Splunk

Splunk jest jednym z najpopularniejszych narzędzi do analizy danych maszynowych - zapisów transakcji użytkownika, jego interakcji z systemem lub urządzeniem, zachowania urządzeń, a także szeroko rozumianych incydentów bezpieczeństwa (nadużyć, ataków, wycieków danych).

System w jednym miejscu gromadzi i udostępnia dane pochodzące zarówno ze środowisk fizycznych, wirtualnych jak i z chmury umożliwiając ich wyszukiwanie, monitorowanie w czasie zbliżonym do rzeczywistego.

Użytkownik może analizować dane kompleksowo (niezależnie od ich ilości i rodzaju) jak również weryfikować zależności między pojedynczymi, pozornie nic nieznaczącymi zdarzeniami.

Przykładowe zastosowania systemu SPLUNK:

- Analiza kontekstowa logów aplikacyjnych i systemowych.
- Prezentacja wydajności systemów.
- Monitoring zdarzeń związanych z bezpieczeństwem (SIEM).
- Wykrywanie anomalii i nadużyć.
- Monitorowanie ciągłości i prawidłowości działania infrastruktury i usług sieciowych.

Splunk – kluczowe cechy:

- **Uniwersalność** - rozwiązanie gromadzi i analizuje dane pochodzące z różnorodnych źródeł. Splunk jest z powodzeniem stosowany w monitoringu sieci IT, jako system SIEM, do zarządzania aplikacjami, a także w takich obszarach jak: Internet of Things, przemysł, lub medycyna. Jego wszechstronność pozwala na zastosowanie jednej spójnej technologii zarządzania danymi w całej organizacji, co istotnie zwiększa opłacalność inwestycji.

- **Elastyczność zastosowania** – system gromadzi dane RAW, które mogą być następnie wykorzystywane na potrzeby dowolnych analiz oraz zapytań. W zależności od potrzeb, Splunk normalizuje dane w locie i tworzy dynamicznie struktury („schema on the fly") bez konieczności przebudowania bazy lub ponownego importu danych.

- **Skalowalność** - Splunk jest z powodzeniem stosowany do analizy pojedynczych gigabajtów danych oraz w środowiskach, w których przetwarzane są setki terabajtów nowych danych dziennie. Co ważne, licencja Splunk w żaden sposób nie ogranicza zarówno liczby analizowanych źródeł jak i serwerów, na których może być zainstalowany.

- **Łatwość pobierania różnych typów danych** – system umożliwia gromadzenie logów dowolnego typu i formatu, w tym logów wielolinijkowych. Dzięki tzw. Modular Input API możliwa jest obsługa tych źródeł danych, które nie wspierają standardowych protokołów lub API. Korzystając ze strony SplunkBase (https://splunkbase.splunk.com) można pozyskać kilkadziesiąt różnych dodatków (addons) wspierających niestandardowe protokoły.

- **Niezawodność** - rozproszona, klastrowa architektura rozwiązania oraz mechanizmy replikacji danych gwarantują wysoką dostępność danych i usług.

Splunk Enterprise może zostać rozszerzony o szereg zawansowanych aplikacji z zakresu monitorowania i zarządzania bezpieczeństwem danych i aplikacji przeznaczonych dla analityków i zespołów SOC:

- Enterprise Security – system klasy SIEM do agregacji i analizy danych z różnych źródeł.

- User Behaviour Analytics – aplikacja wspomagająca zarządzanie bezpieczeństwem, bazującą na analizach behawioralnych użytkowników.

- Phantom – rozwiązanie typu SOAR do automatyzacji procesów związanych z zarządzaniem bezpieczeństwem.

- Security Essentials - darmowa aplikacja umożliwiająca identyfikację typowych incydentów z zakresu cyberbezpieczeństwa.

- Splunk Apps – gotowe zestawy narzędzi analitycznych, przeznaczone dla różnych technologii lub produktów firm trzecich.

Splunk Enterprise pozwala na swobodne wyszukiwanie konkretnych zdarzeń wraz z ekstrakcją metadanych w momencie wyszukiwania.

Platforma Splunk dla działów bezpieczeństwa - od zbierania danych do reakcji na zagrożenie

SPLUNK – NOWOCZESNE ROZWIĄZANIE SIEM

Platforma Splunk Enterprise (lub Splunk Cloud) realizuje wszystkie niezbędne funkcje SIEM takie jak gromadzenie informacji, indeksowanie, wyszukiwanie i raportowanie. Pozwala zarówno na prowadzenie kompleksowych analiz, jak i badanie związku między pojedynczymi, pozornie nic nieznaczącymi zdarzeniami.

Dodatkowy moduł Enterprise Security (ES), posiada wbudowane i gotowe do użycia pulpity nawigacyjne, schematy wyszukiwań oraz korelacji, a także predefiniowane raporty. Aplikacja może pracować zarówno w sieci lokalnej, środowisku wielochmurowym jak i w modelu SaaS z wykorzystaniem chmury Splunk Cloud. Bez względu na model wdrożenia Splunk Enterprise Security zapewnia kompleksowy i spójny obraz monitorowanego środowiska dostarczając dane zarówno na potrzeby działów bezpieczeństwa, jak i kierownictwa firmy.

Wybrane obszary zastosowania Splunk Enterprise Security:

Analiza zagrożeń

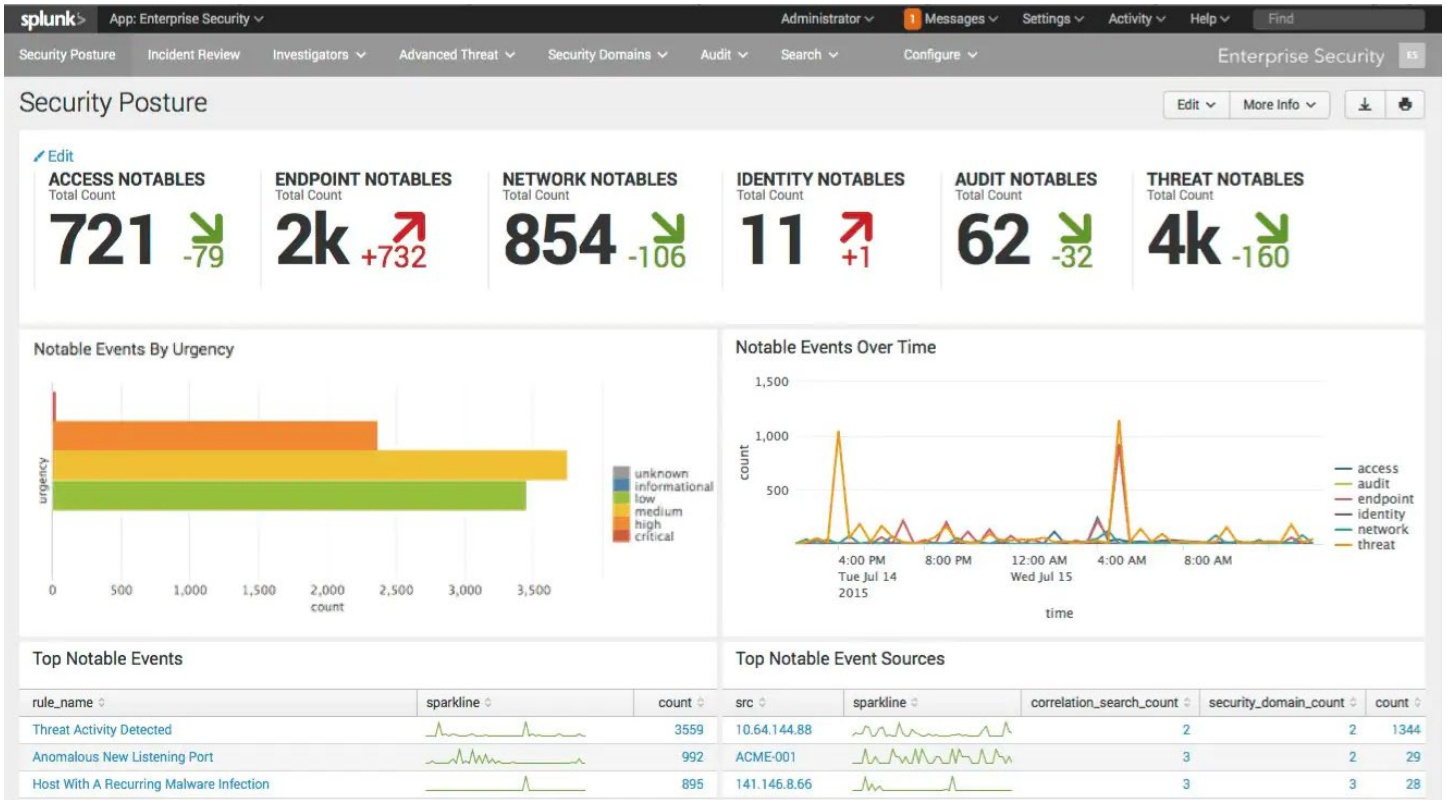
Splunk ES prezentuje szereg wskaźników pozwalających określić stan bezpieczeństwa całego środowiska z uwzględnieniem informacji o taktykach i technikach wykorzystywanych przez intruzów. Predefiniowane dashboardy ułatwiają analizę kontekstu zagrożenia, znaczenie atakowanego zasobu dla organizacji, a także rolę, odpowiedzialność i status zatrudnienia użytkownika danego zasobu. Ten dodatkowy kontekst związany z użytkownikiem jest często niezwykle ważny, zwłaszcza na etapie analizy ryzyka i oceny potencjalnych skutków incydentu.

Reagowanie na incydenty

Wbudowane workflowy ułatwiają zarządzanie procesem identyfikacji i obsługi incydentów, w tym przekazaniem odpowiednich informacji na potrzeby dalszej analizy lub informatyki śledczej. Funkcja Adaptive Response pozwala skonfigurować oraz automatycznie wywołać określone działania umożliwiając natychmiastową reakcję na cyberatak i przerwanie go bez ingerencji człowieka (np. zablokować ruch ze stacji roboczej, na której zostało wykryte szkodliwe oprogramowanie).

Monitorowanie aktywności użytkowników

Splunk ES wykorzystuje w analizach zarówno dane o tożsamości użytkowników, jak i informacje pochodzące z procesu uwierzytelniania. Dzięki analizom kontekstowym ostrzega o podejrzanych zachowaniach i naruszeniach reguł korporacyjnych, norm i przepisów prawa. Monitoring obejmuje także użytkowników uprzywilejowanych, którzy najczęściej stają się celami ataków, a ich kompromitacja może oznaczać największe szkody.



Enterprise Security zapewnia przejrzysty interfejs użytkownika, gdzie obsługiwane są wszystkie zadania związane z bezpieczeństwem.

Najważniejsze funkcje rozwiązania Splunk ES:

- Zbieranie danych z logów – Splunk gromadzi i analizuje wszystkie zapisy zdarzeń prezentując kompleksowy stan zabezpieczeń w czasie rzeczywistym. Pozwala to zespołom zajmującym się IT i bezpieczeństwem zarządzać logami z jednej centralnej lokalizacji, korelować dane (w tym dane historyczne) z wielu urządzeń oraz wykorzystać do analizy dane z innych źródeł (takich jak zmiany rejestru i logi ISA Proxy).
- Stosowanie reguł korelacji w czasie rzeczywistym – analiza sekwencji zdarzeń ułatwia zbadanie wielu zdarzeń związanych z bezpieczeństwem i zawężenie działań do obszarów tych, które faktycznie mają znaczenie dla funkcjonowania organizacji.
- Analiza predykcyjna - wykorzystanie technik uczenia maszynowego umożliwia wykrycie wzorców na podstawie danych historycznych oraz wykorzystania ich na potrzeby przewidywania i identyfikacji potencjalnych zagrożeń.
- Przechowywanie danych historycznych - Splunk przechowuje dane historyczne danych z logów przez długi okres. Pomaga spełnić wymagania dotyczące zgodności z przepisami powszechnie obowiązującego prawa. Dostęp do historycznych danych maszynowych umożliwia analitykom przeprowadzanie analiz bezpieczeństwa związanych z przeszłymi przestępstwami, na przykład w celu śledzenia trasy ataku.
- Wyszukiwanie i raportowanie ustrukturyzowanych danych – Splunk ES umożliwia stworzenie dowolnych modeli danych. Wyniki analiz i wyszukiwań mogą być następnie zapisane w formie raportów i tabeli przestawnych, wykorzystywane do konfigurowania alertów oraz prezentowane na pulpitach nawigacyjnych.
- Wyszukiwanie i raportowanie nieustrukturyzowanych danych - Splunk ES może zostać zasilony danymi surowymi niemal z każdego źródła. Dane te można wykorzystać w analizach i raportach dystrybuowanych bezpośrednio z platformy SIEM do odpowiednich osób.
- Przetwarzanie danych kontekstowych – analizy uwzględniające kontekst ograniczają liczbę fałszywych alarmów i ułatwiają priorytetyzację. Splunk ES jest w stanie dodać kontekst do analizy zagrożeń zewnętrznych, wewnętrznych operacji IT i wzorców zdarzeń.

SPLUNK USER BEHAVIOR ANALYTICS

Splunk User Behavior Analytics (UBA) jest rozwiązaniem służącym do wykrywania zagrożeń i nadużyć w oparciu o analizę zachowań użytkowników oraz systemów informatycznych. Posiada zdolność uczenia się i określania bazowych aktywności użytkownika, dzięki czemu może np. wysyłać ostrzeżenie, gdy wykryje aktywność wykraczającą poza normę. Do tworzenia modelu standardowych zachowań użytkownika, wykorzystuje informacje dotyczące m.in. urządzeń wykorzystanych do logowania, lokalizacji oraz uprawnień użytkownika.

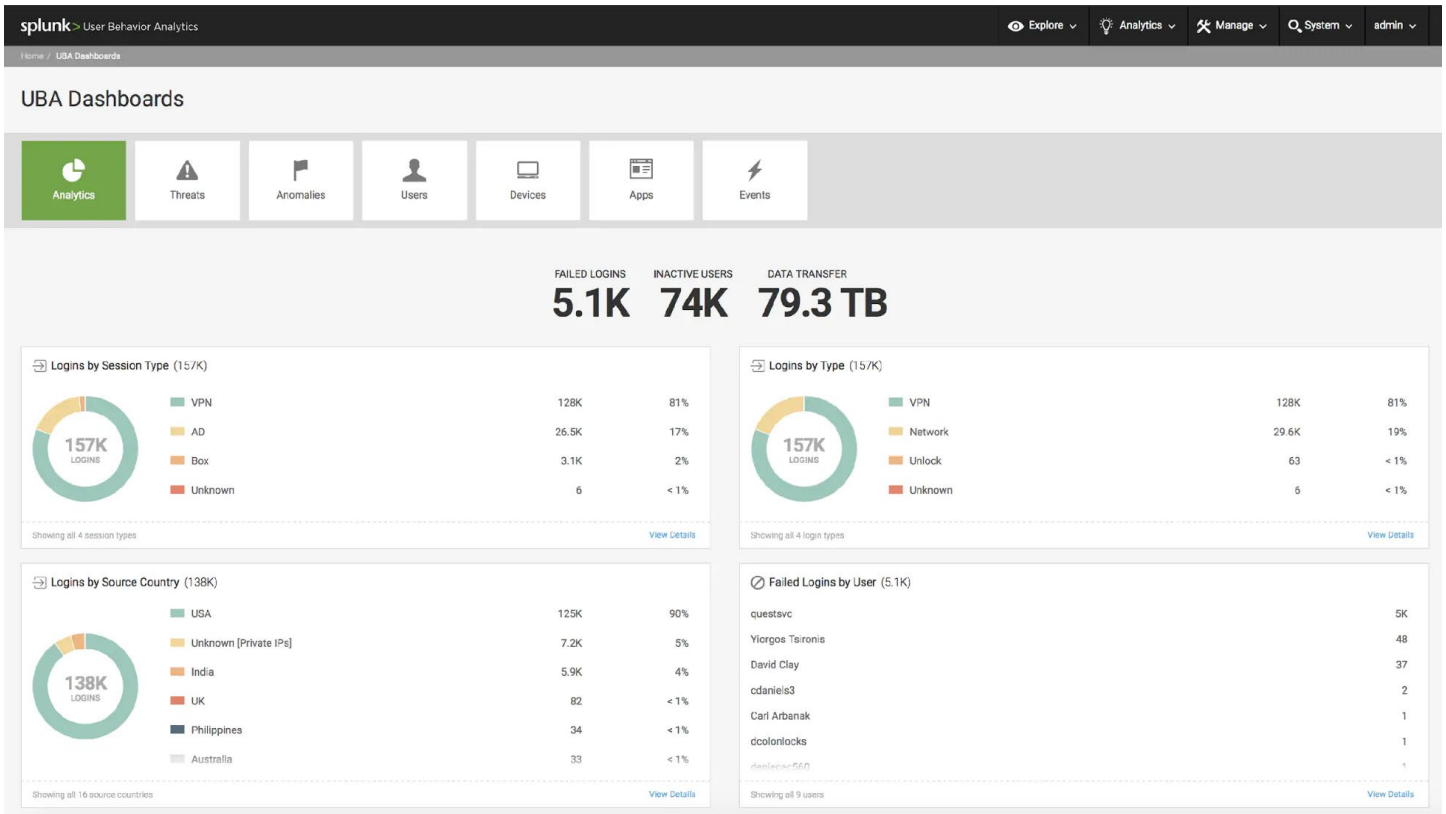
Wybrane funkcje Splunk User Behavior Analytics (UBA):

- Wykrywanie penetracji sieci przez złośliwe oprogramowanie.
- Wykrywanie rozprzestrzeniania się zagrożeń wewnętrznych.
- Reagowanie na anomalie w czasie rzeczywistym (np. dynamicznie generowane nazwy domeny lub nietypowa aktywność AD).
- Wykrywanie nieprawidłowości związanych z zachowaniem urządzeń (np. nietypowy dostęp do komputera, nietypowa aktywność w sieci).
- Namierzanie sieci botnet lub działania CnC (np. wysyłania sygnałów przez złośliwe oprogramowanie - malware beaconing).

Integracja z innymi rozwiązaniami Splunk

Rozwiązania typu UBA najlepsze efekty dają współpracując z rozwiązaniem typu SIEM, dlatego Splunk UBA ściśle integruje się z rozwiązaniami Splunk Enterprise oraz Splunk Enterprise Security zapewniając m.in.:

- Skuteczne wykrywanie zagrożeń i efektywne wdrożenie metod obrony zgodnie z modelem „kill chain".
- Możliwość wykorzystania dodatkowych narzędzi do analizy danych w postaci uczenia maszynowego, profilowania statystycznego oraz zaawansowanych technik wykrywania anomalii.



Dzięki zastosowanym technikom analizy danych, w tym uczenia maszynowego, rozwiązanie Splunk UBA pozwala na bardzo wczesną w pełni automatyczną identyfikację zagrożeń związanych z niestandardowym zachowaniem użytkowników systemów.

SPLUNK PHANTOM

Splunk® Phantom jest rozwiązaniem typu SOAR (Security Orchestration, Automation and Response), które przyspiesza i upraszcza proces reagowania na incydenty bezpieczeństwa. Przetwarzając 50 000 incydentów na godzinę umożliwia koordynację i automatyzację serii współzależnych działań związanych z bezpieczeństwem w obrębie złożonej infrastruktury. Zespoły ds. bezpieczeństwa mogą efektywniej realizować szeroki zakres funkcji SOC, takich jak zarządzanie zdarzeniami, współpraca między zespołami i raportowanie. Splunk Phantom integruje się z produktami Splunk Enterprise i Splunk Enterprise Security tworząc kompleksowe rozwiązanie do zarządzania bezpieczeństwem IT.

Automatyzacja działania Security Operations Center

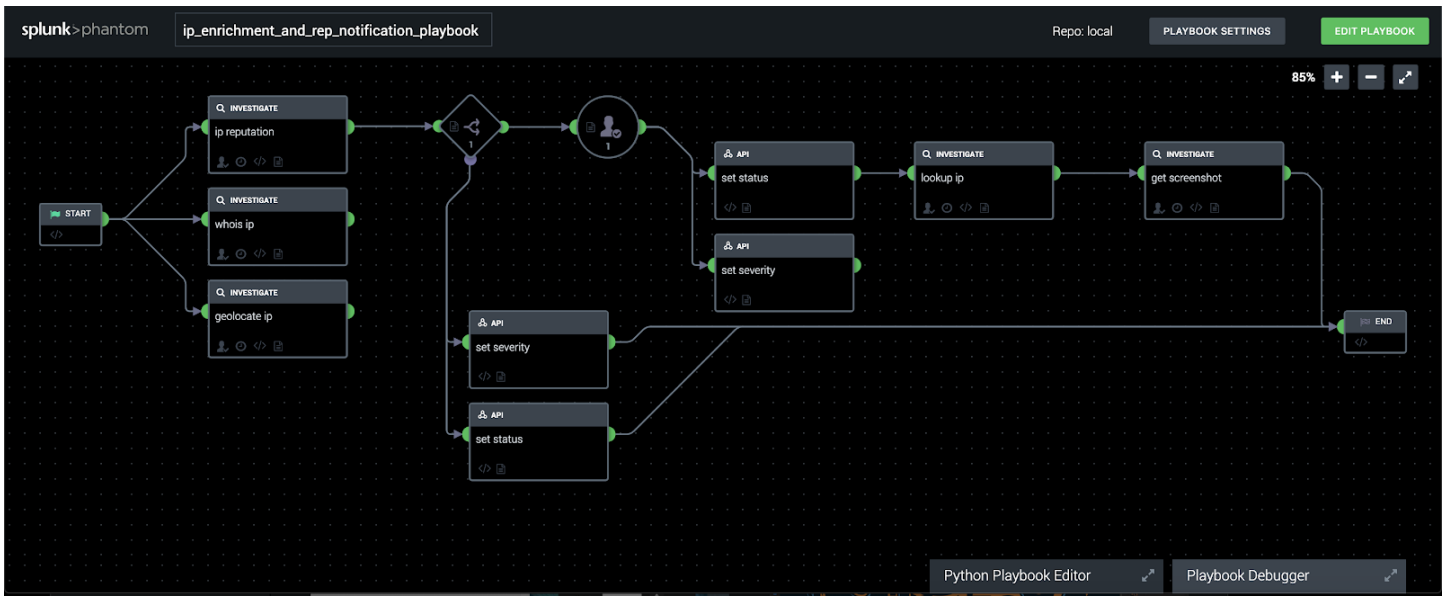
Phantom usprawnia pracę zespołów SOC automatyzując wykonanie szeregu zadań i skracając ich realizację z godzin do sekund. Uwolnienie specjalistów IT od wielu powtarzalnych zadań pozwala skupić się na podejmowaniu decyzji w kluczowych z punktu widzenia organizacji kwestiach. Playbooki Phantoma pozwalają na definiowanie przepływów pracy (workflows) zarówno za pomocą edytora wizualnego (nie są tu wymagane umiejętności kodowania), jak i zintegrowanego z aplikacją środowiska programistycznego.

Orkiestracja

Phantom integruje istniejące narzędzia bezpieczeństwa zapewniając ich lepsze współdziałanie. Koordynuje działania oraz przepływ informacji między zespołem SOC i systemami bezpieczeństwa, sprawiając, że każdy element obrony aktywnie uczestniczy w realizacji spójnej strategii przeciwdziałania zagrożeniom. Zespół SOC może się skupić się na celach i strategii postępowania, podczas gdy platforma Phantom przekłada je na działania specyficzne dla danego urządzenia.

Reagowanie na incydenty

Phantom pomaga zespołom ds. bezpieczeństwa szybciej identyfikować zagrożenia i na nie reagować. Funkcje automatycznego wykrywania, śledzenia i reagowania na niebezpieczeństwa przyczynia się do minimalizacji okresu aktywności złośliwego oprogramowania, a tym samym poprawy wskaźnika MTTR - mean time to resolve. Wykorzystanie aplikacji Phanton on Splunk Mobile pozwala na prowadzenie działań za pomocą urządzeń mobilnych i reakcję z dowolnego miejsca w dowolnym czasie. Co istotne, dane dotyczące konkretnego przypadku są przechowywane i udostępniane z jednego głównego repozytorium. Ułatwia to komunikację ze współpracownikami oraz przypisywanie zadań odpowiednim członkom zespołu.



Splunk Phantom w łatwy sposób daje możliwość automatyzacji działań, oszczędzając czas pracy analityków.

TESTY ROZWIĄZAŃ SPLUNK

Tym z Państwa, którzy są zainteresowani zweryfikowaniem możliwości rozwiązań firmy Splunk proponujemy bezpłatne testy dowolnego produktu znajdującego się w naszej ofercie w środowisku produkcyjnym Państwa organizacji.

Oprócz w pełni funkcjonalnych rozwiązań Splunk zapewniamy:

- Pomoc przy doborze odpowiedniej wersji testowanego rozwiązania.
- Wsparcie inżynierów Passus SA w procesie instalacji rozwiązania oraz jego dostosowania do specyfiki konkretnego środowiska.
- Opracowanie pisemnego raportu podsumowującego wyniki testów.

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., Wisenet sp. z o.o., Chaos Gears S.A. oraz Sycope sp. z o.o.

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);
- projektowanie rozwiązań chmurowych, migracja aplikacji i danych oraz wsparcie w zarządzaniu i optymalizacja środowiska cloud;
- rozwiązania w zakresie utrzymania ciągłości działania infrastruktury IT, a także dostaw, wdrożenia i utrzymania infrastruktury dostępowej.

Tym co wyróżnia grupę Passus spośród firm integracyjnych, 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. 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, Ministerstwo Sprawiedliwości, Orange, PGE, Ikea, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, PKN Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

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. Od lipca 2018 roku spółka notowana jest na rynku NewConnect. Grupa zatrudnia blisko 60 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów.

Firma Passus S.A. od 2013 roku jest partnerem Splunk w Polsce i aktualnie posiada status Splunk Premier Reseller.