LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

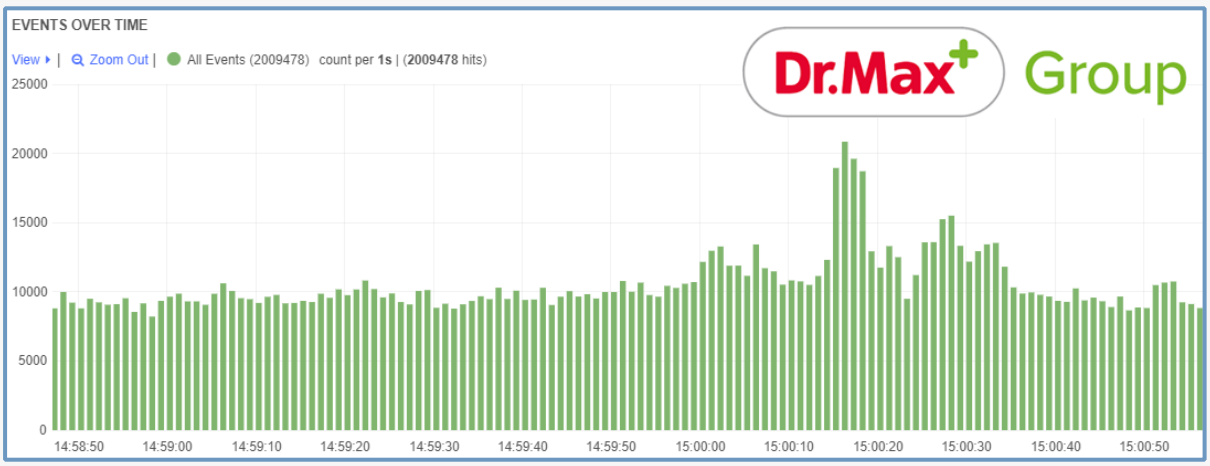
# Studium Przypadku - Dr.Max

## Informacje o Firmie

Dr.Max to najpopularniejsza sieć aptek w Czechach. W skład organizacji wchodzi ponad 400 aptek i 3 000 pracowników. Grupa Dr.Max jest także obecna w 7 innych krajach Europy, w tym w Polsce.

## Wyzwania

Grupa Dr.Max zarządza mocno zróżnicowanym środowiskiem IT, które wspiera nie tylko apteki i magazyny, ale także cały proces dystrybucji, produkcji i rozwoju leków. Infrastruktura IT Dr.Max składa się z wielu serwerów, stacji roboczych, baz danych, aplikacji oraz rozbudowanej sieci łączącej to wszystko w całość. Każdy z posiadanych przez Dr.Max systemów generuje duże ilości istotnych danych maszynowych dotyczących wydajności, błędów, bezpieczeństwa czy aktywności użytkowników i administratorów. Z powodu braku scentralizowanego dostępu do logów, zespoły odpowiedzialne za zarządzanie infrastrukturą klienta miały ogromny problem z efektywnym rozpoznawaniem i rozwiązywaniem problemów – również tych związanych z bezpieczeństwem. W odpowiedzi na te wyzwania oraz w celu osiągnięcia pełnego wglądu w zdarzenia mające miejsce w infrastrukturze, została podjęta decyzja o zunifikowaniu miejsc zbierania i przechowywania logów do pojedynczego rozwiązania. Klientowi zależało na systemie wspierającym przechowywanie logów przez długi czas, zapewniającym jednocześnie bezpieczeństwo danych poprzez brak możliwości ich modyfikacji oraz udostępniającym przejrzysty i elastyczny interfejs, prezentujący zbierane dane w przyjaznej formie. Dodatkowym wymogiem dla poszukiwanego systemu był brak jakichkolwiek ograniczeń licencyjnych (np. ilość procesowanych logów w jednostce czasu czy maksymalna ilość monitorowanych urządzeń) oraz możliwość obsługi dużej liczby zdarzeń na sekundę.



## LOGmanager—Fazy Implementacji

I. Faza

Celem pierwszej fazy była weryfikacja parametrów technicznych rozwiązania. Do testów dostarczony został LOGmanager-M z zasobami dyskowymi o rozmiarze 12TB. Podczas instalacji system został zintegrowany z Active Directory klienta, aby umożliwić logowanie użytkowników bez konieczności manualnego tworzenia kont w systemie. Następnie wybrane systemy klienta zostały skonfigurowane do wysyłania logów do LOGmanagera w celu weryfikacji jego wydajności oraz możliwości analitycznych.

II. Faza

Celem drugiej fazy było wdrożenie produkcyjne. Dostarczony LOGmanager-XL o rozmiarze 100TB został uruchomiony w klastrze z maszyną dostarczoną w Fazie I. Po zakończeniu replikacji danych pomiędzy oboma elementami klastra, LOGmanager-M został odłączony, a LOGmanager-XL został przełączony w tryb produkcyjny.

III. Faza

Wybrane aplikacje i serwery zostały skonfigurowane do wysyłania logów do LOGmanagera, a następnie tam, gdzie było to konieczne (np. dla aplikacji autorskich) zostały utworzone odpowiednie parsery. Ze względu na ekstremalnie wysoką ilość zdarzeń generowanych z systemów bezpieczeństwa klienta, proces zbierania danych został zoptymalizowany, umożliwiając ciągłe procesowanie 10 000 zdarzeń na sekundę (do 25 000 zdarzeń na sekundę w szczycie). Dziennie jest procesowane około 250-350GB danych.

IV. Faza

W końcowej fazie projektu przeprowadzony został trening dla administratorów, specjalistów wsparcia IT oraz reszty zespołów IT, skupiony na obsłudze systemu i tworzeniu własnych parserów. Dodatkowo przeprowadzonych zostało kilka warsztatów, adresujących specyficzne potrzeby każdego z zespołów.

# KORZYŚCI DLA KLIENTA

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

LOGmanager jest wykorzystywany przez zespół bezpieczeństwa do prowadzenia nadzoru nad infrastrukturą, a także przez administratorów i specjalistów wsparcia IT do rozwiązywania codziennych problemów operacyjnych. Najczęściej wykorzystywane funkcjonalności obejmują zbieranie i analizę aktywności użytkowników, 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 także możliwość tworzenia elastycznych dashboardów, prezentujących zbierane logi w logicznej formie grafów i wykresów, a także, dzięki użyciu Blockly, prosty sposób na pisanie własnych parserów, niezbędnych do poprawnej obsługi logów z aplikacji autorskich.

## KLIENT DOCENIA:

⇒ Krótki proces wdrożenia z weryfikacją funkcjonalności przed zakupem oraz natychmiastową gotowość systemu do działania.
⇒ Korelację zdarzeń logon/logoff z całej infrastruktury.
⇒ Łatwy dostęp do zdarzeń z systemów plików (kto i kiedy edytował/usuwał/kopiował dane).
⇒ Możliwość monitorowania zmian wprowadzanych przez administratorów.
⇒ Wsparcie w procesie diagnostyki i rozwiązywania incydentów bezpieczeństwa.
⇒ Bezpieczeństwo przechowywania dowodów incydentów bezpieczeństwa.
⇒ Efektywne wsparcie w rozwiązywaniu codziennych problemów z infrastrukturą.
⇒ Łatwość integracji systemów nie wspieranych natywnie przez LOGmanager.
⇒ Zunifikowany i prosty w wykorzystaniu interfejs.
⇒ Transparentność, wysoką wydajność oraz minimalne wymagania operacyjne.
⇒ Granularny dostęp do danych (możliwość ograniczenia dostępu do danych wybranym grupom użytkowników).

# 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.