CASE STUDY

Wdrożenie rozwiązania Splunk w firmie BEST S.A.

KLIENT

BEST S.A. należy do grona liderów w branży windykacyjnej w Polsce. Firma zarządza dużymi portfelami wierzytelności nieregularnych, rozwiązując problem braku terminowych rozliczeń pomiędzy stronami umów i przywracając równowagę w obiegu gospodarczym. Spółka istnieje na rynku od 1994 roku, a od 1997 roku jej akcje notowane są na GPW w Warszawie. Siedziba firmy znajduje się w Gdyni, w Elblągu usytuowane jest Centrum Usługowe BEST S.A.

BEST S.A. jako Spółka wiodąca w Grupie Kapitałowej BEST, jest odpowiedzialna za środowisko informatyczne oraz zapewnienie bezpieczeństwa informacji i IT we wszystkich podmiotach z Grupy.

OCZEKIWANIA KLIENTA

Ataki cyberprzestępców są kierowane na firmy i instytucje wielu branż. Firmy z sektora finansowego, ze względu na specyfikę prowadzonej działalności i poufność przechowywanych oraz przesyłanych informacji, są szczególnie „atrakcyjnym" celem. Ujawnienie tych informacji może mieć bardzo negatywne skutki - zarówno dla firmy, jak i jej Klientów. Analogicznie jest w instytucjach z sektora poza finansowego - utrata danych, np. wskutek ataku ransomware, może wiązać się z przerwaniem ciągłości jej funkcjonowania i brakiem możliwości kontaktu z Klientami.

Niezależny od pionu IT, Dział Bezpieczeństwa Informacji w BEST S.A., jest świadomy aktualnych zagrożeń i stale aktualizuje wiedzę zarówno z zakresu najnowszych ataków, jak i dostępnych na rynku rozwiązań zapewniających skuteczną ochronę.

Firma stosuje wiele rozwiązań podnoszących bezpieczeństwo Organizacji takich jak Next Generation Firewall, system klasy EDR (Endpoint Detection and Response), system do ochrony przed wyciekiem danych (DLP), skanery podatności, czy system kontroli dostępu do sieci (NAC).

BEST od kilku lat korzystał z rozwiązań klasy SIEM, jednak zaistniała potrzeba wdrożenia nowego rozwiązania, które umożliwiałoby bardziej intuicyjne budowanie scenariuszy incydentów i reguł korelacyjnych, a także przyspieszyłoby analizę zdarzeń mogących stanowić naruszenie bezpieczeństwa i pomogło szybciej reagować na wykryte odstępstwa od przyjętej polityki bezpieczeństwa.

W tym celu Dział Bezpieczeństwa Informacji w firmie BEST S.A. zdecydował o potrzebie wdrożenia nowego systemu klasy SIEM, który w szczególności spełni następujące funkcje:

- umożliwi podłączenie źródeł danych ze wszystkich systemów używanych w GK BEST,
- będzie posiadać czytelny, intuicyjny interface - możliwość tworzenia dedykowanych dashboard-ów oraz łatwy język budowania korelacji,
- będzie monitorować zdarzenia zachodzące w sieci wewnętrznej i próby przełamania zabezpieczeń,
- umożliwi zbudowanie powtarzalnych i skutecznych scenariuszy działań reakcji na zdarzenia wskazujące na incydent bezpieczeństwa informacji, w tym w oparciu o tabelę ATT@CK MITRE,
- zabezpieczy materiał dowodowy w przypadku naruszeń bezpieczeństwa,
- umożliwi generowanie przejrzystych i czytelnych raportów biznesowych dla kierownictwa i Zarządu firmy,
- będzie charakteryzował się wysoką skalowalnością.

ROZWIĄZANIE

Za realizację projektu odpowiedzialni byli pracownicy Działu Bezpieczeństwa Informacji, przy wsparciu pracowników Pionu IT, którzy również są odbiorcami docelowego rozwiązania. Początkowo brano pod uwagę 7 rozwiązań różnych producentów. Po wstępnej selekcji przeprowadzono testy typu PoC (proof of concept) kliku z nich. Ostatecznie zdecydowano o wyborze rozwiązania firmy Splunk - jednego ze światowych liderów rozwiązań do analizy dużych zbiorów danych. Podejmując decyzję, zwrócono uwagę na kilka elementów wyróżniających Splunk wśród konkurentów:

- łatwość w budowaniu zapytań - intuicyjny język SPL (Splunk Processing Language) pozwala przygotować i zapisać dowolne zapytania w zbiorach Big Data, zasilanych przez infrastrukturę IT,
- korelacja zdarzeń ze wszystkich źródeł logów, tj. systemów wykorzystywanych w BEST S.A. – Splunk umożliwia rejestrowanie danych pochodzących zarówno z systemów zabezpieczeń (firewall, IDS, antywirusy), jak i z urządzeń sieciowych, baz danych, systemów operacyjnych - w jednym miejscu i ich analizę za pomocą jednego UI,
- intuicyjny interfejs – podejście drill-down zapewnia łatwy dostęp do szczegółowych informacji o zdarzeniu bezpośrednio z poziomu wykresu lub tabeli z możliwością tworzenia indywidualnych dashboardów,
- szerokie „community" ułatwiające rozwój systemu oraz powszechność stosowania rozwiązania, która daje gwarancję rozwoju produktu przez kolejne kilka lat,
- wzbogacenie wyników wyszukiwania o informacje z framework ATT@CK MITRE, dzięki czemu analityk otrzymuje dodatkowe informacje o incydencie i jego impakcie na organizację.

WDROŻENIE

Pierwszym krokiem było wdrożenie platformy Splunk Enterprise w celu gromadzenia i indeksowania logów oraz innych danych z dowolnego źródła sieciowego, umożliwiając Pracownikom wyszukiwanie i korelowanie tych informacji, oraz wyświetlanie wyników na pulpitach nawigacyjnych.

Następnie inżynierowie Passus wdrożyli Splunk Enterprise Security (Splunk ES), rozwiązanie bezpieczeństwa klasy premium, które rozszerzyło platformę Splunk, ułatwiając zespołom ds. bezpieczeństwa szybkie wykrywanie i reagowanie na wewnętrzne i zewnętrzne

> O wyborze rozwiązania Splunk zdecydowały łatwość w budowaniu zapytań, korelacja zdarzeń ze wszystkich systemów wykorzystywanych w naszej firmie, intuicyjny interfejs, szerokie community ułatwiające rozwój systemu oraz powszechność stosowania rozwiązania, która daje gwarancję rozwoju produktu przez kolejnych kilka lat.
> **Magdalena Bodus, Kierownik Działu Bezpieczeństwa Informacji w firmie BEST S.A.**

ataki oraz uprościło zarządzanie zagrożeniami. Splunk ES zapewnił wygodny i czytelny dostęp do informacji o stanie bezpieczeństwa organizacji, dostarczając kompleksowy zestaw gotowych dashboardów, raportów i wskaźników, które pozwalają szybko reagować na zagrożenia.

Dodatkowo, biorąc pod uwagę potrzeby Klienta, inżynierowie Passus przygotowali dodatkową dedykowaną aplikację agregującą logi z systemów nieobsługiwanych przez Splunk np. ze skanera podatności.

ARCHITEKTURA ROZWIĄZANIA SPLUNK:

- w dwóch lokalizacjach – w Gdyni oraz Elblągu zainstalowano serwery Heavy Forwarders, odpowiadające za zbieranie danych z poszczególnych systemów. Forwarder zbiera dane, a następnie przekazuje do Indexera.

- Indexer odpowiada za przechowywanie i indeksację danych, dzieli je na kilka logicznych magazynów danych.

- Search Heady pomagają w przesyłaniu wyszukiwań do różnych Indexerów. Zarządzają funkcjami wyszukiwania, dostarczając użytkownikowi wyniki zapytania.

PO WDROŻENIU – PODSUMOWANIE

Dzięki wdrożeniu Splunk Enterprise i Splunk ES, firma BEST S.A. jest w stanie agregować i korelować w jednym miejscu dane, pochodzące z wielu systemów bezpieczeństwa. Firma posiada rozwiązanie do obsługi terabajtów danych i szybkiej obsługi alertów zgłaszanych przez systemy. Ma możliwość natychmiastowego zidentyfikowania problemu, a co za tym idzie szybkiego zaadresowania i rozwiązania w krótkim czasie od wykrycia, nie tylko oszczędza mnóstwo i czasu pracy pracowników IT i działu bezpieczeństwa, ale również może pozwolić uchronić organizację przed poważnymi konsekwencjami incydentu, który nie zostałby w porę wykryty. W ramach wdrożenia przygotowano specjalne dashboard'y prezentujące informacje istotne z punktu widzenia Zarządu, przedstawiające w przejrzysty sposób aktualną sytuację w obszarze cyberbezpieczeństwa oraz dające możliwość analizy efektywności pracy i obciążenia działu bezpieczeństwa w ujęciu historycznym (np. z uwzględnieniem ilości ataków w miesiącach).

Dla Działu Bezpieczeństwa firmy BEST S.A. istotnym aspektem był krótki czas instalacji i uruchomienia rozwiązania Splunk, który można liczyć w dniach, a nie miesiącach.

W kolejnym etapie firma planuje wdrożenie systemu SOAR (Splunk Phantom), które pozwoli na automatyzację procesów związanych z zarządzaniem bezpieczeństwem, w związku z tym, jeszcze efektywniejsze wykorzystanie zasobów Działu Bezpieczeństwa informacji w firmie BEST S. A.

PASSUS SA

Passus Spółka Akcyjna jest polskim producentem, integratorem i dostawcą wysoko specjalizowanych rozwiązań informatycznych obejmujących w szczególności:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT m.in. do wykrywania podatności, zabezpieczenia sieci, aplikacji oraz danych przed zaawansowanymi atakami oraz zagrożeniami wskutek nadużyć lub zaniedbań wewnętrznych;
- rozwiązania do projektowania, budowy i modernizacji wydajnych sieci WiFi w tym realizacji specjalistycznych projektów „pod klucz" (m.in. captive portal, lokalizacja zasobów, dostęp WiFi w środkach komunikacji i transportu);
- narzędzia interpretujące dane w ruchu sieciowym, logach oraz bazach danych, które pozwalają wyodrębnić określone pliki, treści lub metadane, które mogą być następnie przesłane do zewnętrznych systemów analitycznych, takich jak SIEM czy antyfraud;
- rozwiązania do optymalizacji i konsolidacji infrastruktury serwerowej;
- rozwiązania zabezpieczające przed nadużyciami finansowymi (antyfraud).

Tym, co wyróżnia Passus SA spośród firm integracyjnych, jest elastyczność i koncentracja na rzeczywistych potrzebach Klienta. Płaska i przejrzysta struktura organizacyjna spółki oraz ograniczone do niezbędnego minimum procedury pozwalają szybko i skutecznie reagować na oczekiwania Klienta. Ponad 20 lat współpracy z firmami oraz instytucjami z Polski i z zagranicy zaowocowało znajomością uwarunkowań biznesowych i technicznych tych organizacji. Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Swedwood, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Bazując na własnych produktach i usługach oraz technologiach uznanych światowych producentów, Passus SA tworzy i wdraża rozwiązania, precyzyjnie dostosowane do wymagań klienta. Spółka zapewnia klientom kompleksową obsługę, począwszy od analizy potrzeb, przez planowanie, usługi wdrożeniowe, szkolenia pracowników, aż po opiekę serwisową oraz posprzedażną. Oferowane rozwiązania są przygotowywane w oparciu o produkty własne jak i uznanych światowych dostawców. Firma jest partnerem takich producentów jak: Riverbed (Riverbed Premier Partner), Core Security (wyłączny dystrybutor w Polsce), Fidelis Cybersecurity (rekomendowany Partner w Polsce), NetScout, Cisco (Premier Partner), FlowMon (Gold Partner), Symantec oraz Qualys. Passus posiada także własny zespołów programistów i inżynierów realizujących projekty na indywidualne zamówienie. Na bazie zebranych doświadczeń, w maju 2014 roku, zespół ten przygotował unikalne w skali światowej rozwiązanie umożliwiające identyfikację nadużyć i incydentów w oparciu o analizę ruchu sieciowego - Passus Ambience.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Zatrudnia blisko 30 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 oraz Fluke Networks Application Performance Appliance Certified 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 jak i NATO oraz Unii Europejskiej.