporty – Keď organizácia vykonáva bezpečnostný audit, je nevyhnutné mať systém, ktorý je schopný vytvárať reporty podľa požiadaviek audítora. LOGmanager vám umožní vytvárať reporty nielen v grafickej forme, ale aj v CSV formáte, štruktúrovanom podľa požiadaviek audítora. Môžete si vybrať ktorýkoľvek z logov uložených v databáze a zahrnúť ho do reportu. Ak je to potrebné, môžete dokonca exportovať súbor so stovkami tisíc riadkov. LOGmanager navyše podporuje možnosť prístupu do svojej databázy logov cez REST-API, takže je možné zadávať databázové požiadavky priamo zo svojho vlastného reportovacieho nástroja.

Radikálna jednoduchosť

Nedostatok zdrojov môže zmariť aj tie najlepšie projekty. Manažment logov by nemal vyčerpať vaše interné ľudské zdroje. Na našom log manažmente sa typicky oceňujú hodnoty ako rýchla implementácia, krátke zaškolenie a jednoduché integrované rozhranie, ktoré dokáže obsluhovať aj junior operátor.





Unikátnou vlastnosťou LOGmanageru je využitie blokových schém, zjednodušujúce operátorom bez znalosti programovania život.

Časté otázky:

Log manažment alebo SIEM?

Mnohí IT špecialisti vyhlasujú, že pre každú stredne veľkú spoločnosť je SIEM nevyhnutnosťou. My v LOGmanageru sme iného názoru. Nezabúdajme, že SIEM je zameraný primárne na kybernetickú bezpečnosť. Pokiaľ nejaká spoločnosť nemá vlastný tím technikov bezpečnosti IT alebo je príliš malý, veľká investícia do komplikovaného SIEM riešenia je kontraproduktívna. Pri obmedzených možnostiach ľudských zdrojov nie je čas na učenie sa a obsluhu komplexného SIEM produktu. Ten potom skôr či neskôr ostáva nevyužitý. Moderný log manažment dokáže nahradiť rad SIEM funkcionalít za cenu omnoho nižších nákladov aj úsilia, počnúc dynamickými vizualizáciami logov, pripravenými a nastaviteľnými upozorneniami a koreláciami cez reporty bezpečnostných udalostí, aktuálne údaje o kybernetických hrozbách až po forenzné analýzy. Pokiaľ spoločnosť stále zvažuje SIEM, moderné log manažment riešenie môže znížiť náklady.

Skrátka, log manažment v reálnom čase zbiera/ukladá všetky logy, ale odovzdáva do SIEM len tie, ktoré súvisia s bezpečnosťou. Tento prístup zlepšuje celkovú funkčnosť a znižuje počet logov prijatých do SIEM, čím znižuje náklady na SIEM licencie.

Aké strojové dáta máme zbierať?

Odpoveď spočíva v pochopení hlavného účelu zberu strojových dát. Pravidlom je, že všetko, čo má zmysel zbierať, by sa zbierať malo. Existujú tri hlavné dôvody – prevádzkové, bezpečnostné a zákonné. Podľa toho by malo byť upravené nastavenie každého zo zdrojových systémov. Je to sústavná činnosť, pretože nové systémy sa priebežne pridávajú a aktuálne modifikujú alebo odstraňujú. Je nutné neustále sledovať zmeny v IT infraštruktúre a do systému manažmentu zmien zahrnúť aj logovanie a audity. Čo sa týka objemu dát, vždy je lepšie zbierať čo najviac informácií s čo najviac detailmi. Odfiltrovanie irelevantných dát je s LOGmanagerom jednoduché. Môžeme použiť prirovnanie: so správnym nástrojom sa ľahko nájde ihla v kope sena, ale je nemožné nájsť ju, pokiaľ ju tam nikto nevložil. Preto sú v dokumentácii LOGmanagera detailné návody, ako správne nakonfigurovať typické zdrojové zariadenia (vrátane kompletného návodu pre politiky Microsoft Audit).

Ako dlho uchovávať strojové dáta?

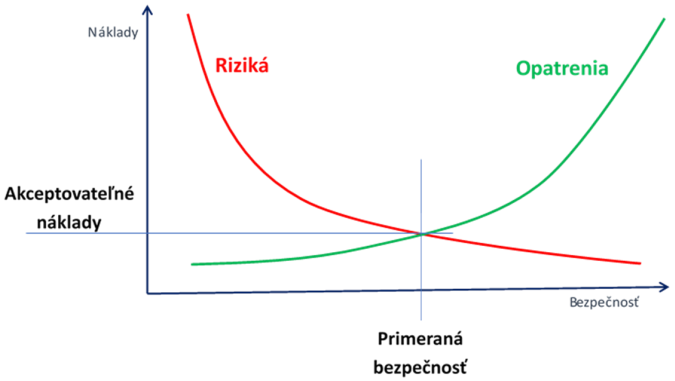
Odpoveď je jednoduchá. LOGmanager ponúka viac než dostatočnú kapacitu rýchlo prístupného vnútorného úložiska. Takýto prístup spĺňa takmer všetky požiadavky legislatívy alebo nejakej uznávanej autority. Navyše, LOGmanager umožňuje automatické zálohovanie zhromaždených denných dát na lacné externé úložisko s virtuálne neobmedzenou lehotou retencie.

Je to drahé?

Odpoveď je, samozrejme, relatívna, ale LOGmanager je systémom bez skrytých nákladov, pretože nepoužíva žiadnu formu licencovania. Využíva maximálny možný výkon hardvéru a dokonca je ešte výkonnejší (vďaka unikátnemu subsystému vyrovnávacej pamäte). Ceny uvedené v cenníku zahŕňajú kompletné riešenia vrátane optimalizovaného hardvéru od overených výrobcov, rovnako ako výmenu chybných HW dielov priamo u zákazníka. Aktualizácia softvéru a technická podpora na prvý rok sú zahrnuté v cene. Cena za predĺženie podpory je nastavená na 15 % ceny produktu.

Ako vybrať to správne riešenie?

Overením, referencií a voľbou vhodného pomeru cena-výkon. Vyskúšajte a otestujte si rôzne riešenia. Pokiaľ vás LOGmanager zaujal, kontaktujte niektorého z našich partnerov, vyžiadajte si demo LOGmanager a rozbehnite „proof of concept“ test v prostredí svojej vlastnej infraštruktúry. Vezmite do úvahy pomer ceny a úžitkovej hodnoty každého z porovnávaných produktov ako celku. Nezabudnite na cenu potrebného hardvéru a úložiska, inštalácie, zaškolenia, údržby a aktualizácie.



Informácie o výrobcovi a referencie

LOGmanager sa vyvíja od roku 2014 ako nosný produkt firmy Sirwisa, a.s., ktorá sídli v Prahe. Na www.logmanager.sk nájdete referencie. Medzi našich zákazníkov patrí nielen štátna správa, ale aj priemyselné podniky všetkých veľkostí a odvetví, obchodné spoločnosti, banky, poisťovne a ďalšie. Ohľadom ďalších referencií priamo z oblasti, ktorá vás zaujíma, nás neváhajte kontaktovať. Príslušné kontakty na existujúcich zákazníkov, ktorí súhlasia s uvádzaním na referenčnom liste, radi poskytneme.