Attivo NETWORKS®

PRZEGLĄD ROZWIĄZAŃ TYPU DECEPTION

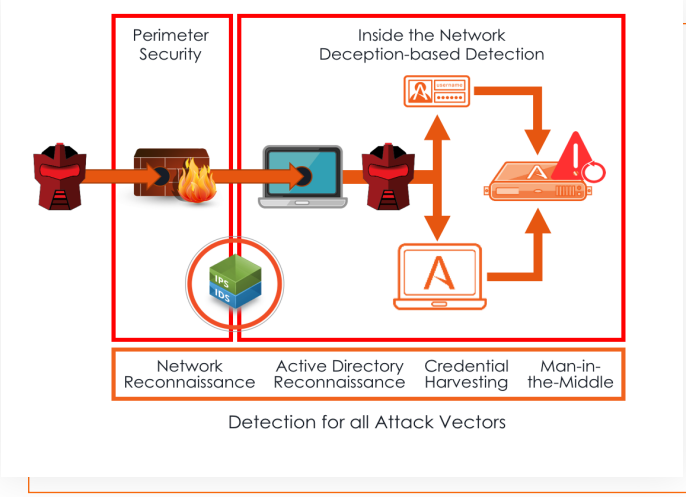
WPROWADZENIE

Ataki cybernetyczne odbywają się w niesłabnącym tempie, ponieważ hakerzy znajdują coraz bardziej wysublimowane sposoby pozwalające na ominięcie firmowych systemów bezpieczeństwa. W przypadku każdego naruszenia specjaliści ds. bezpieczeństwa stają w obliczu rosnącej presji, aby jak najszybciej wykryć i powstrzymać zagrożenia, zanim napastnik wyrządzi realne szkody organizacji. Ponadto, zgodnie z oczekiwaniami dotyczącymi zapewniania zgodności z unormowaniami formalnymi, wprowadzane są nowe przepisy wymuszające powiadamianie o naruszeniach wraz z nieuchronnymi sankcjami finansowymi grożącymi jednostkom niewywiązującym się z obowiązku informowania odpowiednich organów. Organizacje różnej wielkości i z różnych branż poszukują więc innowacyjnych rozwiązań zwiększających poziom bezpieczeństwa poprzez wypełnienie luki w aktywnym wykrywaniu zagrożeń i ataków, dzięki czemu możliwe jest lepsze zrozumienie metodologii destrukcyjnych działań napastników a przez to znacznie efektywniejsze ich eliminowanie.

Co więcej, organizacje migrują obecnie swoje strategie bezpieczeństwa z koncepcji bazujących na obronie reaktywnej do wariantu proaktywnego, który nie opiera się wyłącznie na działaniach będących wynikiem następstw ataku, lecz wykorzystuje zrównoważone inwestycje w narzędzia wczesnego wykrywania zagrożeń.

TECHNOLOGIA DECEPTION

Technologia deception dostarcza innowacji niezbędnych do przeprowadzenia wspomnianej transformacji systemów cyberbezpieczeństwa w kierunku aktywnej obrony. Wdrażając systemy oszukujące napastników w całej infrastrukturze IT firmy są w stanie nie tylko utrudnić i spowolnić działania hackerów, ale przede wszystkim skutecznie wykryć każde zagrożenie oraz poszczególne fazy aktywnych ataków.



Wykorzystując wabiki i przynęty o konfiguracji łudząco przypominającej rzeczywiste stacje robocze, serwery i inne urządzenia teleinformatyczne, zwodzimy atakujących, zmuszając ich do ujawnienia swojej obecności, równocześnie identyfikując w ten sposób również luki w wykrywaniu zagrożeń przez inne podsystemy bezpieczeństwa organizacji.

Wczesne wykrywanie naruszeń bezpieczeństwa oraz dostarczanie hackerom fałszywych, potencjalnie wartościowych z ich punkty widzenia danych, daje użytkownikom systemów klasy Deception bezcenny czas na skuteczne działania prewencyjne, zapewniając równocześnie pełną kontrolę i monitoring aktywności napastników. To czyni z technologii Deception ważne ogniwo kompleksowego łańcucha współdziałających ze sobą narzędzi bezpieczeństwa.

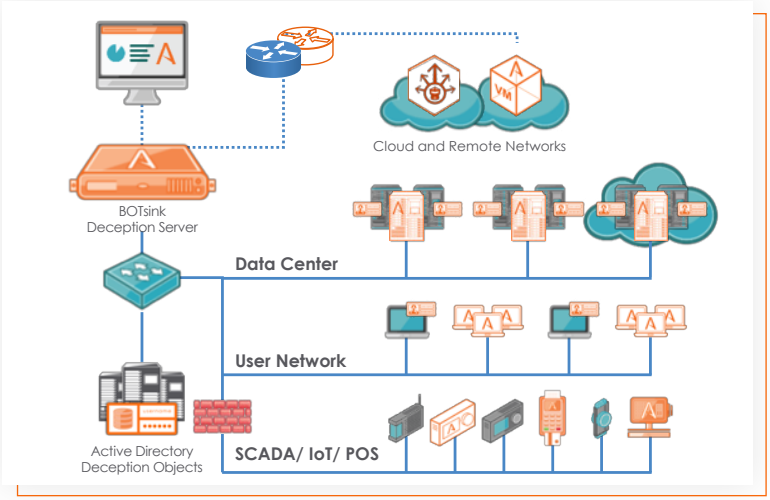
Organizacje na całym świecie, niezależnie od stopnia zaawansowania wykorzystywanych systemów cyberbezpieczeństwa, coraz intensywniej wykorzystują technologie Deception w celu ograniczenia ryzyka związanego z kradzieżą poświadczeń użytkowników, infiltracją cennych zasobów firmowych, atakami typu ransomware, jak również atakami zaburzającymi dostępność kluczowych usług biznesowych. Skuteczność i łatwość praktycznego wykorzystania technologii Deception są głównymi czynnikami powodującymi wzrost zainteresowania, ułatwiającymi podjęcie decyzji o testach praktycznych, a finalnie o zakupie i wdrożeniu tego typu rozwiązania.

W 2018 roku analitycy docenili technologię Deception za jej skuteczność w wykrywaniu zaawansowanych zagrożeń, a firma Gartner Inc., trzeci rok z rzędu zaleciła tę właśnie technologię jako strategiczny priorytet bezpieczeństwa. Potwierdzeniem zasadności takich wytycznych Gartnera, są niewątpliwie wyniki badań rynkowych, w których wiele organizacji wyraziło ogromne zainteresowanie wykorzystaniem rozwiązań Deception do zoptymalizowania firmowych mechanizmów kontroli bezpieczeństwa.

ROZWIĄZANIE ATTIVO NETWORKS

Platforma ThreatDefend® Deception and Response została zaprojektowana w taki sposób, aby zamienić całą infrastrukturę teleinformatyczną w pułapkę. Rozwiązanie to łączy w sobie przynęty i wabiki wymagające dużej interakcji z siecią i punktami końcowymi, zaprojektowane w celu zapewnienia wczesnego wglądu w zagrożenia sieciowe, wydajnego oraz ciągłego zarządzania zagrożeniami i przyspieszonej reakcji na incydenty.

Uznana za najbardziej kompleksowe rozwiązanie w branży, platforma ThreatDefend oferuje predefiniowane wabiki, gotowe do umieszczenia zarówno w chmurze, jak i w sieci lokalnej. Są one dostępne w wielu postaciach: np.: jako stacje końcowe, serwery aplikacji, bazy danych, urządzenia sieciowe, urządzenia IoT, systemy przemysłowe SCADA, a nawet terminale POS. Dzięki takiemu zróżnicowaniu są one wysoce skuteczne w wykrywaniu zagrożeń z praktycznie wszystkich wektorów, takich jak m.in.: zaawansowane, trwałe zagrożenia, skradzione poświadczenia Active Directory, ataki typu Man-in-the-Middle, czy ransomware i wiele innych.



Platforma ThreatDefend® Deception to modułowe rozwiązanie składające się m.in. z:

- serwera **Attivo BOTsink®** - wabiki oraz pułapki wraz z niezbędną infrastrukturą zarządzania i raportowania,
- **ThreatStrike®** - automatyczne tworzenie pakietów fikcyjnych zestawów poświadczeń użytkowników, udziałów sieciowych, czy też stacji i serwerów,
- **ThreatPath®** wizualizacja potencjalnych ścieżek ataku przy wykorzystaniu poświadczeń użytkowników, dostępnych w środowisku produkcyjnym,
- **ThreatDirect®** - funkcjonalność zwiększająca skalowalność całej platformy – dzięki niej w łatwy sposób jako wabik możemy wykorzystać dowolną stację końcową/serwer znajdujący się nawet w odległej zdalnej placówce firmowej,
- **ThreatOps®** - zaawansowane playbook'i do zautomatyzowanego reagowania na wykryte incydenty,
- **Attivo Central Manager** ACM pozwala na zarządzanie wieloma serwerami BOTsink w dużych firmach o złożonej strukturze organizacyjnej.

PODSTĘP W CELU WYKRYCIA I KONTROLI ŚCIEŻKI ATAKU

Platforma Attivo ThreatDefend Deception and Response pozwala na łatwą identyfikację zagrożeń występujących w infrastrukturze organizacji, w tym na analizę tzw. z ruchów lateralnych wykonywanych przez napastników oraz wykrywanie poszczególnych faz ataków. Jest to możliwe dzięki dostępności specjalnych wabików i przynęt, gotowych do rozmieszczenia w krytycznych punktach środowiska produkcyjnego. Ich głównym zadaniem jest zmylenie hackerów poprzez upodobnienie się do realnych elementów infrastruktury IT w zakresie nie tylko nazwy i konfiguracji sprzętowo-aplikacyjnej, ale także poświadczeń użytkowników oraz dokumentów i danych. Dzięki wbudowanym funkcjonalnościom każdy wabik potrafi już na wstępnym etapie infiltracji wykryć intruza i natychmiast zaalarmować główny serwer BOTsink. Daje to niezbędny czas na skuteczną reakcję zespołom bezpieczeństwa, angażując przestępcę w infiltrację spreparowanych, fikcyjnych zasobów.

Przynęty i wabiki są tak skonfigurowane, aby jak najwierniej imitować prawdziwe systemy i urządzenia. Platforma Attivo oferuje zestaw gotowych do wykorzystania maszyn wabiących, jak również możliwość przygotowania własnej wersji środowiska, począwszy od systemu operacyjnego, poprzez zainstalowanie aplikacje, a skończywszy na zestawach poświadczeń użytkowników. Całość jest wspierana przez algorytmy uczenia maszynowego, które w sposób zautomatyzowany adaptują konfigurację pułapek do bieżących zmian środowiska produkcyjnego. Wszystko to pozwala to skutecznie przyciągnąć uwagę napastników, a w konsekwencji w czasie rzeczywistym wykrywać naruszenia bezpieczeństwa, generować alerty i monitorować aktywność hackerów.

Aby zwiększyć autentyczność systemów-wabików a zarazem umożliwić pełniejszy wgląd w aktywność intruzów, rozwiązanie Attivo wzbogacone jest o dedykowaną funkcjonalność ochrony usług katalogowych Active Directory. Obejmuje ona nie tylko możliwość dodawania fikcyjnych kont do produkcyjnego serwera AD, ale także pozwala na stworzenie kompletnego, wirtualnego środowiska imitującego rzeczywistą domenę z usługami katalogowymi, połączonego jednokierunkową relacją zaufania z serwerem produkcyjnym. W zakresie ochrony stacji końcowych Attivo pozwala m. in. na efektywną ochronę przed atakami typu ransomeware, angażując złośliwe oprogramowanie do szyfrowania fikcyjnych danych, spowalniając dodatkowo szybkość komunikacji z udziałami sieciowymi oraz generując nieskończoną liczbę plików do zaszyfrowania. Daje to czas niezbędny na wyizolowanie zainfekowanej stacji i zabezpiecza cenne produkcyjne dane i zasoby.

Platforma Attivo ThreatDefend jest również dostępna dla środowisk chmurowych pochodzących od najbardziej popularnych dostawców, tj.: AWS, Azure, Google i Oracle. Wsparcie w tym zakresie obejmuje dedykowane wabiki i przynęty do kontenerów, modele bezserwerowe i współdzielone zabezpieczenia w chmurze. Możliwości platformy ThreatDefend obejmują także obsługę funkcji AWS Lambda, kluczy dostępu, rekonesansu, zbierania danych uwierzytelniających jako środka do weryfikacji skuteczności kontroli bezpieczeństwa wraz z monitorowaniem CloudWatch / SIEM w celu znalezienia prób użycia fałszywych danych uwierzytelniających.

W celu proaktywnego zapobiegania zagrożeniom i redukcji zasięgu ataków funkcjonalność ThreatPath umożliwia graficzną analizę potencjalnych ścieżek ruchów lateralnych, które osoba atakująca może wykorzystać przez źle skonfigurowane systemy operacyjne z zapisanymi poświadczeniami użytkowników.

PODSTĘP DLA AKTYWNEJ OBRONY I PRZYSPIESZONEJ REAKCJI NA INCYDENTY

Oprócz wczesnego wykrywania atakujących i samych ataków, platformie ThreatDefend oferuje użytkownikom również szczegółowe alerty, automatyczne analizy i szeroki wachlarz możliwości integracji z systemami firm trzecich w celu automatycznej obsługi incydentów. Wszystko po to, aby radykalnie skrócić czas od wykrycia zdarzenia do skutecznego zablokowania intruza. Kiedy tylko napastnik wchodzi w interakcję z wabikiem bądź fikcyjnymi poświadczeniami usługi ThreatStrike, serwer BOTsink rejestruje taką czynność i natychmiastowo alarmuje dział bezpieczeństwa, jednocześnie odpowiadając atakującemu fałszywymi danymi. Wszelkie dane związane z atakami i aktywnością hackerów są dostępne w skonsolidowanym w panelu użytkownika, który udostępnia wszelkie informacje niezbędne do analizy poincydentalnej, koreluje zdarzenia i generuje alerty dotyczące złośliwej aktywności.

Alerty pojawiają się tylko w przypadku potwierdzonych interakcji atakującego z wabikami i w przeciwieństwie do innych metod wykrywania, nie są zależne od sygnatur ani analizy behawioralnej. Alerty są poparte analizą ataków, która może być wykorzystana do zautomatyzowanego blokowania atakującego, odizolowania zainfekowanego systemu i poszukiwania innych zagrożeń, tak aby organizacja mogła całkowicie wyeliminować zagrożenie z sieci. Eliminacja fałszywych alarmów i precyzyjne alerty pozwalają zaoszczędzić cenne godziny dla zespołów bezpieczeństwa.

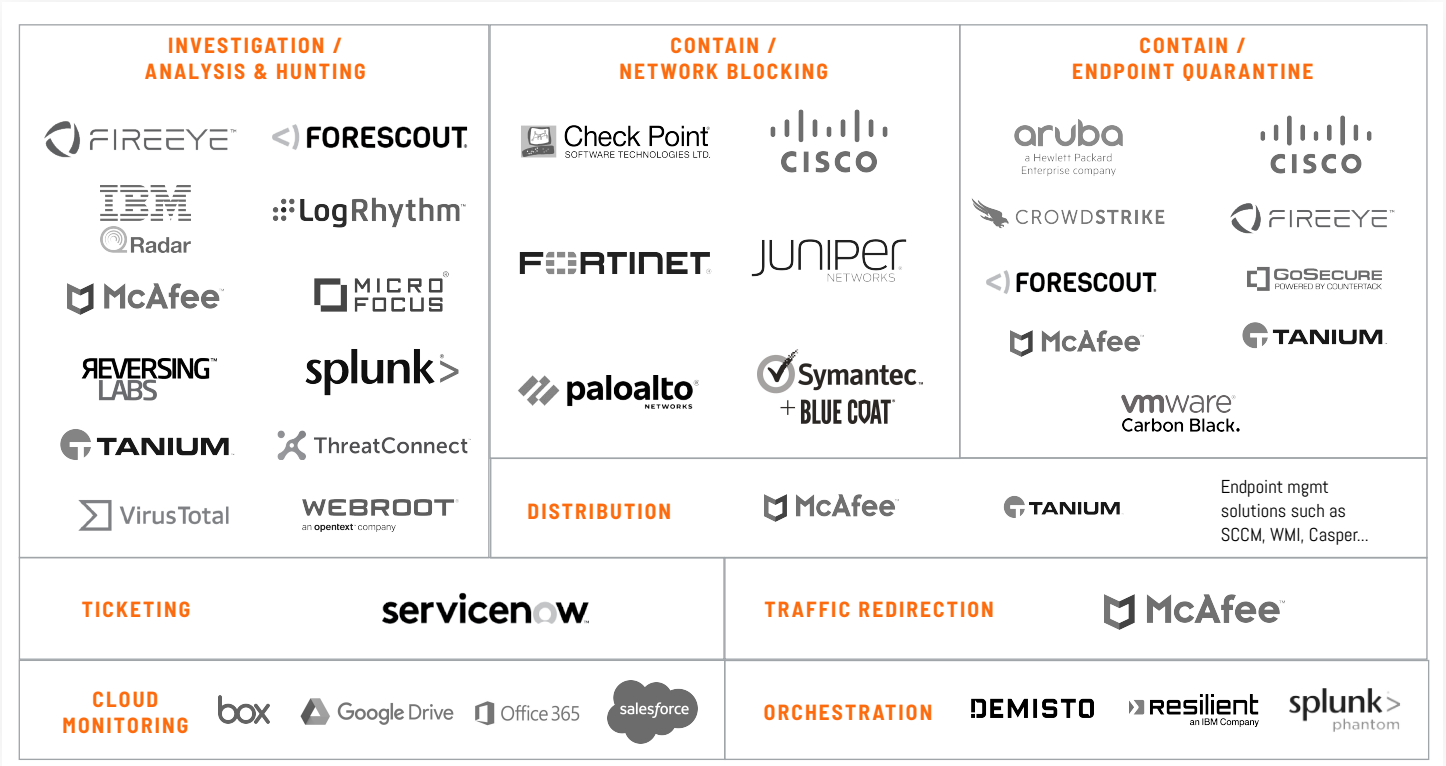
Raporty dostępne w platformie Attivo obejmują identyfikację zainfekowanych systemów i adresów C&C i są tworzone w zgodności ze standardami IOC, PCAP i STIX, aby umożliwić łatwe udostępnianie informacji i rejestrowanie ataków. Dzięki korelowaniu wszystkich istotnych informacji ze zdarzenia w jednym interfejsie, pulpit informacyjny zapewnia analitykom i zespołom reagowania na incydenty syntetyczny wgląd w najistotniejsze dane związane z atakiem, co pozwala skutecznie powstrzymać intruza i zaradzić potencjalnym stratom.

Wprowadzanie w błąd przestępców to ofensywna forma zakłócenia zdolności atakującego do gromadzenia cennych informacji pochodzących z systemów produkcyjnych. Takie podejście zapewnia również funkcje obronne, ponieważ odwraca ataki od kluczowych aktywów firmowych. Attivo oferuje dodatkowo tzw. dokumenty-pułapki (ang. Decoy Docs), umożliwiając śledzenie skradzionych dokumentów w sieci lub poza nią.

Organizacje mogą również skorzystać z funkcjonalności ThreatOps do automatyzacji obsługi incydentów i tworzenia powtarzalnych scenariuszy reagowania na incydenty. Taką aranżację zagrożeń można w pełni dostosować do środowiska i obowiązujących polityk, dzięki czemu można szybciej i pewniej podejmować decyzje dotyczące reakcji na incydenty.

AKTYWNI PARTNERZY

Wbudowane integracje do udostępniania informacji i automatycznej odpowiedzi na zagrożenia



PLATFORMA THREATDEFEND DECEPTION AND RESPONSE OFERUJE KLIENTOM:

- Wczesne wykrywanie zagrożeń w sieci dla dowolnego wektora zagrożeń
- Analizę ryzyka oraz potencjalnych ścieżek ataku w celu minimalizacji jego docelowego zasięgu
- Łatwe wdrożenie i niskie koszty utrzymania
- Kompleksowe rozwiązanie skalowalne we wszystkich środowiskach
- Wiarygodne alerty, szczegółowe analizy i raporty poincydentalne
- Natywne integracje partnerów technologicznych, które przyspieszają reakcję na incydenty

O ATTIVO NETWORKS

Attivo Networks®, lider w technologii deception, zapewnia aktywną ochronę w celu wczesnego wykrywania, analizy kryminalistycznej i automatycznej reakcji na incydenty związane z atakami w sieci. Platforma Attivo ThreatDefend® Deception oferuje wszechstronne i dokładne wykrywanie zagrożeń dla sieci użytkowników, centrów danych, chmur i szerokiej gamy wyspecjalizowanych powierzchni ataku. Zwodnicza struktura sieci, punktów końcowych, aplikacji i oszustw danych skutecznie przekierowuje i ujawnia ataki ze wszystkich wektorów zagrożeń. Zaawansowane uczenie maszynowe upraszcza wdrażanie i operacje w organizacjach każdej wielkości. Zautomatyzowana analiza ataków, analiza śledcza, przydatne alerty i natywne integracje przyspieszają i usprawniają reakcję na incydenty. Firma zdobyła ponad 125 nagród za innowacje technologiczne i przywództwo.

SKONTAKTUJ SIĘ Z NAMI

Bakotech Sp. z o.o.

Strona: www.bakotech.pl
E-mail: kontakt@bakotech.com
Telefon: +48 12 376 95 08
Adres: Ul. Drukarska 18/5
30-348 Kraków