STINET

VECTRA

Vectra Cognito™

Najważniejsze cechy

- Wyszukuje aktywne zagrożenia w sieci
- Automatyzuje proces znajdowania zagrożeń i podpowiada, jak reagować
- Stale śledzi zagrożenia we wszystkich fazach ataku
- Monitoruje cały ruch sieciowy – wewnątrz organizacji i wymianę danych z Internetem
- Analizuje logi z systemów bezpieczeństwa oraz uwierzytelniania i aplikacji SaaS
- Obejmuje ochroną wszystkie urządzenia – dowolne systemy operacyjne, BYOD i IoT
- Zabezpiecza infrastrukturę wirtualną i fizyczną
- Integruje się z wiodącymi rozwiązaniami typu SIEM, firewallami, NAC-ami i oprogramowaniem ochronnym na stacjach końcowych

Vectra Cognito™ jest najszybszym i najskuteczniejszym sposobem na znalezienie i zatrzymanie ataku w sieci. Wykorzystuje sztuczną inteligencję, aby zapewnić wykrycie ataku w czasie rzeczywistym, przedstawić szczegóły i umożliwić podjęcie natychmiastowych działań naprawczych.

Łącząc zaawansowane algorytmy uczenia (takie jak sieci neuronowe oraz głębokie uczenie maszynowe) oraz dynamiczne modele zachowań sieci, Vectra Cognito szybko i efektywnie znajduje zarówno ukryte jak i nieznane zagrożenia, zanim wyrządzą szkody.

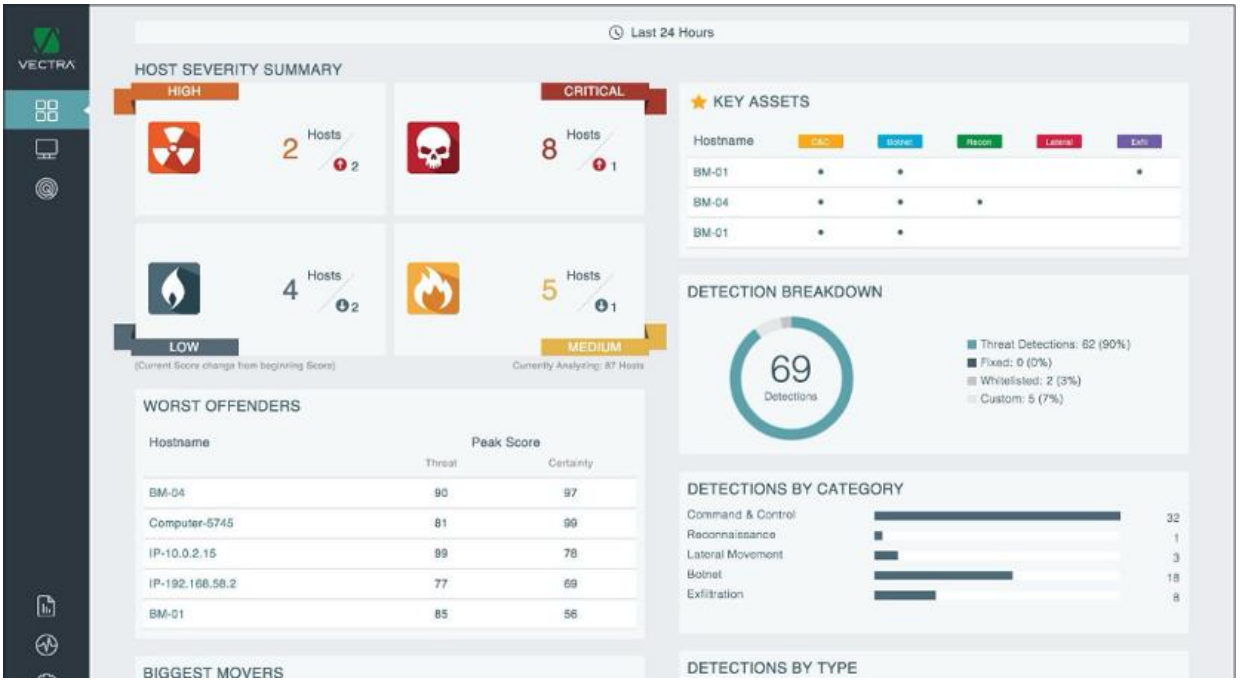
Vectra Cognito eliminuje tzw. martwe punkty, niemonitorowane obszary sieci, analizując cały ruch sieciowy oraz dzienniki zdarzeń z systemów bezpieczeństwa, uwierzytelniania oraz aplikacji typu SaaS. Takie podejście gwarantuje pełny obraz komunikacji w sieci firmowej, od urządzeń IoT do centrów danych lub chmury, nie pozostawiając atakującym miejsca do ukrycia.

Analityk bezpieczeństwa w formie oprogramowania

Vectra Cognito automatyzuje polowanie na cyberprzestępców, wskazuje miejsca, w których się ukrywają i informuje o ich aktywności. Zagrożenia o najwyższym poziomie ryzyka są wskazane natychmiast, korelowane z konkretnymi hostami i oznaczone jako krytyczne. Dzięki temu zespoły bezpieczeństwa mogą reagować szybciej, aby zatrzymać trwające ataki i zapobiec utracie danych.

Automatyzując ręczną i czasochłonną analizę zdarzeń bezpieczeństwa, Vectra Cognito skraca tygodnie lub miesiące pracy do kilkunastu minut. W rezultacie, znacząco redukuje obciążenie analityka bezpieczeństwa.

Vectra Cognito priorytetyzuje zagrożenia, koreluje z kluczowymi zasobami oraz pokazuje, gdzie konkretnie znajduje się intruz i co aktualnie robi.



Jak działa Vectra Cognito?

Zaawansowane metadane

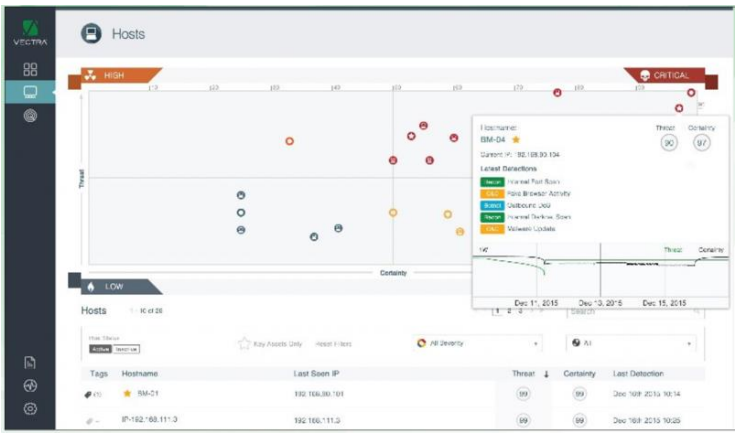
Vectra analizuje ruch sieciowy w czasie rzeczywistym. Wyodrębnia metadane z pakietów, zamiast przeprowadzać ich głęboką inspekcję (DPI). Analizowany jest cały ruch sieciowy, w tym wewnętrzny ruch organizacji (wschód zachód), wymiana danych z Internetem (północ południe) oraz ruch w ramach infrastruktury wirtualnej i chmury publicznej. Vectra Cognito identyfikuje, śledzi i ocenia każde urządzenie z dostępem do sieci IP w infrastrukturze korporacji. Ochrona rozciągnięta jest na laptopy, serwery, drukarki, urządzenia typu BYOD i IoT, wspierając wszystkie systemy operacyjne i aplikacje, w tym przepływ ruchu w środowiskach wirtualnych, chmurze publicznej, a także w aplikacjach typu SaaS.

Logi systemowe, uwierzytelniania oraz SaaS wzbogacają metadane ruchu sieciowego w celu umożliwienia precyzyjnej identyfikacji systemów i użytkowników.

Vectra Cognito wykorzystuje wskaźniki IoC STIX do wykrywania znanych zagrożeń, uzyskanych na podstawie analizy. Wskaźniki są korelowane z innymi zachowaniami intruzów w celu wykrycia urządzeń będących źródłem ataku.

Identyfikuj zachowania atakujących

Zgromadzone metadane są analizowane z wykorzystaniem algorytmów określających zachowanie intruzów, co pozwala wykryć ukryte i nieznane ataki. Analiza behawioralna umożliwia wyróżnienie podstawowych zachowań atakującego, takie jak użycie narzędzi zdalnego dostępu, zestawione ukryte tunele komunikacji, backdoor'y, nadużycia poświadczeń oraz wewnętrzny rekonesans i rozprzestrzenianie się.



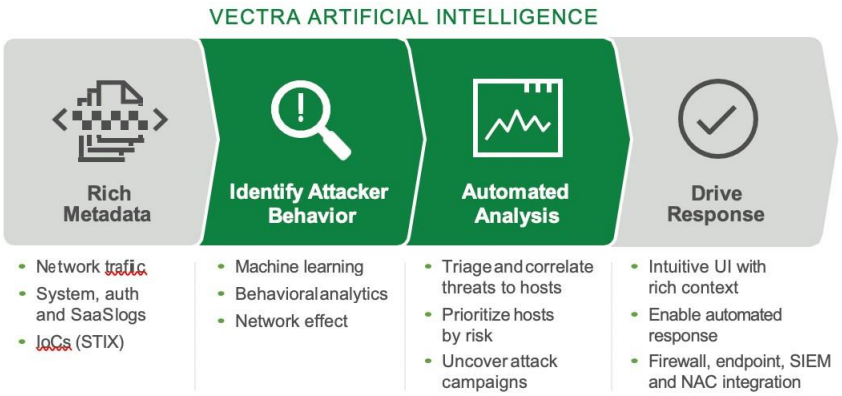
Wskaźnik Vectra Threat Certainty Index™.

Vectra Cognito nieustannie uczy się lokalnego środowiska i śledzi aktywność wszystkich hostów, fizycznych i wirtualnych, odsłaniając oznaki włamania lub kompromitacji systemów.

Duża część wariantów danego zagrożenia jest automatycznie wykrywana we wszystkich fazach cyberataku, takich jak na przykład:

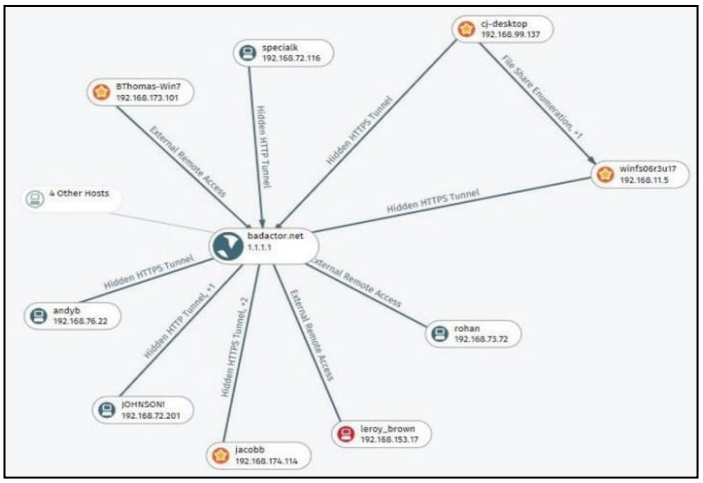
- Komunikacja z centrami sterowania oraz ukryte tunele
- Wewnętrzny rekonesans
- Rozprzestrzenianie się
- Nadużycie uprawnień uwierzytelniania
- Wykradanie danych
- Wczesne objawy aktywności ransomware
- Aktywność botnet

Vectra Cognito monitoruje i wskazuje na podejrzany dostęp do krytycznych zasobów przez upoważnionych pracowników, a także wykrywa naruszenia zasad związanych z wykorzystaniem zasobów w chmurze, pamięci USB i innych metod umożliwiających wynoszenie danych na zewnątrz korporacji.



Automatyczna analiza

Wskaźnik Threat Certainty Index™ zestawia tysiące zdarzeń z historycznym kontekstem zachowania pojedynczego hosta, aby w rezultacie wskazać konkretne urządzenia, które stanowią największe zagrożenie. Zamiast generować tysiące alarmów wymagających dalszej analizy, Vectra Cognito skraca proces wyszukiwania tego, co jest realnym niebezpieczeństwem i wskazuje konkret. W rezultacie system generuje powiadomienia dla zespołu SOC, wysyła odpowiedni komunikat do SIEM lub innych narzędzi.



Cognito prezentuje zwięzły widok kampanii ataku

Funkcja Attack Campaigns dodatkowo automatyzuje wykrywanie zagrożeń, łącząc ze sobą kolejne zdarzenia, zachowania w sieci, ilustrując relacje między hostami, wykrywając kanały komunikacyjne typu command-and-control.

W czasie, gdy intruz wykonuje rozpoznanie i przenosi się od stacji do stacji, Vectra Cognito koreluje zachowanie pomiędzy wszystkimi zaangażowanymi w ten proces i prezentuje zwięzły widok całej kampanii ataku.

Vectra Cognito przedstawia widok na elementy sieci i powiązanych z nimi rozpoznanymi kampaniami ataku. Analizuje historię zdarzeń obejmującą okres aktywności intruza, tak aby lepiej zrozumieć daną aktywność i pełen zakres ataku.

Rozwiąż problem

Szybko i zdecydowanie reaguj na zagrożenia. System wskaże najważniejsze informacje na temat kontekstu ataku oraz określi wskazówki dotyczące dalszych działań. W przeciwieństwie do typowych produktów bezpieczeństwa, Vectra Cognito eliminuje ręczną analizę poprzez automatyczne ustalanie priorytetów i skorelowanie zagrożeń z hostami i kluczowymi zasobami, które są celem ataku.

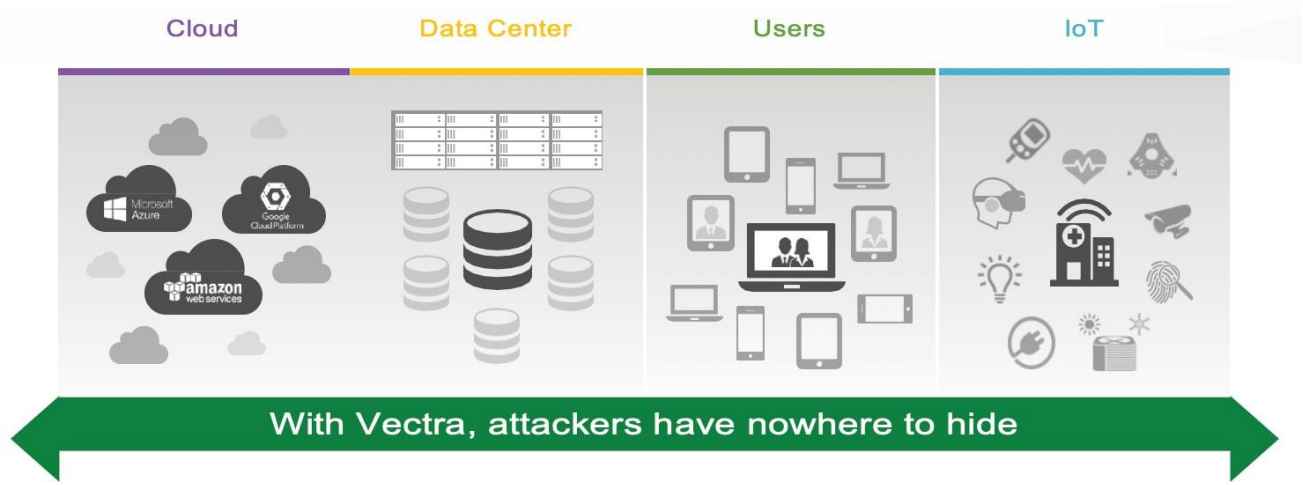
Vectra Cognito pokazuje szczegóły dotyczące wykrytych zagrożeń, włączając informacje dotyczące hostów, kontekstu przechwyconych pakietów oraz wartość wskaźnika Threat Certainty Index™

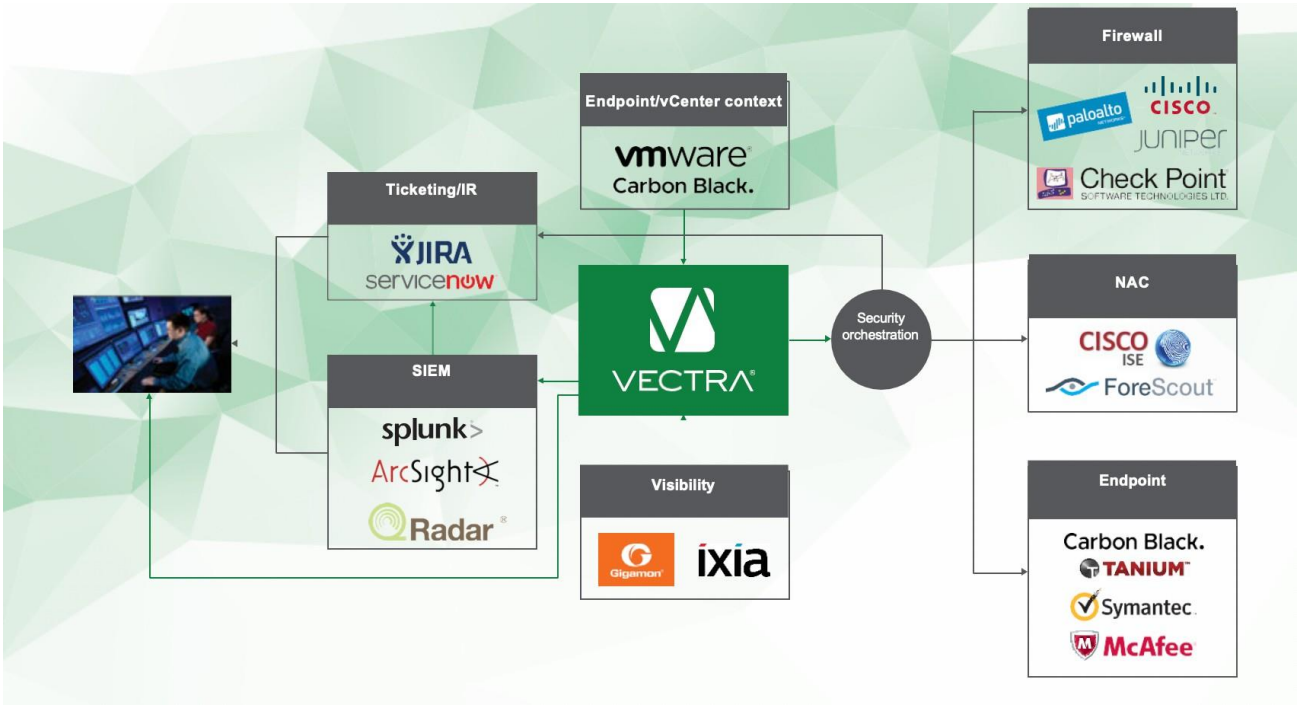
Dodatkowo Vectra Cognito współpracuje z zaporami ogniowymi następnej generacji, zabezpieczeniami punktów końcowych, systemami NAC i innymi rozwiązaniami bezpieczeństwa w celu automatycznego blokowania nieznanych i celowanych cyberataków. Vectra stanowi punkt wyjścia do wyszukiwania zagrożeń, wpływając na efektywność rozwiązań SIEM lub innych narzędzi informatyki śledczej.

Vectra Cognito - bezpieczeństwo, które myśli

Oszczędność czasu i zasobów

Vectra Cognito odciąża i wzmacnia zespoły ds. bezpieczeństwa, które często nie mają wystarczających zasobów ludzkich. Wszystko to dzięki zautomatyzowaniu czasochłonnej analizy zdarzeń. Każde wykrycie jest szczegółowo wyjaśnione, wraz z towarzyszącym mu zdarzeniem i historycznym kontekstem, który do niego doprowadził.



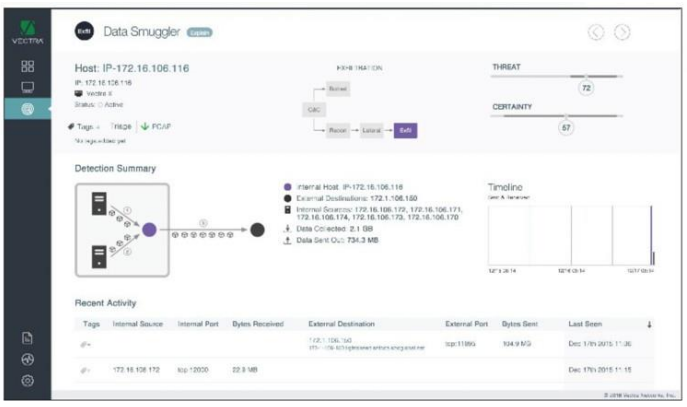


Vectra Cognito integruje się z szeroką gamą rozwiązań bezpieczeństwa

Vectra Cognito zapewnia również dostęp na żądanie do metadanych z przechwyconych pakietów w celu dalszego dochodzenia i analizy. Daje to zespołom ds. bezpieczeństwa niezbędne dowody potrzebne do podjęcia natychmiastowych i zdecydowanych działań.

Wzmocnij swoją istniejącą infrastrukturę bezpieczeństwa

Vectra Cognito integruje się z wiodącymi rozwiązaniami bezpieczeństwa na stacjach końcowych, aby automatycznie dodawać wzbogacony materiał do analizy i umożliwić zespołom ds. bezpieczeństwa izolowanie zainfekowanych urządzeń. Niezależnie od tego czy inteligencja wykorzystana jest do blokowania nowych zagrożeń przez korporacyjną zaporę, systemy NAC lub inne narzędzia, Vectra Cognito zapewni więcej korzyści z istniejących technologii bezpieczeństwa.



Interfejs API umożliwia automatyczną reakcję i wywołanie akcji praktycznie z każdym dostawcą bezpieczeństwa. Vectra Cognito generuje powiadomienia syslog i logi CEF dla wszystkich wykrytych zdarzeń, jak również powiadomi o stacjach w sieci z najwyższym indeksem ryzyka. Dzięki temu Vectra Cognito jest czymś więcej niż tylko kolejnym źródłem logów i stanowi idealny czynnik wyzwalający dochodzenia i wspomagający definicję procesów dla systemów typu SIEM.

Wykrywanie pełnego cyklu kampanii ransomware

Vectra Cognito wykrywa kampanie ransomware we wszystkich fazach ataku. Monitorując cały wewnętrzny ruch sieciowy, Vectra szybko identyfikuje podstawowe zachowania ataku ransomware.

Oprócz wykrywania bezpośrednio kampanii ransomware Cognito wykrywa wcześniejsze wersje tego ataku, wliczając w to fazy komunikacji kanałem command-and-control, skanowanie sieci, rozprzestrzenianie się w celu odnalezienia wrażliwych serwerów i ich zaszyfrowaniu.

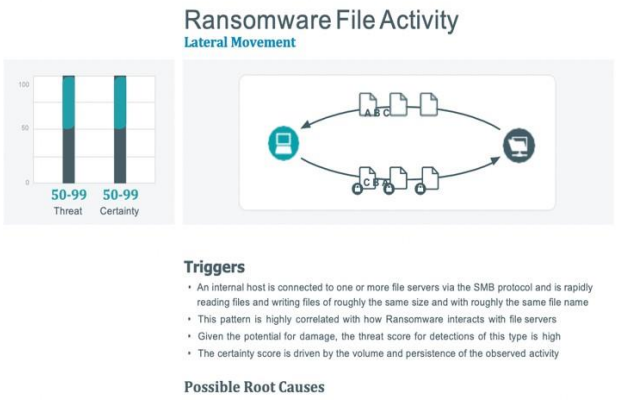
Podgląd podglądających

Początkowo celem atakującego jest stacja użytkownika końcowego, jednak prawdziwa walka toczy się o zdobycie uprawnień administracyjnych i przejęciu roli zarządzającego infrastrukturą. Cognito wykracza poza proste monitorowanie zachowań użytkowników. System śledzi protokoły sieciowe służące do zarządzania, uczy się charakterystyki tego ruchu i reaguje na wszystkie anomalie.

Bezpieczeństwo dla środowisk chmurowych

Infrastruktura chmury prywatnej staje się sercem i duszą wielu organizacji, ale często pozostaje niekontrolowanym obszarem dla zespołów ds. bezpieczeństwa. Vectra Cognito nieustannie monitoruje krytyczne aplikacje, dane i infrastrukturę centrum przetwarzania danych, umożliwiając wykrywanie nawet najbardziej wyrafinowanych ataków.

Około 80% ruchu w centrum danych nigdy go nie opuszcza, tym samym nie jest monitorowane przez tradycyjne systemy bezpieczeństwa, umiejscowione na brzegu sieci. Wirtualne sensory Vectra Cognito (vSensors) łączą się z dowolnym przełącznikiem VMware vSwitch, aby zapewnić widoczność całego ruchu. System integruje się również z VMware vCenter, zapewniając autorytatywny, zawsze aktualny widok wirtualnego środowiska.



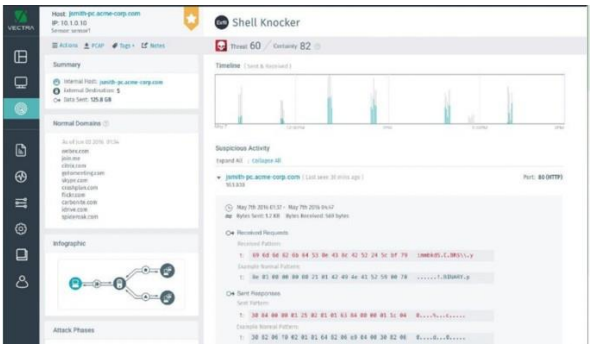
The Vectra Cognito ransomware detection

Bezpieczeństwo w warstwie sprzętowej

Ochrona centrów danych wykracza poza wirtualizację i obejmuje fizyczny sprzęt serwerowy oraz narzędzia niskiego poziomu używane do zarządzania centrum danych. Vectra Cognito zapewnia bezprecedensowe wykrywanie zagrożeń, które rozciąga się od warstwy aplikacji do najniżej warstwy sprzętowej.

Dla przykładu, wykrycie przez Cognito metody ataku “Port Knocking” polega na wskazaniu serwerów zainfekowanych przez rootkity, które działają w warstwie poniżej fizycznego systemu operacyjnego. Ponadto Vectra Cognito monitoruje i wykrywa niewłaściwe wykorzystanie protokołów niskiego poziomu zarządzania, takie jak IPMI lub iDRAC.

Powszechnie używane przez administratorów narzędzia do zarządzania sprzętem w serwerowni oraz wykorzystywane do tego protokoły są coraz częściej celem ataków. Protokoły tego typu dają duże możliwości do przejęcia systemów w wyższej warstwie, ponieważ są często niemonitorowane oraz nielogowane.



Vectra Cognito, wykrycie Shell-Knocker detection

Ujednolicanie operacji centrum danych

Nowoczesne centra danych wymagają ciągłej koordynacji między zespołami tworzącymi sieci, zajmującymi się rozwojem aplikacji, zespołami wirtualizacyjnymi i oczywiście zespołem ds. bezpieczeństwa. Vectra Cognito ułatwia wszystkim grupom synchronizację i zachowuje pełną widoczność w środowisku wirtualnym. Dzięki pełnej integracji z VMware vCenter, Vectra Cognito zapewnia zawsze aktualny widok środowiska i ostrzega o wszelkich zasobach, które nie są monitorowane pod kątem zagrożeń.

Vectra Cognito na próbę bez ryzyka

Analizując tylko lustrzany ruch sieciowy, Vectra może zostać zainstalowana w ciągu kilku minut i nie zakłóca działania infrastruktury.

Stinet sp. z o.o., Solec 18 lok. U61, 00-410 Warszawa
Tel.: 22 740 42 20, fax: 22 740 42 19
KRS: 0000712461, Sąd Rejonowy dla m. st. Warszawy
XIII Wydział Gospodarczy Krajowego Rejestru Sądowego,
NIP: 9522172992, REGON: 368897634,
Kapitał zakładowy 500 000 PLN