CISCO SECURITY PLATFORM

Kompleksowe podejście do cyberbezpieczeństwa

CISCO SECURITY jest otwartą i zintegrowaną platformą, która pozwala zabezpieczyć sieci i aplikacje największych firm i instytucji. Odciąża zespoły ds. bezpieczeństwa IT od żmudnych procesów integracji różnych systemów ochrony. Stosowana przez Cisco filozofia „Zero Trust" oznacza kompleksowe podejście do zabezpieczenia dostępu do sieci, aplikacji oraz danych – obejmuje użytkowników i ich urządzenia, interfejsy API, IoT, mikro usługi, środowiska wirtualne, kontenery itp. Wykorzystanie rozwiązań Cisco umożliwia:

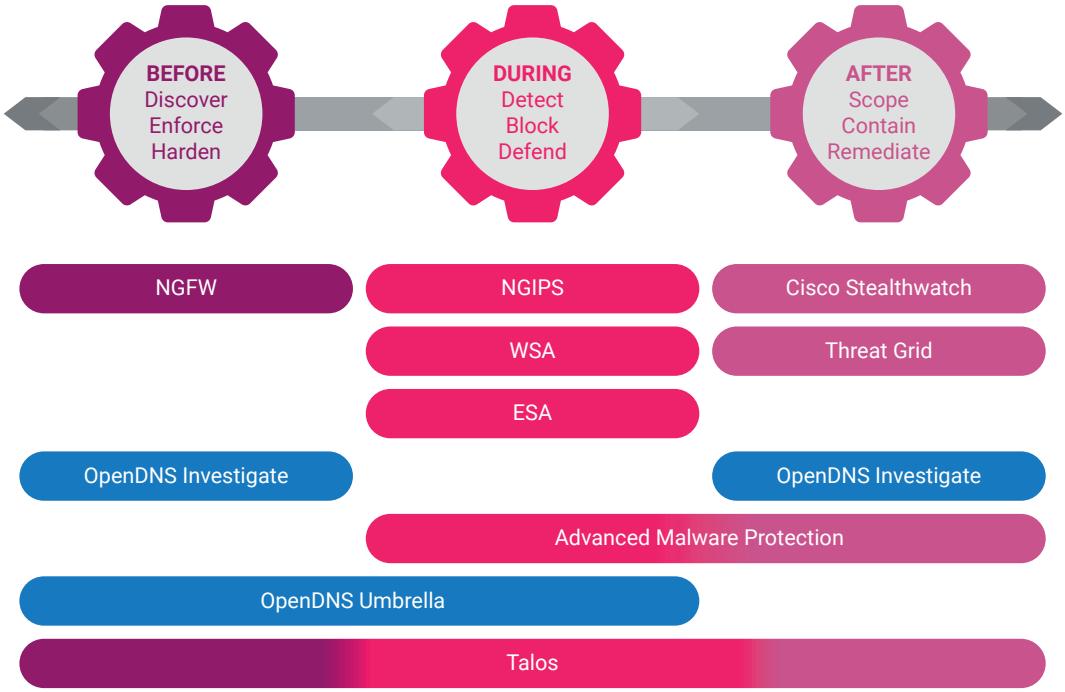
- W fazie „przed atakiem" ograniczenie ryzyka przeprowadzenia udanego ataku poprzez skuteczne egzekwowanie polityki bezpieczeństwa i monitorowanie wszystkich komponentów.
- W fazie „w trakcie ataku" identyfikację rodzaju zagrożeń i wektorów ataku poprzez korelację zdarzeń w czasie i różnych punktach infrastruktury i jego całkowite zablokowanie.
- W fazie „po ataku" identyfikację „punktu zero", od którego rozpoczął się atak oraz dalszego jego przebiegu w celu eliminacji ryzyka ponownej infekcji, a także analizę skutków ataku.

Passus Spółka Akcyjna | ul. Goraszewska 19, 02-910 Warszawa | tel.: +48 695 444 803 | e-mail: passus@passus.com | www.passus.com

Oferowane rozwiązania zapewniają:

- Zabezpieczenie brzegu sieci - rozwiązania NGFW Cisco Firepower wykrywają zagrożenia, pozwalają na wgląd w aplikacje wykorzystywane w sieci oraz tworzenie polityki bezpieczeństwa w oparciu o tę aplikację.
- Ochronę DNS - rozwiązanie Cisco Umbrella wykorzystuje globalną widoczność dotyczącą cyberataków oraz mechanizmy uczenia maszynowego.
- Bezpieczną komunikację e-mail z wykorzystaniem Cisco Email Security Appliance (ESA).
- Ochronę ruchu www dzięki rozwiązaniom klasy Web Proxy - Cisco Web Security Appliance (WSA).
- Wykorzystanie NetFlow, swoistego billingu naszej sieci w służbie bezpieczeństwu przy pomocy rozwiązania Cisco Stealthwatch.
- Przeciwdziałanie złośliwemu oprogramowaniu z Cisco Advanced Malware Protection (AMP), dostarczającemu kompleksową ochronę przed malwarem.
- Zarządzanie całą architekturą bezpieczeństwa dzięki rozwiązaniu Cisco Threat Response, które agreguje rozwiązania Cisco w jednym zunifikowanym interfejsie i pozwala z jednego miejsca podejmować efektywne działania prewencyjne.

Mocną stroną rozwiązań jest stałe wsparcie ze strony Cisco Talos – największej na świecie grupy ekspertów zajmujących się cyberbezpieczeństwem. Cisco Talos analizuje codziennie 1,5 miliona przypadków złośliwego oprogramowania i na bieżąco uaktualnia wspierane zabezpieczenia.



Portfolio produktów bezpieczeństwa Cisco wraz z ich przyporządkowaniem do fazy ataku.

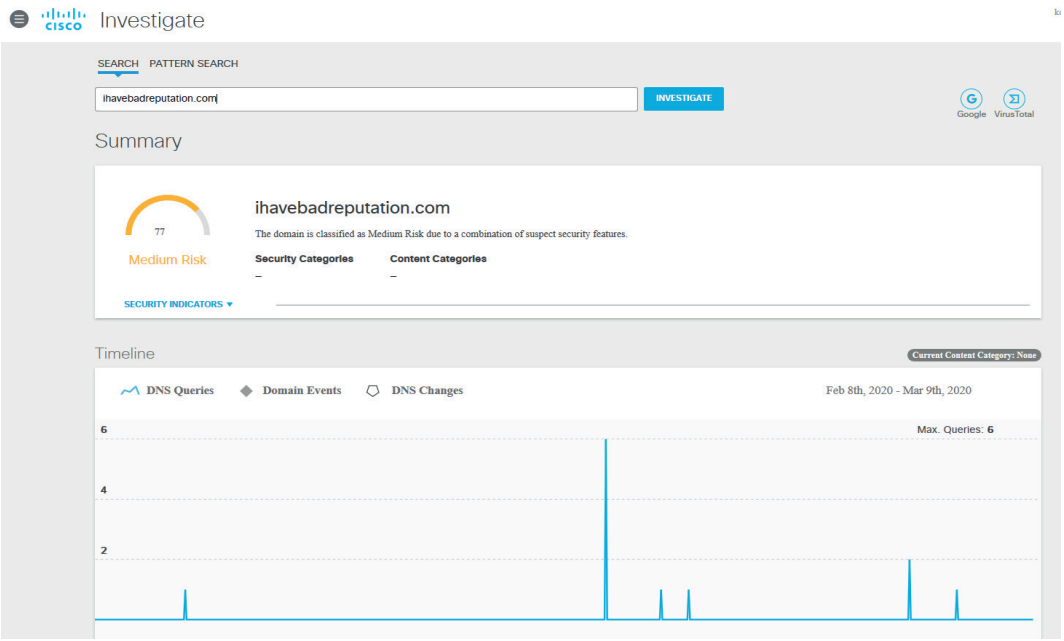
OCHRONA BRZEGÓW SIECI

Zapory sieciowe Cisco FirePower automatycznie zapobiegają naruszeniom zabezpieczeń, dają pełen wgląd w informacje o sieci i pozwalają wykrywać nawet subtelne zagrożenia. Zastosowane rozwiązania sprawiły, że firma Cisco w raporcie Garnera 2019 w kategorii Network Firewalls, została uznana Liderem

Główne cechy rozwiązania:

- Ochrona brzegów i segmentów sieci na styku z Internetem – filtry „stateful Inspection", rozpoznawanie i kontrola aplikacji, zintegrowane mechanizmy threat intelligence.
- Zautomatyzowane procesy stosowania i egzekwowania zasad oraz reguł opracowanych przez inżynierów CISCO i Talos.
- Ciągła analiza aktywności plików pozwala wychwycić złośliwe oprogramowanie, które ominęło zabezpieczenia 1 linii obrony.
- Integracja z Identity Service Engine – śledzenie użytkowników, kontrola dostępu i wymuszanie zasad zapory na urządzeniach w sieci.
- Pełna integracja z innymi rozwiązaniami Cisco – wgląd w informacje o wielu obszarach zagrożonych atakami.

OCHRONA DNS



Rozwiązanie Cisco Umbrella umożliwia kontrolowanie ruchu sieciowego poprzez monitorowanie zapytań DNS. W momencie, gdy użytkownik wysyła zapytanie DNS do domeny stanowiącej zagrożenie, automatycznie blokowany jest do niej dostęp - w odpowiedzi nie uzyskuje adresu IP umożliwiającego komunikację z serwerem. Rozwiązanie w ramach jednej platformy łączy funkcje firewalla, bezpiecznej bramy internetowej, brokera zapewniającego bezpieczny dostęp do chmury (CASB) i systemu do analizy zagrożeń. Cisco Umbrella jest największym systemem DNS zapewniającym abonentom dostęp do danych, obsługując ponad 600 miliardów zapytań dziennie, dzięki czemu pozwala błyskawicznie identyfikować nowe ataki i je odfiltrowywać. Cisco Umbrella pozwala też na bardziej tradycyjne formy filtrowania – kategorie, białe i czarne listy czy filtrowanie w oparciu o lokalizację.

Moduł Cisco Investigate jest wyposażony w efektywny API dzięki czemu może być wykorzystywany nie tylko przez rozwiązania Cisco, ale również przez badaczy bezpieczeństwa, czy firmy przygotowujące własne rozwiązania z zakresu security.

Główne cechy rozwiązania:

- Pełen wgląd w ruch DNS - przejrzyste wykresy informują o takich elementach, jak liczba zablokowanych zapytań, rozkład czasowy wysyłanych zapytań, a także pozwalają na podgląd ogólnego ruchu sieci, pokazujące szczegółowe statystyki z możliwością filtrowania wg ustalonych kryteriów.

- Błyskawiczne wdrożenie - nie wymaga nowego sprzętu lub modyfikacji już istniejącego, nie są potrzebne zasoby korporacyjnych maszyn, ani urządzeń użytkowników końcowych. Działa jako usługa chmurowa, więc nie ma również potrzeby instalacji oprogramowania wymagającego późniejszych aktualizacji. Wystarczy na ruterze brzegowym przekierować ruch DNS do Umbrelli - użytkownicy końcowi nie odczuwają żadnej różnicy - połączenie z internetem odbywa się z taką samą, jak zawsze, szybkością.

- Wysoka skuteczność - wykorzystuje zaawansowany zestaw narzędzi Cisco Security pozwalający na najbardziej kompleksowy przegląd, identyfikację i blokowanie zagrożeń we wczesnym stadium. W jego skład wchodzą między innymi oparte na modelach uczenia maszynowego mechanizmy do wykrywania znanych i nowych, pojawiających się zagrożeń oraz blokowania szkodliwych połączeń już w warstwach DNS i IP, funkcje AMP (Cisco Advanced Malware Protection), które umożliwiają wykrywanie szkodliwych plików i blokowanie ich w chmurze oraz analityka zagrożeń prowadzona przez Cisco Talos, pozwalająca na blokowanie szkodliwych adresów URL w warstwie HTTP/S.

BEZPIECZNA KOMUNIKACJA E-MAIL

Cisco Email Security (ESA) to kompleksowe rozwiązanie do zabezpieczenia ruchu typu e-mail, instalowane w formie fizycznego urządzenia lub wirtualnej maszyny dla środowiska VMware lub MS Hyper-V, dostępne także jako subskrypcja usługi w chmurze Cisco.

Cisco ESA daje bardzo wiele możliwości filtrowania wiadomości email oraz sprawdzania ich pod wieloma względami. Wstępna weryfikacja wiadomości przychodzących odbywa się na zasadzie sprawdzenia reputacji serwera nadawcy, wykorzystując usługę SBRS (Sender Base Reputation Score) we współpracy z Cisco Talos. Po pozytywnej weryfikacji można sprawdzać maile czy nie zawierają złośliwego oprogramowania, a także budować szereg zaawansowanych filtrów sprawdzających m. in.: nagłówki czy treść wiadomości.

Główne cechy rozwiązania:

- Ochrona poczty przychodzącej poprzez filtrowanie spamu, wiadomości zawierających malware lub wirusy, czy chroniąc przed fraudem czy phishingiem.

- Możliwość zarządzania tzw. wiadomościami typu graymail (kampaniami mailowymi, reklamami czy wiadomościami pochodzącymi z social mediów) dając możliwość bezpiecznego „wypisania się" z otrzymywania tego typu korespondencji (Safe Unsubscribe).

- Zabezpieczenie poczty wychodzącej przed wyciekiem ważnych czy poufnych dla firmy informacji (usługa DLP – Data Loss Prevention).

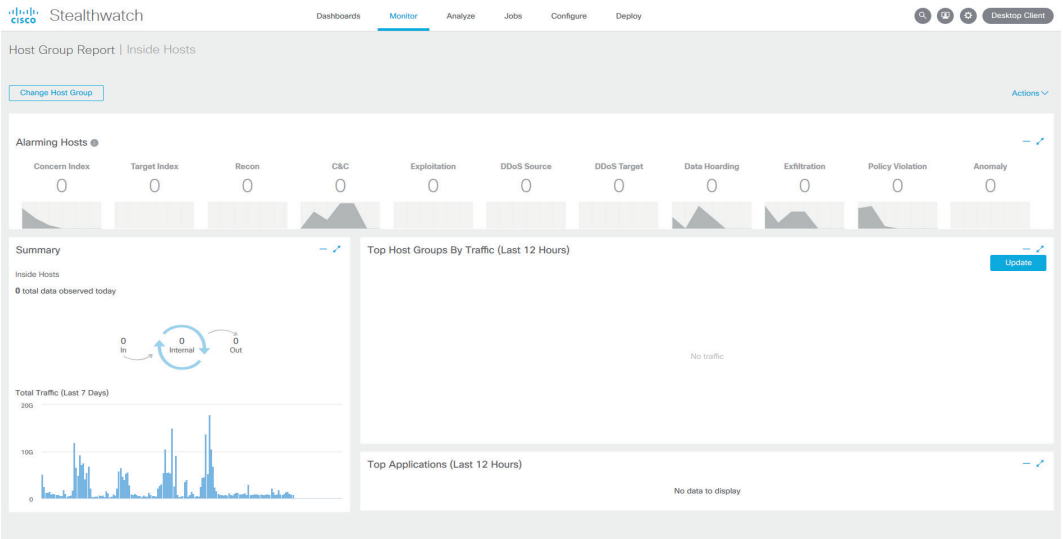
OCHRONA KOMUNIKACJI WWW

Cisco Web Security Appliance (WSA) to zaawansowane rozwiązanie oferujące kontrolę oraz analizę ruchu „web". Identyfikuje setki aplikacji i ponad 150 tysięcy mikroaplikacji, dając administratorowi możliwość blokowania dostępu użytkownikom do takich funkcjonalności jak czaty, audio, video zgodnie z wymogami firmy.

Główne cechy rozwiązania:

- Łączy tradycyjne filtrowanie adresów URL z dynamiczną analizą treści.
- Identyfikuje setki aplikacji i ponad 150 tysięcy mikroaplikacji.
- Pomaga administratorom na tworzenie zasad polityki bezpieczeństwa.
- Daje możliwość administratorowi blokowania dostępu użytkownikom do takich funkcjonalności jak: czaty, czytniki wiadomości, audio, wideo, zgodnie z wymogami bezpieczeństwa firmy (nie blokując jednocześnie całych stron).
- Integruje się za pomocą Internet Content Adaptation Protocol (ICAP) z rozwiązania DLP innych producentów w celu kontroli treści i egzekwowania zasad DLP.
- Posiada możliwość integracji z rozwiązaniem AMP do ochrony przed złośliwym oprogramowaniem. AMP umożliwia wykrywanie i blokowanie malware'u, ciągłą analizę i retrospektywne ostrzeganie.

MONITORING BEZPIECZEŃSTWA



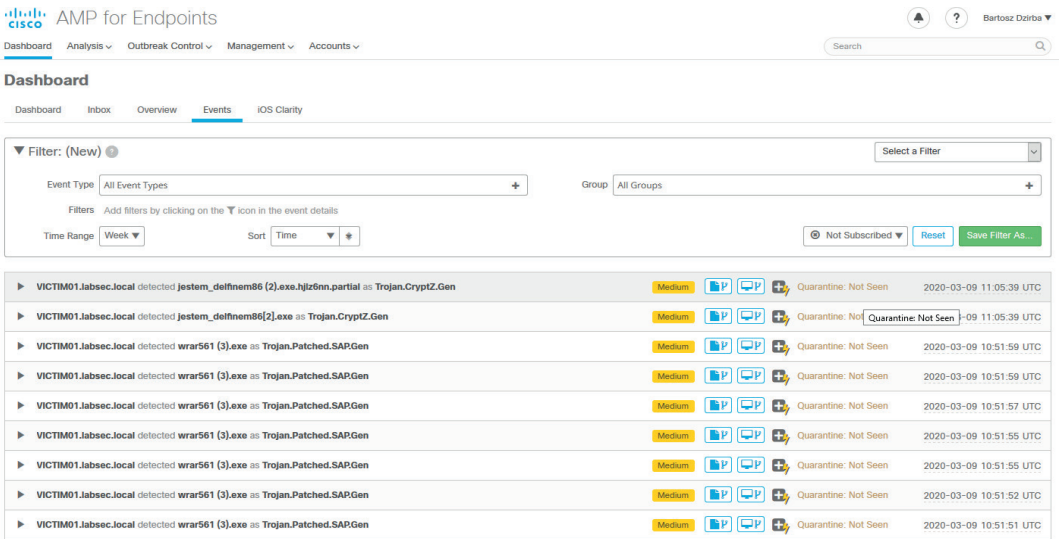
Cisco Stealthwatch® Enterprise kompleksowo monitoruje sieć w celu wykrywania zagrożeń i reagowania na nie w czasie rzeczywistym. Dzięki połączeniu metod takich jak uczenie maszynowe, zasilanie danymi z Cisco Talos, Stealthwatch wykrywa zagrożenia, takie jak ataki Command and Control, ransomware, ataki DDoS, nieznane złośliwe oprogramowanie i zagrożenia wewnętrzne. Jest rozwiązaniem bezagentowym umożliwiającym kompleksowe monitorowanie zagrożeń w całym ruchu sieciowym, nawet jeśli jest on szyfrowany.

W przeciwieństwie do ogromu rozwiązań typu „kolektor flowów", Cisco Stealthwatch zajmuje się podejściem do agregacji ruchu sieciowego pod kątem incydentów bezpieczeństwa. Obsługuje protokoły eksportu metadanych z ruchu sieciowego takie jak Cisco NetFlow, IPFIX standaryzowany NetFlow), sFlow, cFlow, jFlow, Packeteer 2, NetStream oraz Cisco NSEL, może też bezpośrednio odbierać ruchu z portu typu „span", zamieniając poszczególne sesje na metadane samodzielnie. Silnik analityczny pracuje w czasie rzeczywistym nad zebranymi metadanymi. Po zdeduplikowaniu ruchu, Stealthwatch określa anomalie, znane rodzaje ataków, problemów i następnie dla wygody analityka bezpieczeństwa priorytetyzuje je wg poziomu zagrożenia dla firmy w proste do zrozumienia i podjęcia decyzji kategorie.

Główne cechy rozwiązania:

- Koncentracja na incydentach, redukcja false-positives - wykorzystując siłę modelowania behawioralnego oraz wielowarstwowe uczenie maszynowe, Stealthwatch redukuje fałszywe alarmy skupiając swoja uwagę na krytycznych zagrożeniach
- Ciągły monitoring sieci i wykrywanie zaawansowanych zagrożeń w czasie rzeczywistym - ataki są zwykle poprzedzone czynnościami takimi jak skanowanie portów, ciągłe pingowanie itp. Stealthwatch rozpoznaje te wczesne oznaki, aby zapobiec głównemu atakowi. Po zidentyfikowaniu zagrożenia można przeprowadzić dochodzenie, aby wskazać źródło zagrożenia i ustalić, gdzie jeszcze mogło się rozprzestrzeniać.
- Wykorzystanie danych zebranych z istniejącej infrastruktury do poprawy bezpieczeństwa - dzięki pojedynczemu rozwiązaniu bez agentów Stealthwatch wykorzystuje bogate źródło wiedzy – dane telemetryczne generowane przez istniejącą infrastrukturę sieciową.
- Skalowalność - wraz z rozwojem organizacji - uruchamianiem nowych oddziałów, rozbudową data center migracją do chmury, wdrożenie Stealthwatch można łatwo rozszerzyć, aby objęło swoim zasięgiem całą infrastrukturę. Rozwiązanie może być wdrażane lokalnie lub w chmurze, może być wykorzystywany jako rozwiązanie typu SaaS lub na licencji. Dodatkowo Stealthwatch posiada funkcję automatycznej klasyfikacji ról, aby automatycznie klasyfikować nowe urządzenia dodawane do sieci.

OCHRONA PRZED MALWAREM



Cisco AMP jest systemem klasy EDR (Endpoint Detection&Response) służącym do kompleksowej ochrony przed złośliwym oprogramowaniem (malware).

Rozwiązanie aktywnie analizuje i śledzi aktywność plików wymienianych w sieci, na bieżąco badając kontekst zachodzących zdarzeń, koreluje te informacje z danymi telemetrycznymi, danymi ze środowiska sandbox, jest także zasilany modelami budowanymi przez Cisco Talos.

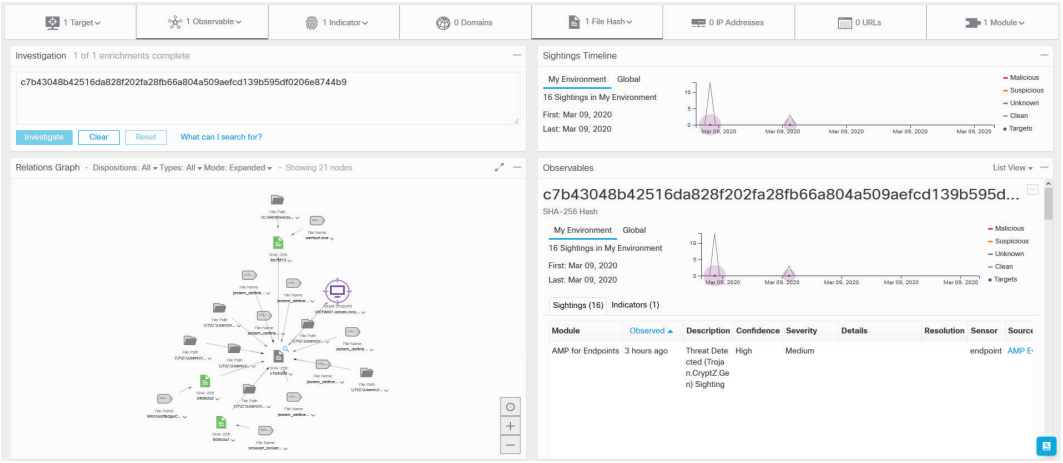
Rozwiązanie ściśle współpracuje także z rozwiązaniem Cisco o nazwie Threat Grid - wyizolowanym sandboxem, w którym badane jest zachowanie podejrzanych plików i odnośników. AMP jest zatem często pierwszą ale i ostatnią linią obrony przed atakami - zapewnia kompleksową ochronę organizacji we wszystkich jego fazach – przed, podczas i po ataku.

- ochrona przed atakiem - AMP wykorzystuje cały zestaw technologii zapobiegawczych, aby zatrzymać złośliwe oprogramowanie w czasie rzeczywistym, chroniąc punkty końcowe przed atakami takich jak: reputacja plików, antywirus, wykrywanie oprogramowania polimorficznego, wykorzystanie machine learning do analizy, ochrona przed exploitami.

- wykrywanie ataków - Rozwiązanie AMP stale monitoruje punkty końcowe, aby pomóc wykrywać nowe i nieznane zagrożenia. Wykorzystuje do tego celu metody takie jak: monitorowanie aktywności stacji końcowej pod katem podejrzanych zachowań, skanowanie sieci pod katem wskaźników kompromitacji (opartych na chmurze lub własnych opartych na hoście), identyfikacja podatności na stacjach końcowych, wykrywanie plików wykonywalnych rzadko występujących na urządzeniach końcowych i ich analiza w środowisku sandbox.

- obrona po ataku - AMP monitoruje, analizuje i rejestruje całą aktywność plików i komunikację na urządzeniach końcowych, urządzeniach mobilnych i w sieci, aby szybko wykryć ukryte zagrożenia, które wykazują podejrzane lub złośliwe zachowanie.

ANALIZA ŚLEDCZA/FORENSIC



Cisco Threat Response zbiera informacje o zagrożeniach z różnych źródeł w ramach jednej aplikacji. Rozwiązanie ułatwia i przyspiesza wykrywanie, analizowanie i neutralizowanie zagrożeń. Wizualizuje przebieg incydentu, dodaje kontekst oraz potrafi skorelować zdarzenia zachodzące na posiadanych rozwiązaniach bezpieczeństwa. Rozwiązanie jest dostępne bez dodatkowych opłat w pakiecie z wybranymi rozwiązaniami bezpieczeństwa firmy Cisco.

Główne cechy rozwiązania:

- Podsumowanie informacji o zagrożeniach - łączy informacje o zagrożeniach od Cisco Talos oraz ze źródeł osób trzecich w celu automatycznego sprawdzenia wskaźników zagrożenia (IOCs) i jego szybkiego potwierdzenia.

- Zautomatyzowane wzbogacanie - automatycznie pokazuje kontekst ze zintegrowanych produktów Cisco Security oraz informuje, które systemy i w jaki sposób zostały zaatakowane.

- Intuicyjne i interaktywne wizualizacje - pokazuje wyniki na intuicyjnych wykresach, które można skonfigurować w celu uzyskania większej widoczności i szybszego wyciągania wniosków.

- Śledzenie incydentów - umożliwia zbieranie i przechowywanie najważniejszych informacji dotyczących dochodzeń, a także zarządzanie i dokumentowanie postępów oraz wniosków.

- Bezproblemowe docieranie do szczegółów - ułatwia przeprowadzanie dogłębnych dochodzeń, w tym poprzez zintegrowane produkty Cisco Security. Jeżeli chcemy dokładnie sprawdzić, dokąd złośliwy plik został przesłany wystarczy jedno kliknięcie, aby wejść do Cisco AMP for Endpoints, i w ten sposób dowiedzieć się wszystko o jego drodze.

- Bezpośrednie podjęcie działań naprawczych - umożliwia podjęcie działań naprawczych bezpośrednio z poziomu interfejsu np. blokowanie podejrzanych plików, domen i innych, bez potrzeby wcześniejszego logowania się do innych produktów.

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. oraz Chaos Gears 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 tego środowiska cloud;
- rozwiązania zabezpieczające przed nadużyciami finansowymi (antyfraud).

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 należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Ikea, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

W lutym 2020 roku Firma Passus SA uzyskała status Cisco Advanced Security Architecture Specialization. Specjalizacja jest potwierdzeniem kompetencji, doświadczenia i potencjału niezbędnego do skutecznej realizacji dowolnej skali przedsięwzięć w zakresie wdrożeń rozwiązań Cisco do ochrony infrastruktury IT.