AUTOFOCUS

Wzmocnij swoją ochronę przed zagrożeniami.

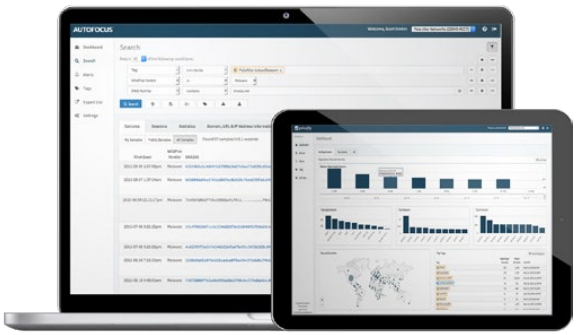
Usługa AutoFocus dostarczana przez Palo Alto Networks przyspiesza analizę zagrożeń i wykrywanie najbardziej szkodliwych, unikalnych i ukierunkowanych ataków. Rozwiązania te rozszerzają platformę zabezpieczeń Palo Alto Networks o pełen podgląd i kontekst, wymagany do szybszej reakcji na ataki, bez konieczności angażowania dodatkowych zasobów w działach odpowiedzialnych za zabezpieczenia.

Wzmocnij swoją ochronę przed zagrożeniami.

- **Przyspieszenie analizy zagrożeń, ich wykrywania oraz skrócenie czasu odpowiedzi poprzez priorytetyzację alertów o najbardziej krytycznych zdarzeniach**
- **Uzyskiwanie kontekstowej informacji odnośnie ataków, zagrożeń oraz prowadzonych działań, również w branżach szczególnie często atakowanych przez cyberprzestępców**
- **Rozbudowa platformy bezpieczeństwa Palo Alto Networks o kontekstową informację o zagrożeniach, jako część systemów PAN-OS oraz Panorama, włącznie z dostępnością otwartego API pozwalającego na integrację z systemami zabezpieczeń dostarczanymi przez firmy trzecie**

Rozbudowa platformy Palo Alto Networks

Cyberataki przebiegają w coraz bardziej zautomatyzowany sposób, a ich ilość i poziom wyrafinowania są obecnie większe, niż kiedykolwiek wcześniej. Przepracowany personel odpowiedzialny za bezpieczeństwo nie jest w stanie skutecznie zająć się każdym zagrożeniem, co pozostawia wąski przedział czasowy na sprawdzanie wysoko zaawansowanych ataków. Unikalna platforma zabezpieczeń Palo Alto Networks® zapewnia nowy sposób działania, począwszy od podejścia ukierunkowanego na zapobieganie zagrożeniom, po przekazanie kontroli nad automatyzacją zabezpieczeń w ręce odpowiednich pracowników.



Ponieważ cała platforma uniemożliwia działanie większości zagrożeń, personel odpowiedzialny za bezpieczeństwo może skoncentrować swoje zasoby na tropieniu specyficznych, dobrze ukierunkowanych ataków, korzystając z narzędzia AutoFocus™. Usługa ta rozbudowuje platformę zabezpieczeń o możliwość korzystania z globalnych mechanizmów wykrywania zagrożeń oraz zapewnia kontekstową informację o atakach, co pozwala na przyspieszenie analizy i udaremnienia działania złośliwego kodu. Korzystająca również z mechanizmu AutoFocus platforma daje możliwość przejścia od tradycyjnego reagowania na rosnącą liczbę alertów i łagodzenia skutków ataków, do zapobiegania możliwości wystąpienia naruszenia bezpieczeństwa i aktywnego wykrywania zagrożeń.

Priorytetyzacja alertów

AutoFocus pozwala wyróżnić spośród zdarzających się codziennie prób naruszenia bezpieczeństwa najważniejsze zagrożenia, dokonując – poprzez mechanizm tagów – kontekstowej kwalifikacji zdarzeń w sieci. Unikalne dla AutoFocus tagi pozwalają na identyfikację, z jakiego rodzaju szkodliwym kodem, atakami, zagrożeniami, niepożądanymi zachowaniami lub exploitami ma się do czynienia. W sytuacji, w której tag jest zgodny ze zdarzeniem w danej sieci, alert wysyłany jest pocztą elektroniczną, publikowany na tablicy zarządzania AutoFocus lub wyświetlany na witrynie www, wraz z pełną informacją o kontekście wystąpienia danego zdarzenia. Możliwa

jest pełna konfiguracja alertów, co tym samym pozwala na zwiększenie skuteczności działania, poprzez odpowiednie ustawienia priorytetów i informacji o kontekście najbardziej krytycznych zagrożeń.

Tagi

Tagi zwiększają przejrzystość podczas wyświetlania informacji o najbardziej krytycznych zagrożeniach, kompleksowo przedstawiając wykryty szkodliwy kod, podjęte przezeń działania, złośliwe oprogramowanie i zachowania oraz wykorzystane exploity. Mogą być one tworzone w systemie AutoFocus na podstawie dowolnej aktywności danego hosta, uruchamiając alarm w sytuacji, w której specyficzny rodzaj aktywności został zaobserwowany wewnątrz sieci danej organizacji. Poza priorytetyzacją alertów możliwe jest również pełne ich przeszukiwanie pod kątem określonych tagów, co pozwala na skuteczne i szybkie identyfikowanie podejrzanych próbek lub wskaźników.

Po identyfikacji nowego zagrożenia, Unit 42 (dział badawczy Palo Alto Networks), Twoja firma oraz globalna społeczność korzystająca z AutoFocus dodaje właściwe tagi do wykrytej podejrzanej aktywności. Tagi dostarczają informacji o:

- Rodzinie złośliwego kodu
- Rodzaju ataku
- Głównych wykonawcach złośliwego kodu
- Podejrzanych zachowaniach
- Exploitach

Unit 42 – dział analizy zagrożeń

Unit 42 to dział Palo Alto Networks zajmujący się badaniem i analizą zagrożeń, w którym pracują branżowi eksperci od zabezpieczeń. Unit 42 gromadzi, bada i analizuje nowe zagrożenia, zapewniając wgląd w najnowsze działania mające na celu naruszenie bezpieczeństwa oraz dzielenie się informacjami zarówno z klientami firmy Palo Alto Networks, jak i społecznością zainteresowaną tymi zagadnieniami. Unit 42 dodaje ekspercką wiedzę do automatycznych mechanizmów AutoFocus poprzez tagowanie zagrożeń oparte na własnych badaniach, a także dostępnych na zasadach open source informacjach od społeczności, co pozwala na uzyskanie kontekstowej informacji oraz priorytetyzacji i identyfikacji zagrożeń, znacząco podnosząc świadomość personelu odpowiedzialnego za zabezpieczenia.

AutoFocus jest podstawowym narzędziem analitycznym wykorzystywanym w dziale Unit 42 do identyfikacji nowych zagrożeń, korelacji globalnie zbieranych danych, identyfikacji połączeń między próbkami złośliwego kodu i budowy bazy wiedzy o złośliwym kodzie. Sprawdź informacje o najnowszych zagrożeniach zebranych przez Unit 42 z wykorzystaniem mechanizmu AutoFocus.

Rozbudowa platformy zabezpieczeń o inteligentne wykrywanie zagrożeń

AutoFocus pozwala działom IT na przejście od personelu polegającego na małej grupie specjalistów, do grupy korzystającej z doświadczeń szerokiego grona osób zajmujących się bezpieczeństwem. Zagrożenia rozpoznane przez tę usługę są natychmiast dostępne na platformach Palo Alto Networks, włącznie z rozwiązaniami PAN-OS® oraz Panorama™. AutoFocus przyspiesza czas reakcji personelu odpowiedzialnego za zagadnienia bezpieczeństwa, pozwalając na szczegółową inspekcję podejrzanej aktywności, bez konieczności angażowania specjalistycznych zasobów. W przypadkach, w których wymagana jest dodatkowa analiza, użytkownicy mogą przełączać się między systemami AutoFocus, PAN-OS lub Panorama, jednocześnie wysyłając zapytania do wszystkich tych systemów.

Korzystając z platformy rozbudowanej o system AutoFocus, użytkownicy mogą uzyskać odpowiedzi dotyczące następujących zagadnień:

- W jaki sposób zagrożenia lub ukierunkowane ataki widoczne są w danej sieci.
- Dalszej analizy próbek podejrzanego kodu.
- Historii rozwiązywania nazw domenowych w celu identyfikacji podejrzanych zapytań do serwerów DNS.

Wyszukiwanie

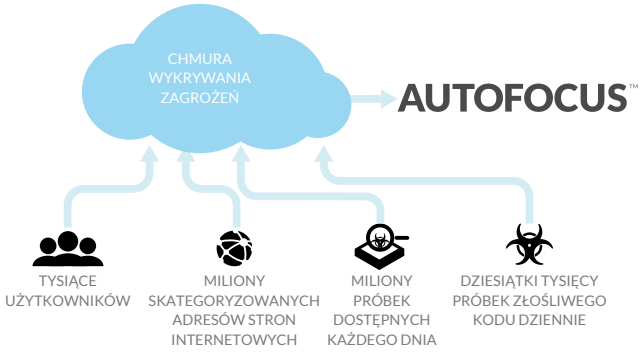
Reakcje na unikalne, specyficznie ukierunkowane ataki często wymagają analizy wykonywanej przez człowieka. Dla skutecznej odpowiedzi na mający miejsce atak, krytyczna jest szybka analiza oraz korelacja zebranych danych. System AutoFocus pozwala na zbudowanie zaawansowanego, wielowarstwowego wyszukiwania wewnątrz danej sieci i precyzowania zapytań filtrami dotyczącymi danej organizacji, czasu i innymi, co pozwala wychwycić podczas analizy połączenia między różnymi atakami. AutoFocus udostępnia na wyciągnięcie ręki całą wiedzę Palo Alto Networks dotyczącą zagrożeń, znacznie skracając czas potrzebny na przeprowadzenie analizy, inspekcji zebranych danych i powstrzymania zagrożeń.

Silnik oparty o analizę statystyczną

Podczas analizy zagrożeń personel odpowiedzialny za bezpieczeństwo musi szybko zidentyfikować wskaźniki naruszeń (IOC), które mogą dać najlepsze rezultaty podczas dalszego ich badania. Każdy plik to potencjalnie setki lub tysiące zmiennych, z których tylko część można powiązać z unikalnymi wskaźnikami naruszeń występującymi w szerokim spektrum ataków. AutoFocus wykorzystuje innowacyjny mechanizm analizy statystycznej, dokonujący korelacji miliardów zmiennych zbieranych globalnie i udostępniający zestaw wskaźników naruszeń (IOC), które można powiązać z konkretnymi metodami ataku. Usługa ta automatycznie aplikuje unikalny system oceny wagowej w celu identyfikacji krytycznych wskaźników naruszeń, ukierunkowując analizę i reakcję na najbardziej istotne zagrożenia.

Zapobieganie unikalnym, ukierunkowanym atakom

Personel odpowiedzialny za bezpieczeństwo potrzebuje czegoś więcej, niż tylko narzędzia do priorytetyzacji, analizy i korelacji danych dotyczących zagrożeń – potrzebuje mechanizmów pozwalających na przekształcenie ich w skuteczne narzędzia pozwalające na zapobieganie kolejnym atakom. AutoFocus umożliwia tworzenie nowych polityk bezpieczeństwa na platformie udostępnianej przez Palo Alto Networks, poprzez eksport znaczników zagrożeń (IOC) do list blokad w systemie PAN-OS oraz natychmiastowe zatrzymywanie ruchu do i z rozpoznanych adresów stron internetowych, domen lub



adresów IP zawierających złośliwy kod. AutoFocus umożliwia również eksport znaczników do oprogramowania firm trzecich w postaci plików w formacie CSV. Personel korzystający z systemu AutoFocus może identyfikować specyficzne, ukierunkowane bezpośrednio na daną infrastrukturę ataki oraz łagodzić ich skutki i powstrzymywać kolejne.

Architektura AutoFocus oraz źródła danych

AutoFocus oparty jest o rozproszoną infrastrukturę chmurową, administrowaną i zarządzaną przez Palo Alto Networks. W odróżnieniu od innych rozwiązań, usługa ta udostępnia dane odnośnie wskaźników zagrożeń i wykracza poza proste przedstawienie podsumowania logów w interfejsie zarządzania. AutoFocus umożliwia bezprecedensowy wgląd w informacje o zagrożeniach zebranych i udostępnianych przez tysiące firm, dostawców usług oraz organizacji rządowych. Usługa koreluje i zbiera dane z:

- Największego na świecie wirtualnego środowiska WildFire™
- Serwisu filtrowania adresów stron internetowych będącego usługą PAN-DB
- Globalnej, pasywnej sieci serwerów DNS Palo Alto Networks
- Działu analizy zagrożeń Unit 42
- Informacji z rozwiązań firm trzecich, włącznie z rozwiązaniami otwartymi i zamkniętymi.

AutoFocus obsługuje ponad miliard próbek i sesji, zawierających miliardy charakterystycznych danych pozwalających na natychmiastową analizę i reakcję personelu odpowiedzialnego za kwestie bezpieczeństwa.

Prosta integracja z rozwiązaniami firm trzecich

Analiza zagrożeń, ich kwalifikacja oraz metody reagowania przez zespoły ds. bezpieczeństwa często opierają się o szeroki zakres skryptów, narzędzi o otwartym kodzie oraz urządzeń pozwalających na inspekcję potencjalnych incydentów. AutoFocus pozwala na znaczące skrócenie czasu potrzebnego na analizę, poprzez możliwość wykorzystania narzędzi firm trzecich z użyciem interfejsu API, możliwość zdalnej pracy oraz obsługi plików w formacie STIX.

- Interfejs API rozwiązania AutoFocus oparto na prostym w użyciu frameworku RESTful, co pozwala na jego integrację w setkach narzędzi korzystających z mechanizmów SIEM (Security Information and Event Management – Informacja o zabezpieczeniach oraz zarządzanie zdarzeniami), udostępniając tym samym dane do dalszej analizy zagrożeń lub automatyzację blokad przez konkretnych użytkowników.
- Użytkownicy AutoFocus mają możliwość korzystania zarówno z wewnętrznych, jak i zewnętrznych mechanizmów wprost z systemu AutoFocus. Personel odpowiedzialny za bezpieczeństwo może zdefiniować do 10 zewnętrznych systemów, pozwalając na współbieżną analizę zagrożeń dla całej infrastruktury, z wykorzystaniem korelacji zebranych danych z nowej generacji firewalli lub informacji przekazywanych przez narzędzia SIEM.
- AutoFocus natychmiastowo zapewnia integrację z infrastrukturą STIX i umożliwia eksport danych do plików w formacie STIX.

Ochrona prywatności

System AutoFocus zapewnia skuteczną ochronę prywatności i bezpieczeństwa w celu uniemożliwienia uzyskania dostępu do informacji poufnych lub umożliwiających identyfikację konkretnych użytkowników. Usługa pozwala na podgląd zebranych danych w obrębie organizacji wyłącznie autoryzowanym użytkownikom oraz możliwość przesłania zanonimizowanych danych innym osobom. AutoFocus nie zezwala na dostęp do jakichkolwiek plików użytkownika w obrębie usługi – udostępnia wyłącznie rezultaty analizy próbek obserwowanych w obrębie danej sieci, bez ujawniania oryginalnej zawartości plików. Każdy dostęp do usługi realizowany jest poprzez bezpieczne, szyfrowane połączenie. Chmurowe środowisko usługi AutoFocus jest stale monitorowane i chronione przez rozwiązania Palo Alto Networks.

Wymagania systemu AutoFocus

AutoFocus jest oferowany w postaci usługi nie wymagającej żadnych zmian w konfiguracji firewalli Palo Alto Networks i nie ma wpływu na wydajność już wykorzystywanych rozwiązań. W celu korzystania z usługi klienci muszą posiadać ważne konto serwisowe, co dotyczy również firm, które wykupiły rozwiązania typu firewall lub ochronę stacji roboczych realizowaną przez rozwiązanie Traps™. AutoFocus nie jest zależny od sprzętu i nie wymaga żadnych zmian w samym urządzeniu, nie ma też specyficznych wymagań co do wersji systemu PAN-OS lub konieczności inwestycji w dodatkowy sprzęt. Aby w pełni wykorzystać możliwości systemu AutoFocus zaleca się wykupienie subskrypcji rozwiązania WildFire (system PAN-OS w wersji 4.1 lub nowszej).

Informacje odnośnie licencji

AutoFocus jest oferowany jako roczna subskrypcja jednostanowiskowa. W celu uzyskania dodatkowych informacji odnośnie proponowanych licencji, prosimy skontaktować się z autoryzowanym partnerem lub przedstawicielem handlowym Palo Alto Networks.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054
Kontakt: +1.408.753.4000
Dział sprzedaży: +1.866.320.4788
Wsparcie techniczne: +1.866.898.9087
www.paloaltonetworks.com