LOGmanager

> Central Log Repository
> Affordable SIEM

4SYNC

HELP TO RESOLVE CRITICAL IT INCIDENT

Studium Przypadku - Budimex

Informacje o Firmie

Budimex SA jest spółką z pięćdziesięcioletnią tradycją, która ma znaczący udział w rozwoju gospodarczym Polski. Firma zrealizowała tysiące nowoczesnych inwestycji infrastrukturalnych, kubaturowych i przemysłowych. Kultura innowacyjności, doskonalenie i kierowanie się zasadami zrównoważonego rozwoju pozwoliły Budimeksowi zdobyć pozycję lidera polskiego rynku budowlanego. Firma stopniowo zwiększa swoje zaangażowanie w sektorze facility management (obsługa nieruchomości i obiektów infrastruktury) oraz gospodarki odpadami. Budimex SA od 1995 roku jest notowany na warszawskiej GPW, a od 2011 roku wchodzi w skład indeksu RESPECT – najbardziej odpowiedzialnych spółek giełdowych. Inwestorem strategicznym spółki jest hiszpańska firma o globalnym zasięgu – Ferrovial.

Wyzwania

Początkowo klient nie wyrażał zdecydowanego zainteresowania rozwiązaniem do zarządzania logami, ale prezentacja produktu w której brali udział jej przedstawiciele sprawiła, że podjęto decyzję o przeprowadzeniu testów i ocenie przydatności we własnej infrastrukturze.

Klientowi zależało na prostocie działania oraz sprawnej obsłudze źródeł logów. W trakcie testów okazało się, że jeden z istotnych systemów klienta nie jest jeszcze natywnie wspierany przez system LOGmanager, dlatego też klient poprosił o zaprezentowanie możliwości produktu pod kątem obsługi nowych typów źródeł. Po dwóch godzinach od otrzymania reprezentatywnej próbki logów powstała pierwsza wersja parsera umożliwiająca kontynuowanie testów, a po tygodniu dostarczony został końcowy, oficjalnie wspierany parser dla tego typu źródła logów.

Podczas miesięcznego okresu trwania testów klient ocenił pozytywnie: działanie platformy LM, przydatność w rozwiązywaniu problemów operacyjnych IT, wsparcie w optymalizacji działania infrastruktury pod kątem bezpieczeństwa oraz łatwość obsługi i elastyczność.

LOGmanager—Fazy Implementacji

I. Faza

W pierwszej fazie projektu wykonana została instalacja urządzenia demo dostarczonego bezpośrednio do klienta. Celem uruchomienia instalacji testowej była weryfikacja możliwości zaadresowania potrzeb klienta oraz odpowiednie wyskalowanie platformy LOGmanager.

II. Faza

Poza wykorzystaniem LM do standardowych zadań i potwierdzeniu jego przydatności do powiadamiania o zdarzeniach czy analizie incydentów, klient wykorzystał także rozwiązanie do dokładnego przeanalizowania logów z najważniejszych źródeł. Przeprowadzona analiza w formie wizualizacji danych pomogła zoptymalizować m.in. konfigurację zapór sieciowych, poprawiając tym samym poziom bezpieczeństwa infrastruktury.

III. Faza

Czas realizacji był dla klienta kluczowy, dlatego zamówiony model LOGmanager-XL został dostarczony w dwa tygodnie od momentu otrzymania zamówienia. Następnie dzięki prostocie obsługi systemu klient samodzielnie zainstalował i skonfigurował rozwiązanie do użytku produkcyjnego, a następnie przeprowadził migrację danych zgromadzonych podczas testów na urządzeniu demo.

KORZYŚCI DLA KLIENTA

Pomimo braku wcześniejszego zapotrzebowania na rozwiązanie do zarządzania logami, klient docenił przydatność i skuteczność systemu LOGmanager. Dzięki kompetencjom i profesjonalnemu wsparciu inżyniera 4Sync (certyfikowany VAD), rozwiązanie zostało szybko i efektywnie przetestowane, co umożliwiło podjęcie decyzji o zakupie. LOGmanager jest na co dzień wykorzystywany przez administratorów do bieżącego monitorowania kondycji środowiska oraz informowania o najistotniejszych zdarzeniach. Najczęściej wykorzystywane funkcjonalności obejmują monitorowanie kondycji systemów bezpieczeństwa oraz systemów realizujących zdalny dostęp pracowników do infrastruktury wewnętrznej.

KLIENT DOCENIA:

⇒ Wizualizacje ułatwiające analizę informacji z systemów bezpieczeństwa.

⇒ Łatwość obsługi umożliwiająca samodzielną instalację i konfigurację produktu, bez konieczności angażowania zespołów w długotrwałe wdrożenie i szkolenia.

⇒ Szybkie wsparcie w procesie dołączania nowych źródeł.

⇒ Prostotę architektury.

OPINIA KLIENTA:

"Prosta architektura systemu LOGmanager, oparta o jedno urządzenie pomogła szybko uruchomić kolekcjonowanie logów z wielu systemów. Możliwość przesyłania części logów do innych systemów była dla naszego działu kluczową funkcjonalnością. Rozwiązanie pozwala wzbogacać zdarzenia o dodatkowe informacje w postaci tagów. Dzięki intuicyjnemu interfejsowi GUI przeglądanie i wyszukiwanie logów różnego typu nie jest skomplikowane. Dużą korzyścią jest wsparcie udzielane przez polskich inżynierów producenta oraz dystrybutora 4Sync. Szkolenie przeprowadzone w naszej firmie oraz treści edukacyjne dostępne przez YouTube umożliwiły nam szybkie przeszkolenie zespołu i dogłębne poznanie systemu."

Michał Jobski — Dyrektor Biura Systemów Korporacyjnych

O PRODUCENCIE ORAZ REFERENCJE

LOGmanager jest rozwijany od 2014 roku jako flagowy produkt Czeskiej firmy Sirwisa a.s. Baza klientów LOGmanager składa się z organizacji o różnych wielkościach i profilu działalności: finanse, bankowość, telekomunikacja, e-commerce, a także jednostki rządowe, uniwersytety, publiczna telewizja itd. Wybrane case study można znaleźć na stronie www.logmanager.pl, a w przypadku zainteresowania prosimy o kontakt, na życzenie udostępnimy bardziej szczegółowe referencje od naszych obecnych klientów z wybranego sektora.