LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Studium Przypadku - Szpital Jihlava

Informacje o Firmie

Szpital Jihlava jest jednostką budżetową utworzoną przez region Vysočina. Zatrudnionych jest tutaj ponad 1,500 osób i jest to największy szpital w regionie,. Jako szpital rejonowy, w zależności od specjalizacji, obsługuje od 200 000 do nawet 500 000 mieszkańców regionu. Oferuje 621 łóżek na intensywnej terapii, 75 łóżek pozabiegowych oraz 10 łóżek do opieki paliatywnej. Szpital jest głównie odpowiedzialny za świadczenie opieki zdrowotnej, w tym diagnostyki szpitalnej i ambulatoryjnej, leczenie, profilaktykę oraz usługi aptekarskie. Dodatkowo, szpital prowadzi również badania naukowe, działania edukacyjne i informacyjne oraz inne działania związane z działalnością zakładu opieki zdrowotnej.

Wyzwania napotykane przez Firmę

Departament Informatyki w Szpitalu Jihlava obecnie zarządza dziesiątkami systemów IT, łącznie z tysiącem różnych komponentów programowych i sprzętowych. W specyfikacji zamówienia klient zażądał możliwości zbierania informacji o statusie z zarządzanych urządzeń, w tym w szczególności z elementów bezpieczeństwa i sieci a także przechowywania informacji w archiwach. Najważniejszym, kluczowym kryterium była wysoka wydajność tego rozwiązania oraz oferowana pojemność przechowywania danych. Klient preferował produkt krajowy, który miałby obsługę w języku czeskim. Wielką zaletą programu LOGmanager, opisywanego już w studium, była jego bardzo korzystna cena. Zazwyczaj duży system SIEM jest rozwiązaniem nieodpowiednim, bo zbyt skomplikowanym i nieosiągalnym finansowo dla organizacji tego typu. Z kolei LOGmanager zapewnia rozwiązanie dopasowane do potrzeb i dostępne, mogące być dobrą "kartą przetargową" w ramach procedury zamówień publicznych.

Zakres projektu oraz OPIS

Priorytetem klienta była poprawa bezpieczeństwa sieci teleinformatycznej (IT), łącznie z wszystkimi jej podsystemami. Fakt ten został też uwzględniony podczas procesu wdrażania. Instalacja całego sprzętu trwała około 4-5 godzin, po czym wszelkie ustawienia zostały zdefiniowane zgodnie z wymaganiami klienta, uwzględniając najpierw zapory firewall oraz pozostałe elementy sieciowe. Po tym, jak LOGmanager działał przez miesiąc, klient przy wsparciu wykonawcy przeprowadził odpowiedni tuning systemu. Na etapie wdrożenia, pracownicy szpitala zapoznali się z tematem normalizacji logów i alarmów, ponieważ stopniowo wdrażano je do rozwiązania. Podczas implementacji odkryto wiele nieznanych i trudnych do zidentyfikowania logów, w przypadku których konieczne było określenie odpowiednich reguł, aby umożliwić efektywne wykorzystanie zawartych w nich informacji. Wdrażanie programu LOGmanager jest procesem ciągłym, który musi się stale dostosowywać do rosnących wymagań w zakresie ruchu danych (ilość danych klienta rośnie o kilkadziesiąt GB dziennie) oraz do rozwoju i zmian w środowisku IT. W szpitalu w Jihlavie LOGmanager okazał się niedrogim, ale jednocześnie wysokiej jakości systemem do zarządzania logami oraz rozwiązaniem SIEM.

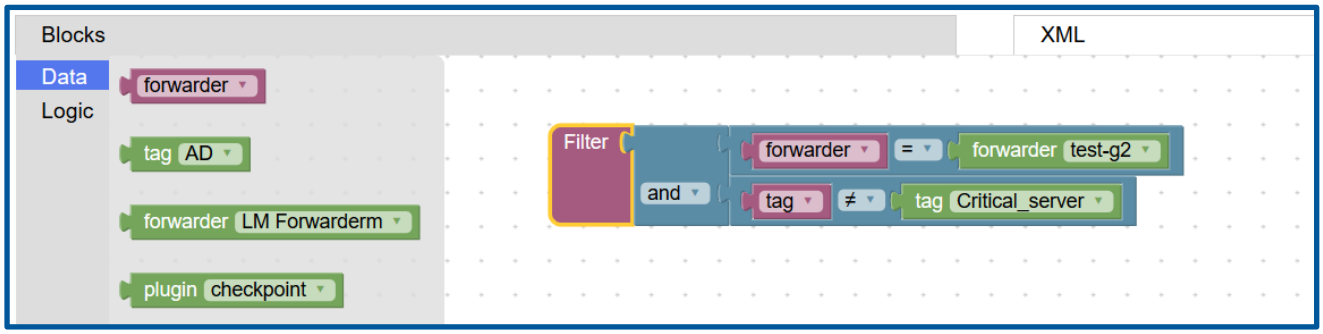
Korzyści dla klienta oraz najważniejsze funkcje

LOGmanager może być w prosty sposób zintegrowany z istniejącymi już środowiskami operacyjnymi w celu obsługi zbierania danych maszynowych z dowolnego systemu źródłowego w organizacji. Łatwość integracji jest jedną z mocnych stron tego produktu. Integracja z różnymi systemami zapewnia opcję zapisywania (rejestrowania) oraz prezentacji w przystępnej formie graficznej lub tekstowej zdarzeń i logów z dowolnych aktywnych elementów sieci, urządzeń bezpieczeństwa, systemów operacyjnych lub aplikacji. Prostota i łatwość użycia rozwiązania pozwalają na dostarczanie informacji i wysyłanie alertów zgodnie z wymaganiami administratorów ICT.

Dzięki szybkości wyszukiwania i analizy logów LOGmanager doskonale spełnił oczekiwania klienta. Klient docenił także prostotę aktualizacji systemu i dostęp do Webinarów, dających mu możliwość pozyskania informacji o zmianach i nowościach oraz innych informacjach technicznych od twórców LOGmanager. Kolejną korzyścią dla klienta jest pełna dostępność logów z zapór firewall i pozostałych elementów sieciowych, z równoczesnym zapewnieniem długoterminowej ich retencji. Dzięki wdrożeniu rozwiązania LOGmanager wykryto także przypadki naruszenia zabezpieczeń, w tym m.in. podszywania się pod serwer DHCP oraz ataku polegającego na wykorzystaniu urządzeń sieciowych klienta jako koparki do kopania kryptowalut.

Które funkcje są najbardziej doceniane przez szpital Jihlava

- ⇒ Szybkie wdrożenie
- ⇒ Wysoka wydajność, długie przechowywanie danych , prosty backup
- ⇒ Łatwa identyfikacja głównych przyczyn awarii systemu na podstawie logów przekazywanych przez systemy do LOGmanagera
- ⇒ Identyfikacja awarii i wysyłanie automatycznych alertów w czasie rzeczywistym
- ⇒ Dopasowane do potrzeb klienta zapytania, wykresy, raporty i panele kontrolne
- ⇒ Szybka identyfikacja zdarzeń opisujących przyczynę określonego problemu, utratę danych lub awarię komunikacji
- ⇒ Dokumentacja źródłowa do audytów bezpieczeństwa
- ⇒ Możliwość ograniczenia praw dostępu i filtrowania danych pokazywanych nieuprzywilejowanym użytkownikom



INFORMACJE NA TEMAT WYKONAWCY ORAZ REFERENCJE KLIENTÓW

LOGmanager powstał w 2014 roku i jest to flagowy produkt firmy Sirwisa a.s., z siedzibą w Pradze. Do momentu wydania tego studium przypadku, LOGmanager działał już u ponad 140 zadowolonych klientów, których referencje można znaleźć na stronie www.logmanager.pl. Naszymi klientami są nie tylko instytucje rządowe, ale także firmy dowolnej wielkości ze wszystkich sektorów takich jak korporacje biznesowe, organizacje bankowe i wiele innych. Nie wahaj się, jeśli chcesz się z name skontaktować. Uzyskasz szczegółowe referencje klientów bezpośrednio z Twojej branży.