LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Studium Przypadku - G.EN. GAZ Energia

Informacje o Firmie

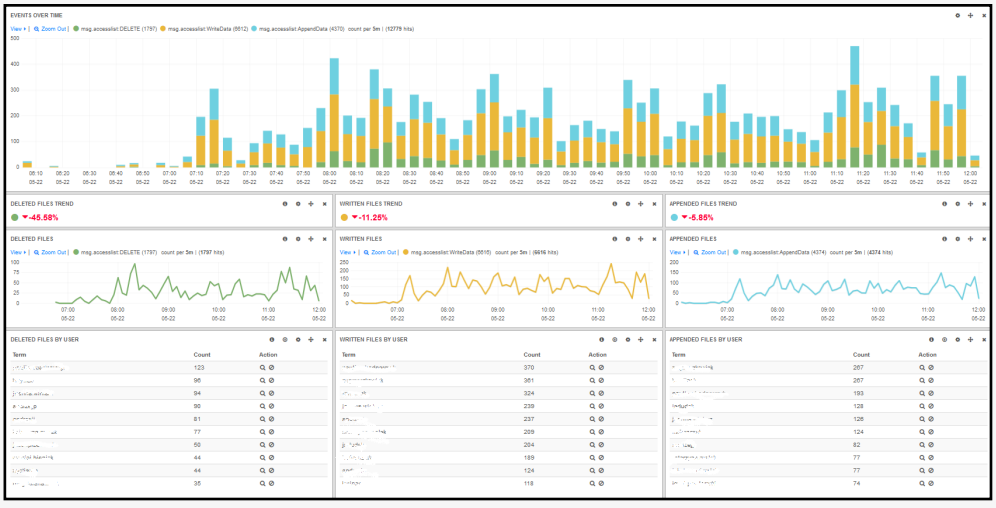
G.EN. GAZ ENERGIA Sp. z o.o. to największy prywatny dystrybutor gazu ziemnego w Polsce, obejmujący obszar 87 gmin w 5 województwach, posiadający około 40,000 klientów i mogący pochwalić się wynikami sprzedaży na poziomie 1 mln MWh gazu ziemnego w 2019 roku.

Wyzwania

Dział Informatyczny Klienta zarządzający setkami systemów, potrzebował rozwiązania, które pozwoliłoby na agregację informacji pochodzących z rozproszonego środowiska oraz prowadzenie analiz zaistniałych zdarzeń/incydentów bezpieczeństwa związanych z dostępem do wewnętrznych zasobów plikowych w różnych lokalizacjach. Dodatkowo Klientowi zależało na rozwiązaniu, które umożliwiłoby przechowywanie danych w sposób niezmieniony. Wysoka wydajność, szybki proces wdrożenia i brak ograniczeń licencyjnych były dodatkowymi atutami które Klient brał pod uwagę.

Podczas 4 tygodniowego okresu trwania testów, Klient pozytywnie ocenił działanie platformy LM, łatwość obsługi, brak ograniczeń licencyjnych oraz elastyczność, pozwalającą na zbierane danych z szerokiej gamy systemów, co pozwoliło na podjęcie decyzji o zakupie platformy LOGmanager.

Jako alternatywę klient rozważał zakup rozwiązania typu SIEM, jednakże po głębszej analizie systemy te okazały się nieodpowiednie ze względu na skomplikowaną obsługę i utrzymanie oraz wysokie koszty związane z zakupem licencji.



LOGmanager—Fazy Implementacji

I. Faza

W pierwszej fazie projektu wykonana została instalacja "Proof of Concept" na urządzeniu demo dostarczonym bezpośrednio do Klienta. Celem PoC była weryfikacja możliwości zaadresowania potrzeb Klienta oraz odpowiednie wyskalowanie platformy LOGmanager.

II. Faza

W kolejnej fazie, na platformie demo LOGmanager skonfigurowane zostały spersonalizowane dashboardy (prezentujące dane w formie wykresów) oraz alerty związane z bezpieczeństwem danych, monitorujące masowe kasowanie plików w zadanym interwale czasowym. Dodatkowo, testy PoC obejmowały konfigurację regularnych raportów dotyczących dostępu do kluczowych plików, a także wykonana została optymalizacja ilości zbieranych informacji.

III. Faza

Do klienta dostarczony został model LOGmanager-M, a instalacja rozwiązania obejmowała skonfigurowanie brakujących źródeł (m.in. VMware oraz Windows). Wdrożenie odbyło się bez ingerencji w infrastrukturę produkcyjną klienta. Dodane zostały także alerty, rozszerzające funkcjonalność platformy, pozwalające na monitorowanie kont użytkowników pod kątem bezpieczeństwa np. wprowadzanie zmian na kontach użytkowników, nieudane próby logowania czy zablokowane konta.

KORZYŚCI DLA KLIENTA

LOGmanager w pełni spełnił wymagania klienta, a dzięki profesjonalnemu podejściu oraz ciągłemu wsparciu dostarczanemu przez Advatech (certyfikowany partner), system został szybko i bezproblemowo wdrożony, a następnie zmigrowany ze środowiska testowego do produkcyjnego.

LOGmanager jest wykorzystywany przez administratorów do nadzorowania infrastruktury, m.in. platformy wirtualizacji VMware i do rozwiązywania codziennych problemów operacyjnych. Najczęściej wykorzystywane funkcjonalności obejmują zbieranie, analizę i raportowanie aktywności użytkowników na kluczowych plikach, szybkie wyszukiwanie i filtrowanie informacji operacyjnych (np. stan urządzenia) niezbędnych do rozwiązywania problemów oraz automatyczne powiadomienia dotyczące wykrycia wystąpienia zdefiniowanych zdarzeń (np. wiele nieudanych prób logowania).

KLIENT DOCENIA:

⇒ Krótki proces wdrożenia z weryfikacją funkcjonalności przed zakupem oraz natychmiastową gotowość systemu do działania.
⇒ Łatwy dostęp do zdarzeń z systemów plików (kto i kiedy edytował/usuwał/kopiował dane).
⇒ Wsparcie w procesie diagnostyki i rozwiązywania incydentów bezpieczeństwa.
⇒ Bezpieczeństwo przechowywania dowodów incydentów bezpieczeństwa.
⇒ Efektywne wsparcie w rozwiązywaniu codziennych problemów z infrastrukturą.
⇒ Brak ograniczeń licencyjnych.
⇒ Transparentność, wysoką wydajność oraz minimalne wymagania operacyjne.

OPINIA KLIENTA:

"Ze względu na permanentny brak czasu związany z dużym nakładem zadań poszukiwaliśmy rozwiązania które ułatwi naszą pracę, zamiast ją komplikować. Konkurencyjne produkty, pomimo tego że skuteczne, nie wpisywały się w tę konwencję. LOGmanager idealnie zaadresował nasze potrzeby—jest prosty w obsłudze i utrzymaniu przy jednoczesnym zachowaniu kluczowych funkcjonalności."

- Artur Lech, Kierownik Sekcji Informatycznej

O PRODUCENCIE ORAZ REFERENCJE

LOGmanager istnieje od 2014 roku jako flagowy produkt Sirwisa a.s., firmy z siedzibą w Pradze. W dniu wydania tego Case Study, LOGmanager został wdrożony u ponad 160 zadowolonych klientów – wybrane referencje dostępne są na stronie **www.logmanager.pl**. Nasi klienci pochodzą z każdego sektora rynku, od organizacji rządowych, przez korporacje, banki, telekomunikację, e-commerce i inne. Zachęcamy do kontaktu w celu poznania szczegółowych referencji z Twojego obszaru zainteresowania.