LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Studium Przypadku - Telco Pro Services S.A., członek grupy CEZ

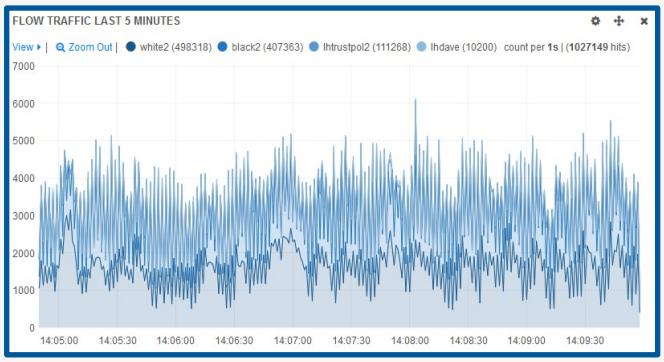
O Firmie

Telco Pro Services S.A. jest operatorem telekomunikacyjnym, którego działalność koncentruje się przede wszystkim na świadczeniu usług telekomunikacyjnych dla klientów na rynku czeskim, głównie dla spółek Grupy ČEZ. Ich portfolio obejmuje zarówno usługi komunikacji publicznej, jak i usługi ukierunkowane na klienta indywidualnego. Ich zasięg działania sprawił, że firma ma dominującą pozycję na rynku telekomunikacyjnym. Firma posiada i prowadzi rozległe systemy telekomunikacyjne, tworząc techniczną bazę dla szerokiej gamy usług głosowych oraz transmisji danych. Znaczna część z nich składa się z telekomunikacji dostosowanej do potrzeb klientów z sektora energetycznego i jest wykorzystywana między innymi do systemów przemysłowych, zapewniających obsługę sterowania dyspozytorskiego w zakresie wytwarzania i dystrybucji energii elektryczne.

Co oferuje klientom?

Telco Pro Services S.A. jest operatorem telekomunikacyjnym dysponującym rozległą infrastrukturą opartą zarówno na klasycznej technologii do przesyłania danych i usług głosowych TDM (PDH / SDH, sieć cyfrowych centrali PBX, w tym przekierowania ruchu), jak i zaawansowanych sieciach danych zbudowanych na uniwersalnej platformie architektury wielosystemowej (MPLS). Firma świadczy głównie następujące usługi :

- Publiczny dostęp do usług łączności elektronicznej
- Zapewnienie dostępu do transmisji danych i głosu w sieciach korporacyjnych
- Przesyłanie danych w celu kontroli działania systemów
- Dzierżawa obwodów informatycznych, usługi dostępne dla operatorów i dostawców usług internetowych.
- Systemy sterowania dla energetyki
- Zarządzanie obsługiwanymi/posiadanymi technologiami klienta



LOGmanager został przede wszystkim wybrany w celu zapewnienia zgodności z ustawą nr 181/2014 Dz. i służy jako technologia wspierająca działanie Infrastruktury Krytycznej IT (CII), która jest zarządzana przez firmę. Dane zdarzeń operacyjnych, które są wysyłane do LOGmanagera za pomocą systemu CII, są zapisywane jako logi operacyjne, a system przekazuje dalej uzyskane dane do rozwiązania SIEM. Zapewnia to dostępność do informacji wymaganych do analizy zdarzeń i incydentów związanych z cyberbezpieczeństwem .

Implementacja LOGmanager w Telco Pro Services S.A.

LOGmanager zapewnia szybkie wdrożenie oraz wszechstronność, a także rozszerzenie zakresu widoczności całej heterogenicznej infrastruktury. Klient testował rozwiązanie przez dłuższy czas i doświadczenia były bardzo pozytywne - docenili szeroki zakres możliwości wykorzystania systemu oraz łatwość użytkowania dzięki intuicyjnemu interfejsowi graficznemu, co sprawiło że podjęli decyzje by wdrożyć rozwiązanie w całej swojej infrastrukturze. Teraz LOGmanager w pełni zaspokaja potrzeby klienta w zakresie zbierania danych o zdarzeniach operacyjnych z systemów telekomunikacyjnych, bezpieczeństwa i systemów pomocniczych. Dzięki prostej logice opartej na regułach, klient był w stanie niezależnie definiować struktury zdarzeń i reguły monitorowania poszczególnych technologii, co umożliwiło konfigurację powiadamiania o wybranych zdarzeniach wymagających uwagi operatora.

Obecnie system jest stosowany rutynowo przez kadry zarządzające i administratorów pojedynczych technologii, dla których spersonalizowano zasady wykrywania zdarzeń oraz pulpit i usługę powiadamiania. Dzięki wysokiej wydajności programu LOGmanager, łatwo możemy odnaleźć dane historyczne dotyczące pierwszych wystąpień zdarzenia, pobrać powiązane informacje z innych zasobów infrastrukturalnych lub znaleźć dodatkowy kontekst. Pojedyncze zespoły mogą korzystać ze swoich własnych środowisk, takich jak systemy do zarządzania firewall, monitorowanie zmian konfiguracji w zasobach telekomunikacyjnych, monitorowanie i raportowanie stanu platform serwerów HW, zarządzanie infrastrukturą AAA i wiele innych .

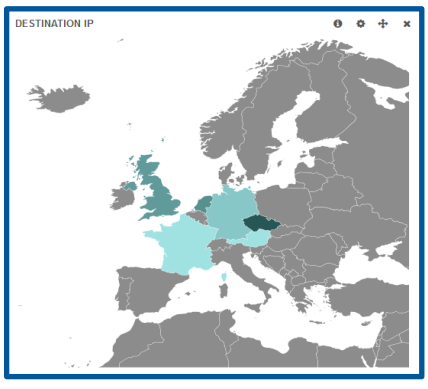
KORZYŚCI OSIĄGANE PRZEZ ODBIORCÓW I WYBRANE ZALETY

System jest zgodny z wymaganiami do pełnienia funkcji magazynu danych śledczych, gdzie dane są gromadzone przez ponad rok, w celu wsparcia analizy wydarzeń mających miejsce w przeszłości lub jako dowód w trakcie dochodzenia w sprawie naruszenia incydentów bezpieczeństwa cybernetycznego. Ze względu na gwarancję integralności i poufności danych, LOGmanager jest używany jako zaufane źródło informacji do zabezpieczania dowodów.

LOGmanager działa jako system do wspomagania i jest współdzielony przez poszczególne zasoby CII i inne środowiska pracy. Aby umożliwić działania operacyjne i zapewnić zgodność z ustawą nr 181/2014 Dz., system został opracowany w taki sposób, aby zapewniał pełnoprawne, funkcjonalne gromadzenie logów operacji bez żadnych ograniczeń licencyjnych. Został również zaprojektowany tak, aby działał wydajnie, intuicyjnie i żeby mógł być szybko wdrożony. Zapewnia niezawodne środowisko do zbierania logów z poszczególnych technologii CII i innych operacyjnych systemów komunikacyjnych firmy oraz służy jako pojedynczy punkt zbierania i dostarczania informacji o zdarzeniach operacyjnych o wystarczającej przepustowości, wydajności i niezawodności. LOGmanager odniósł w Telco Pro Services S.A. sukces do tego stopnia, że firma obecnie realizuje projekty dotyczące rozwoju i rozbudowy infrastruktury LOGmanager tak, aby objąć również systemy zapasowe i inne, mniejsze dedykowane instalacje w odizolowanych częściach ich infrastruktury komunikacyjnej.

Najbardziej doceniane funkcje:

- ⇒ Łatwość użytkowania
- ⇒ Diagnostyka awarii lub problemów operacyjnych nawet do poziomu aplikacji
- ⇒ Prognozowanie i zapobieganie wypadkom, naruszeniom bezpieczeństwa danych, przeglądanie nietypowych i podejrzanych transakcji i prób dostępu itp.
- ⇒ Możliwość monitorowania zmian konfiguracji wprowadzanych przez operatorów systemu
- ⇒ Diagnozowanie i rozwiązywanie problemów związanych z bezpieczeństwem
- ⇒ Śledzenie dostępu, działań użytkownika, wypełniania umów SLA, wymagań dotyczących audytu itp.
- ⇒ Zabezpieczanie dowodów na potrzeby analizy sądowej i dochodzeń w sprawie incydentów z naruszeniem bezpieczeństwa
- ⇒ Przeglądanie i monitorowanie zgodności



INFORMACJE O PRODUCENCIE I REFERENCJE KLIENTÓW

Prace nad LOGmanager trwają od 2014 roku I jest to flagowy produkt firmy Sirwisa S.A. z siedzibą w Pradze. Do daty wydania tego studium przypadku, LOGmanager miał ponad 130 zadowolonych klientów i można znaleźć konkretne referencje na stronie www.logmanager.pl. Naszymi klientami są nie tylko władze rządowe, ale także firmy dowolnej wielkości ze wszystkich sektorów tj. korporacje biznesowe, organizacje bankowe i inne. Śmiało, skontaktuj się z nami, aby uzyskać szczegółowe referencje klientów bezpośrednio z Twojej branży.