CASE STUDY

WDROŻENIE ROZWIĄZANIA SYCOPE W FIRMIE VEOLIA

KLIENT

Grupa Veolia działa w Polsce od 25 lat i jest sprawdzonym partnerem dla miast i przemysłu. Jest jednym z czołowych dostawców usług w zakresie zarządzania energią, gospodarki wodno-ściekowej i odpadowej. Oferuje szereg innowacyjnych usług dostosowanych do potrzeb klientów i, co istotne w tej branży, zgodnych z Celami Zrównoważonego Rozwoju przyjętymi przez ONZ. Zatrudnia w Polsce około 4600 pracowników.

Grupa Veolia w Polsce prowadzi działalność na terenie 123 miejscowości, w 58 miejscowościach zarządza sieciami ciepłowniczymi. Działa poprzez spółki operacyjne: Veolia Energia Polska (holding), Veolia Energia Warszawa, Veolia Energia Łódź, Veolia Energia Poznań, Veolia term, Veolia Industry Polska, Veolia Energy Contracting Polska, Przedsiębiorstwo Wodociągów i Kanalizacji w Tarnowskich Górach oraz ich spółki zależne w tym Veolia Centrum Usług Wspólnych Sp. z o.o., oferującą m.in. obsługę i wsparcie IT dla wszystkich spółek Grupy.

Veolia Polska jest częścią holdingu Veolia notowanego na giełdzie w Paryżu, zatrudniającego łącznie około 220 000 pracowników na całym świecie, którzy tworzą i wdrażają rozwiązania w zakresie energetyki, gospodarki wodno-ściekowej oraz gospodarki odpadami. W 2021 roku Grupa Veolia dostarczyła wodę pitną 79 milionom ludzi, obsłużyła 61 mln osób w zakresie usług ściekowych, wyprodukowała prawie 48 milionów MWh energii i przetworzyła 48 mln ton odpadów.

OCZEKIWANIA KLIENTA

Dział IT Centrum Usług Wspólnych odpowiada za utrzymanie infrastruktury teleinformatycznej i łączności we wszystkich 87 lokalizacjach Veolia Polska. Infrastruktura sieciowa firmy jest zróżnicowana - do jej budowy wykorzystano urządzenia między innymi Cisco Meraki, Cisco oraz CheckPoint. Wiele usług, w tym m.in.: eBOK udostępnionych jest za pośrednictwem internetu.

Aby zapewnić dostępność i wydajność aplikacji niezbędne stało się wykorzystanie wydajnego rozwiązania do monitorowania połączeń i pracy urządzeń sieciowych. Wykorzystanie oprogramowania dostarczanego przez poszczególnych producentów wymagało jednoczesnej pracy na kilku konsolach i utrudniało reagowanie na incydenty pojawiające się na styku technologii.

Dział IT Veolia Polska szukał rozwiązania do monitorowania obciążenia różnych typów urządzeń sieciowych (routery, firewalle, przełączniki) dostarczanych przez różnych producentów. Istotną jego cechą powinna być zdolność do gromadzenia danych niezbędnych do przyspieszenia napraw i optymalizacji sieci. Nowo wdrożone oprogramowanie miało też umożliwić monitorowania rzeczywistego ruchu w sieci i ocenę jego zgodności z matrycą połączeń zaakceptowaną przez dział bezpieczeństwa IT.

Ważnym kryterium branym pod uwagę podczas wyboru rozwiązania była też jego elastyczność i możliwość samodzielnego dostosowania dashboardów analitycznych, tak, by zapewniały szybki dostęp do niezbędnych informacji.

Ponadto dział IT, pod kierownictwem pana Macieja Oziembło, zdefiniował dodatkowe kryteria dla nowego systemu monitorowania infrastruktury IT:

- Analiza obciążenia urządzeń sieciowych i wykrywanie tzw. wąskich gardeł oraz segmentów sieci odpowiadających za spadek jakości transmisji.
- Identyfikacja przyczyn powolnego działania aplikacji.
- Analiza stopnia wysycenia łączy w danych okresach (datach, godzinach).
- Łatwość konfigurowania i obsługi - z racji wielu obowiązków, pracownicy działu IT mogą w ograniczonym stopniu zaangażować się we wdrożenie i naukę nowego systemu.
- Współpraca z systemem SIEM – nowo wdrożone rozwiązanie musi być wyposażone w mechanizmy umożliwiające integrację z rozwiązaniem SIEM.
- Wykrywanie i analiza potencjalnych ataków typu DDoS.

WDROŻENIE – PRZEBIEG PRAC

Po analizie dostępnych na rynku rozwiązań, podjęto decyzję o weryfikacji systemu Sycope w środowisku produkcyjnym Veolii. Ostatecznie po 3 miesięcznych testach w trakcie których przygotowano prototypy dashboardów, dokonano parametryzacji reguł bezpieczeństwa oraz potwierdzono możliwość integracji z rozwiązaniem SIEM, Klient zdecydował się na zakup dwóch modułów wchodzących w skład systemu Sycope. Pierwszym był moduł Visibility, który odpowiada za monitorowanie obciążenia urządzeń sieciowych oraz ruchu pomiędzy urządzeniami w sieci. Drugim modułem był moduł Security, który analizuje ruch sieciowy wykrywając zagrożenia, anomalie bezpieczeństwa oraz niepożądaną komunikacją wykorzystując w tym celu zarówno zaawansowane reguły bezpieczeństwa jak i stale aktualizowane zewnętrzne białe i czarne listy oraz sygnatury zagrożeń.

Wdrożenie miało miejsce w grudniu 2022 roku i obejmowało:

- instalację maszyny wirtualnej w środowisku Klienta,
- instalację licencji,
- wstępną konfigurację systemu, która obejmowała m.in. adresację sieciową, integrację z Active Directory do wykorzystania przy logowaniu użytkowników oraz integrację z systemem SIEM,
- konfigurację dedykowanych dashboardów, służących m.in. do monitorowania stanu urządzeń sieciowych oraz weryfikacji ruchu sieciowego z matrycą zgodności opracowaną przez dział bezpieczeństwa IT,
- stworzenie mechanizmu do eksportowania logów audytowych do systemu SIEM umożliwiających monitorowanie dostępu do Systemu Sycope.

Instalacja i konfiguracja Systemu Sycope w infrastrukturze Klienta zajęła jeden dzień, a stworzenie predefiniowanych dashboardów jedynie 7 dni.

Równolegle opracowano skrypt, który odpowiadał za gromadzenie logów rejestrujących dostępy poszczególnych osób do Systemu Sycope, a następnie ich wysyłkę za pośrednictwem protokołu Syslog do rozwiązania SIEM.

PO WDROŻENIU – PODSUMOWANIE

Dzięki informacjom zawartym we flowach sieciowych dział IT otrzymuje szczegółowe informacje o ruchu generowanym przez użytkowników, komunikacji między serwerami oraz wykorzystanych w organizacji urządzeniach i aplikacjach. Dzięki temu może szybko podejmować decyzje dotyczące alokacji zasobów i działań zabezpieczających przed nieplanowanymi przestojami związanymi z awariami infrastruktury IT, a także wykrywać incydenty bezpieczeństwa.

Szybki dostęp do najważniejszych z punktu widzenia Klienta informacji zapewniają przygotowane przez inżynierów Passus dashboardy. Prezentują one komunikację między poszczególnymi urządzeniami z możliwością filtrowania portów, pozwalają na budowanie tabel ruchu, weryfikuję i wizualizują obciążenia konkretnych urządzeń i portów oraz wyliczają procentowe obciążenie poszczególnych interfejsów.

Istotną korzyścią z wdrożenia jest lepsza widoczność anomalii sieciowych i zagrożeń bezpieczeństwa z poziomu całej organizacji. System Sycope stał się istotnym źródłem informacji dla oprogramowania SIEM, które koreluje logi z różnych źródeł. Z racji tego, że monitorowane są flowy sieciowe ze wszystkich istotnych urządzeń organizacji, widać wszystkie komunikacje sieciowe. Obecnie w celu wysłania alertów bezpieczeństwa z systemu Sycope do SIEM wystarczy podać w konfiguracji adres IP oraz port serwera Syslog. Analiza flowów sieciowych odbywa się w rozwiązaniu Sycope, a nie bezpośrednio w silniku analitycznym systemu SIEM. Przynosi to wymierne korzyści finansowe eliminując koszty licencji SIEM niezbędnych do analizowania miliardów flowów sieciowych dziennie.

> Szukaliśmy rozwiązania, które umożliwiłoby monitoring całej sieci, będąc również źródłem danych dla systemu SIEM, który posiadamy. System Sycope doskonale wpisał się w nasze potrzeby pozwalając ponadto zoptymalizować koszty działania obecnego SIEM-a.
> **Maciej Oziembło, Kierownik Obszaru Data Center**

PASSUS SA

Grupa Passus specjalizuje się w projektowaniu i wdrażaniu wysoko specjalizowanych rozwiązań informatycznych z zakresu monitorowania i poprawy wydajności sieci i aplikacji oraz bezpieczeństwa IT zarówno w architekturze on-premise jak i środowiskach hybrydowych, chmurze prywatnej i publicznej. W skład Grupy wchodzą firmy Passus S.A., Chaos Gears S.A. oraz Sycope S.A.

Oferta Grupy obejmuje:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT w szczególności wykrywanie podatności, zabezpieczenie sieci, aplikacji oraz danych, systemy monitorowania i zarządzania incydentami bezpieczeństwa (SIEM/SOC);
- projekty realizowane z wykorzystaniem platformy chmurowej Amazon Web Services obejmujące migracje aplikacji oraz infrastruktury i danych, usługi z zakresu Cloud Manage Services, tworzenie aplikacji SaaS oraz rozwiązań do analizy danych z wykorzystaniem sztucznej inteligencji.

Tym co wyróżnia grupę Passus spośród firm integratorskich, jest doświadczenie pozyskane podczas realizacji szeregu skomplikowanych projektów dla największych firm i instytucji. Nasi inżynierowie zrealizowali największe w Polsce projekty z zakresu Application and Network Performance Management oraz SIEM. Ponad 20 lat współpracy z firmami oraz instytucjami z Polski i z zagranicy zaowocowało znajomością uwarunkowań biznesowych i technicznych tych organizacji.

Grupa kieruje swoją ofertę do dużych, polskich i zagranicznych podmiotów, które są największymi odbiorcami zaawansowanych rozwiązań IT. Jej głównymi Klientami są podmioty z sektora publicznego (służby mundurowe, organy Państwa, urzędy administracji rządowej i samorządowej) Skarbu Państwa oraz podmioty z sektora prywatnego, zaliczane do tzw. TOP 500 największych przedsiębiorstw w Polsce. Do ich grona należy pięć największych polskich firm telekomunikacyjnych, osiem z dziesięciu największych banków i osiem z dziesięciu największych podmiotów z branży paliwowo-energetycznej i przesyłowej, a także międzynarodowe firmy produkcyjne i handlowe.

Grupa Passus jest partnerem takich producentów jak: Riverbed, Brocade (Symantec), Splunk, NetScout, Cisco, Trellix (FireEye), ManageEngine a także Digi, Fidelis Cybersecurity, Tenable oraz Fudo Security. Passus posiada także własny zespołów programistów i inżynierów dostosowujących istniejące rozwiązania oraz realizujących projekty na indywidualne zamówienie. Na bazie zebranych doświadczeń zespół ten przygotował własne rozwiązania tworzące System Sycope zintegrowane, modułowe rozwiązanie składające się z aplikacji Visibility (monitoring), Performance (wydajność), Security (bezpieczeństwo IT). Jego zastosowanie w organizacji istotnie ogranicza ryzyko wystąpienia strat związanych z awarią lub spadkiem wydajności infrastruktury IT oraz strat spowodowanych cyberatakami.

Firma Passus S.A. powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. W lipcu 2018 roku, Spółka zadebiutowała na rynku New Connect, **a od stycznia 2023 r. jest na notowana na rynku regulowanym Giełdy Papierów Wartościowych.** Obecnie Grupa zatrudnia ponad 100 wykwalifikowanych pracowników - inżynierów, programistów i specjalistów. Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.: poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S (routing & switching), Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed Network and Application Performance Management Qualified Trainer.

W 2017 roku firma spełniła wymagania stawiane przez Agencję Bezpieczeństwa Wewnętrznego i uzyskała świadectwa bezpieczeństwa przemysłowego, które potwierdzają zdolność spółki do realizacji usług w instytucjach i gałęziach przemysłowych związanych z dostępem do informacji niejawnych - krajowych, NATO oraz Unii Europejskiej.