LOGmanager

> Central Log Repository
> Affordable SIEM

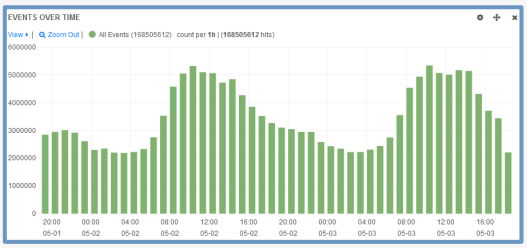
HELP TO RESOLVE CRITICAL IT INCIDENT

# Studium Przypadku ČD Cargo a.s.

## Informacje o Firmie

ČD Cargo a.s. ("ČDC") jest największym czeskim przewoźnikiem towarowym. ČDC jest spółką zależną krajowego przewoźnika České dráhy, a.s. Obie firmy, wraz z innymi spółkami zależnymi, należą do grupy ČD. ČD Cargo a.s. została założona 1 grudnia 2007 r. i zatrudnia 7000 pracowników. Obsługuje 859 lokomotyw i ponad 24 000 wagonów towarowych. Pod względem wielkości przewożonych towarów plasuje się w Unii Europejskiej wśród pięciu największych przewoźników kolejowych.

## Wyzwania napotykane przez Firmę




Środowisko ICT w ČDC składa się z wielu podsystemów, między innymi finansowych, księgowych, operacyjnych, technologicznych oraz wielu aplikacji o różnym stopniu współzależności. Łącznie obejmuje ona dziesiątki fizycznych i wirtualnych serwerów, obsługiwanych na platformach wiodących producentów takich jak Microsoft, Oracle, SAP, a także rozwiązań typu open source. Większość kluczowych aplikacji obsługiwana jest przez spółkę siostrzaną ČDC. Niektóre z podsystemów są obsługiwane bezpośrednio przez ČDC, przy użyciu własnych zasobów i aktywów, podczas gdy inne są zlecane do zewnętrznych dostawców. ČDC nie jest właścicielem znacznej części wykorzystywanej infrastruktury teleinformatycznej. Najczęściej korzysta z owej struktury jako usługi świadczonej przez swojego partnera, ČD Telematika. Ze względu na złożoność infrastruktury teleinformatycznej oraz na stosunki umowne między ČDC a jej dostawcami usług, ČDC często brakowało przejrzystości zarządzania i operowania systemami zlecanymi na zasadzie outsourcingu.

Klienci zarządali by mogli korzystać z przechowywanych logów, w celu uzyskania kompleksowego przeglądu bezpieczeństwa i statusu operacyjnego swojego środowiska teleinformatycznego, aby móc reagować na pojawiające się nowe wydarzenia i incydenty oraz aby mieć możliwość śledzenia informacji o działaniach i transakcjach wpływających na dane oraz konta i uprawnienia użytkowników. Klienci potrzebowali repozytorium logów, które zapewniłoby długoterminowe przechowywanie łatwo dostępnych informacji zabezpieczonych przed ingerencją, co w konsekwencji pozwalałoby uzyskać przegląd aktualnego stanu obsługiwanych systemów oraz dostęp do poszczególnych aplikacji. Kolejnym atutem byłaby możliwość dokładnego nadzorowania działań wykonywanych przy użyciu uprzywilejowanych kont. Dodatkowym wymogiem było to, aby wybrane rozwiązanie nie było związane z żadnymi ograniczeniami licencyjnymi, takimi jak maksymalna liczba zdarzeń przetwarzanych w określonej jednostce czasu lub maksymalna liczba monitorowanych urządzeń. LOGmanager został wybrany jako najlepsze rowzwiązanie.Poza centralizacją i długoterminowym przechowywaniem logów z wybranych technologii i systemów, firma ČDC zidentyfikowała także konta użytkowników w poszczególnych repozytoriach tożsamości jako priorytetowy obszar główny, który jest monitorowany i analizowany na początkowym etapie projektu przez program LOGmanager. Szczegółowe wymagania klienta:

### Śledzenie i ocena logów SAP

- ⇒ Pomyślne i nieudane próby logowania użytkownika
- ⇒ Najważniejsze operacje
- ⇒ W przypadku kont utworzonych dla pracowników ČDC i dla personelu zewnętrznego, mających dostęp do części systemu ČDC: tworzenie i usuwanie konta, przypisywanie i usuwanie ról

### Śledzenie i ocena logów na serwerze LDAP

- ⇒ Pomyślne i nieudane próby logowania użytkownika
- ⇒ Pomyślne i nieudane logowanie się na konta uprzywilejowane (w tym konta dostawców)
- ⇒ Zarządzenie kontami: tworzenie konta, usuwanie konta, aktywacja konta, dezaktywacja konta, przypisywanie oraz usuwanie ról

### Aplikacje kadrowo-płacowe

- ⇒ Pomyślne i nieudane próby logowania użytkownika
- ⇒ Pomyślne i nieudane zalogowanie się na konta uprzywilejowane (w tym konta dostawców)
- ⇒ Kluczowe operacje na danych osobowych

### Active Directory

- ⇒ Pomyślne i nieudane próby logowania użytkownika
- ⇒ Pomyślne i nieudane logowanie się na konta uprzywilejowane (w tym konta dostawców)
- ⇒ Najważniejsze operacje

# ZAKRES PROJEKTU ORAZ OPIS

## Etap I

Urządzenia LOGmanager z pojemności kilkudziesięciu TB do przechowywania logów zostały dostarczone. Zostały one zainstalowane w środowisku ČDC, zgodnie z dostarczonym planem adresowym. Aby zapewnić wysoką dostępność klastra składającego się z dwóch instalacji LOGmanager, urządzenia zostały zainstalowane w dwóch osobnych lokalizacjach. Natychmiast po instalacji, w odpowiednich centrach danych instalacje LOGmanager zostały skonfigurowane w klastrze. Oba urządzenia w klastrze są kontrolowane za pośrednictwem jednego interfejsu WWW. Podczas początkowej instalacji, uwierzytelnianie użytkowników programu LOGmanager zostało zmapowane do usługi Active Directory.

## Etap II

Wybrane aplikacje i serwery zostały skonfigurowane tak, aby wysyłać logi do LOGmanagera, który stale je gromadzi i przechowuje. Gdy log staje się dostępny w LOGmanager, tworzą się określone parsery. Parser działa jak "Translator", co oznacza, że konwertuje dane dostarczane do urządzenia w formatach natywnych (RAW) do znormalizowanego, łatwego do przesukiwania znormalizowanego formatu, który umożliwia korzystanie z dodatkowych zaawansowanych funkcji, takich jak alarmowanie, system przewidywania zachowań, korelacja i raportowanie.

## Etap III

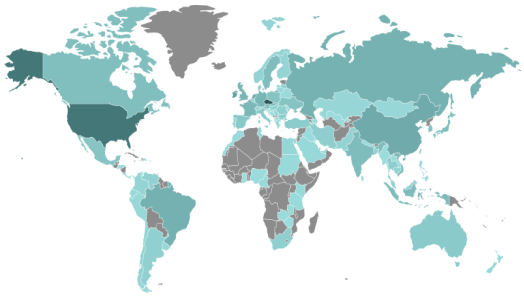
Zorganizowano szkolenia dla administratorów, zespołu wsparcia i pracowników działu IT, koncentrując się na sposobie korzystania z systemu i tworzeniu nowych analizatorów składni i alertów.

# KORZYŚCI DLA KLIENTA ORAZ NAJWAŻNIEJSZE FUNKCJE

System spełnił wszystkie wymagania klienta. Służy przede wszystkim jako narzędzie wsparcia dla techników IT, administratorów oraz do zarządzania bezpieczeństwem. Jednak jego wdrożenie nie kończy się wraz z początkową implementacją. W kolejnych krokach zostaną dodane inne aplikacje i systemy, które nie były częścią początkowego projektu. Ta ciągła rozbudowa jest możliwa dzięki otwartej architekturze LOGmanagera, która ułatwia tworzenie dedykowanych raportów, pulpitów i widoków dla każdego monitorowanego systemu a dzięki prostym do stworzenia analizatorom składni umożliwia także przetwarzanie informacji z systemów i aplikacji generujących nietypowe logi. System LOGmanager został łatwo zintegrowany z istniejącym, złożonym i niejednorodnym środowiskiem teleinformatycznym w ČDC. Klienci wysoko cenią sobie kompleksowe pobieranie i przetwarzanie rozszerzonych logów z systemów Microsoft, możliwość szybkiego pobierania i filtrowania niezbędnych informacji z ogromnej ilości logów, możliwość otrzymywania automatycznych powiadomień o wszelkich nieprawidłowościach oraz zdolność rozumienia logów z obsługiwanej infrastruktury sieciowej, w tym urządzeń zabezpieczających.

## Które funkcje są najbardziej doceniane przez ČDC

- ⇒ Diagnostyka błedów lub problemów działania indywidualnych aplikacji w środowisku ČDC ICT
- ⇒ Prognozowanie i zapobieganie incidentom, naruszeniom bezpieczeństwa danych, przegląd nietypowych i podejrzanych transakcji, naruszeniom dostępu itp.
- ⇒ Możliwość monitorowania zmian przez zewnętrznych i wewnętrznych administratorów i operatorów systemu
- ⇒ Gromadzenie logów generowanych przez systemy informatyczne i przechowywanie ich w niezależnym, odpornym na modyfikację i kontrolowanym rejestrze a przez to zapewnienie dostępu do wiarygodnych danych niezbędnych z punktu widzenia bezpieczeństwa i spełnienia wymagań prawnych. Logi mogą być użyte do monitorowania i analizy operacji wykonywanych przez użytkowników systemów (zarówno autoryzowanych jak i nieautoryzowanych)
- ⇒ Diagnozowanie i rozwiązywanie problemów związanych z bezpieczeństwem
- ⇒ Śledzenie dostępu, aktywności użytkownika, wypełniania umów SLA, spełnienie wymagań audytowych itp.
- ⇒ Udostępnianie dowodów z analizy kryminalistycznej podczas śledztwa związanego z naruszeniem bezpieczeństwa
- ⇒ Monitorowanie zgodności oraz audyt



# 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 130 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. Chętnie przekażemy Ci informacje o naszych obecnych klientach, którzy wyrazili zgodę na umieszczenie ich na naszej liście referencji.