LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Dlaczego organizacje potrzebują zarządzania logami ?

W dzisiejszym, coraz bardziej cyfrowym świecie, funkcjonowanie dowolnej organizacji jest uzależnione od infrastruktury IT która rośnie w miarę rozwoju biznesu – nawet mała firma może posiadać skomplikowaną sieć złożoną z setek komponentów: serwerów, aplikacji, bazy danych, stacji użytkowników, urządzeń IoT etc. Każdy z tych komponentów chce z nami rozmawiać poprzez dane maszynowe które produkuje – informując o zmianach w konfiguracji, aktywnościach użytkowników, statusie i innych. Posiadanie właściwych logów jest kluczowe dla najważniejszych procesów IT takich jak monitorowanie, diagnostyka, audytowane, śledzenie, raportowanie i osiąganie zgodności z regulacjami/prawem. **Każdy, kto chce na poważnie zająć się zarządzaniem logami, powinien wziąć pod uwagę kilka wyzwań:**

- ### Format danych

Nie został osiągnięty konsensus odnośnie tego jaki format powinny mieć dane maszynowe. Każdy producent stosuje własne podejście. Co gorsze, każdy update może wprowadzić zmiany do istniejącego formatu. To wszystko powoduje, że manualne procesowanie logów jest wyjątkowo trudne. Adaptacja do różnych formatów i ich ciągłych zmian jest kluczowa dla wydajnego zarządzania logami.

- ### Zmienność

Nowe logi nadpisują stare, toteż mogą nie być dostępne kiedy będziesz ich potrzebować. Natomiast w przypadku incydentu bezpieczeństwa jest niemalże gwarantowane, że atakujący usunie logi aby zatrzeć swoje ślady i utrudnić śledztwo.

- ### Regulacje/standardy/prawo

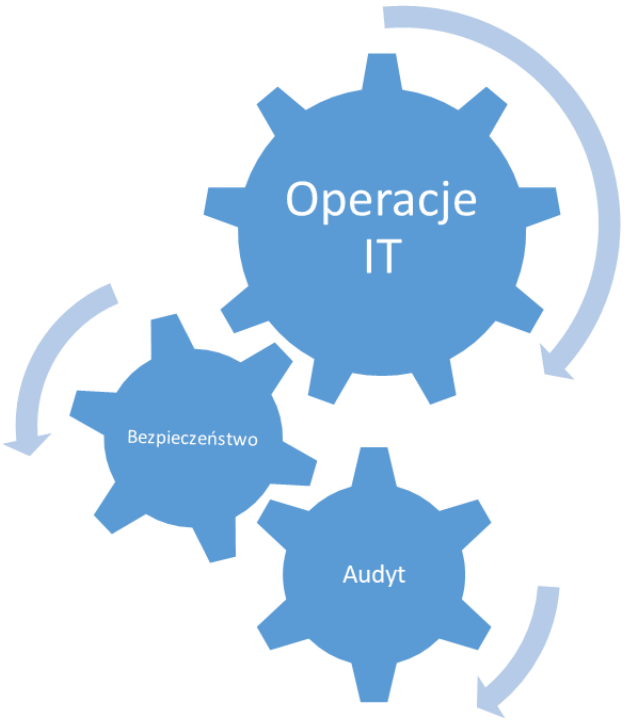
Posiadanie rozwiązania do zarządzania logami jest kluczowe dla osiągnięcia zgodności z różnymi standardami branżowymi, regulacjami oraz prawem specyficznym dla danego kraju.

- ### Brak centralnego wyszukiwania

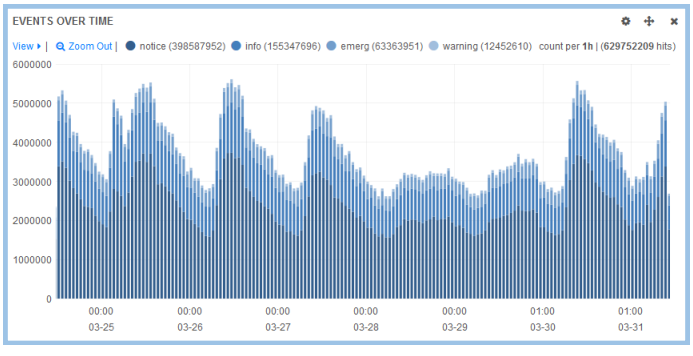
Przechowywanie logów na urządzeniu które je produkuje jest kłopotliwe w przypadku awarii – trudniejsze do znalezienia dane to dłuższy czas rozwiązywania problemów, a jak wiadomo czas = pieniądze.

Biorąc pod uwagę powyższe wyzwania staje się jasne, że każda organizacja potrzebuje skutecznego rozwiązania do zarządzania logami. Niestety, najpopularniejsze produkty dostępne na rynku zostały zaprojektowane pod specyficzne potrzeby większych organizacji, co oznacza wysoki stopień skomplikowania wymagający eksperckiej wiedzy technicznej i dużego zespołu. Ten problem w połączeniu z wysoką ceną zmusił średnie i małe organizacje do zwrócenia się w stronę rozwiązań open-source, które często są trudne do wdrożenia i utrzymania, a także brakuje im istotnych funkcjonalności.

Zarządzanie logami wspiera wszystkie obszary IT



LOGmanager to system zaprojektowany z myślą o zapełnieniu luki pomiędzy tradycyjnymi rozwiązaniami do zarządzania logami, a open-source. Przeznaczony dla małych-średnich organizacji, łatwy w wykorzystaniu, utrzymaniu i wdrożeniu, wyposażony we wszystkie najważniejsze funkcjonalności i o najlepszym stosunku cena/jakość dzięki zintegrowanej platformie sprzętowej i braku licencji ograniczających wydajność zbierania logów .



Nawet mała instancja systemu do zarządzania logami musi być w stanie obsłużyć duże ilości danych. Szybkie procesowanie i dużo przestrzeni dyskowej to kluczowe parametry.

Gdzie zarządzanie logami przydaje się najbardziej ?

Operacje IT

Krytyczny incydent to kluczowe określenie w dzisiejszym świecie IT. Tak jak podatki i śmierć, nie da się go uniknąć, ponieważ wcześniej czy później na pewno się wydarzy. Przede wszystkim czym jest krytyczny incydent ? Jest to sytuacja w której aplikacja biznesowa (generująca przychód), bądź podległa infrastruktura przestaje działać. W takim przypadku niezbędna jest natychmiastowa reakcja zespołu IT, który musi być w stanie szybko wykryć źródło problemu i go rozwiązać. W tym kontekście najczęściej wykorzystywana jest następująca terminologia – **MTTR (Mean Time To Repair; Średni Czas Rozwiązania)** oraz **RCA (Root Cause Analysis; Analiza Przyczyn Źródłowych)**. Rolą departamentu IT jest jak najszybsze wykrycie przyczyny incydentu, jego eliminacja, a następnie analiza całego zdarzenia, potrzebna do podjęcia akcji mających na celu uniknięcie identycznego bądź podobnego problemu w przyszłości.

Unifikacja formatu i centralizacja logów.
Każdy producent przyjmuje inne podejście do tworzenia logów; zapisuje je w różnych formatach i ustawia własne czasy retencji w zależności od lokalnie dostępnej przestrzeni dyskowej. To tworzy problemy – administrator traci czas na manualne przeszukiwanie urządzeń dostępnych w sieci, a ponieważ formaty się różnią, to dane są trudniejsze to zrozumienia. Dodatkowo, jeżeli problemem jest przerwa w pracy urządzenia, logi zapisane lokalnie mogą nie być dostępne. W związku z tym kluczowe jest zbieranie, a następnie przechowywanie logów w centralnej lokalizacji.

LOGmanager umożliwia zbieranie i przechowywanie logów ze wszystkich urządzeń w sieci. Zbierane logi w procesie parsowania są przekształcane we wspólny, łatwy do zrozumienia format oraz indeksowane w celu umożliwienia szybkiego wyszukiwania.

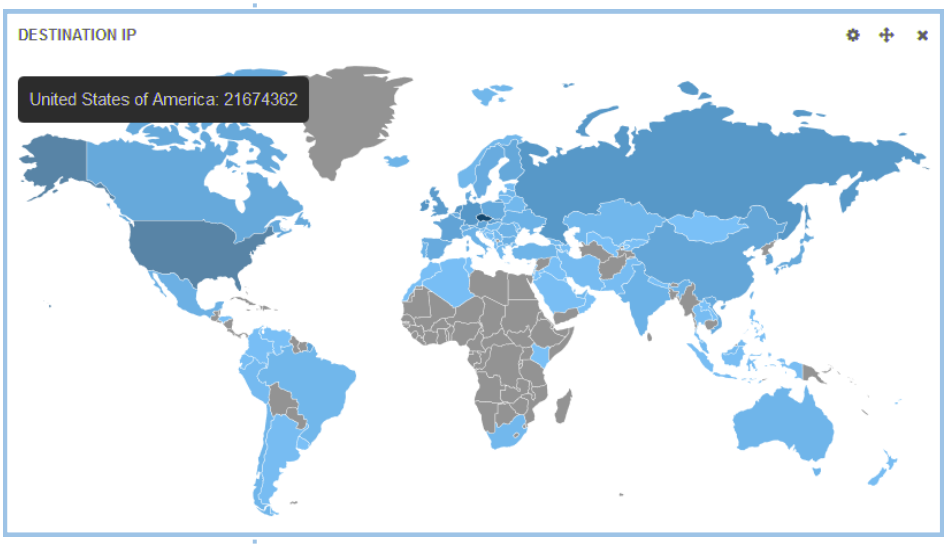
W przypadku wystąpienia awarii wymagającej szczegółowej analizy informacji dotyczących kontekstu zdarzenia, LOGmanager stanowi pojedyncze źródło do którego administrator może się zwrócić – w celu wyszukania logów wygenerowanych przez serwery, aplikacje czy urządzenia sieciowe przed awarią.

Szybkie wyszukiwanie i analiza
Dzięki centralizacji logów operator systemu może szybko analizować wiele źródeł informacji bez konieczności uzyskiwania bezpośredniego dostępu do urządzeń które je generują. Centralizacja logów umożliwia zastosowanie holistycznego podejścia do przechowywanych informacji. Dane mogą być prezentowane w formie najróżniejszych wykresów, umożliwiających wyciąganie szybkich wniosków, rozpoznanie trendów czy problemów. Responsywny interfejs umożliwia także przejście od ogółu do szczegółu (drill down) – zaczynając od wysokopoziomowego widoku wszystkich logów w systemie, w miarę postępu analizy schodząc do pojedynczych logów.

Bezpieczeństwo

Najważniejsze korzyści w obszarze bezpieczeństwa to ochrona przed sfałszowaniem, możliwość proaktywnego wykrywania incydentów oraz śledzenie zmian w konfiguracji. Log raz zapisany w bazie LOGmanager nie może być usunięty ani zmodyfikowany – co ma nie małe znaczenie w sytuacji kiedy atakujący skutecznie zatrze za sobą ślady swojej działalności w sieci. Odtworzenie kroków atakującego jest dzięki temu łatwiejsze, a to w konsekwencji umożliwia podjęcie działań mających na celu mitygację zagrożenia i poprawienie bezpieczeństwa organizacji w przyszłości .

Istotnym czynnikiem jest także **integracja z danymi o zagrożeniach**. Cyber zagrożenia ciągle ewoluują, toteż posiadanie aktualnych danych śledczych może ułatwić detekcję incydentów i umożliwić szybką remediację. LOGmanager wykorzystuje własną bazę danych reputacji, stworzoną we współpracy z Czeskim operatorem CESNET.



Proaktywność

Nowoczesne rozwiązania do zarządzania logami muszą umożliwiać tworzenie alertów mających na celu detekcje pojedynczych zdarzeń, takich jak usunięcie krytycznych danych, oraz korelację zdarzeń, przykładowo wystąpienie określonej ilości logów tego samego rodzaju w zdefiniowanym oknie czasowym - np. konsekwentne nieudane próby logowania do systemu. Funkcjonalność alertowania wyposaży Twoją organizację w środki do wczesnej detekcji pojawiających się problemów, a tym samym umożliwi ich szybkie rozwiązanie zanim zdążą wyrządzić poważne szkody.

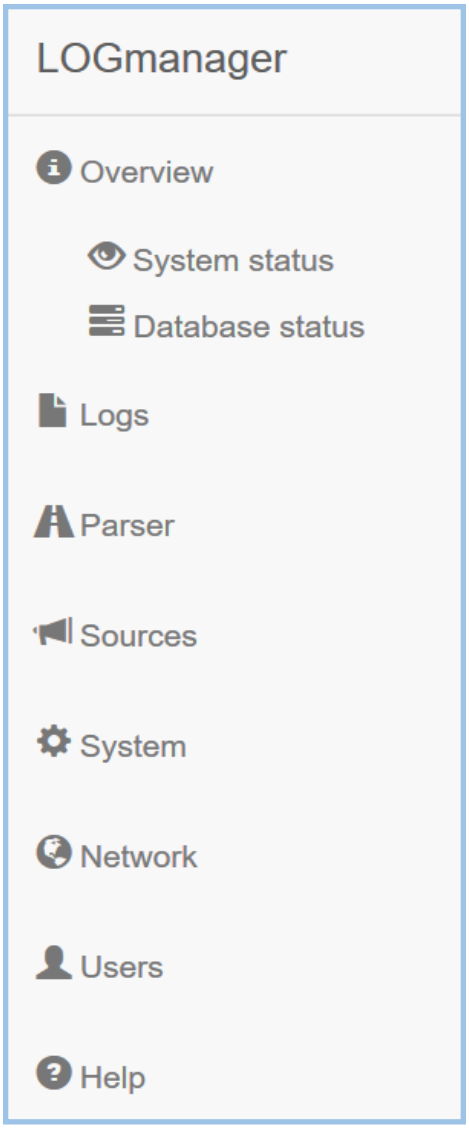
Zgodność z przepisami

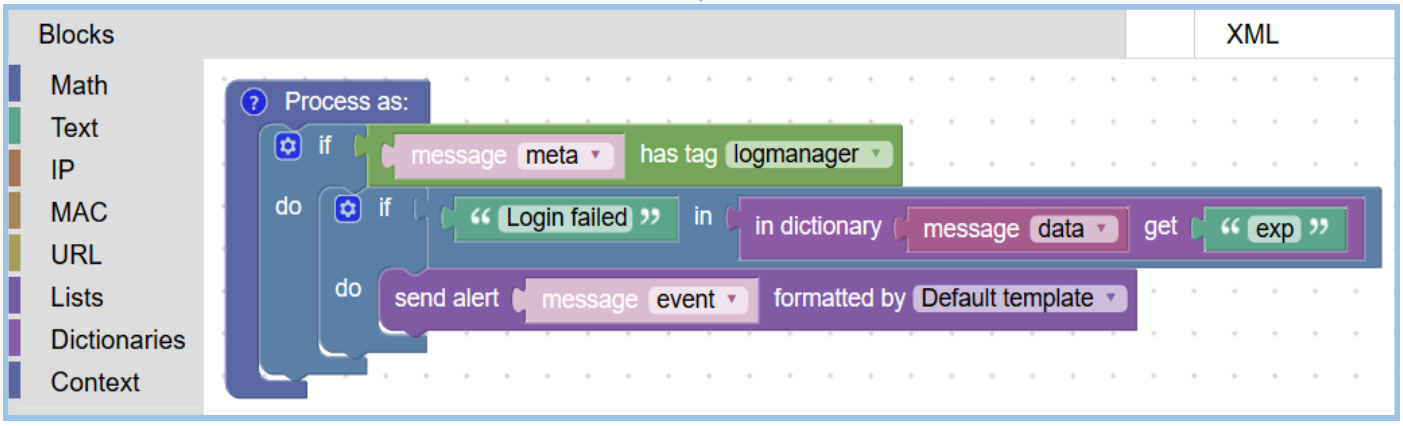
Obszar zgodności z wymaganiami poszczególnych praw, standardów i regulacji jest pełen wyzwań. Od organizacji oczekuje się ciągłego analizowania logów, zapisywania aktywności użytkowników, a także archiwizację i przechowywanie logów z krytycznych systemów przez określony czas. GDPR, NIST CSF, PCI-DSS, ISO 27001:2013, NISD 2016/1148/EU, HIPPA – nie ma znaczenia jakie wymagania Twoja organizacja stara się spełnić – prawidłowe zarządzanie logami jest zawsze częścią rozwiązania.

Audyt i raportowanie – Kluczowe w czasie trwania audytu bezpieczeństwa w organizacji jest generowanie raportów zgodnych z wymaganiami audytora. LOGmanager umożliwia prezentowanie informacji nie tylko w formie graficznej, ale także w pliku CSV ze strukturą zdefiniowaną pod wymagania audytu, o długości tysięcy linii. Dowolny log zapisany w bazie LOGmanager może być uwzględniony w raporcie. Dodatkowo, LOGmanager umożliwia dostęp do logów bezpośrednio przez REST-API w celu procesowania wyników zapytania bezpośrednio po stronie zewnętrznego rozwiązania.

Radykalna Prostota

Brak zasobów może zaszkodzić nawet najlepszemu projektowi. Zarządzanie logami to wymagające zadanie, jednak nie można pozwolić aby zabierało zbyt dużo czasu Twojemu personelowi technicznemu. Wartości promowane przez LOGmanager to szybka implementacja, krótki cykl treningowy oraz prosty interfejs web GUI, który może być obsługiwany nawet przez mniej doświadczonych członków zespołu .





*Unikalna funkcjonalność **LOGmanager** umożliwia programowanie przy wykorzystaniu uproszczonego, graficznego podejścia .*

Najczęściej zadawane pytania:

LOGmanager czy SIEM?

Każda organizacja potrzebuje w jakiś sposób zarządzać logami. Najczęściej w tym celu wykorzystywane są systemy SIEM. Rozważmy jednak następujący problem: SIEMy skupiają się głównie na bezpieczeństwie. Jeżeli dana organizacja (mała bądź średnia) nie posiada własnego zespołu bezpieczeństwa, bądź jest on skromny, inwestowanie budżetu w taki produkt może przynieść stratę - ze względu na ograniczoną ilość czasu i skomplikowanie typowych rozwiązań SIEM, administratorzy będą wykorzystywać go w tylko w minimalnym zakresie, bądź całkowicie porzucą. Nasza odpowiedź na ten problem to wykorzystanie nowoczesnych rozwiązań do zarządzania logami takich jak LOGmanager, które skutecznie zastępują najważniejsze funkcjonalności SIEM, przy zachowaniu jednoczesnego niższego kosztu i mniejszego wysiłku. Natomiast jeżeli z różnych względów posiadanie systemu SIEM jest dla organizacji kluczowe – system do zarządzania logami może być wykorzystany jako wsparcie. Przykładowo - LOGmanager zbiera logi ze wszystkich systemów w sieci, a do SIEM wysyła tylko najistotniejsze dane dotyczące bezpieczeństwa. Taka integracja poprawią ogólną funkcjonalność i redukuje ilość logów odbieranych przez SIEM, tym samym oszczędzając na licencji.

Jakie logi powinniśmy zbierać?

Odpowiedź brzmi: wszystkie. Im więcej logów zbieramy, tym lepiej jesteśmy przygotowani na wszelkie nieprzewidziane okoliczności. Musimy jednak brać pod uwagę, że wydajność dowolnego rozwiązania do zarządzania logami nie jest nieskończona. Reguła kciuka mówi, że wszystko co spełnia przynajmniej jeden z 3 celów zbierania danych – operacyjny, bezpieczeństwa i prawny - powinno być zbierane. Konfiguracja systemów źródłowych generujących logi powinna odzwierciedlać te cele, aby uniknąć tworzenia nadmiarowych, nieistotnych informacji. Przykładowo: systemy Windows domyślnie generują wiele różnych logów, ale duża część z nich jest nieistotna z punktu widzenia operacji, bezpieczeństwa czy prawa – takie logi możemy pominąć. Proces decyzyjny odnośnie tego co należy zbierać, a co nie, jest ciągły, ponieważ systemy, aplikacje i urządzenia są wciąż dodawane, zmienianie i usuwane. LOGmanager ułatwia to zadanie, dzięki prostemu mechanizmowi filtrowania zbieranych danych, oraz kompletnej dokumentacji opisującej w szczegółach konfigurację wielu systemów źródłowych .

Jak długo należy przechowywać logi?

Na to pytanie nie ma jednoznacznej odpowiedzi. LOGmanager dostarcza więcej niż wystarczająco przestrzeni dyskowej, aby zaspokoić wymagania regulacji i standardów. Dodatkowo, rozwiązanie umożliwia automatyczny backup zebranych danych na zewnętrznym systemie dedykowanym do przechowywania danych przez długi czas.

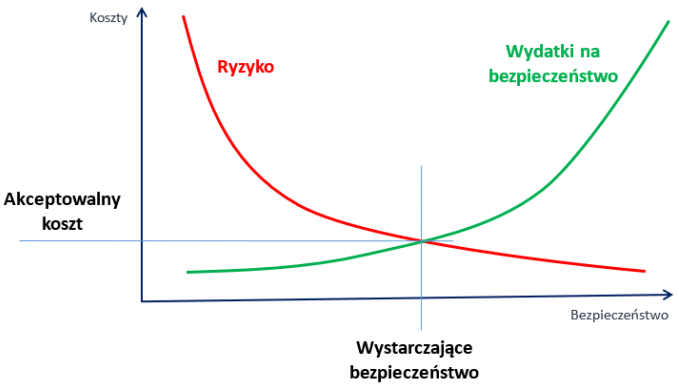
Czy zarządzanie logami jest drogie?

Odpowiedź jest relatywna, ale ogólnie rzecz biorąc LOGmanager jest rozwiązaniem bez ukrytych kosztów. Przede wszystkim nie ma żadnych ograniczeń licencyjnych. Ilość jak i szybkość zbierania logów jest uzależniona jedynie od wydajności platformy sprzętowej. Cena rozwiązania zawiera pełen produkt wraz z dedykowaną platformą sprzętową i usługą naprawy na miejscu. Aktualizacje oprogramowania jak i wsparcie techniczne za pierwszy rok są wliczone w cenę. Kolejne lata liczone są już od 15% bazowej ceny.

Jak wybrać najlepsze rozwiązanie dla nas?

Zawsze sugerujemy przetestowanie kilku rozwiązań przed podjęciem decyzji. Należy wziąć pod uwagę stosunek ceny do wartości jaką dane rozwiązanie wnosi i nie zapominać o dodatkowych kosztach takich jak platforma sprzętowa, wdrożenie, trening, wsparcie i aktualizacje. W przypadku zainteresowania rozwiązaniem LOGmanager, PoC realizowane jest przez certyfikowanych partnerów przy wykorzystaniu platformy demo.

.



O producencie

LOGmanager jest rozwijany od 2014 roku jako flagowy produkt Czeskiej firmy Sirwisa a.s.. Wybrane referencje klientów można znaleźć na www.logmanager.com. Baza klientów LOGmanager składa się z organizacji różnego rozmiaru z wielu branż: finanse, bankowość, telekomunikacja, e-commerce, a także jednostki rządowe, uniwersytety, publiczna telewizja itd. W przypadku zainteresowania prosimy o kontakt, na życzenie chętnie udostępnimy bardziej szczegółowe referencje do naszych obecnych klientów z wybranego sektora.