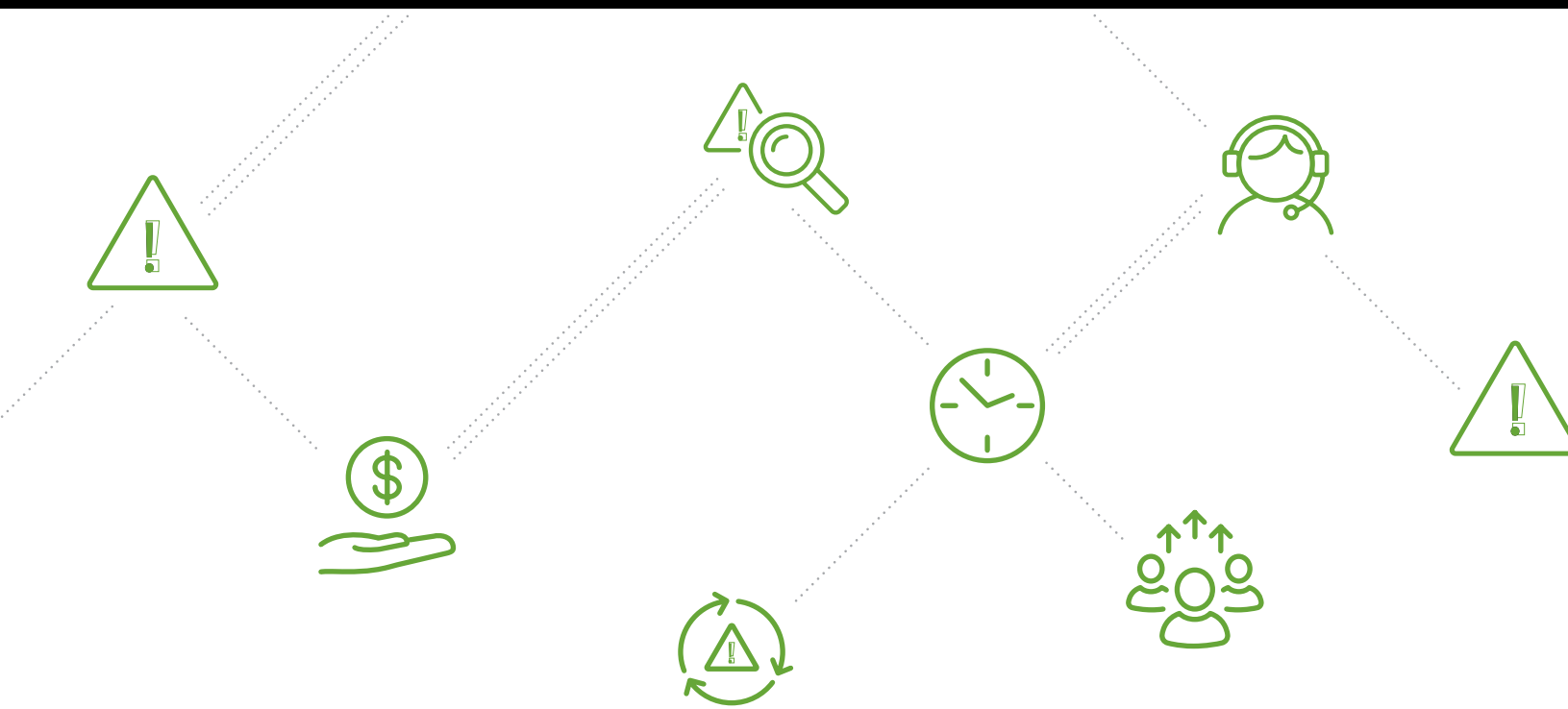
Przewodnik dla kupujących SIEM na rok 2020

Wszystko, co musisz wiedzieć przed zakupem opartego na dogłębnej analizie systemu zarządzania bezpieczeństwem

SPIS TREŚCI



1. CZYM JEST SIEM

Zarządzanie informacją i zdarzeniami bezpieczeństwa można porównać do systemu radarowego, z którego korzystają piloci i kontrolerzy ruchu lotniczego - bez odpowiednio wdrożonego systemu SIEM, zarządzanie bezpieczeństwem IT w firmie jest prowadzone na oślep.

I choć urządzenia zabezpieczające i oprogramowanie systemowe dobrze wychwytują i rejestrują pojedyncze ataki oraz nietypowe zachowania, współcześnie najpoważniejsze zagrożenia wykorzystują cechy systemów i zaawansowane techniki podszywania się, by niezauważenie przejść przez bariery ochronne. Bez SIEM drobne ataki mogą się rozwijać i ostatecznie przerodzić w katastroficzne w skutkach zdarzenia. Potrzeba stosowania SIEM jest coraz większa przez rosnące wyrafinowanie hakerów i powszechność korzystania z usług w chmurze, co tylko zwiększa podatność na ataki.

W tym przewodniku chcemy wyjaśnić, czym rozwiązanie SIEM jest, a czym nie jest, opisać jego rozwój i wyjaśnić, jaki jest jego cel, oraz jak ustalić, czy to odpowiednie rozwiązanie dla Twojej organizacji.

Zatem czym jest SIEM?

Gartner definiuje SIEM jako "technologię, która wspiera wykrywanie zagrożeń i reagowanie na wypadki związane z bezpieczeństwem poprzez zbieranie danych w czasie rzeczywistym i analizę historyczną zdarzeń związanych z bezpieczeństwem z szerokiej gamy zdarzeń i kontekstowych źródeł danych".

W niniejszym poradniku stosujemy termin „oparte na dogłębnej analizie rozwiązanie SIEM". Jest to sformułowanie opisujące takie rozwiazanie SIEM, które wykorzystuje zaawansowane algorytmy sztucznej inteligencji (AI – Artificial Intelligence) w połączeniu z mechanizmami uczenia maszynowego (ML - Machine Learning) w czasie rzeczywistym i jest nowszą generacją tradycyjnego SIEM.

O co w tym wszystkim chodzi?

Mówiąc jak najprościej: SIEM to platforma bezpieczeństwa, która przetwarza zapisy zdarzeń i zbiera je w jednym miejscu, oferując pojedynczy widok tych danych opatrzony dodatkowymi informacjami.

Rozwój SIEM

SIEM nie jest nową technologią. Podstawowe możliwości platformy istnieją w różnych formach od prawie 15 lat. Z czasem rozwiązania SIEM przekształciły się w rodzaj platformy informacyjnej - ich zastosowanie zostało rozszerzone o raportowanie zgodności, agregowanie logów z zapór sieciowych i innych urządzeń. Jednak technologia SIEM była często złożona i mało uniwersalna, a do tego żeby w ogóle zidentyfikować ataki, specjaliści IT musieli wiedzieć, czego dokładnie szukają. Technologia stała się zbyt skomplikowana i nieskalowalna.

Taka sytuacja doprowadziła ostatecznie do skutecznego rozwoju systemów SIEM, które stały się bardziej elastyczne i łatwiejsze w użyciu. Dziś wydaje się to szczególnie istotne, ponieważ organizacje przyjęły rozwiązania w chmurze, a cyfrowa transformacja dotyczy niemal każdego aspektu naszego życia.

Dlatego ważne jest, aby zrozumieć i pokazać wyraźną różnicę między tradycyjnym SIEM i nowoczesnym rozwiązaniem SIEM opartym na dogłębnej analizie, do którego przejdziemy później.

Istotne jest także zrozumienie rodzajów zastosowań z obszaru SIEM i określenie, czy Twoja organizacja rzeczywiście potrzebuje rozwiązania SIEM, czy czegoś innego.

To wszystko prowadzi do jasnego rozróżnienia pomiędzy starszą generacją SIEM a nowoczesnymi, opartymi na dogłębnej analizie rozwiązaniami SIEM.

Tradycyjne rozwiązania SIEM to już przeszłość

Znalezienie mechanizmu gromadzenia, przechowywania i analizowania danych służących wyłącznie bezpieczeństwu jest stosunkowo proste - nie brakuje sposobów przechowywania danych. Jednak zebranie wszystkich danych istotnych dla bezpieczeństwa i przekształcenie ich w zbiór przydatnych informacji umożliwiających działanie to już zupełnie inna sprawa.

Wiele przedsiębiorstw IT, które zainwestowały w tradycyjny SIEM, doświadczyło tego na własnej skórze. Okazało się bowiem - i to dopiero po wykorzystaniu znacznych zasobów czasu i pieniędzy na rejestrowanie zdarzeń związanych z bezpieczeństwem - że problemem było nie tylko to, ile czasu pochłania przetworzenie danych, lecz także statyczność systemu tworzącego SIEM.

Co więcej, możliwe do przeanalizowania dane pochodziły wyłącznie ze zdarzeń związanych z bezpieczeństwem. Utrudniało to powiązanie ich z tym, co dzieje się równolegle w pozostałej części środowiska IT. Kiedy pojawia się problem, zbadanie zdarzenia związanego z bezpieczeństwem i osadzenie go we właściwym kontekście zajmuje cenny czas, którego większość organizacji IT zwyczajnie nie ma.

Ponadto tradycyjne rozwiązania SIEM nie nadążają już za tempem, w jakim należy badać zdarzenia związane z bezpieczeństwem. Ciągłe wdrażanie usług w chmurze zwiększa wrażliwość na potencjalne zagrożenia, a przedsiębiorstwa muszą jednocześnie monitorować aktywność użytkowników, zachowanie, dostęp do kluczowych aplikacji w chmurze, trybie SaaS (SaaS - *Software as a Service*) czy usługi lokalnej w celu określenia pełnego zakresu potencjalnych zagrożeń i ataków.

Tradycyjny SIEM – problemy i charakterystyka

PROBLEM	SKUTEK
Brak dostępu do wymaganych danych	Ogranicza wykrycie, śledzenie i reakcję
Trudny w utrzymaniu i obsłudze	Wymaga wykwalifikowanego personelu
Wysoki poziom zafałszowanych wyników	Obciąża SecOps
Niestabilny	Liczne awarie
Nieelastyczne dane	Nie dostosowuje się do konkretnych przypadków
Statyczne algorytmy	Ograniczony i powolny
Nie wykrywa współczesnych zagrożeń	Zwiększa ryzyko biznesowe

Alternatywa: oparte na dogłębnej analizie rozwiązania SIEM

To, czego potrzebuje dziś branża IT, to prosty sposób na wprowadzenie korelacji pomiędzy informacjami zebranymi ze wszystkich danych powiązanych z bezpieczeństwem; rozwiązanie, które umożliwi IT łatwe zarządzanie nim. Zamiast jedynie obserwować zdarzenia już po ich wystąpieniu, organizacja IT powinna być w stanie je przewidzieć i wdrożyć środki zapobiegawcze w celu ograniczenia podatności na zagrożenia w czasie rzeczywistym. W tym celu przedsiębiorstwa potrzebują opartej na dogłębnej analizie platformy SIEM.

Właśnie na tym polega różnica między starszą generacją SIEM i nowoczesnym rozwiązaniem. Gartner pisze, że **„nowoczesny SIEM działa nie tylko na danych pochodzących z logów i potrafi więcej niż stosować proste reguły korelacji do analizy danych”.**

W tym momencie konkretny typ współczesnego SIEM - taki, który nazywamy rozwiązaniem SIEM opartym na dogłębnej analizie - wkracza na scenę. To nowoczesne rozwiązanie pozwala IT monitorować zagrożenia w czasie rzeczywistym i szybko reagować na wszystkie zdarzenia, co umożliwia całkowite uniknięcie lub przynajmniej znaczne ograniczenie szkód. Warto jednak pamiętać, że nie wszystkie ataki mają charakter zewnętrzny - dział IT potrzebuje także sposobu na monitorowanie aktywności użytkowników. Takie działanie pozwoli zminimalizować ryzyko związane z zagrożeniami wewnętrznymi lub przypadkowym naruszeniem bezpieczeństwa. Analiza zagrożeń, którą oferuje nowoczesny SIEM, ma kluczowe znaczenie dla zrozumienia rodzaju konkretnych ataków oraz ich środowiska, czyli umieszczenia zagrożeń w odpowiednim kontekście. SIEM zorientowany na analitykę musi wyróżniać się w działaniach związanych z bezpieczeństwem, dając zespołom IT możliwość stosowania wyszukanych metod ilościowych w celu uzyskania wglądu w niezbędne działania i ustalenia ich priorytetów. Współczesny SIEM musi być także wyposażony w specjalistyczne narzędzia niezbędne do zwalczania zaawansowanych zagrożeń - już w ramach podstawowej platformy.

Kolejną istotną różnicą między SIEM opartym na dogłębnej analizie a starszą generacją SIEM jest elastyczny charakter nowoczesnego rozwiązania, dzięki któremu możliwe jest wdrożenie go zarówno w trybie on-premise, jak i w chmurze czy nawet w środowisku hybrydowym.

7 powodów, dla których warto zastąpić dotychczasowy system SIEM

Firmy są często powiązane z przestarzałymi architekturami tradycyjnych SIEM korzystającymi z bazy danych SQL o stałej strukturze - mogą one stać się przyczyną awarii lub mieć ograniczoną wydajność i elastyczność.

1. OGRANICZONE RODZAJE OCHRONY	Przez ograniczenie rodzaju przetwarzanych danych musisz liczyć się z ograniczeniami wykrywania i rozpoznawania zagrożeń oraz wydłużonym czasem reakcji.
2. BRAK EFEKTYWNEGO PRZETWARZANIA DANYCH	W przypadku tradycyjnego SIEM, przetwarzanie danych może być pracochłonnym procesem lub okazać się bardzo kosztowne.
3. POWOLNE ŚLEDZTWA	W przypadku tradycyjnego SIEM nawet tak podstawowe czynności jak wyszukiwanie nieprzetworzonych logów mogą zająć dużo czasu - często wiele godzin czy dni.
4. OGRANICZONA STABILNOŚĆ I SKALOWALNOŚĆ	Im większe są bazy danych oparte na SQL, tym mniejsza ich stabilność. Klienci często cierpią z powodu niskiej wydajności i przeciążeń serwerów, a co za tym idzie - możliwości przestroju.
5. SCHYŁEK TECHNOLOGII I BRAK PLANÓW NA ROZWÓJ	Zmiany własnościowe u dostawców tradycyjnych SIEM powodują spowolnienie prac badawczo-rozwojowych niemal do zera. Bez ciągłych inwestycji i wdrażania innowacji rozwiązań dla bezpieczeństwa nie można nadążyć za rosnącym wachlarzem zagrożeń.
6. ZAMKNIĘTY EKOSYSTEM	Dostawcy tradycyjnego SIEM często nie mogą zapewnić zintegrowania systemu z innymi narzędziami na rynku. Klienci mogą korzystać tylko z tego, co oferuje ich SIEM, lub zakupić niestandardowe oprogramowanie i profesjonalne usługi.
7. OGRANICZENIA LOKALNE	Tradycyjne systemy SIEM mogą być wdrożone jedynie w systemie on-premise, podczas gdy współcześnie specjaliści ds. bezpieczeństwa w sieci muszą mieć możliwość korzystania z chmury i rozwiązań hybrydowych.

Przenieś swój SIEM do chmury

Uruchamianie SIEM w chmurze lub jako SaaS może pomóc zniwelować problemy wielu organizacji z zakresu bezpieczeństwa, a mimo to wielu liderów IT wciąż nie pokłada zaufania w bezpieczeństwo i niezawodność chmury. Zanim odrzucisz rozwiązanie SIEM oparte na chmurze, wiedz, że praktyki i technologie bezpieczeństwa w większości dużych usług w chmurze mogą być znacznie bardziej wyrafinowane niż w typowym przedsiębiorstwie. SaaS jest już szeroko stosowany w systemach o kluczowym znaczeniu dla biznesu, takich jak CRM, HR, ERP i analityka biznesowa.

Te same powody, które czynią SaaS dobrym wyborem dla firmowego oprogramowania - szybkie, wygodne wdrażanie, niskie koszty operacyjne, automatyczne aktualizacje, rozliczanie w oparciu o użytkowanie i skalowalna, solidna infrastruktura - sprawiają, że chmura jest doskonałym środowiskiem dla nowoczesnego systemu SIEM.

Rozwiązania oparte na chmurze zapewniają elastyczność w użytkowaniu szerokiej gamy zestawów danych zarówno w systemie on-premise, jak i w chmurze. Ponieważ coraz więcej firm zaczyna pracować w modelach takich jak infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) i wspomniane już oprogramowanie jako usługa (SaaS), łatwość integracji z systemami innych firm pokazuje, że SIEM w chmurze ma jeszcze większy sens. Najważniejsze korzyści płynące z przeniesienia SIEM do chmury to przede wszystkim elastyczność, jaką zapewnia architektura hybrydowa, automatyczne aktualizacje oprogramowania, uproszczona konfiguracja, skalowalna infrastruktura, duże możliwości dopasowania systemu do indywidualnych potrzeb oraz wysoka dostępność.

Obszary zastosowań SIEM w przedsiębiorstwach

Teraz, gdy już poznałeś rozwój SIEM i cechy, które odróżniają nowoczesny, oparty na analityce system od tradycyjnego SIEM, przyszedł czas na wyjaśnienie, jakie zastosowania ma ta technologia w przedsiębiorstwach

Wczesne wykrycie, szybka reakcja i współpraca w celu ograniczenia zaawansowanych zagrożeń nakładają znaczne oczekiwania na dzisiejsze zespoły ds. bezpieczeństwa. Raportowanie i monitorowanie logów i zdarzeń nie jest już wystarczające. Specjaliści potrzebują szerszego wglądu w źródła wszystkich danych wygenerowanych przez firmę - od elementów IT, przez organizację, po chmurę. Aby uprzedzać ataki zewnętrzne i wewnętrzne, firmy potrzebują zaawansowanego rozwiązania dla bezpieczeństwa, które pozwoli na szybkie reagowanie na zagrożenia, badanie poszczególnych incydentów i koordynowanie scenariuszy naruszenia CSIRT. Ponadto firmy muszą mieć możliwość wykrywania i reagowania na znane, nieznane i zaawansowane zagrożenia.

Zespoły ds. bezpieczeństwa w przedsiębiorstwach muszą korzystać z rozwiązania SIEM, które potrafi odpowiedzieć nie tylko na typowe przypadki użycia zabezpieczeń, lecz także te zaawansowane. Aby móc nadążyć za dynamicznie zmieniającym się wachlarzem zagrożeń, oczekuje się, że nowoczesne systemy SIEM będą w stanie:

- Centralizować i agregować na bieżąco wszystkie istotne dla bezpieczeństwa zdarzenia.
- Obsługiwać różne formy odbioru plików, mechanizmy ich zbierania, w tym Syslog, a także transmisję i gromadzenie plików.
- Dodawać informacje o kontekście i analizę zagrożeń do zdarzeń związanych z bezpieczeństwem.
- Korelować zdarzenia z całego zakresu danych i ostrzegać o nich.
- Wykrywać zaawansowane i nieznane zagrożenia.
- Profilować zachowania użytkowników w obrębie całej organizacji.
- Przetwarzać wszystkie dane (użytkowników, aplikacje) i udostępniać je do użytku - monitorowanie, alarmowanie, śledzenie, wyszukiwanie ad hoc.
- Zapewniać wyszukiwanie ad hoc i dokładne raportowanie na podstawie dostępnych danych umożliwiające zaawansowaną analizę naruszeń bezpieczeństwa.
- Badać podejrzane incydenty i rozpatrywać je w celu wykonania szczegółowej analizy śledczej.
- Umożliwić ocenę i tworzenie raportów zgodności.
- Korzystać z danych analitycznych i tworzyć raporty dotyczące poziomu bezpieczeństwa.
- Śledzić ataki hakerskie dzięki usprawnionej analizie ad hoc i sekwencjonowaniu zdarzeń.

Mimo że dane gromadzone przez SIEM pochodzą przede wszystkim z serwerów i logów urządzeń sieciowych, mogą również być zbierane z urządzeń końcowych, urządzeń do zabezpieczania sieci, aplikacji, usług w chmurze, systemów uwierzytelniania i autoryzacji oraz dostępnych w sieci baz danych o podatnościach i zagrożeniach.

Ale agregacja danych to zaledwie połowa historii. Po zebraniu odpowiednich informacji, oprogramowanie SIEM koreluje dane w repozytorium i szuka nietypowych zachowań, anomalii systemowych i innych sygnałów, które mogą wskazywać na zagrożenie. Informacje te są wykorzystywane nie tylko do powiadamiania o zdarzeniach w czasie rzeczywistym, ale także do audytowania i raportowania zgodności oraz wydajności, analizy trendów z przeszłości czy wyników analityki śledczej.

Biorąc pod uwagę coraz większą liczbę i zaawansowanie zagrożeń w sieci, a także rosnącą wartość zasobów cyfrowych w niemal każdej organizacji, nie jest zaskakujące, że wdrażanie systemów bezpieczeństwa SIEM opartych na dogłębnej analizie jest coraz bardziej powszechne w całym środowisku IT.

Czy rzeczywiście potrzebujesz systemu SIEM?

Skoro już rozumiesz, do czego służy SIEM, czas na poważniejszą dyskusję: faktycznie potrzebujesz rozwiązania SIEM czy jednak czegoś innego? Być może Twoja organizacja jeszcze nie jest gotowa na tak zaawansowane narzędzie, a zamiast tego możesz wdrożyć prostsze rozwiązanie - takie jak centralne zarządzanie logami (CLM) - zapewniające wgląd w dane maszynowe. Bez ogródek zachęcamy: poznaj **Splunk Enterprise dla bezpieczeństwa i zarządzania logami.**

Czym jest centralne zarządzanie logami? CLM można najprościej zdefiniować jako rozwiązanie, które daje ogólny, scentralizowany wgląd w dane logów. Żeby lepiej to zrozumieć, zadajmy kolejne pytanie: czym właściwie są dane z logów?

Dane z logów to wygenerowane komputerowo wiadomości i komunikaty, które stanowią ostateczny zapis tego, co dzieje się w każdej firmie, organizacji lub agencji, i często pozostają niewykorzystanym zasobem gdy zajdzie potrzeba rozwiązywania problemów i wspierania szerszych celów biznesowych.

Wróćmy do CLM. Celem zarządzania logami jest zbieranie ich i udostępnianie do celów wyszukiwania i raportowania. Mówiąc w języku bezpieczeństwa, CLM może pomóc z badaniem niebezpiecznych zdarzeń i alarmowaniem o nich na czas.

Zarządzanie logami jest jedną z najważniejszych funkcji oferowanych przez SIEM od początków istnienia tego systemu. Ale jeśli jedyne, czego potrzebujesz, to wgląd w dane z Twoich logów, czy SIEM na pewno jest odpowiednim rozwiązaniem dla Ciebie? Zwróćmy się z tym pytaniem do poważanego w środowisku **analityka SIEM, Antona Chuvakina:**

Mówiąc bardziej bezpośrednio, jeśli używasz SIEM wyłącznie do agregacji logów, przepłacasz. Kluczowe w systemie SIEM jest właśnie to, że można go wykorzystywać do rozwiazywania zarówno prostych, jak i bardzo zaawansowanych przypadków.

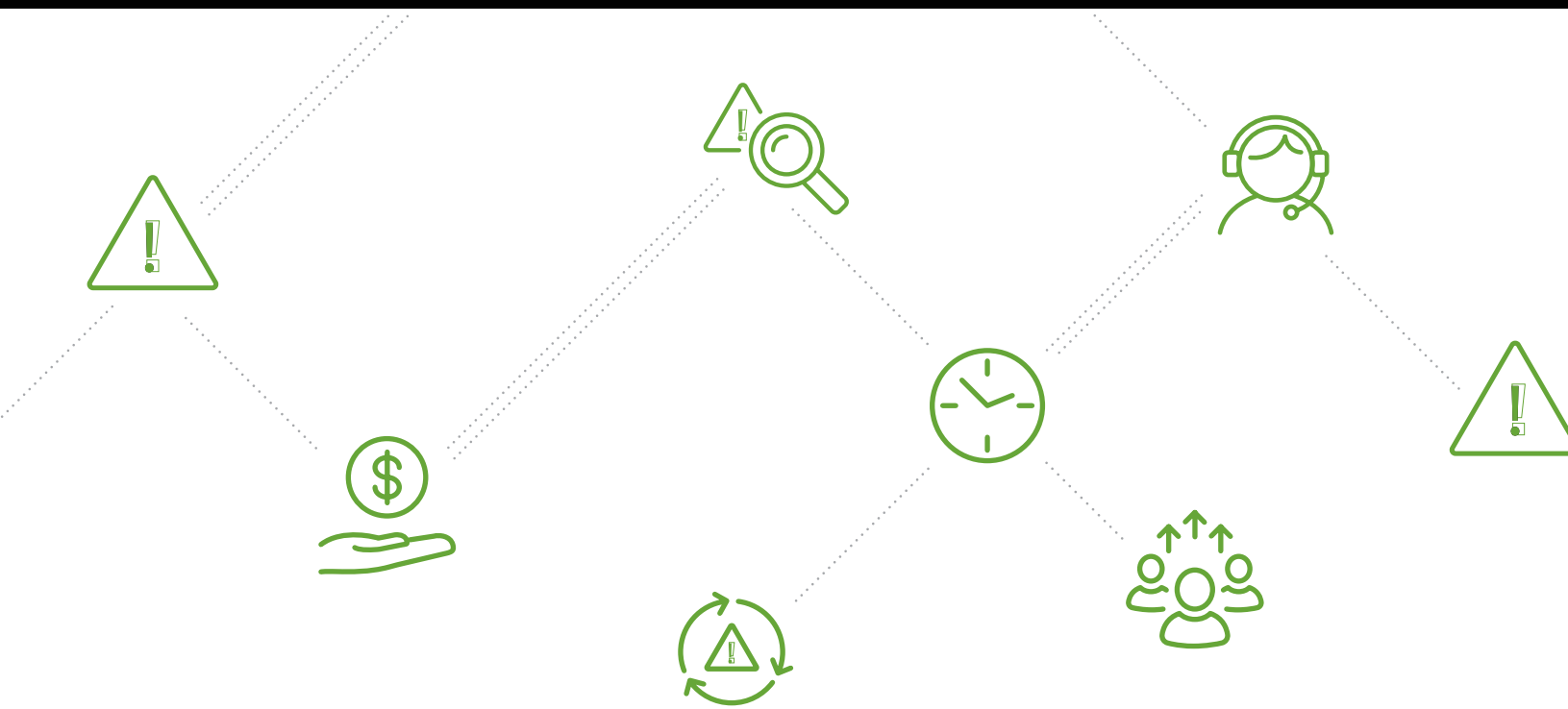
Warto przytoczyć **opracowany przez firmę Gartner termin** - analiza zachowania użytkowników i podmiotów (UEBA - *User and Entity Behavior Analytics*). Warto wiedzieć, że istnieją inne nazwy dla określenia tej samej technologii, na przykład **preferowana przez Forrester** analiza zachowania użytkowników dla celów bezpieczeństwa (*Security User Behavior Analytics*) i **stosowana przez Splunk** analiza zachowania użytkowników (UBA - *User Behavior Analytics*). Tym ostatnim terminem będziemy się tu posługiwać. Wszystkie są zasadniczo różnymi sposobami odwoływania się do tych samych działań.

UBA wykorzystuje się do wykrywania niebezpieczeństw, by rozpoznać i usunąć wewnętrzne i zewnętrzne zagrożenia. UBA często jest postrzegane jako bardziej zaawansowana technologia, m.in. dlatego, że posiada zdolność uczenia się i określania bazowych nawyków użytkownika. Dzięki temu może np. wysyłać ostrzeżenie, gdy wydarzy się coś wychodzącego poza normę. Aby stworzyć zestaw standardowych zachowań użytkownika, rozwiązanie UBA może śledzić takie działania jak:

- Z jakiej lokalizacji zwykle się loguje
- Jakie uprawnienia posiada
- Do jakich plików, serwerów i aplikacji ma dostęp
- Z jakich urządzeń zwykle się loguje

Co ciekawe, niektórzy dostawcy UBA - najczęściej nowi na rynku - próbują konkurować z systemami SIEM. Faktem jest, że UBA to naprawdę użyteczne rozwiązanie, ale samo w sobie nie może zastąpić SIEM, nie jest też jego nową kategorią. To samodzielnie funkcjonująca technologia bezpieczeństwa. Oczywiście warto pamiętać, że najlepsze efekty dałaby współpraca UBA z rozwiązaniem SIEM opartym na dogłębnej analizie.

Mówiąc prościej: tak samo jak rozwiązanie CLM, tak i rozwiązanie UBA nie jest SIEM. **Gdyby tylko doktor Chuvakin napisał o tym tweeta...**



2. KLUCZOWE FUNKCJE SIEM

Nadszedł wreszcie czas na przejście do samego sedna, czyli do tego, co składa się na system SIEM oparty na dogłębnej analizie. Możemy wyróżnić siedem kluczowych funkcji, które oferuje:

MONITOROWANIE W CZASIE RZECZYWISTYM	Nowoczesne zagrożenia rozprzestrzeniają się naprawdę szybko, dlatego dział IT musi mieć możliwość monitorowania zagrożeń i korelowania zdarzeń w czasie rzeczywistym, by wykryć i powstrzymać zagrożenia.
ZARZĄDZANIE INCYDENTAMI	Dział IT potrzebuje sprawnego rozwiązania, dzięki któremu potencjalne naruszenia bezpieczeństwa będą mogły być szybko zneutralizowane, a następstwa takiego incydentu mniej odczuwalne. Sprawne reagowanie na włamania ograniczy wyrządzone szkody i poniesione koszty.
MONITOROWANIE UŻYTKOWNIKÓW	Kontekstowe monitorowanie aktywności użytkownika ma kluczowe znaczenie dla identyfikowania naruszeń i wykrywania przypadków niewłaściwego użycia oprogramowania. Monitorowanie uprzywilejowanych użytkowników jest też częstym wymogiem podczas raportowania zgodności.
ANALIZA ZAGROŻEŃ	Analiza zagrożeń może pomóc IT w wykrywaniu nieprawidłowych działań, ocenie ryzyka dla biznesu i nadaniu priorytetów reakcjom na ataki i zagrożenia.
ZAAWANSOWANA ANALITYKA	Analityka jest kluczem do wyciągnięcia wniosków z analizy dużej ilości danych, a uczenie maszynowe może zautomatyzować ją i usprawnić identyfikowanie ukrytych zagrożeń.
ZAAWANSOWANE METODY WYKRYWANIA ZAGROŻEŃ	Specjaliści ds. bezpieczeństwa potrzebują zaawansowanych narzędzi do monitorowania, analizy i wykrywania zagrożeń w całym procesie.
BIBLIOTEKA ZASTOSOWAŃ	Rozumienie zagrożeń i szybka reakcja w czasie rzeczywistym są konieczne dla ograniczenia ryzyka działania organizacji.

Wszystkie te funkcje pozwalają organizacjom korzystać z rozwiązania SIEM dla wielu zastosowań, takich jak zarządzanie bezpieczeństwem i kontrola zgodności. Dzięki nim możemy także zdefiniować SIEM w oparciu o jego możliwości. Przyjrzyjmy się bliżej każdej niezbędnej funkcji, którą oferuje oparty na dogłębnej analizie system SIEM.

Monitorowanie w czasie rzeczywistym

Im dłużej trwa wykrycie zagrożenia, tym więcej szkód może ono wyrządzić. Organizacje IT potrzebują systemu SIEM, który umożliwia monitorowanie w czasie rzeczywistym każdego rodzaju danych, niezależnie od tego, czy są one ulokowane w siedzibie firmy czy w chmurze. Co więcej, monitorowanie musi obejmować zarówno dane kontekstowe, takie jak dane o zasobach i tożsamości, jak i kanały analizy zagrożeń, które mogą być używane do generowania alertów.

SIEM oparty na dogłębnej analizie musi być w stanie zidentyfikować wszystkie podmioty w środowisku IT, w tym użytkowników, urządzenia i aplikacje, a także wszelkie działania niezwiązane bezpośrednio z tożsamością. SIEM powinien wykorzystywać te dane w czasie rzeczywistym do identyfikowania szerokiej gamy różnych typów i klas podejrzanych zachowań, a później z łatwością wprowadzić je do algorytmów mających na celu ocenę potencjalnego ryzyka, które niesie ze sobą konkretne zagrożenie.

Powinny istnieć także takie udogodnienia jak biblioteka konfigurowalnych, predefiniowanych reguł korelacji, konsola zdarzeń bezpieczeństwa, która zapewni widok zdarzeń związanych z bezpieczeństwem w czasie rzeczywistym, oraz pulpity nawigacyjne zapewniające wizualizacje bieżącej aktywności zagrożeń - również w czasie rzeczywistym.

Co istotne, wszystkie te możliwości dobrze jest rozszerzyć o gotowe do użycia procesy wyszukiwania powiązań między zdarzeniami, które będzie można uruchamiać w czasie rzeczywistym lub zaplanować ich regularne uruchamianie w określonym czasie. Nie mniej ważny jest fakt, że wyszukiwania te powinny być dostępne za pośrednictwem intuicyjnego interfejsu, który wyeliminuje potrzebę opanowania specyficznego języka wyszukiwania przez administratorów IT.

Na koniec przypomnijmy jeszcze, że oparty na dogłębnej analizie SIEM musi zapewniać możliwość lokalnego wyszukiwania danych historycznych w czasie rzeczywistym w taki sposób, by zredukować ilość ruchu sieciowego generowanego na potrzeby wyszukiwań.

Autodesk oszczędza czas i koszty inwestycji ze Splunk na AWS

Klienci z branży produkcyjnej, architektonicznej, budowlanej, medialnej i rozrywkowej - w tym 20 ostatnich laureatów Oscara za najlepsze efekty wizualne - używają oprogramowania Autodesk do projektowania, wizualizacji i symulacji swoich pomysłów. Biorąc pod uwagę tak szeroki globalny zasięg, Autodesk stanął przed dwoma szczególnie istotnymi wyzwaniami: potrzebą uzyskania wglądu w obszary biznesu, operacji i bezpieczeństwa w oddziałach na całym świecie oraz koniecznością wyboru odpowiedniej infrastruktury do wdrożenia oprogramowania do analityki biznesowej. Od czasu wdrożenia platformy Splunk firma odnotowała korzyści, w tym:

- Oszczędności na poziomie setek tysięcy dolarów.
- Dostęp do kluczowych informacji operacyjnych i dotyczących bezpieczeństwa.
- Kontrola wyników sprzedaży linii produktowych w czasie rzeczywistym.

Dlaczego Splunk?

Splunk po raz pierwszy znalazł się w Autodesk w 2007 roku jako sposób na wykorzystanie danych maszynowych do rozwiązywania rozmaitych problemów operacyjnych. Obecnie wykorzystanie to zostało rozszerzone o monitorowanie w czasie rzeczywistym, dostarczanie szczegółowych informacji o bezpieczeństwie i analizy biznesowe istotne dla kadry kierowniczej w trzech działach firmy Autodesk, w tym:

- Enterprise Information Services (EIS) - dział odpowiedzialny za globalne zarządzanie IT firmy, w tym bezpieczeństwo informacji i zarządzanie informacjami.
- Autodesk Consumer Group (ACG) - dział odpowiedzialny za wszystkie produkty firmy Autodesk skierowane do konsumentów.
- Information Modeling & Platform Products (IPG) - dział odpowiedzialny za rozwiązania Autodesk dla klientów komercyjnych, w tym projektantów i inżynierów ze wszystkich branż.

Autodesk wykorzystuje Splunk Enterprise Security (Splunk ES), by ograniczyć czas potrzebny na zidentyfikowanie i usunięcie problemów związanych z bezpieczeństwem. Firma wykorzystuje także Splunk App for AWS do zarządzania zasobami dostarczanymi dla Splunk Enterprise i innych krytycznych aplikacji.

Podejmuj decyzje w oparciu o dane

Splunk Enterprise, aplikacja Splunk dla AWS, Splunk Enterprise Security i inne rozwiązania Splunk umożliwiają Autodesk uzyskanie wglądu w czasie rzeczywistym w obszary dotyczące wydajności operacji biznesowych, zarządzania bezpieczeństwem i produktów. Elastyczne, oparte na analizie danych oprogramowanie Splunk i platforma AWS oszczędzają czas firmy Autodesk i zmniejszają koszty kapitału, a przy tym ułatwiają podejmowanie kluczowych decyzji. **Czytaj dalej.**

Reagowanie na incydenty

Podstawą każdej skutecznej strategii reagowania na incydenty jest solidna platforma SIEM, która nie tylko umożliwia samą identyfikację różnorodnych incydentów, lecz także zapewnia środki do ich śledzenia i ponownego przypisania, a także dodawania adnotacji.

Co ważne przy doborze SIEM, technologia ta powinna zapewnić działowi IT możliwość nadania członkom organizacji adekwatnego do ich ról poziomu dostępu do zabezpieczeń. Inne kluczowe funkcje obejmują możliwość wybrania ręcznego lub automatycznego agregowania zdarzeń, obsługę interfejsów programowania aplikacji (API), które mogą być używane do pobierania danych lub przekazywania informacji do systemów zewnętrznych, a także możliwość bezpiecznego gromadzenia prawnie dopuszczalnych dowodów przestępstw w sieci oraz poradników, które dostarczają organizacjom wskazówek, jak reagować na określone rodzaje incydentów.

Co jednak najważniejsze, SIEM oparty na dogłębnej analizie musi być wyposażony w możliwości automatycznego reagowania na cyberataki, co umożliwi mu przerwanie ich nawet bez ingerencji człowieka.

W efekcie platforma SIEM musi być hubem, wokół którego można stworzyć konfigurowalny system algorytmów skuteczny w zarządzaniu incydentami. Oczywiście nie każdy incydent ma taki sam poziom ważności. SIEM oparty na dogłębnej analizie zapewnia organizacjom informatycznym możliwość odgórnego określania dotkliwości każdego potencjalnego zagrożenia za pomocą pulpitów nawigacyjnych (dashboards). Można ich używać do segregowania nowych, istotnych zdarzeń, przypisywania ich analitykom do przeglądu oraz badania szczegółów przeznaczonych dla zarządzających śledztwem. Oparty na dogłębnej analizie system SIEM może uzbroić organizacje IT w wiedzę kontekstową niezbędną do ustalenia właściwej reakcji na każde zdarzenie.

Takie możliwości obejmować powinny także rozpoznawanie istotnych zdarzeń, ich statusu i dotkliwości, co z kolei pozwoli na rozpoczęcie procesu naprawy i zapewni audyt całego procesu powiązanego z niebezpiecznym zdarzeniem.

Dodajmy jeszcze, że zespół IT powinien posiadać pulpit nawigacyjny umożliwiający wygodne stosowanie filtrów podczas śledzenia sprawy, aby rozszerzyć lub zmniejszyć zakres analizy za pomocą kilku kliknięć. Ostatecznym celem powinno być umożliwienie dowolnemu członkowi zespołu ds. bezpieczeństwa umieszczenia wydarzeń, działań i adnotacji na osi czasu, która ułatwi innym członkom zespołu łatwe zrozumienie tego, co się dzieje bądź działo. Takie osie czasu można następnie umieścić w dzienniku, który ułatwi przegląd ataków i wdrożenie powtarzalnej metodologii procesu unieszkodliwienia ataku w celu radzenia sobie ze zdarzeniami określonego typu.

PagerDuty zapewnia kompleksową widoczność dzięki Splunk Cloud i Amazon Web Services

Klienci korzystają z PagerDuty, korporacyjnej usługi reagowania na incydenty, aby szybko i skutecznie zarządzać i rozwiązywać swoje problemy informatyczne. Kiedy Pager Duty, firma działająca w chmurze, potrzebowała rozwiązania spełniającego potrzeby skutecznej analizy operacyjnej i segregacji danych, zdecydowała się skorzystać z usługi Splunk Cloud działającej na Amazon Web Services (AWS). Dzięki Splunk Cloud i AWS, PagerDuty zapewnia wysoką dostępność i skalowalność usług w odpowiedzi na zmieniające się potrzeby klientów.

Od czasu wdrożenia Splunk Cloud, PagerDuty odnotował znaczące korzyści, w co wlicza się:

- Wysoki poziom satysfakcji klientów i dostępu usług w chmurze.
- O 30% większe oszczędności w porównaniu do poprzednio stosowanej usługi.
- Skrócony czas rozwiązywania problemów związanych z IT i bezpieczeństwem - od niespełna godziny do kilku minut lub nawet sekund.

Dlaczego Splunk?

Arup Chakrabarti jest dyrektorem inżynierii infrastruktury w PagerDuty. Do niego należą kwestie takie jak stabilność witryny, wewnętrzne systemy i zarządzanie bezpieczeństwem. Jego zadaniem jest dbanie o produktywność i wydajność organizacji inżynierskiej PagerDuty, w której skład wchodzi wiele różnorodnych zespołów dbających o rozwój produktu w firmie.

Przed wdrożeniem Splunk Cloud, PagerDuty polegał na systemie logów, którego nie można było w żaden sposób skalować, ponieważ firma codziennie indeksowała setki gigabajtów danych. Co gorsza, zespołowi trudno było z tak wielu danych wyciągnąć przydatne informacje, aby z ich użyciem sprawnie podejmować decyzje i rozwiązywać problemy. Po uruchomieniu równolegle poprzedniej usługi i Splunk Cloud zespół ustalił, że Splunk Cloud zapewnia szybkość wymaganą do rozwiązywania problemów na wysokim poziomie i zapewnia klientom doskonałą dostępność usługi. W ciągu kilku dni inżynierowie przeprowadzili migrację do Splunk Cloud.

„Kiedy korzystaliśmy z poprzedniego rozwiązania, dla niektórych zapytań samo przygotowanie danych i dostarczenie potrzebnych informacji zajmowało nawet 30 minut, a to było po prostu nie do przyjęcia", mówi Chakrabarti. „Ostatecznie udało nam się skrócić ten czas z dziesiątek do zaledwie kilku minut lub sekund dzięki Splunk Cloud."

Chakrabarti zauważa, że chociaż koszt nie był głównym czynnikiem decydującym o wyborze Splunk Cloud, **„Mój zespół księgowy był absolutnie zachwycony, kiedy powiedziałem im: «Dostaniemy najlepsze rozwiązanie, a tak swoją drogą, jest o 30% tańsze w porównaniu z tym, które obecnie używamy.»"** **Czytaj dalej.**

Monitorowanie użytkowników

Nawet w najbardziej podstawowej wersji, monitorowanie aktywności użytkowników musi obejmować możliwość analizowania danych dotyczących dostępu i uwierzytelniania, ustalenia kontekstu zachowań użytkownika i ostrzegania o podejrzanych zachowaniach i naruszeniach reguł korporacyjnych i urzędowych.

Niezwykle ważne jest, aby monitorowanie użytkowników zostało rozszerzone na uprzywilejowanych użytkowników, którzy najczęściej stają się celami ataków, a ich narażenie może oznaczać największe szkody. Właśnie z uwagi na to ryzyko, monitorowanie uprzywilejowanych użytkowników jest częstym wymogiem w zakresie raportowania zgodności w branżach podlegających najbardziej restrykcyjnym regulacjom.

Osiągnięcie tych celów wymaga stałego podglądu sytuacji w czasie rzeczywistym i takiej formy raportowania, która nie tylko pozwoli wykorzystywać różnorodne mechanizmy identyfikowania tożsamości, lecz także może zostać rozszerzona o dowolną liczbę aplikacji i usług innych firm.

Travis Perkins PLC zastosował oparty na dogłębnej analizie SIEM, aby umożliwić przejście do chmury hybrydowej

Travis Perkins PLC jest brytyjskim dystrybutorem i sprzedawcą artykułów budowlanych z 2000 punktów sprzedaży i 28 000 pracowników. W 2014 r. organizacja rozpoczęła działania w systemie cloud-first, jednak dotychczasowe rozwiązanie służące do zarządzania informacjami i zdarzeniami związanymi z bezpieczeństwem nie zapewniało niezbędnych zabezpieczeń w środowisku hybrydowym. Firma Travis Perkins PLC przejrzała dostępne alternatywy i wybrała Splunk Cloud, Splunk Enterprise oraz Splunk Enterprise Security (ES) jako swoje SIEM.

Od czasu wdrożenia platformy Splunk Travis Perkins PLC uzyskał korzyści takie jak:

- Lepsza przejrzystość działań w infrastrukturze hybrydowej.
- Zdolność wykrywania kompleksowych cyberzagrożeń i reagowania na nie.
- Obniżone koszty działań IT dzięki lepszemu wykorzystaniu zasobów.

Dlaczego Splunk?

W obliczu trudnych warunków rynkowych spowodowanych recesją, Travis Perkins PLC obniżył priorytet inwestycji w technologię. Ostatnio jednak, wraz z poprawą warunków biznesowych, firma przeszła strategiczny przegląd całej infrastruktury technologicznej i przyjęła podejście oparte na chmurze, które pozwoliło zmniejszyć koszty i zwiększyć elastyczność. Gdy Travis Perkins PLC wprowadził szereg usług w chmurze, w tym G Suite od Google Cloud, Amazon Web Services i Infor CloudSuite, szybko stało się jasne, że dotychczasowy SIEM nie był w stanie zapewnić wymaganych informacji na temat zdarzeń bezpieczeństwa w złożonym środowisku hybrydowym. Po przejrzeniu alternatywnych rozwiązań, w tym ofert HP, IBM i LogRhythm, Travis Perkins PLC wybrał Splunk Cloud, Splunk Enterprise i Splunk ES, aby zapewnić pełen wgląd we wszystkie działania w obszarze bezpieczeństwa.

Budowanie bezpieczeństwa od podstaw

Travis Perkins PLC wykorzystał okazję, jaką dało wdrożenie Splunk ES, aby podnieść świadomość bezpieczeństwa wszystkich osób z działu IT, zamiast skupiać się wyłącznie na zespole ds. bezpieczeństwa. Dzięki temu zabiegowi pracownicy zespołów operacyjnych IT mają teraz dostęp do określonych pulpitów nawigacyjnych i alertów, dzięki czemu mogą działać jako pierwsi, reagując bezzwłocznie na potencjalne zagrożenia. W razie potrzeby są w stanie podjąć natychmiastowe działania, jeszcze zanim przekażą informacje do dedykowanego zespołu ds. bezpieczeństwa. W rezultacie Travis Perkins PLC opracował wysoce skuteczne i sprawne Centrum Operacji Bezpieczeństwa (SOC - security operations center), bez konieczności inwestowania w to znacznych zasobów, które zazwyczaj są do tego wymagane.

Automatyzacja obrony przed zagrożeniami

Mając na pokładzie 24 000 pracowników z Wielkiej Brytanii korzystających z różnych urządzeń w celu uzyskania dostępu do danych firmowych, Travis Perkins PLC musiał zautomatyzować znaczną część swojego cyberbezpieczeństwa. Dzięki Splunk ES, Travis Perkins PLC może oceniać ryzyka dla różnych działań związanych z zagrożeniami na podstawie wcześniej skorelowanych z tym danych lub alertów z istniejących już rozwiązań bezpieczeństwa firmy. Ponieważ firma napotykała szczególny problem z wiadomościami e-mail typu phishing, aktualnie każdy zainfekowany klient jest natychmiast identyfikowany podczas wyszukiwania korelacji na platformie Splunk, co generuje automatyczny alert.

Następny krok to reakcja odpowiednich zespołów, które korzystają z wcześniej przygotowanej odpowiedzi z listy działań. Przepływ informacji w Splunk ES zapewnia całościowy obraz zasobu lub użytkownika i znacznie skraca czas potrzebny do zbadania i rozwiązania incydentów bezpieczeństwa**. Czytaj dalej.**

Analiza zagrożeń

SIEM oparty na dogłębnej analizie musi zapewniać dwie podstawowe formy analizy zagrożeń. Pierwsza obejmuje wykorzystanie usług śledzenia zagrożeń, które dostarczają bieżących informacji na temat wskaźników poziomu zainfekowania, taktyk atakującego, jego technik i procedur, a także dodatkowego kontekstu dla różnego rodzaju incydentów i działań.

Tego typu wsparcie ułatwia rozpoznawanie takich nietypowych działań jak na przykład identyfikowanie połączeń wychodzących z zewnętrznym adresem IP, który jest jednocześnie aktywnym serwerem typu command-and-control. Przy takim poziomie analizy zagrożeń analitycy dysponują informacjami potrzebnymi do oceny ryzyka, wpływu i celu ataku, czyli danymi, które są niezbędne do ustalenia priorytetu sprawy i dobrania odpowiedniej reakcji.

Druga forma analizy zagrożeń obejmuje ocenę ważności zasobów, ich wykorzystania, poziomu łączności, własności, a wreszcie nawet roli, odpowiedzialności i statusu zatrudnienia użytkownika. Ten dodatkowy kontekst jest często niesamowicie ważny, gdy mówimy o analizie ryzyka i potencjalnych skutków niechcianego incydentu. Dlatego właśnie SIEM oparty na dogłębnej analizie powinien być w stanie na przykład zidentyfikować pracownika, a następnie skorelować te dane z logami uwierzytelniania VPN, aby zapewnić szeroki kontekst dla zlokalizowania pracownika w sieci korporacyjnej. Aby zapewnić jeszcze głębsze poziomy analizy operacyjnej, SIEM powinien również mieć możliwość wykorzystania interfejsów API REST, a także łączenia danych strukturalnych z danymi maszynowymi.

Dane dotyczące zagrożeń powinny być zintegrowane z danymi maszynowymi generowanymi przez różnego rodzaju infrastrukturę IT i aplikacje w celu tworzenia list obserwacyjnych, reguł korelacji i zapytań w taki sposób, który zwiększy skuteczność wczesnego wykrywania zagrożeń. Informacje te warto automatycznie skorelować z danymi zdarzeń i dodać do pulpitu nawigacyjnego i raportów lub przekazać do zapór sieciowych lub systemów zapobiegania włamaniom, które mogą następnie zniwelować podatność.

Pulpit nawigacyjny zapewniony przez SIEM powinien być w stanie śledzić status i aktywność wdrażanych w środowisku IT narzędzi wykrywających zagrożenia, a co za tym idzie - sprawdzać kondycję systemów skanujących i identyfikować systemy, które nie są już skanowane w poszukiwaniu luk.

W największym skrócie: kompleksowa funkcja analizy zagrożeń musi zapewniać obsługę każdego zagrożenia, automatycznie identyfikować nadmiarowe dane, rozpoznawać i oceniać zagrożenia oraz przypisywać priorytet poszczególnym problemom celem zidentyfikowania rzeczywistego ryzyka, jakie stanowią dla biznesu.

Los Angeles integruje analizę bezpieczeństwa w czasie rzeczywistym z ponad 40 agencji

Aby chronić swoją infrastrukturę cyfrową, miasto Los Angeles potrzebuje świadomości swojego stanu bezpieczeństwa i zapewnienia analizy zagrożeń akcjonariuszom i departamentom. W przeszłości ponad 40 agencji z LA korzystało z różnych środków bezpieczeństwa, co utrudniało konsolidację i analizę danych. Dlatego właśnie miasto szukało skalowalnego rozwiązania do zarządzania informacjami i bezpieczeństwem w modelu SaaS, by móc skutecznie identyfikować, priorytetyzować i neutralizować zagrożenia, a także uzyskać wgląd w podejrzane działania i ocenę ryzyka w całym mieście.

Od momentu wdrożenia Splunk Cloud i Splunk Enterprise Security, miasto dostrzegło liczne korzyści, takie jak:

- Utworzenie aglomeracyjnego centrum operacji bezpieczeństwa (SOC - security operations center).
- Analiza zagrożeń w czasie rzeczywistym.
- Niższe koszty operacyjne.

Kontrola sytuacji w czasie rzeczywistym

Splunk Cloud zapewnia Los Angeles całościowy wgląd w stan bezpieczeństwa miasta. Splunk wysyła surowe logi i inne dane z departamentów miasta do Splunk Cloud, gdzie są one normalizowane i wracają do zintegrowanego SOC. Następnie są poddawane analizie i wizualizowane w pulpitach nawigacyjnych Splunk.Korzystając z gotowych, łatwych do dostosowania pulpitów nawigacyjnych w Splunk ES, kierownictwo i analitycy mają zawsze aktualny wgląd w zdarzenia związane z bezpieczeństwem w całej infrastrukturze sieciowej miasta.

Mając wszystkie dane dotyczące bezpieczeństwa w jednej, stale aktualizowanej bazie danych, zespół Lee przegląda i porównuje dane generowane maszynowo, w tym różne logi oraz dane zarówno strukturalne, jak i niestrukturalne. Ma to na celu uzyskanie wszystkich możliwych do rozpoznania i zastosowania danych dotyczących bezpieczeństwa.

Analiza zagrożeń w odpowiednim czasie

Zintegrowany SOC miasta nie tylko gromadzi informacje; on również dostarcza informacji. Przekształca dane z chmury Splunk Cloud na informacje o zagrożeniach w krótkim czasie. Miasto dzieli się odkryciami ze swoimi agencjami, a także zewnętrznymi zainteresowanymi stronami, takimi jak FBI, Departament Bezpieczeństwa Wewnętrznego, Secret Service i inne organy ścigania. Dzięki tym informacjom miasto może współpracować z agencjami federalnymi i identyfikować zagrożenia, a nawet opracowywać strategię zapobiegania przyszłym atakom w sieci.

„Dzięki świadomości sytuacji wiemy, co robi miasto" - mówi Lee. „Ale dzięki analizie zagrożeń wiemy, co robi nasz wróg. Obecnie działamy na zintegrowanym programie do analizy, a nasz Splunk SIEM jest jednym z kluczowych rozwiązań dla scentralizowanej platformy zarządzania informacjami, którą wdrażamy w ISOC (Integrated Security Operation Centre)".
Czytaj dalej.

Zaawansowana analityka

SIEM oparty na dogłębnej analizie może przeprowadzać zaawansowane analizy, stosując wyszukane metody ilościowe, takie jak statystyki czy opisowe i predykcyjne wyszukiwanie danych, a także uczenie maszynowe, symulacja i optymalizacja. Wszystko to ma na celu uzyskanie dodatkowych, ale jakże kluczowych informacji. Takie metody pozwalają na wykrywanie anomalii, profilowanie grup pokrewieństwa i modelowanie powiązań między podmiotami.

Co równie istotne, oparty na dogłębnej analizie SIEM musi zapewnić narzędzia, które umożliwią wizualizację i skorelowanie danych (na przykład poprzez mapowanie skategoryzowanych zdarzeń względem łańcucha zagrożeń lub tworzenie map rozkładu) oraz usprawnienie działań. Wprowadzenie tego wszystkiego w życie wymaga dostępu do platformy SIEM, która korzysta z algorytmów zdolnych do samodzielnego uczenia się, jak wygląda normalne zachowanie, a co jest anomalią.

Taki poziom analizy behawioralnej można następnie wykorzystać do budowania, sprawdzania i ostatecznie wdrażania modeli przewidywania. Co więcej, powinno być nawet możliwe zastosowanie takiego modelu utworzonego przy użyciu narzędzi innych firm na platformie SIEM.

Wdrożenie innowacyjnego, opartego na chmurze systemu SIEM zapewnia praktyczną analizę bezpieczeństwa dla Equinix

Equinix, Inc. łączy wiodące firmy na świecie z ich klientami, pracownikami i partnerami na 33 rynkach i 5 kontynentach. Bezpieczeństwo ma ogromne znaczenie w Equinix - tysiące firm na całym świecie polegają na centrach danych Equinix i ich usługach. Aby uzyskać jednolite spojrzenie na całą infrastrukturę bezpieczeństwa, Equinix potrzebował dwóch rzeczy: rozwiązania w chmurze ze scentralizowaną widocznością oraz funkcjonalnego SIEM, który można wdrożyć łatwo, szybko i bez znacznego wysiłku operacyjnego.

Od czasu wdrożenia Splunk Cloud i Splunk Enterprise Security (ES), Equinix odczuł korzyści takie jak:

- Pełna przejrzystość operacyjna.
- Zwiększone bezpieczeństwo.
- Oszczędność czasu i kosztów.

Nadrzędny wgląd w infrastrukturę dzięki Splunk Cloud i Splunk Enterprise Security

Przed współpracą ze Splunk Cloud, Equinix był przytłoczony ponad 30 miliardami surowych zdarzeń bezpieczeństwa generowanych co miesiąc. Dzięki Splunk ES i Splunk Cloud zespół ds. bezpieczeństwa może teraz zredukować 30 miliardów surowych zdarzeń bezpieczeństwa do około 12 tysięcy powiązanych zdarzeń, a następnie do 20 aktywnych alertów, zapewniając w ten sposób niezbędne i możliwe do wykorzystania informacje o bezpieczeństwie i podstawę działania dedykowanego SOC.

Po przeniesieniu wszystkich danych na platformę Splunk, zespół bezpieczeństwa może porównywać dane między systemami, umożliwiając im wyszukiwanie, badanie i reagowanie na incydenty o 30% szybciej niż wcześniej.

„Priorytetowym celem jest ochrona naszych klientów, pracowników i danych. Dzięki ES i Splunk Cloud jako naszej platformie SIEM potrzebne informacje są zawsze na wyciągnięcie ręki - mówi George Do, Equinix CISO. „Za każdym razem, gdy potrzebujemy zbadać niepokojące zdarzenie, po prostu wyświetlamy odpowiednie dane w pulpitach nawigacyjnych Splunk, aby dostęp do tych samych informacji mogli uzyskać wszyscy członkowie naszego zespołu ds. bezpieczeństwa, a także kluczowi kierownicy. Oszczędność czasu i nakładu pracy jest ogromna, podobnie jak oszczędności czysto finansowe w wysokości 50% TCO w porównaniu do wdrożenia tradycyjnego SIEM."

Dzięki Splunk ES, Equinix jest teraz uzbrojony w kompleksową analizę bezpieczeństwa. Co to oznacza? Na przykład to, że za każdym razem, gdy konto użytkownika wykazuje oznaki podejrzanej aktywności, np. nieoczekiwane zalogowanie się lokalnego pracownika z innego kontynentu, powiadomienia o wysokim priorytecie są natychmiast generowane i przesyłane zespołowi bezpieczeństwa. Ponadto użycie Splunk Cloud z ES umożliwia Equinix zapobieganie wyciekom poufnych informacji biznesowych. W szczególności korzystają na tym administratorzy, którzy mają teraz możliwość ustalenia, czy odchodzący pracownik może próbować ukraść poufne dane. **Czytaj dalej.**

Zaawansowane metody wykrywania zagrożeń

Zagrożenia dla bezpieczeństwa nieustannie ewoluują. Oparty na dogłębnej analizie SIEM może dopasować się do nowych, zaawansowanych zagrożeń poprzez możliwość monitorowania bezpieczeństwa sieci, wykrywanie zagrożeń i izolację zagrożeń w odpowiedzi na podejrzane zachowania. Większość zapór i systemów bezpieczeństwa nie może samodzielnie zapewnić żadnej z tych możliwości, a już na pewno nie kombinacji ich wszystkich.

Celem jest nie tylko wykrywanie zagrożeń, lecz także określenie ich potencjalnego zakresu poprzez zidentyfikowanie, dokąd mogło dotrzeć od momentu wykrycia, w jaki sposób je izolować oraz jak wszystkie te informacje powinny być udostępniane.

Biblioteka zastosowań

Nie tylko zagrożenia związane z bezpieczeństwem stale ewoluują - także analitycy muszą być w stanie wykrywać zagrożenia i reagować na nie w krótkim czasie. Oparte na dogłębnej analizie rozwiązanie SIEM zwiększa bezpieczeństwo dzięki gotowym do użycia schematom działania dostosowanym do konkretnych przypadków. Biblioteka zastosowań może również pomóc analitykom w automatycznym wykrywaniu nowych zdarzeń i określaniu, które z nich można wykorzystać w przyszłości na podstawie danych zebranych w momencie ich przetwarzania. Ostatecznie przynosi to korzyść w postaci zmniejszenia ryzyka dzięki szybszemu wykrywaniu i reagowaniu na incydenty i zagrożenia.

SAIC poprawia zauważalność i wykrywanie zagrożeń

Science Applications International Corp. (SAIC) jest wiodącym integratorem technologii, który specjalizuje się w środowiskach technicznych, inżynieryjnych i informacyjnych skierowanych dla przedsiębiorstw. Dzięki specjalistycznej wiedzy w dziedzinach takich jak badania naukowe, zarządzanie programami i usługi IT, większość dochodów SAIC pochodzi od rządu USA.

Firma musiała zbudować solidne centrum organizacji bezpieczeństwa (SOC - security operations center) i zespół reagowania na incydenty komputerowe (CIRT - computer incident response team), by bronić się przed cyberatakami.

Od czasu wdrożenia platformy Splunk firma odnotowała korzyści, wśród których wyróżnia się:

- Poprawiony poziom bezpieczeństwa i większa dojrzałość w działaniu.
- Ponad 80% krótszy czas wykrywania incydentów i działań naprawczych.
- Kompleksowy widok danych w całym środowisku przedsiębiorstwa.

Dlaczego Splunk?

Po tym, jak pierwotny SAIC podzielił się na dwie firmy w 2013 r., SAIC musiał zbudować SOC w ramach nowego programu bezpieczeństwa, aby uniknąć konfliktu interesów. Mimo że dysponował większością potrzebnych narzędzi bezpieczeństwa, SAIC nie posiadał wystarczających zabezpieczeń informacji i zdarzeń, aby stworzyć pełny system ochronny. Tradycyjny SIEM stosowany przez firmę jako podstawowe narzędzie do kontroli poziomu bezpieczeństwa miał pewne ograniczenia. SAIC uzupełnił swój SIEM o Splunk Enterprise, wykorzystując platformę do wykrywania incydentów poprzez wyszukiwanie korelacji, a także do dokładnego badania podejrzanych zdarzeń. Pracownicy IT używają teraz również rozwiązania Splunk do monitorowania sieci, zarządzania wydajnością, analizy aplikacji i szczegółowego raportowania.

Gdy SAIC zaczął budować swój nowy SOC, firma zdecydowała się na Splunk jako spójną platformę służącą do analizy bezpieczeństwa i spełniającą wszystkie potrzeby podobne do tych pokrywanych przez możliwości SIEM, w tym wykrywanie incydentów, dochodzenia i raporty służące ciągłemu monitorowaniu, alarmowaniu i analizom.

Pełna widoczność i wykrywanie zagrożeń w środowisku

SAIC używa teraz oprogramowania Splunk do monitorowania swojego środowiska w poszukiwaniu wszelkich możliwych zagrożeń. W SOC analitycy monitorują niestandardowe pulpity nawigacyjne Splunk pod kątem alertów i oznak nieprawidłowego lub nieautoryzowanego zachowania. Są teraz od razu świadomi zagrożeń - zarówno tych znanych (takich jak te rejestrowane przez IDS lub złośliwe oprogramowanie), jak i nieznanych (takich jak konto uprzywilejowanego użytkownika o nietypowej aktywności).

Tradycyjne SIEM zazwyczaj prowadzą swoje analizy przy użyciu gotowych, sztywnych modeli wyszukiwań, które nie wychwytują zaawansowanych zagrożeń i generują dużą liczbę fałszywych alarmów. Dzięki platformie Splunk analitycy SAIC opracowali nowe, bardzo dokładne wyszukiwania powiązań danych, które mogą służyć szybkiemu wykrywaniu zagrożeń i wskaźników ryzyka specyficznych dla SAIC, umożliwiając zespołowi zarządzanie bezpieczeństwem na wysokim poziomie. Kierownictwo, w tym CISO, może teraz zobaczyć kluczowe wskaźniki dotyczące działań związanych z zagrożeniami, m.in. trendy, zagregowaną lokalizację źródła danych i najnowsze wskaźniki poziomu zainfekowania. **Czytaj dalej.**

Architektura

Współczesne zagrożenia wymagają elastycznych i skalowalnych rozwiązań. SIEM oparty na dogłębnej analizie musi działać sprawnie zarówno przy wdrożeniu lokalnym, jak i w chmurze czy chmurze hybrydowej. Nowoczesne rozwiązanie SIEM musi być również dostępne dla każdego rozmiaru organizacji i wystarczająco elastyczne, aby można je było skalować wraz z rozwojem firmy i wzrostem potrzeb w zakresie bezpieczeństwa.

Aflac adaptuje platformę Splunk zapewniającą bezpieczeństwo oparte na dogłębnej analizie

Aflac jest wiodącym dostawcą dobrowolnych ubezpieczeń w USA. W obliczu wzrostu zagrożeń związanych z bezpieczeństwem, Aflac potrzebował nowoczesnego podejścia opartego na dogłębnej analizie, aby chronić swoich klientów, prawie 10 000 pracowników, a także swoją reputację w branży. Firma wykorzystuje platformę Splunk jako najważniejszą część wewnętrznego systemu analizy zagrożeń (TIS). Od czasu wdrożenia Splunk Enterprise Security (ES) i Splunk User Behaviour Analytics (UBA), Aflac odczuł znaczne korzyści, w tym:

- Szybkie, dwutygodniowe wdrożenie systemu dla całego przedsiębiorstwa.
- Zablokowanie ponad 2 milionów zagrożeń bezpieczeństwa w ciągu 6 miesięcy.
- Oszczędność 40 godzin miesięcznie uzyskana przez wyeliminowanie ręcznego gromadzenia danych i raportowania, co umożliwiło zespołom skupienie się na aktywnym monitorowaniu i analizie bezpieczeństwa.

Dlaczego Splunk?

Wraz z wchodzeniem na nowe rynki i wprowadzaniem kolejnych usług, Aflac musi stale dostosowywać swój program zabezpieczeń, aby nadążyć za szybko zmieniającym się spektrum zagrożeń (od phishingu po rozprzestrzenianie złośliwego oprogramowania). Przed wdrożeniem platformy Splunk Aflac polegał na starszym rozwiązaniu do zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), ale firma potrzebowała silniejszej platformy analizy zagrożeń, aby odpowiednio wykrywać ataki i dostosowywać do nich skuteczną reakcję.

Według D.J. Goldsworthy'ego, dyrektora ds. operacji bezpieczeństwa i zarządzania zagrożeniami w Aflac, „Kiedy korzystaliśmy z poprzedniego SIEM, musieliśmy naprawdę dobrze zapoznać się z danymi, zanim mogliśmy podjąć jakiekolwiek działania, za to Splunk pomaga bardzo szybko poznać wszystkie dane. Dzięki Splunk poznaliśmy dużo sprytnych rozwiązań i mogliśmy szybko pokazać zwrot z inwestycji naszym akcjonariuszom."

Pierwotnie Splunk ES został wybrany przez Aflac jako system wyszukiwania zagrożeń. „Zasadniczo chcieliśmy wykorzystać Splunk ES do poszukiwaniu wiszących nad nami zagrożeń, a stosunek wartości do ceny znacznie przekroczył nasze oczekiwania", mówi Goldsworthy. „Byliśmy w stanie zrobić niezwykłe rzeczy w bardzo krótkim czasie i wykryć nawet zaawansowane zagrożenia. To właśnie wtedy podjęliśmy decyzję dokonaniu znacznie większej inwestycji w Splunk ES i UBA we wszystkich obszarach związanych z bezpieczeństwem."

Natychmiastowy zwrot inwestycji

Według Goldsworthy'ego, czas niezbędny do zaimplementowania Splunk i przygotowania go do działania był naprawdę krótki - zaledwie kilka tygodni. "To było całkiem zaskakujące, biorąc pod uwagę objętość danych, które posiadaliśmy, i liczbę zagadnień, które chcieliśmy rozwiązać", tłumaczy. "Zobaczyliśmy natychmiastowy zwrot inwestycji w Splunk."

Dziś dzięki Splunk ES jako części firmowego SOC, Aflac zaoszczędził czas wielu pracownikom zatrudnionym w pełnym wymiarze godzin. „Obliczamy, że oszczędzamy ponad 40 godzin miesięcznie, jeśli chodzi o tworzenie raportów, które były tworzone ręcznie, a teraz są w pełni zautomatyzowane", mówi Goldsworthy. „Splunk bardzo ułatwił gromadzenie danych z różnych źródeł, a następnie prezentowanie ich w sposób czytelny dla akcjonariuszy, takich jak nasz zarząd lub inne kierownictwo".

6 zespołów złożonych z około 40 osób polega na platformie Splunk do zarządzania różnorodnymi rodzajami zastosowań w obszarze bezpieczeństwa, w tym tzw. *threat huntingiem* (polowaniem na zagrożenia), analizą zagrożeń, operacjami bezpieczeństwa, reagowaniem na incydenty, bezpieczeństwem aplikacji oraz zarządzanie bezpieczeństwem i kontrola nadużyć.

„Najpierw wdrożyliśmy Splunk do analizy zagrożeń, a następnie operacji bezpieczeństwa. Zdając sobie sprawę z tego, jak wszechstronne jest to rozwiązanie, ustaliliśmy, że kolejnym logicznym krokiem jest dla nas zastosowanie go do wykrywania nadużyć", mówi Goldsworthy.

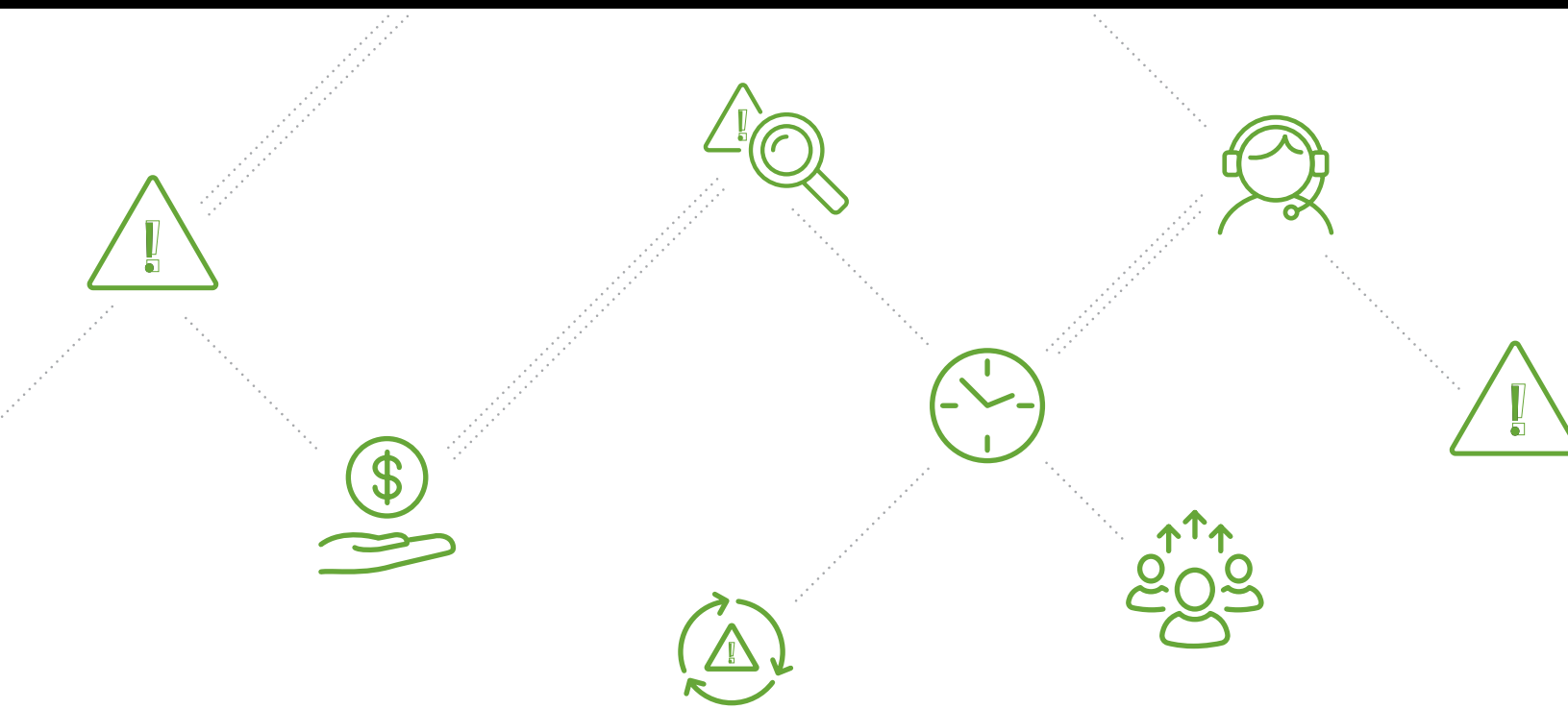
Wdrażanie, operacje i wsparcie

Istnieje powszechne przekonanie, że rozwiązania SIEM mogą być trudne do wdrożenia, a po uruchomieniu wymagają stałej konserwacji. Dobrze zaprojektowany SIEM oparty na dogłębnej analizie bierze jednak pod uwagę niedobór inżynierów posiadających wiedzę z tego zakresu, dlatego właśnie musi zapewniać wstępnie zdefiniowane funkcje i pulpity nawigacyjne oraz oferować wsparcie od dostawców, w które wchodzą profesjonalne usługi z zakresu rozwiązywania wszelkich pojawiających się problemów.

Zarządzanie logami i danymi

Dane logów to ostateczny zapis tego, co dzieje się w każdej firmie, organizacji lub agencji. Logi często pozostają niewykorzystanym zasobem w rozwiązywaniu problemów i wspieraniu szerszych celów biznesowych.

A biorąc pod uwagę szerokie spektrum współczesnych zagrożeń i fakt, że atak może pochodzić z dowolnego miejsca, absolutnie wszystkie dane są istotne z punktu widzenia bezpieczeństwa. Logi są często punktem wyjścia do wykrywania zagrożeń, automatyzacji zgodności i wykrywania zaawansowanych zagrożeń zanim jeszcze wystąpią. Coraz częściej rozwiązania SIEM muszą posiadać miejsce do przechowywania nieustrukturyzowanych, nieprzetworzonych danych, które następnie mogą udoskonalić prowadzenie takich zadań jak threat hunting, zaawansowane analizy i badanie incydentów.



3. DZIEWIĘĆ MOŻLIWOŚCI TECHNICZNYCH NOWOCZESNEGO SIEM

Teraz, gdy już rozumiesz **siedem podstawowych możliwości opartego o analizę systemu SIEM**, czas zagłębić się w technologię, która tworzy nowoczesne rozwiązanie SIEM. Wszystko to po to, by pomóc Ci w dalszym odróżnieniu nowoczesnego SIEM od tego tradycyjnego, a także open source SIEM i nowych graczy na rynku SIEM, na przykład dostawców UBA.

Coroczny raport *Magic Quadrant for Security Information and Event Management* tworzony przez firmę Gartner jest zalecany jako obowiązkowa lektura dla każdego, kto śledzi wydarzenia na rynku SIEM. W miarę rozwoju, raport objął swoją analizą także dostawców open source SIEM i UEBA.

Gartner publikuje również dodatkowe raporty dotyczące SIEM. W kolejnej pracy badawczej podkreśla 9 możliwości technicznych odróżniających współczesny SIEM (taki jak ten dostarczany przez Splunk), od pozostałych rodzajów.

Dziewięć możliwości technicznych, które odróżniają nowoczesny SIEM od innych rozwiązań, to:

	SPLUNK	TRADYCYJNY SIEM	OPEN SOURCE	NOWI DOSTAWCY
1. Zbieranie danych z logów i zbiorów zdarzeń	Tak	Tak	Tak	Tak
2. Stosowanie reguł korelacji w czasie rzeczywistym	Tak	Tak	DIY	Tak
3. Zaawansowana analityka i uczenie maszynowe w czasie rzeczywistym	Tak	Ograniczone	DIY	Tak
4. Analiza danych historycznych i uczenie maszynowe	Tak	Ograniczone	DIY	Ograniczone
5. Długoterminowe przechowywanie zdarzeń	Tak	Ograniczone	Tak	Ograniczone
6. Wyszukiwanie i raportowanie ustrukturyzowanych danych	Tak	Tak	Tak	Tak
7. Wyszukiwanie i raportowanie niestrukturyzowanych danych	Tak	Złożone	Tak	Złożone
8. Przetwarzanie danych kontekstowych w celu dodatkowej korelacji i analizy	Tak	Ograniczone	Tak	Ograniczone
9. Rozwiązywanie problemów niezwiązanych z bezpieczeństwem	Tak	Nie	DIY	Nie

1. Zbieranie danych z logów i zbiorów zdarzeń

Rozwiązanie SIEM oparte na analizie powinno być w stanie gromadzić, wykorzystywać i analizować wszystkie zapisy zdarzeń oraz zapewniać spójny wgląd w stan zabezpieczeń w czasie rzeczywistym. Pozwoli to zespołom zajmującym się IT i bezpieczeństwem zarządzać logami z jednej centralnej lokalizacji, korelować dane z wielu urządzeń i dni oraz zadbać o dane z innych źródeł (takich jak zmiany rejestru i logi ISA Proxy), aby uzyskać pełny obraz sytuacji. Specjaliści ds. bezpieczeństwa mają również możliwość kontrolowania i raportowania wszystkich dzienników zdarzeń z jednego miejsca.

2. Stosowanie reguł korelacji w czasie rzeczywistym

Korelacja zdarzeń to najlepszy sposób na zbadanie wielu zdarzeń związanych z bezpieczeństwem i zawężenie ich do tych, które faktycznie mają znaczenie. Warto łączyć fakty i zdarzenia dla pełnego zrozumienia sytuacji.

3. Zaawansowana analityka i uczenie maszynowe w czasie rzeczywistym oraz (4.) analiza danych historycznych i uczenie maszynowe

Istnieje pewna podstawowa forma analizy, która w kontekście SIEM zapewnia wgląd w dane i ułatwia określanie wzorcowych zachowań. Umożliwia to analitykom głębsze badania i wykrywanie zagrożeń oraz potencjalnych przestępstw jeszcze przed ich wystąpieniem.

Niedawna ankieta Forrestera wykazała, że 74% „[...] osób odpowiadających za decyzje dotyczące bezpieczeństwa korporacyjnego uznaje poprawę monitorowania bezpieczeństwa za priorytetową kwestię", a „[...] dostawcy dodają funkcje analizy bezpieczeństwa do istniejących rozwiązań, a nowi dostawcy budują takie systemy [analizy bezpieczeństwa], które wykorzystują najnowsze technologie bez nawiązywania do tradycyjnych rozwiązań."

Uczenie maszynowe (ML - *machine learning*) przenosi analizę danych na jeszcze wyższy poziom. Jego zastosowanie w rozwiązaniu SIEM opartym na dogłębnej analizie umożliwia przeprowadzanie analizy predykcyjnej, która wyciąga wnioski z danych historycznych. Jest to funkcja szczególnie przydatna dla specjalistów ds. bezpieczeństwa w wykrywaniu i przewidywaniu incydentów, a nawet zapobieganiu atakom.

5. Długoterminowe przechowywanie zdarzeń

Oparte na analizie rozwiązanie SIEM daje możliwość przechowywania historycznych danych z logów przez długi czas. Umożliwia to korelację danych nawet po ustąpieniu problemów, a dodatkowo pomaga spełnić wymagania dotyczące zgodności.

Dlaczego ma to tak duże znaczenie dla bezpieczeństwa? Długoterminowe przechowywanie danych maszynowych

umożliwia analitykom przeprowadzanie analiz bezpieczeństwa związanych z przeszłymi przestępstwami, na przykład w celu śledzenia trasy ataku w przypadku naruszenia bezpieczeństwa sieci.

6. Wyszukiwanie i raportowanie ustrukturyzowanych danych

Wyszukiwanie i raportowanie w zakresie SIEM umożliwia użytkownikom odnalezienie ich danych, stworzenie modeli danych, zapisywanie wyników wyszukiwań w formie raportów i tabeli przestawnych, konfigurowanie alertów i tworzenie pulpitów nawigacyjnych, które później można udostępnić.

7. Wyszukiwanie i raportowanie niestrukturyzowanych danych

Wyszukiwanie i raportowanie surowych danych (*raw data*) w odniesieniu do zastosowań SIEM to tak naprawdę gromadzenie danych z różnych źródeł i centralizowanie ich za pomocą systemu SIEM opartego na analizie. Nowoczesne rozwiązanie SIEM, w przeciwieństwie do tradycyjnego systemu, może pobierać surowe dane z prawie każdego źródła. Dane te można następnie przekształcić w użyteczne analizy i łatwe do zrozumienia raporty, dystrybuowane bezpośrednio z platformy SIEM do odpowiednich osób.

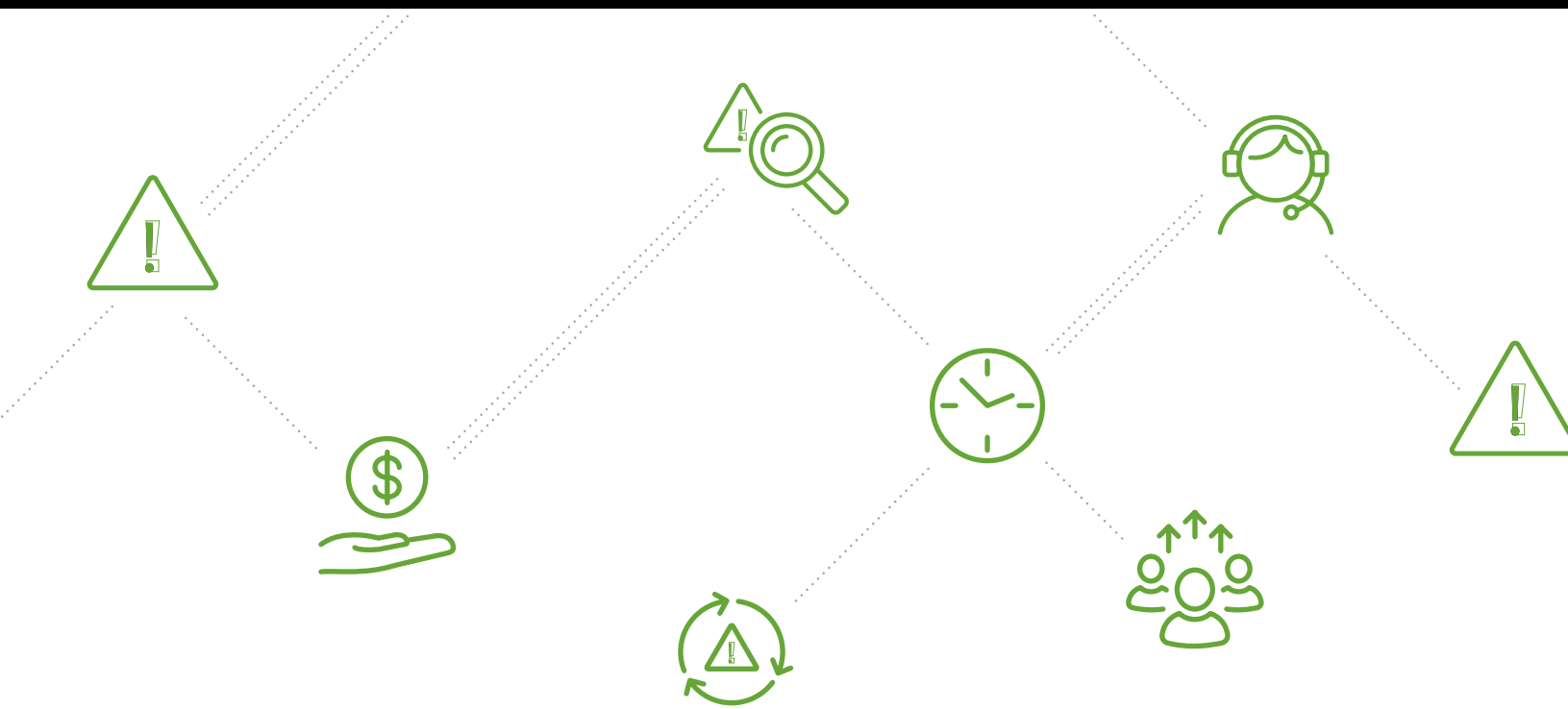
8. Przetwarzanie danych kontekstowych w celu dodatkowej korelacji i analizy

Po zebraniu danych przez nowoczesny SIEM użytkownik potrzebuje jeszcze dodatkowego kontekstu, aby wiedzieć, co zrobić ze zgromadzonymi danymi i poprawnie zrozumieć ich znaczenie. Jest to niezwykle ważne przy odróżnianiu rzeczywistych zagrożeń od fałszywych alarmów, umożliwia też skuteczne wykrywanie i reagowanie na rzeczywiste zagrożenia.

Oparte na analizie rozwiązanie SIEM jest w stanie dodać kontekst do zewnętrznej analizy zagrożeń, wewnętrznych operacji IT i wzorców zdarzeń. Pozwala to użytkownikowi na dogłębną analizę i reagowanie na zagrożenia w czasie rzeczywistym.

9. Rozwiązywanie problemów niezwiązanych z bezpieczeństwem

Kolejna różnica między opartym na analizie rozwiązaniem SIEM a tradycyjnym odpowiednikiem to jego użyteczność także w zastosowaniach niezwiązanych bezpośrednio z bezpieczeństwem, np. IT Ops (*IT Operations)*.



4. POZNAJ SPLUNK

Dane generowane maszynowo to jeden z najszybciej rozwijających się i złożonych obszarów Big Data. Jest on również jednym z najcenniejszych, ponieważ zawiera zapis wszystkich transakcji użytkowników, zachowań klientów i maszyn, zagrożeń bezpieczeństwa, nieuczciwych działań i innych. Splunk zamienia dane maszynowe w cenne informacje, bez względu na to, w jakiej branży jesteś. Nazywamy to Operational Intelligence - inteligencją operacyjną.

Splunk Enterprise monitoruje i analizuje dane maszynowe z każdego źródła, aby zapewnić inteligencję operacyjną celem optymalizacji Twoich systemów informatycznych, bezpieczeństwa oraz wydajności biznesowej. Dzięki intuicyjnym analizom, uczeniu maszynowemu, gotowym aplikacjom i otwartym interfejsom API, Splunk Enterprise jest elastyczną platformą, która umożliwia obsługę zarówno specyficznych zastosowań, jak i budowy stabilnego szkieletu analitycznego w całym przedsiębiorstwie.

Splunk Enterprise:

• Zbiera i indeksuje logi i dane maszynowe z dowolnego źródła.

• Umożliwia sprawne wyszukiwanie, analizy i wizualizacje usprawniające działanie całej organizacji.

• Rozbudowany ekosystem aplikacji Splunkbase zapewnia rozwiązania z zakresu bezpieczeństwa, operacji IT, analiz biznesowych i wiele więcej.

• Jest dostępny jako oprogramowanie on-premise lub usługa w chmurze.

Przekształć swoje dane w wartość dla biznesu

Inteligencja operacyjna pozwala Ci w czasie rzeczywistym zrozumieć, co dzieje się w systemach informatycznych i całej infrastrukturze technologicznej, dzięki czemu możesz podejmować świadome decyzje. Jest to możliwe dzięki platformie Splunk, będącej podstawą wszystkich produktów Splunk, rozwiązań premium, aplikacji i dodatków (add-ons).

Splunk jako Twój SIEM

Rozwiązania Splunk dla bezpieczeństwa nie tylko spełniają wszystkie wymagania stawiane nowoczesnemu SIEM, lecz także dają możliwość analizy bezpieczeństwa, zapewniając cenny kontekst i wgląd w informacje, które pomagają zespołom bezpieczeństwa podejmować szybsze i mądrzejsze decyzje związane z bezpieczeństwem.

Splunk oferuje kilka opcji dla przedsiębiorstw, które chcą wdrożyć SIEM lub przeprowadzić migrację ze swojego dotychczasowego SIEM, oferując do tego wybór opcji wdrażania lokalnego, w chmurze lub hybrydowego.

Klienci mogą wykorzystywać podstawowe zastosowania SIEM przy użyciu Splunk Enterprise lub Splunk Cloud. Splunk Enterprise i Splunk Cloud są podstawowymi platformami Splunk, dającymi możliwość gromadzenia, indeksowania, wyszukiwania i raportowania lub CLM. Wielu klientów Splunk korzysta ze Splunk Enterprise lub Splunk Cloud do tworzenia własnych wyszukiwań korelacji w czasie rzeczywistym i pulpitów nawigacyjnych jako podstawowe wykorzystanie SIEM.

Splunk oferuje rozwiązanie premium Splunk Enterprise Security (ES), które obsługuje zaawansowane zastosowania SIEM z gotowymi do użycia pulpitami nawigacyjnymi, skorelowanymi wyszukiwaniami i raportami. Splunk ES działa w powiązaniu ze Splunk Enterprise, Splunk Cloud lub oboma. Oprócz wbudowanych reguł korelacji i alertów, Splunk ES oferuje przegląd incydentów, opcję zarządzania przepływem zadań oraz kanały informacyjne analizujące zagrożenia zewnętrzne i wspomagające śledztwa.

Ponadto w Splunkbase znajduje się ponad 300 innych aplikacji związanych z bezpieczeństwem: gotowe szablony wyszukiwań, raporty i wizualizacje dla określonych zewnętrznych dostawców zabezpieczeń. Te gotowe do użycia aplikacje, narzędzia i dodatki zapewniają różne funkcje: monitorowanie bezpieczeństwa, zaporę nowej generacji, zaawansowane zarządzanie zagrożeniami i wiele innych. Pozwalają one zwiększyć zakres ochrony i są dostarczane przez Splunk, partnerów Splunk i innych zewnętrznych dostawców.

Splunk ES to także oparty na analizie SIEM złożony z pięciu odrębnych struktur, które można niezależnie wykorzystywać w celu poprawienia zabezpieczeń, w tym zgodności, bezpieczeństwa aplikacji, zarządzania incydentami, zaawansowanego wykrywania zagrożeń, monitorowania w czasie rzeczywistym i innych. Platforma SIEM oparta na analizie łączy uczenie maszynowe, wykrywanie niepokojących zdarzeń i skuteczną korelację w ramach jednego rozwiązania analityki bezpieczeństwa.

Splunk ES pozwala wizualnie korelować zdarzenia w czasie i przekazywać szczegóły ataków wieloetapowych. Jako platforma umożliwia także wykrywanie, monitorowanie oraz raportowanie zagrożeń, ataków i innych nietypowych działań pochodzących ze wszystkich istotnych dla bezpieczeństwa biznesu źródeł.

Dzięki zaawansowanej analizie klienci szybciej wykrywają zagrożenia i mają szansę na sprawną reakcję na incydenty w całym obszarze zabezpieczeń.

Splunk ES jest częścią szerokiej oferty rozwiązań bezpieczeństwa, które zapewnia CLM ze Splunk Enterprise i zaawansowane funkcjonalności UBA ze Splunk User Behaviour Analytics (UBA).

Dlaczego warto wybrać Splunk jako SIEM?

- Oprogramowanie Splunk może być używane do obsługi SOC niezależnie od jego rozmiaru.
- Zapewnia obsługę pełnego zakresu operacji związanych z bezpieczeństwem informacji - w tym zawiera się ocena stanu bezpieczeństwa, monitorowanie, alarmowanie i obsługa incydentów, zespół CSIRT, analiza i reagowanie w przypadku naruszenia oraz korelacja zdarzeń.
- Predefiniowane rozwiązania dla SIEM i zastosowań z obszaru bezpieczeństwa.
- Możesz wykryć znane i nieznane zagrożenia, badać je, określać zgodność z systemem i korzystać z zaawansowanych analiz bezpieczeństwa w celu uzyskania szczegółowych informacji.
- Sprawdzona, zintegrowana platforma analizy bezpieczeństwa oparta na Big Data.
- Masz dostęp do wyszukiwań ad hoc w celu zaawansowanej analizy naruszeń i luk w bezpieczeństwie.
- Dostępne są lokalne, chmurowe i hybrydowe opcje wdrożenia.

Jeden SIEM, by wszystkimi rządzić

Wybór odpowiedniego rozwiązania SIEM może naprawdę pomóc Twojej organizacji osiągnąć sukces w przyszłości i zbudować solidne zabezpieczenia we wszystkich obszarach. Splunk ES może działać jako podstawa do przeprojektowania całego SOC i przeniesienia go w zupełnie nową przyszłość.

Splunk ES staje się centralnym elementem Splunk Security Operations Suite, który łączy wiodące technologie SIEM, UEBA i SOAR, oparte na jednej platformie do zasilania SOC kolejnej generacji.

Splunk nie tylko automatycznie wspiera wszystkie powyższe funkcjonalności, lecz także następujące zastosowania:

- Monitorowanie: Splunk Enterprise lub Splunk Cloud lub Splunk Enterprise Security
- Śledztwo: Splunk Enterprise lub Splunk Cloud lub Splunk Enterprise Security
- Automatyzacja i orkiestracja: Splunk Phantom
- Zaawansowane wykrywanie zagrożeń, w tym wewnętrznych: Splunk User Behavior Analytics i Splunk Enterprise Security
- Reagowanie na incydenty: Splunk Phantom lub Splunk Enterprise Security
- Raporty zgodności: Splunk Enterprise lub Splunk Cloud lub Splunk Enterprise Security

InfoTeK i Splunk dostarczają platformę analizy bezpieczeństwa dla sektora publicznego

Wiele organizacji używa SIEM w celu monitorowania, wykrywania i reagowania na zagrożenia związane z bezpieczeństwem. Jednak w jednej z agencji rządowych USA ta współpraca napotkała na wiele przeszkód, gdy tradycyjny SIEM firmy HP, ArcSight, nie spełnił oczekiwań. Agencja zwróciła się do InfoTeK, wiodącej firmy zajmującej się cyberbezpieczeństwem oraz inżynierią oprogramowania i systemów, aby zastąpić obecnie używany system SIEM.

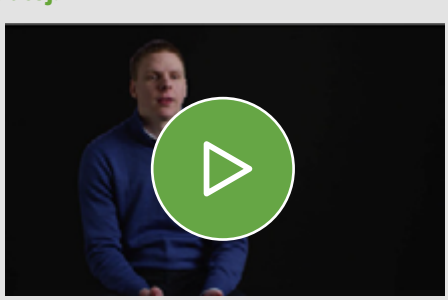
Od czasu wdrożenia platformy Splunk klient odnotował znaczące korzyści, w tym:

- Wdrożenie platformy w zaledwie jeden weekend i powstrzymanie pierwszego ataku już następnego dnia.
- Zredukowanie kosztów przeznaczonych na wsparcie SIEM o 75% .
- Zmniejszenie liczby niezbędnych narzędzi, w tym agregatorów logów i rozwiązań do obsługi urządzeń końcowych.

Dzięki Splunk Enterprise i Splunk ES agencja zyskała oparty na analizie system SIEM, któremu udało się zapewnić zespołowi IT przydatne analizy bezpieczeństwa w rozsądnej cenie. Warto zaznaczyć, że InfoTeK wdrożył dla klienta oprogramowanie Splunk w ciągu jednego weekendu.

Już następnego dnia oprogramowanie udowodniło swoją wartość. Zespół IT był w stanie przeszukać zdarzenia związane z bezpieczeństwem i natychmiast udaremnił nadchodzący atak.

“Coś, co zajmowało godziny, dni czy nawet tygodnie przy użyciu innych produktów i wymagało przełączania się pomiędzy różnymi narzędziami, z platformą Splunk może być zrobione w sekundy, minuty, najwięcej - godziny”, mówi Jonathan Fair, starszy specjalista ds. incydentów i inżynier bezpieczeństwa w InfoTeK. „Byliśmy w stanie zapewnić zwrot z inwestycji jeszcze zanim produkt został w pełni zakupiony, ponieważ Klient skutecznie powstrzymał zagrożenie, które bez Splunk wymagałoby całkowitej przebudowy sieci”.
Czytaj dalej.



Kliknij tu, by zobaczyć jak InfoTek zredukował koszty przeznaczone na utrzymanie SIEM o 75%.

MONITORUJ RAPORTUJ	WYKRYWAJ ALARMUJ	ANALIZUJ ŚLEDŹ	REAGUJ WSPÓŁPRACUJ	SIEM
wstępnie zdefiniowane widoki i reguły	reguły korelacji, wartości progowe	analiza śledcza i wzbogacanie kontekstu	reagowanie i koordynacja w całym przedsiębiorstwie	alarm zarządzania Ops Security i zarządzanie incydentami, gotowe reguły postępowania, gotowe zasady bezpieczeństwa i analizy

Departament rządu Stanów Zjednoczonych oszczędza 900 000 USD na konserwacji tradycyjnego oprogramowania

Obywatele oczekują, że agencje rządowe nie tylko mądrze wydadzą pieniądze podatników, lecz także dołożą wszelkich starań, aby zapewnić skuteczne świadczenie wszelkiego rodzaju usług. Jeden z departamentów w USA korzystał z HP ArcSight, powolnego i drogiego narzędzia do zarządzania informacjami i zdarzeniami, które nie sprostało potrzebom agencyjnym. Od czasu zastąpienia go przez Splunk Enterprise ze względu na bezpieczeństwo i zgodność, dział dostrzegł korzyści, wśród których warto wymienić:

- Oszczędności rzędu 900,000 dolarów na konserwacji oprogramowania.
- Lepsze wykrywanie, reagowanie i neutralizowanie zagrożeń.
- Skrócenie czasu śledztwa z godzin do zaledwie minut.

Proaktywne podejście do bezpieczeństwa

Margulies i jego zespół wspierają SOC departamentalny, w tym 40 analityków, którzy korzystają ze Splunk Enterprise do badania incydentów, a także duży zespół IT wykorzystujący oprogramowanie do raportowania i rozwiązawania problemów. Wśród dodatkowych klientów warto wymienić tych pracowników, którzy muszą dbać o zgodność działu z przepisami bezpieczeństwa.

Heartland Automotive chroni reputację i dane dzięki platformie Splunk

Heartland Automotive Services, Inc., Jiffy Lube, znana ze swoich usług wymiany oleju, jest największym franczyzobiorcą miejsc świadczących usługi z zakresu dbania o stan samochodu w USA. Heartland Automotive potrzebował platformy bezpieczeństwa cybernetycznego do ochrony swojej marki i jej najważniejszego zasobu - danych. Od czasu wdrożenia Splunk ES i Splunk UBA jako zintegrowanej platformy SIEM, Heartland Automotive odnotował korzyści, w tym:

- Wdrożenie rozwiązania SIEM oraz ochrony przed zagrożeniami wewnętrznymi zajęło zaledwie trzy tygodnie.
- Uzyskano platformę do wspierania innowacji z TCO obniżonym o 25%.
- Wprowadzenie śledzenia naruszeń bezpieczeństwa w czasie rzeczywistym i ochrony przed zagrożeniami wewnętrznymi.

Implementacje SIEM są często skomplikowane, ponieważ duże organizacje mają wiele źródeł danych i skonfigurowanie alertów może wymagać długich tygodni. Według Alamsa zespół profesjonalistów Splunk przeprowadził cały proces identyfikacji źródeł danych firmy, dopracował projekt SIEM i bezproblemowo skonfigurował alerty.

„Szybki czas wdrożenia to ogromna zaleta - byliśmy w stanie zaimplementować rozwiązanie SIEM i wykrywanie zagrożeń wewnętrznych w ciągu zaledwie trzech tygodni, co normalnie zajęłoby trzy miesiące", mówi Chidi Alams, szef działu IT i bezpieczeństwa informacji w Heartland Automotive Services. „Dyrektor finansowy i inni członkowie naszego kierownictwa byli pod wrażeniem - poznali projekt jednego dnia, kolejnego był on już niemal wdrożony. Zwiększyło to ich poziom zaufania do nas i pozwoliło udowodnić, jak szybko możemy dostarczać usługi". Czytaj dalej.

Kliknij, aby przeczytać jak Heartland Automotive zmniejszył TCO o 25%.

Zwrot inwestycji w Splunk

Rozwiązanie SIEM oparte na analizie jest często krytykowane za to, że stanowi kosztowną inwestycję. Ale rzeczywistość pokazuje, że jest to subiektywne odczucie.

Jak drogie wydaje się rozwiązanie zabezpieczające oparte na analizie tuż po tym, jak Twoja organizacja padła ofiarą ataku wewnętrznego? Lub po ataku ransomware, o którym będzie głośno?

Nietrudno więc dojść do wniosku, że istnieje natychmiastowy zwrot z inwestycji (ROI) - bezpieczeństwo organizacji i aktywna ochrona przed wewnętrznymi i zewnętrznymi atakami.

Ale na tym nie kończy się zwrot z inwestycji z SIEM.

Rozwiązanie SIEM oparte na analizie obsługuje wszystkie typowe przypadki użycia IT, wśród których trzeba wymienić ustalanie zgodności, radzenie sobie z oszustwami, wykrywanie kradzieży i nadużyć, operacje IT, analizę usług, dostarczanie aplikacji i analitykę biznesową.

Ponieważ zespoły ds. bezpieczeństwa współpracują z innymi działami IT, połączenie obu perspektyw i poznanie innych przypadków użycia zapewnia scentralizowany widok na całokształt sytuacji w firmie, co z kolei zacieśnia współpracę między działami i zwiększa ROI.

A najlepszym sposobem na zrozumienie faktycznego ROI z rozwiązania SIEM opartego na analizie jest wysłuchanie tych, którzy już go mają.

Przyszłość systemów SIEM

Nie wszystkie systemy SIEM są sobie równe, co podkreśla niniejszy przewodnik. Najlepiej pokazują to mocno widoczne różnice pomiędzy tradycyjnym a nowoczesnym SIEM – opartym na dogłębnej analizie.

Dziś właśnie platformy SIEM oparte na analizie wydają się być najbardziej przyszłościowym rozwiązaniem na rynku. Te nowoczesne rozwiązania bezpieczeństwa świetnie nadają się do wykrywania zagrożeń, ich usuwania, ostrzegania, raportowania zgodności, a jednocześnie zapewniają odczuwalny zwrot z inwestycji.

Ponieważ spektrum zagrożeń nieustannie się rozrasta, potrzebujemy rozwiązań, które są w stanie dostosować się i wyprzedzać ataki - rozwiązania SIEM oparte na analizie udowodniły, że doskonale sobie z tym radzą.

ARROW

Kontakt z nami: www.arrow.com/ECS/pl/kontakt

www.arrow.com

Arrow ECS Sp. z o.o. z siedziba w Krakowie, adres: ul. Sosnowiecka 79, 31-345 Kraków, tel. +48 12 616 43 00, wpisana do Krajowego Rejestru Sadowego - Rejestru Przedsiebiorców pod numerem 0000030756, której dokumentacja rejestrowa jest przechowywana przez Sad Rejonowy dla Krakowa-Śródmiescia, Wydział XI Gospodarczy Krajowego Rejestru Sadowego, NIP 678-26-82-866, z kapitałem zakładowym w wysokosci 2.000.000 PLN. Numer rejestrowy BDO: 000005543

© 2019 Splunk Inc. All rights reserved. Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and/or registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.

2019-Splunk-SEC-SIEM Buyers Guide for 2020-103-WP