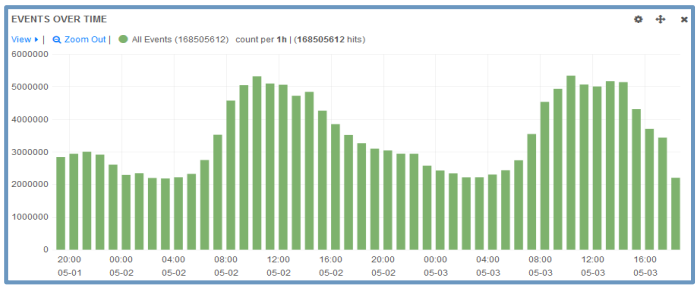
LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

LOGmanager

W dzisiejszym świecie opanowanym przez technologię informacja to zasób krytyczny, umożliwiający podejmowanie właściwych decyzji we właściwym czasie. Ten fakt kontrastuje ze sposobem w jaki przechowujemy dane – rozproszone po urządzeniach i aplikacjach wewnątrz Organizacji, często z nałożonymi ograniczeniami dostępu i w formatach nie zawsze zrozumiałych dla człowieka. Stąd kluczowym dla wydajności działań operacyjnych jest konsolidacja informacji płynących z różnych źródeł, ich konwersja do jednolitego formatu, zapewnienie im bezpieczeństwa i integralności oraz utworzenie reguł mających na celu ich automatyczną obsługę a także zrozumiała interpretacja kolekcjonowanych danych umożliwiająca Organizacjom podejmowanie trafniejszych decyzji. Narzędziem realizującym te wszystkie założenia jest pochodzący z Czech— LOGmanager.



Opis rozwiązania

LOGmanager to rozwiązanie sprzętowe służące do centralnego zarządzania logami i danymi maszynowymi zbieranymi z różnych źródeł. Rozwiązanie wykorzystuje potężną bazę danych o bardzo dużej pojemności, oferującą szybkie przeszukiwanie zbiorów big data oraz natychmiastową wizualizację wyników zapytania. LOGmanager kolekcjonuje dane, przechowuje je z zachowaniem integralności na długiej przestrzeni czasu, udostępnia funkcje analityczne, umożliwia Organizacjom wykonywanie zapytań w czasie rzeczywistym, generowanie analiz statystycznych, raportów oraz alertów wywoływanych w odpowiedzi na zdarzenia korelowane z różnych źródeł.

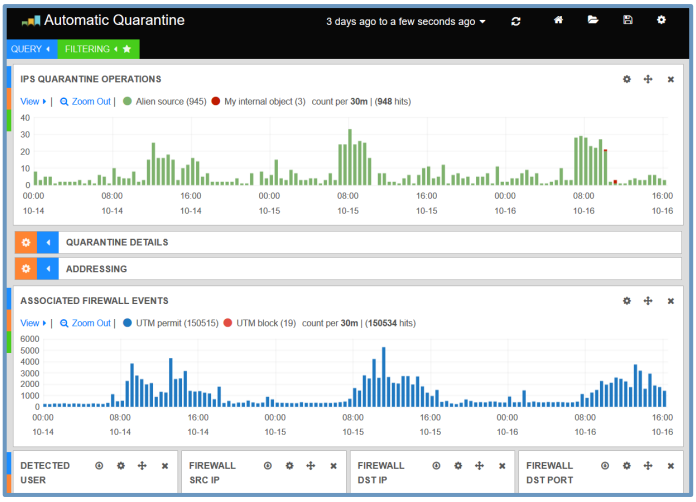
LOGmanager dodatkowo wspomaga osiągnięcie zgodności z regulacjami. Należycie wdrożony pomaga Organizacjom uzyskanie zgodności ze standardem ISO/27001:2013 w kwestii retencji rekordów ścieżek audytowych, a także spełnienie wymagań RODO. Ale LOGmanager jest narzędziem zaprojektowanym nie tylko dla działów bezpieczeństwa IT i w celu osiągnięcia zgodności z regulacjami. Bardzo duży nacisk podczas jego tworzenia został położony na funkcjonalności wspierające działania operacyjne IT. Rozwiązanie mocno przyczynia się do poprawy ich wydajności, dzięki agregowaniu danych operacyjnych ze wszystkich krytycznych systemów. Administratorzy IT są w stanie w kilka sekund wyszukać informacje o statusach działania urządzeń i potencjalnych problemach, na co w innym przypadku musieliby poświęcić godziny manualnej pracy. Dodatkowo, dzięki automatycznemu powiadamianiu poprzez alerty, mogą proaktywnie zapobiegać incydentom bezpieczeństwa.

Wspierane źródła danych

LOGmanager natywnie wspiera ponad 125 źródeł danych ze wszystkich obszarów IT. LOGmanager dodatkowo wspiera ustandaryzowane formaty logów jak CEF, LEEF, RFC5424 czy JSON. Dla własnościowych źródeł, umożliwia tworzenie szybkich i prostych parserów.

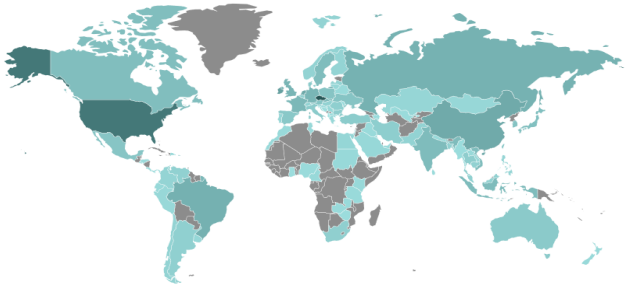
Kluczowe zalety

- Centralne repozytorium logów i danych maszynowych w Organizacji
- Konwersja formatów logów do postaci zrozumiałej dla człowieka
- Procesowanie i wizualizacja napływających danych w czasie rzeczywistym
- Szybkie wyszukiwanie bez konieczności nauki języka SQL
- Funkcjonalność SIEM. Alerty z wartościami granicznymi i korelacją
- Unikalna konfiguracja i programowalne GUI
- Duża łatwość użytkowania i przyjazność dla użytkownika
- Proste tworzenie audytów i raportów
- Ułatwia osiągnięcie zgodności z:
  - Polityką bezpieczeństwa Organizacji
  - RODO
  - ISO27001:2013 w kwestii retencji ścieżek audytowych
  - PCI DSS 3.2
- BRAK LICENCJI = Brak ograniczeń licencyjnych
- Usprawniona integracja z produktami SIEM / UBA innych firm



Konkurencyjność

- Wydajność do 10,000EPS w trybie ciągłym
- Szczytowo 20,000EPS na przestrzeni 10minut
- Hardware z pojemnością dyskową nawet do 100TB
- Wspiera bardzo dużą liczbę źródeł płynących z różnych urządzeń, systemów i aplikacji
- Centralnie zarządzany klient kolekcjonujący logi z systemów Windows OS
- Natywne wsparcie dla konfiguracji HA w trybie active-active
- Szybka i prosta implementacja
- Brak licencji = brak ukrytych dodatkowych kosztów



Przykłady wykorzystania

Zgodność

Twój biznes wymaga centralnego systemu do zarządzania, analizy oraz przechowywania logów audytowych i danych operacyjnych na długiej przestrzeni czasu. Potrzebujesz wydajnego kosztowo rozwiązania bez ograniczeń licencyjnych, które wesprze spełnienie wymogów audytowych oraz polityk bezpieczeństwa …

Kontrola nad dostępem do sieci

Jeżeli planujesz wdrożenie centralnego rozwiązania do kontrolowania dostępu do sieci, Twój dział IT potrzebuje rozwiązania do monitorowania 802.1X. Musisz być w stanie zbierać logi z aktywnych komponentów sieci, zdarzeń Active Directory i serwera RADIUS …

Monitorowanie serwerów plików

Kto skopiował bądź usunął poufne dane z serwera plików? Ransomware zaszyfrował dyski i musisz je odtworzyć z backupu, ale nie wiesz co dokładnie zostało zaszyfrowane? Potrzebujesz kontroli nad operacjami wykonywanymi na serwerze plików i wiedzy odnośnie tego jakie operacje były wykonywane, przez kogo, i kiedy …

Monitorowanie bezpieczeństwa

Monitorujesz infrastrukturę, ale używasz do tego celu różnych rozwiązań i potrzebujesz mieć możliwość konwersji logów i rekordów audytowych do jednolitego formatu, a dedykowane rozwiązania są za drogie i wspierają tylko wyselekcjonowane rozwiązania bezpieczeństwa? LOGmanager procesuje i analizuje logi ze wszystkich źródeł, bez ograniczeń …

Monitorowanie zmian

Kto, kiedy i z jakim wynikiem przeprowadził zmiany w konfiguracji aktywnych komponentów sieci, systemów operacyjnych i aplikacji ? Potrzebujesz rozwiązania które dotrze do tych informacji nawet jeżeli miały miejsce wiele miesięcy temu i udostępni je w formie raportu audytowego …

Funkcje i integracja

LOGmanager zapewnia podstawowe funkcje SIEM. Jeżeli w przyszłości zdecydujesz się na zakup dedykowanej platformy analitycznej, LOGmanager umożliwia selektywne udostępnianie danych w wielu ustrukturyzowanych formatach produktom firm trzecich. Oszczędzasz na opłatach licencyjnych, a integracja jest łatwa …

Weryfikacja zgodności

Potrzebujesz rozwiązania które pomoże Ci zweryfikować, czy konfiguracja Twoich systemów bezpieczeństwa jest w zgodności z wdrożonymi politykami bezpieczeństwa …

Identyfikacja przepływu danych

Kto z pracowników pobrał więcej danych niż zwykle poprzez VPN ? Do jakich zasobów był uzyskiwany dostęp, co zostało wysłane na zewnątrz firmy …

Ochrona informacji

Dane raz zapisane w LOGmanager nie mogą zostać usunięte ani zmodyfikowane. Dzięki certyfikacji ISO27001:2013 możesz wykorzystać LOGmanagera jako platformę do tworzenia raportów i informatyki śledczej …

Specyfikacja techniczna urządzeń LOGmanager

LOGmanager platforma sprzętowa i oprogramowanie w wersji 3.3.0 i nowszej							
CPU	RAM	Dysk	RAID	Pojemność	Retencja danych (Średni EPS[1]/dni)	MAX Stały EPS[1]	Szczytowy EPS[1]
LOGmanager-XL serwer DELL o rozmiarze 2U, z natywnie zintegrowanym Workload Accelerator[2] (5 lat NBD RMA, 1 lub 5 lat SW renewal, 1x LOGmanager-VF)							
2x14core Intel Xeon@2.6GHz	128GB	12*10TB	6	100TB	5000EPS - 365 dni	10000	20000/10min
LOGmanager-L serwer DELL o rozmiarze 2U. (5 lat NBD RMA, 1 lub 5 lat SW renewal, 1x LOGmanager-VF)							
2x12core Intel Xeon@2.2GHz	128GB	12*4TB	6	40TB	3000EPS - 275 dni	5000 (6000[2])	10000/10min
LOGmanager-M serwer DELL o rozmiarze 1U. (3 lata NBD RMA, 1 lub 3 lata SW renewal, 1x LOGmanager-VF)							
1x12core Intel Xeon@2.2GHz	64GB	4*4TB	5	12TB	1000EPS - 230 dni	2000	4000/10min
LOGmanager-S serwer DELL Tower. (3 lata NBD RMA, 1 lub 3 lata SW renewal, 1x LOGmanager-VF)							
1x2core Intel G5500@3.8GHz	32GB	2*4TB	1	4TB	250EPS - 310 dni	500	1000/10min
LOGmanager-Demo platforma Intel NUC - tylko na potrzeby LAB lub PoC. (3 lata RMA, 1 rok SW renewal, 1x LOGmanager-VF)							
1x2core Intel i5@2.9GHz	16GB	1*500GB	N/A	490GB	250EPS - 30 dni	500	1000/10min
LOGmanager Forwarder (rozwiązanie do bezpiecznego i niezawodnego zbierania logów z DMZ oraz zdalnych lokalizacji połączonych przez WAN lub Internet)							
CPU	RAM	Dysk	RAID	Pojemność	Retencja danych	MAX Stały EPS[1]	Szczytowy EPS[1]
LOGmanager-VF maszyna wirtualna z 8, 16 lub 128GB przestrzeni dyskowej na platformie Hyper-V lub VMWARE. (1 rok SW renewal)							
2*vCPU	4GB	8/16/128GB vDisk	N/A	8/16/128GB	N/A;	9000	18000/10min
LOGmanager-HF platforma Intel NUC. (3 lata RMA, 1 rok SW renewal)							
1x2core Intel i3@2.6GHz	8GB	120GB	N/A	120GB	N/A;	9000	18000/10min
LOGmanager WorkLoad Accelerator[2] (Natywnie zintegrowany z LOGmanager-XL i jako opcjonalny komponent dla LOGmanager-L)							
LOGmanager-A moduł NVMe 3.2TB przyśpieszający procesowanie danych w LOGmanager-XL oraz opcjonalnie w LOGmanager-L.							
EPS[1] - Zdarzenia Na Sekundę, liczone dla surowego logu (format RAW) o średnim rozmiarze 700Bajtów; Retencja danych - liczona dla 24h ciągłego procesowania							

Producent i Referencje

LOGmanager powstał w 2014 roku jako flagowy produkt Sirwisa A.S., Organizacji z siedzibą w Pradze. W momencie wydania tej broszury, LOGmanager został wdrożony u ponad 160 klientów – wybrane referencje można znaleźć na stronie www.logmanager.pl . Do grona klientów zaliczają się nie tylko jednostki Rządowe, ale także Organizacje komercyjne każdego rozmiaru i branży, korporacje, banki i inne. Chętnie dostarczymy kontakt do obecnych klientów, którzy zgodzili się na włączenie do listy referencji LOGmanager.