STINET

VECTRA

Vectra Cognito™ Detect

Kluczowe punkty

- Stale uczące się modele behawioralne używają AI, by rozpoznać ukrytych i nieznanych atakujących, umożliwiając szybką reakcję i zapewniając stabilny punkt startowy dla wspomaganego przez AI wykrywania zagrożeń
- Wykrywa zagrożenia przy użyciu AI oraz integruje inne źródła informacji o zagrożeniach
- Analizuje wzbogacone sieciowe metadane, istotne logi oraz zdarzenia w chmurze by zyskać dokładny wgląd w zachowania atakujących na każdej płaszczyźnie: w chmurze, w data center, na urządzeniach końcowych i w IoT
- Unikalny kontekst eliminuje bezowocne polowanie na zagrożenia i umożliwia bezpośrednią akcję, proaktywnie umieszczając najistotniejsze informacje wprost przed Twoimi oczami
- Współpracuje z rozwiązaniami typu EDR, firewall, NAC i innymi systemami obronnymi by blokować nowe klasy zagrożeń
- Stanowi stabilny punkt startowy dla rozbudowanej informatyki śledczej z użyciem Cognito Recall, SIEM'ów i narzędzi klasy forensic.

NAJEFEKTYWNIEJSZA DROGA DO ZATRZYMANIA CYBERATAKÓW W CZASIE RZECZYWISTYM

Główną częścią platformy detekcji cyberataków i zagrożeń Cognito™, stworzonej przez Vectra®, jest Cognito Detect™ - najszybszy i najefektywniejszy sposób powstrzymania cyberprzestępców atakujących środowiska informatyczne, centra danych i zasoby w chmurze publicznej. Cognito Detect™ używa sztucznej inteligencji by umożliwić detekcję ataków w czasie rzeczywistym i bezpośrednio dostarczyć Ci kluczowe informacje.

Prócz wzmocnienia bezpośrednich aktywności w reakcji na trwające ataki, Cognito Detect jest kluczowym punktem startowym dla profesjonalnych łowców zagrożeń, używających Cognito Recall™ do szczegółowych śledztw.

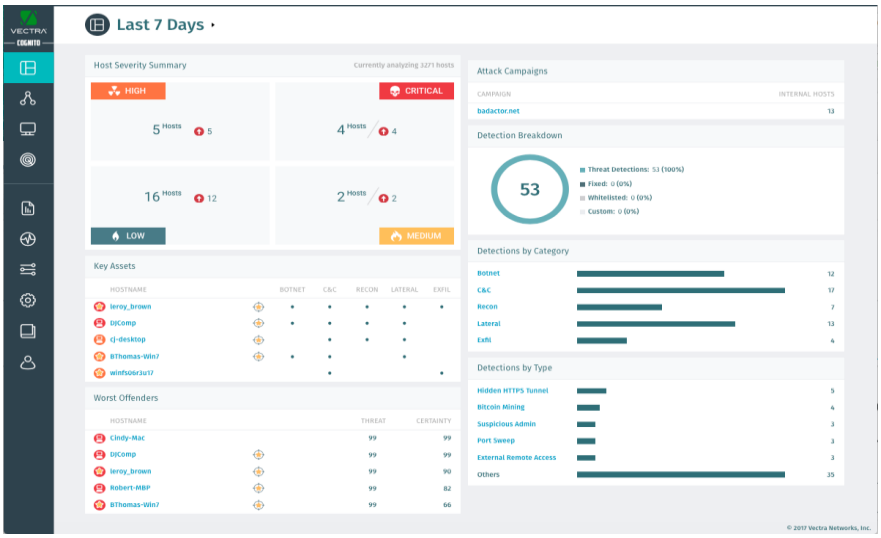
Poprzez połączenie zaawansowanych algorytmów machine learning – włączając deep learning i sieci neuronowe – z nieustannie uczącymi się modelami behawioralnymi, Cognito Detect szybko i efektywnie wykrywa zakamuflowanych i nieznanych agresorów – zanim dokonają zniszczeń.

Cognito Detect zapewnia widoczność dla środowiska klasy korporacyjnej – analizując cały ruch sieciowy, logi z systemów bezpieczeństwa, systemów uwierzytelnienia i aplikacji SaaS. Nie pozostawia to atakującym miejsca do ukrycia się – ani w data center ani na stacjach użytkowników lub IoT.

Częścią subskrypcji Cognito Detect są regularnie dostarczane, nowe algorytmy wykrywania zagrożeń – by zapewnić naszym klientom ochronę przed najnowszymi zagrożeniami.

Cyfrowy analityk bezpieczeństwa IT

Cognito Detect automatyzuje polowanie na cyberprzestępców, pokazuje, gdzie się ukrywają i podpowiada co robią. Zagrożenia o najwyższym stopniu ryzyka są natychmiastowo oceniane, powiązywane z konkretnymi hostami i priorytetyzowane tak by zespoły bezpieczeństwa IT mogły szybciej reagować na trwające ataki i redukować zagrożenia.



SZTUCZNA INTELIGENCJA COGNITO

- Ruch sieciowy
- Logi systemowe, Auth i SaaS, IoCs (STIX)

- Machine learning
- Analityka behawioralna
- Efekty sieciowe

- Natychmiast ocenia i koreluje zagrożenia z hostami
- Priorytetyzuje hosty według ryzyka
- Identyfikuje złożone kampanie malware

- Intuicyjny interfejs ze wzbogaconym kontekstem
- Automatyzacja reakcji
- Integracja z Firewallem, EDR, SIEM i NAC

Automatyzując czasochłonne, manualne analizowanie zdarzeń, Cognito Detect skraca tygodnie do minut i redukuje pracę analityków nawet 32-krotnie.

Pozwala to zespołom operacyjnym, nierzadko zmagającymi się z brakami personelu i oblężeniem ze strony atakujących, zyskać przewagę czasową w odpowiedzi na zagrożenia.

JAK DZIAŁA COGNITO DETECT?

Wzbogacone metadane

Cognito Detect daje Ci wgląd do ruchu sieciowego w czasie rzeczywistym, poprzez ekstrakcję metadanych z pakietów – bez głębokiej analizy pakietów, co pozwala chronić bez zbędnego naruszania prywatności.

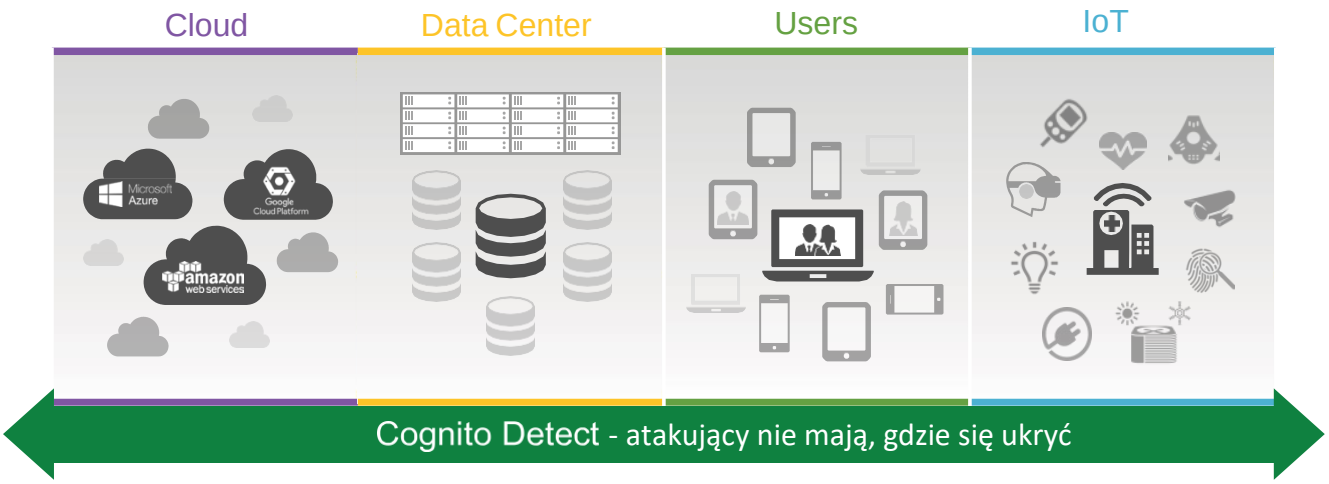
Analiza metadanych obejmuje cały ruch wewnętrzny (east-west), ruch internetowy (north-south), infrastrukturę wirtualną i zasoby chmurowe. Cognito Detect identyfikuje, śledzi i ocenia każde urządzenie korzystające z IP, wewnątrz Twojej sieci.

Widoczność obejmuje laptopy, serwery, drukarki, urządzenia BYOD i IoT, jak i systemy operacyjne i aplikacje, włączając w to ruch między wirtualnymi zasobami w data center i w chmurze, a nawet z aplikacjami SaaS.

Logi systemowe, systemów uwierzytelnienia i SaaS wzbogacają kontekst analizy metadanych by precyzyjnie identyfikować użytkowników i systemy.

Cognito Detect używa systemu opisywania zagrożeń STIX, bazującego na znanych wskaźnikach – pochodnych analizy zagrożeń. Są one skorelowane z innymi zachowaniami atakujących by zapewnić precyzyjne określenie zagrożenia dla urządzeń i stopnie pewności – pozwala to priorytetyzować ryzyko.

Zebrane metadane analizowane są przez alogrytmy behawioralne wykrywające nieuchwytnych bądź nieznanych dotąd atakujących. Eksponuje to podstawowe zachowania w sieci – narzędzia zdalnego dostępu, ukryte tunele, backdoor'y, nadużycie danych dostępu oraz wewnętrzny rekonesans.



By odkryć oznaki infekcji lub zagrożeń wewnętrznych Cognito Detect w stale uczy się Twojego lokalnego środowiska oraz śledzi aktywność wszystkich fizycznych i wirtualnych hostów. Szeroki wachlarz cyberzagrożeń jest wykrywany automatycznie, w dowolnej fazie cyklu ataku, włączając:

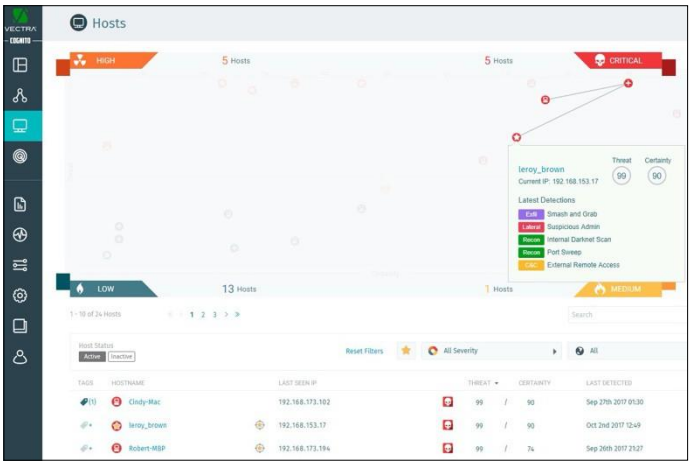
- Command-and-control i inne niewidoczne kanały komunikacji
- Rekonesans wewnętrzny
- Rozprzestrzenianie się wewnętrzne pomiędzy hostami
- Nadużycie danych logowania
- Wycieki danych
- Wczesne wskaźniki działania ransomware
- Wykorzystanie zasobów do wydobycia kryptowalut (Botnet monetization)
- Kampanie malware, włączając w to mapowanie wszystkich hostów i powiązanych z nimi wskaźników ataku

Cognito Detect monitoruje i wykrywa podejrzany dostęp do krytycznych zasobów przez upoważnionych pracowników, a także naruszenia zasad związanych z korzystaniem z pamięci w chmurze, pamięci USB i innych środków przenoszenia danych z sieci.

Zautomatyzowana analiza

Threat Certainty Index™ zawarty w Cognito Detect konsoliduje tysiące zdarzeń w infrastrukturze i historyczny kontekst, aby wskazać hosty, które stanowią największe zagrożenie.

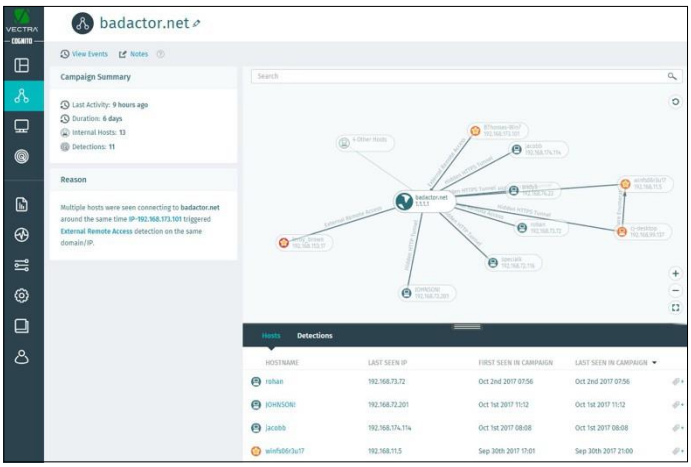
Zamiast generować więcej zdarzeń do analizy, Cognito Detect analizuje ogromne zasoby danych, aby pokazać, co najważniejsze. Wyniki oceny zagrożenia i stopnie pewności skutkują powiadomieniem zespołu bezpieczeństwa IT lub wyzwoleniem reakcji systemów bezpieczeństwa IT, SIEM czy narzędzi śledczych.



Rysunek 1. Threat Certainty Index zawarty Cognito Detect

Funkcja “Attack Campaigns” dodatkowo automatyzuje skany bezpieczeństwa, łącząc je z wzorcami zachowania atakującego i ujawnia relacje między hostami, zewnętrznymi komendami command-and-control oraz łącznością ze wspólną infrastrukturą C&C.

Gdy atakujący przeprowadzają rekonesans i przemieszczają się z hosta na hosta w sieci, Cognito Detect koreluje ich zachowania na wszystkich zaangażowanych hostach i wykrytych komputerach oraz przedstawia zsyntetyzowany widok całej kampanii ataku.



Rysunek 2. Cognito Detect prezentuje zsyntetyzowany widok całej kampanii ataku

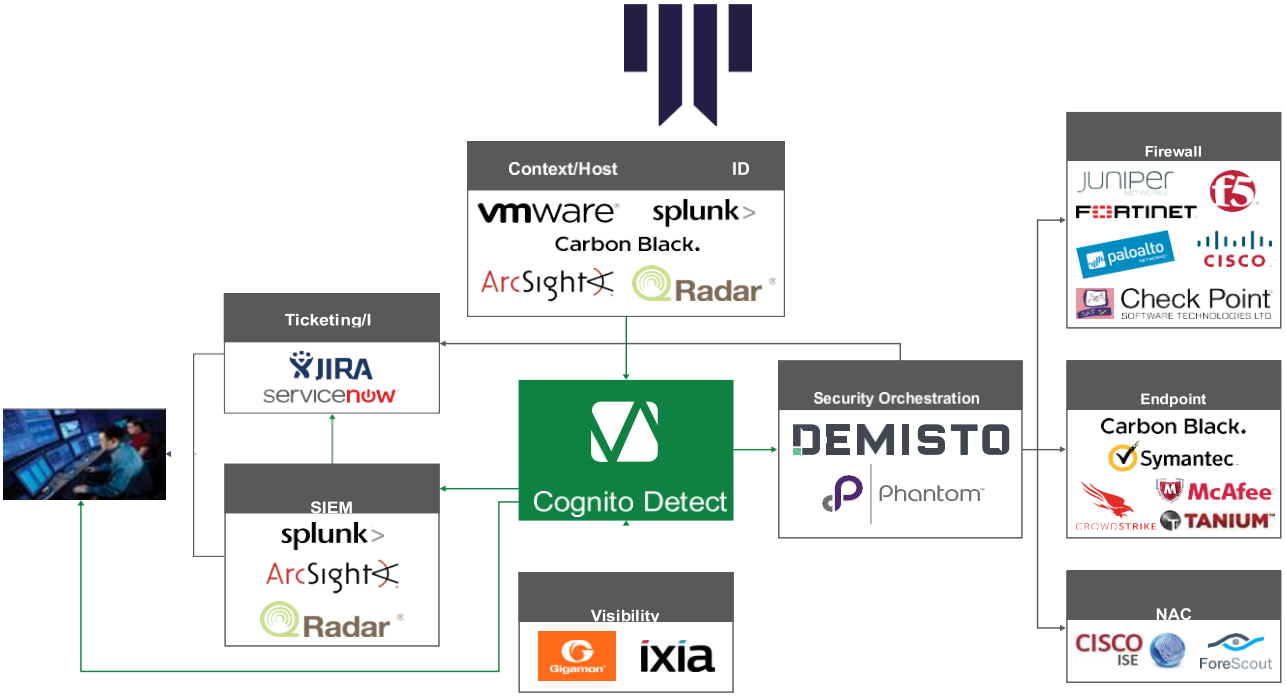
Cognito Detect samodzielnie dobiera panele interfejsu graficznego z informacjami najistotniejszymi w danym momencie, aby wskazać zaatakowane hosty lub powiązane kampanie. System analizuje historię zdarzeń przez cały okres ich życia, by lepiej zrozumieć pełny zakres ataku i poszczególne aktywności w jego trakcie.

Efektywnie zarządzaj reakcją na atak

Szybko i zdecydowanie reaguj na zagrożenia, umieszczając na pulpicie najistotniejsze informacje i kontekst. W przeciwieństwie do produktów analityki bezpieczeństwa, Cognito Detect eliminuje ręczne analizy, automatycznie ustalając priorytety i korelując zagrożenia z hostami i kluczowymi zasobami, które są celem ataku.

Cognito Detect czytelnie wskazuje szczegóły wykrywania zagrożeń - w tym kontekst hosta, przechwycone pakiety oraz oceny zagrożenia i stopnie pewności.

Ponadto Cognito Detect współpracuje z firewallami, rozwiązaniami typu EDR, NAC i innymi punktowymi systemami bezpieczeństwa, aby automatycznie blokować nieznane i targetowane cyberataki. Cognito Detect zapewnia również świetny punkt wyjścia do zaawansowanej analizy zagrożeń, co zwiększa efektywność SIEM i narzędzi analizy śledczej.



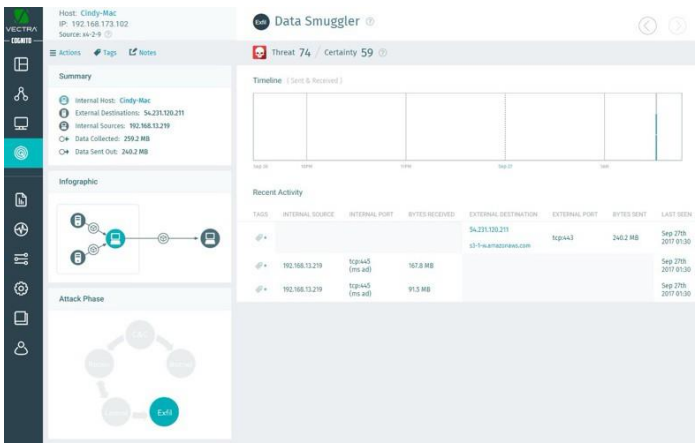
Ochrona Twojego systemu - która myśli

Oszczędność czasu przez użycie kontekstu bezpieczeństwa.

Cognito Detect odciąża i wspiera zespoły operacji bezpieczeństwa, które nierzadko zmagają się z niedoborem personelu. Jest to możliwe dzięki automatyzacji czasochłonnej analizy zdarzeń związanych z bezpieczeństwem i eliminacji potrzeby ciągłego szukania ukrytych zagrożeń.

Każda detekcja jest szczegółowo wyjaśniona i przedstawiona wraz z kontekstem historycznym, który doprowadził do wykrycia. Analitycy bezpieczeństwa mogą natychmiast wyświetlić mapę połączeń dowolnego hosta, aby zobaczyć inne hosty, z którymi urządzenie się komunikuje i sposób w jaki to robi.

Cognito Detect zapewnia również dostęp do wzbogaconych metadanych z przechwyconych pakietów w celu dalszej analizy śledczej. Zapewnia to zespołom bezpieczeństwa niezbędne dowody i dokładność, których potrzebują do podjęcia natychmiastowych, zdecydowanych działań.



Wzmocnij swoją istniejącą infrastrukturę bezpieczeństwa

Niezależnie od tego, czy chodzi o zapewnienie informacji niezbędnych do blokowania nowej klasy zagrożeń za pomocą Firewalla, zabezpieczeń typu EDR, NAC i innych systemów, czy też wyraźny punkt wyjścia do bardziej szczegółowego wyszukiwania za pomocą SIEM i narzędzi śledczych, Cognito Detect zapewnia większą efektywność wykorzystania istniejących technologii bezpieczeństwa.

Cognito Detect integruje się z wiodącymi rozwiązaniami bezpieczeństwa urządzeń końcowych, aby automatycznie dodawać wzbogacony kontekst do dochodzeń i umożliwia zespołom operacji bezpieczeństwa izolowanie zagrożonych zasobów.

Cognito Detect

Rozbudowany interfejs API umożliwia automatyczną reakcję i egzekwowanie polityk we współpracy z praktycznie każdym rozwiązaniem bezpieczeństwa. Cognito Detect generuje również komunikaty syslog i zdarzenia w formacie CEF dla wszystkich wykrytych zdarzeń, a także wyniki bezpieczeństwa hostów według priorytetu. To sprawia, że Cognito Detect jest czymś więcej niż tylko kolejnym źródłem logów i stanowi idealny punkt wyjścia dla dochodzeń i pracy analitycznej w systemie SIEM.

Wykrywanie ransomware na każdym etapie cyklu życia

Cognito Detect identyfikuje kampanie typu ransomware na wszystkich etapach ataku. Monitorując cały wewnętrzny ruch sieciowy, Cognito Detect w kilka sekund identyfikuje podstawowe zachowania ataku ransomware, ujawnia prekursory oprogramowania ransomware, w tym ruch typu command-and-control, skanowanie sieci i techniki rozprzestrzeniania, których ransomware używa do wyszukiwania i szyfrowania krytycznych zasobów.

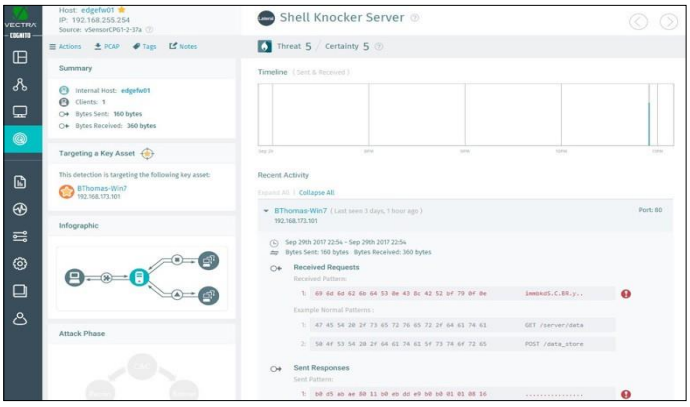
Obserwuj obserwujących

Podczas gdy osoby atakujące mogą początkowo narazić na szwank urządzenie końcowe, prawdziwym celem są dane uwierzytelniające administratora lub systemu. Cognito Detect wykracza poza proste monitorowanie zachowań użytkowników w celu wykrycia oznak naruszenia bezpieczeństwa administratorów.

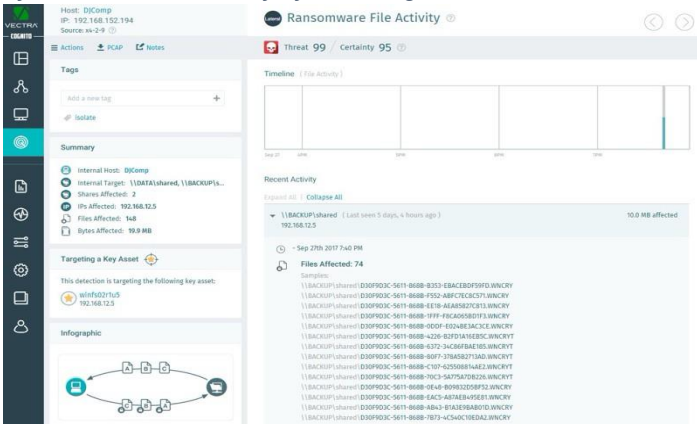
Cognito Detect śledzi protokoły administracyjne i uczy się zachowania określonych maszyn lub systemów używanych do zarządzania określonymi hostami, serwerami i zasobami. W ten sposób szybko ujawnia, kiedy cyberprzestępca próbuje użyć poświadczeń administracyjnych i protokołów w celu eskalacji ataku w sieci.

Natywna ochrona Twojej chmury prywatnej

Centrum danych w chmurze prywatnej jest dziś sercem i duszą wielu organizacji, ale często pozostaje niewidocznym punktem dla zespołów bezpieczeństwa. Cognito Detect stale monitoruje krytyczne aplikacje, dane i infrastrukturę centrów danych z możliwością wykrywania nawet najbardziej wyrafinowanych ataków.



Rysunek 3. Mechanizm wykrywania Cognito Detect Shell-Knocker



Rysunek 4. Cognito Detect wykrywanie ataków ransomware

Około 80% ruchu w centrum danych nigdy nie opuszcza centrum danych i nie jest monitorowane przez tradycyjne zabezpieczenia działające na perymetrze. Wirtualne czujniki Cognito Detect (vSensors) łączą się z każdym przełącznikiem VMware vSwitch, aby zapewnić widoczność całego ruchu i wykryć zagrożenia przechodzące między obciążeniami w środowisku wirtualnym.

Cognito Detect integruje się również z VMware vCenter, aby zapewnić wiarygodny, zawsze aktualny widok środowiska wirtualnego. W istocie rzeczy firma Vectra jako pierwsza połączyła widoczność, kontekst i inteligencję, aby wykrywać zaawansowane ataki w centrum danych.

Bezpieczeństwo od sprzętu po aplikację

Bezpieczeństwo centrum danych wykracza poza wirtualizację i obejmuje sprzęt fizyczny serwera oraz narzędzia używane do zarządzania centrum danych. Cognito Detect zapewnia wykrywanie zagrożeń, które rozciąga się od warstwy aplikacji aż po sprzęt.

Na przykład - Cognito Detect Port Knocking ujawnia serwery zagrożone przez rootkit, który może znajdować się w warstwie poniżej samego systemu operacyjnego. Ponadto Cognito Detect monitoruje i wykrywa niewłaściwe stosowanie protokołów zarządzania niskiego poziomu, takich jak IPMI i iDRAC.

Protokoły te są zwykle wykorzystywane przez administratorów do zarządzania sprzętem serwerowym. Protokoły te są coraz częściej atakowane, ponieważ zapewniają zawsze aktywne wejście do środowiska wirtualnego, ale nie są rejestrowane i rzadko są monitorowane przez zabezpieczenia.

Ujednolicenie operacji centrum danych

Nowoczesne centra danych wymagają stałej koordynacji między pracownikami działu sieci, programistami aplikacji, zespołami wirtualizacji i oczywiście zespołem ds. bezpieczeństwa. Cognito Detect ułatwia synchronizację wszystkich grup i zapewnia pełny wgląd w środowisko wirtualne, nawet gdy obciążenia są w ciągłym ruchu.

Cognito Detect wizualizuje połączenia między wszystkimi zasobami i rodzaj ruchu pomiędzy nimi. Dzięki pełnej integracji VMware vCenter, Cognito Detect zapewnia zawsze aktualny widok środowiska i ostrzega o wszelkich zasobach, które nie są monitorowane pod kątem zagrożeń.

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