STINET

VECTRA COGNITO

- DETEKCJA ZAGROŻEŃ
- OSZCZĘDNOŚĆ CZASU
- SZYBKA REAKCJA

VECTRA
Security that thinks®

VECTRA COGNITO – NAJSZYBSZY I NAJSKUTECZNIEJSZY SPOSÓB NA ZNALEZIENIE I ZATRZYMANIE ATAKU W SIECI W CZASIE RZECZYWISTYM

Przedstawiamy **Vectra Cognito,** która dzięki wykorzystaniu sztucznej inteligencji, wykrywa atak w czasie rzeczywistym, przedstawia szczegóły i umożliwia 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 100% ruchu sieciowego na poziomie metadanych, poprzez SPAN port lub TAP 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.

DOŁĄCZ DO GRONA ZADOWOLONYCH KLIENTÓW, KTÓRZY WYMIENIAJĄ KORZYŚCI Z ULEPSZEŃ W ZAKRESIE BEZPIECZEŃSTWA DZIĘKI WYKRYWANIU ZAGROŻEŃ I USTALANIU PRIORYTETÓW W OPARCIU O SZTUCZNĄ INTELIGENCJĘ (AI).

GŁÓWNE 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 (np. Office 365)
- 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

GŁÓWNE KORZYŚCI

- Brak konieczności ręcznej i czasochłonnej analizy zdarzeń bezpieczeństwa
- Automatyczne nadawanie priorytetów wykrytym zdarzeniom
- Konsolidacja setek zdarzeń połączona z historycznym kontekstem w celu wskazania hosta, który stanowi największe zagrożenie
- Szybkość reakcji w celu zatrzymania trwających ataków oraz złagodzenia potencjalnych zagrożeń
- Oszczędność czasu oraz odciążenie zasobów osobowych dzięki pełnej automatyzacji procesów oraz łatwość obsługi połączonej z niskim poziomem hałasu
- Wysoka skuteczność potwierdzona przeprowadzonymi testami z użyciem Red Team
- Obejmuje 55 z 60 (92%) technik sieciowych zidentyfikowanych w modelu MITTRE ATT&CK
- Pełna zgodność z RODO dzięki badaniu zawartości ruchu tylko na poziomie metadanych wzbogaconych o kontekst bezpieczeństwa – bez konieczności głębokiej inspekcji wewnątrz przesyłanych pakietów

Solec 18 lok.U61,
00-410 Warszawa

+48 22 740 42 20

biuro@stinet.pl

STINET

Ponad 4,5:1 – stosunek wymiernych korzyści do kosztów inwestycji

5 miesięcy do zwrotu z inwestycji

63% mniejsze ryzyko wystąpienia poważnego incydentu cybernetycznego

3x więcej proaktywnie zidentyfikowanych zagrożeń związanych z bezpieczeństwem

85% skuteczniejsze identyfikowanie realnych zagrożeń w czasie rzeczywistym

2x wyższa produktywność, wpływająca na członków zespołów ds. bezpieczeństwa

Solec 18 lok.U61,
00-410 Warszawa

+48 22 740 42 20

biuro@stinet.pl

www.stinet.pl