GATEWATCHER

IDENTYFIKUJ CYBERZAGROŻENIA W SIECI ZANIM WPŁYNĄ NA TWOJĄ FIRMĘ

Firmom zagrażają zorganizowane cyberataki

Rozwój i cyfryzacja przedsiębiorstw powiązane są z ciągłą rozbudową przez nie systemów cyberbezpieczeństwa. Jednocześnie obserwowana jest coraz większa profesjonalizacja organizacji cyberprzestępczych, które dużo częściej przeprowadzają zaawansowane ataki o charakterze celowanym na sieci IT przedsiębiorstw. Tego rodzaju ataki bazują na głębokim rozpoznaniu strategii cyberbezpieczeństwa organizacji i skutecznym wykorzystaniu luk w firmowej infrastrukturze oraz słabości pracowników.

Czy wiesz że...

$4,24 mln

Średni koszt naruszenia bezpieczeństwa danych na całym świecie w 2020 r.[1]

255%

O tyle wzrosła pomiędzy 2019 a 2020 r. liczba ataków ransomware we Francji.[2]

207 dni

Średni czas potrzebny firmie na wykrycie naruszenia bezpieczeństwa systemów IT.[3]

53%

Udanych ataków nie jest wykrywane przez obecnie używane zabezpieczenia.[4]

Źródła: [1] Ponemon Institute, [2] ANSSI, [3] IBM, [4] FireEye Mandiant

Rozwiązaniem może być Gatewatcher

Gatewatcher to powstały w 2015 r. europejski producent rozwiązań cyberbezpieczeństwa, którego główna siedziba znajduje się w Paryżu. Firma specjalizuje się w wykrywaniu zaawansowanych cyberataków, takich jak Advanced Persistent Threat. Łącząc wysokowydajne rozwiązania oparte na metodach sygnaturowych i wykorzystując uczenie maszynowe, Gatewatcher stał się liderem na rynku dostawców rozwiązań cyberbezpieczeństwa. W swoim portfolio posiada trzy komplementarne rozwiązania: AionIQ® (NDR), AionBytes® (Sandbox) i LastInfoSec® (CTI).

W 2018r. Gatewatcher uzyskał uznaną w branży IT certyfikację ANSSI (National Agency for Information Systems Security), potwierdzającą jakość i skuteczność tworzonych zabezpieczeń. Wspomniana certyfikacja uprawnia do wykorzystywania rozwiązań Gatewatcher w jednostkach Francuskiej infrastruktury krytycznej, w tym m.in. w centralnych instytucjach państwowych czy wojskowych. Wyjątkowe podejście łączące szereg technologii ze sztuczną inteligencją, pozwala zagwarantować optymalną ochronę każdej organizacji.

AIONIQ®

Zobacz co kryje się w sieci Twojej organizacji

AionIQ® to rozwiązanie klasy Network Detection & Response (NDR), aktywnie monitorujące ruch sieciowy organizacji w celu identyfikacji zagrożeń.

Monitoring ruchu sieciowego

Źródłem danych do analizy dla AionIQ® jest pełna kopia ruchu sieciowego (full packet capture). Zapewnia to możliwość skanowania obiektywnego, niezmodyfi-kowanego pasma informacji.

Modułowa architektura

Architektura rozwiązania umożliwia adaptację do specyfiki każdej infrastruktury, w tym takiej która jest rozproszona geograficznie.

Dywersyfikacja silników detekcji

Każde połączenie przekazane do AionIQ® jest skanowane przez szereg silników detekcji o różnym profilu, umożliwiając wykrycie zróżnicowanych technik wykorzystywanych przez cyberprzestępców.

Integracja z obecnymi systemami

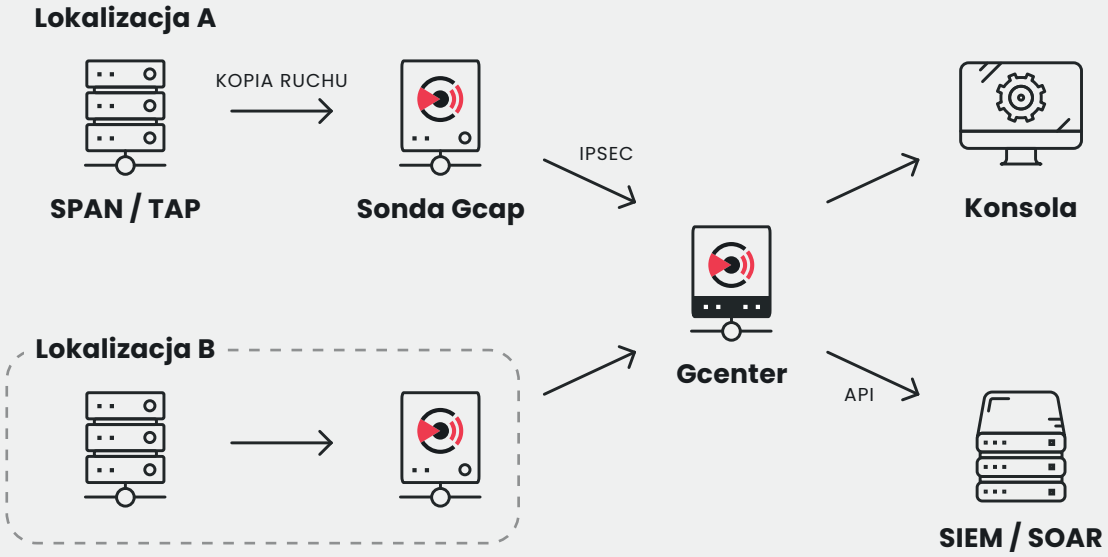
Dzięki otwartym API i możliwości integracji z systemami typu EDR, XDR, SIEM czy SOAR, AionIQ® w łatwy sposób stanie się integralną częścią infrastruktury bezpieczeństwa.

Skuteczność i łatwa obsługa

AionIQ® jest łatwy w konfiguracji, a jego działanie nie wpływa na środowisko produkcyjne. Wychodząc naprzeciw wymaganiom klientów, platforma występuje w kilku różnych pakietach, aby idealnie dopasować się do potrzeb infrastruktury i obecnie wykorzystywanych technologii, dzięki czemu oferuje idealnie dopasowaną strategie bezpieczeństwa. Wyjątkowe podejście łączące szereg technologii ze sztuczną inteligencją, pozwala zagwarantować optymalną ochronę każdej organizacji.

Architektura on-premise

Wszystkie analizy sieci dokonywane przez AionIQ® są realizowane lokalnie, dzięki czemu dane dotyczące zasobów infrastruktury IT nie są nigdzie przekazywane.



1. W głównych węzłach sieci kopia ruchu zostaje przekazana do Sondy AionIQ®. Rolę dostawców kopii mogą pełnić switche obsługujące port-mirroring lub dedykowane Test Access Pointy.

2. Kopie pakietów trafiają do sondy Gcap, gdzie dokonuje się wstępnej analizy. Następnie ruch zostaje zoptymalizowany i z pomocą szyfrowanego połączenia przekazany dalej. W konfiguracji może występować tylko jedna sonda lub zależności od potrzeb, większa ich ilość (np. oddziały znajdujące się w różnych lokalizacjach).

3. Centralnym elementem systemu jest Gcenter. W tym miejscu zbierane są dane ze wszystkich skojarzonych sond, gdzie poddawane są kolejnym analizom bezpieczeństwa. Gcenter odpowiedzialny jest za administrację całego zestawu rozwiązania, a także za utrzymanie niezbędnej retencji danych.

4. Wyniki analizy bezpieczeństwa prezentowane są w konsolach administracyjnych, a także mogą być na bieżąco przekazywane do innych systemów poprzez otwarte API.

Skuteczny Threat hunting

AionIQ® zapewnia pełną transparentność i obszerne informacje związane z analizowanym ruchem oraz konfiguracjami silników detekcji. Celem takiego zabiegu jest zapewnienie operatorowi wszelkich niezbędnych danych do podjęcia adekwatnej reakcji na występujące zagrożenie.

Silniki detekcji

W celu wykrycia wszystkich metod, które mogą być wykorzystane w przebiegu cyberataku AionIQ® stosuje szereg silników skanujących wszystkie połączenia w sieci.

SIGFLOW

Wykorzystuje mechanizm działania rozwiązania Intrusion Detection System (IDS), oparty na sygnaturach połączeń mających znamiona niebezpiecznej aktywności.

CODEBREAKER

Silnik przeznaczony do dekodowania oraz detekcji prób wykorzystania w procesie ataku shellcode i powershell, wliczając w to nawet kod polimorficzny.

MALCORE

Każdy plik przesyłany w ruchu sieciowym zostaje wyizolowany i przeskanowany przez 16 niezależnych silników antywirusowych. Dzięki dywersyfikacji źródeł sygnatur redukcji ulega ryzyko wystąpienia false-negative.

RETROACT

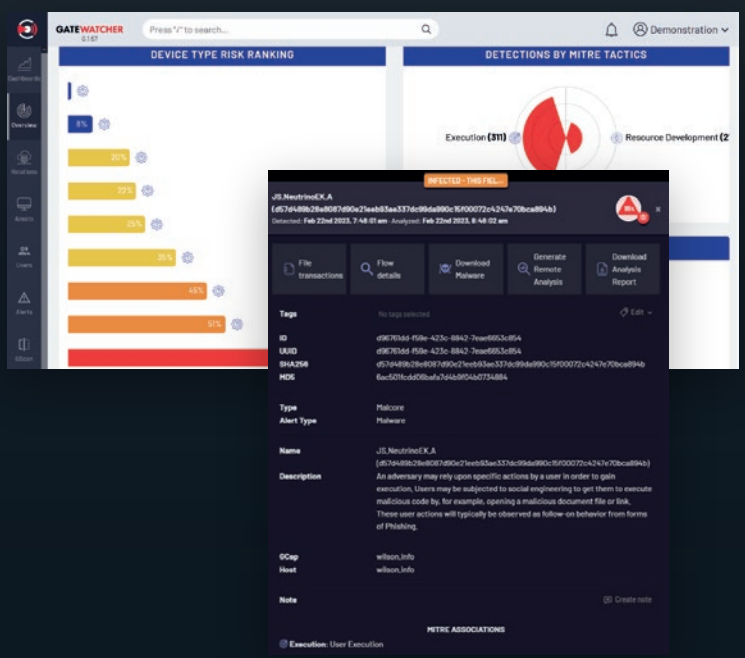
Wszystkie pliki utrzymane w pamięci urządzenia podlegają regularnym ponownym skanom po aktualizacji baz sygnatur, a administarator zyskuje dostęp do historycznych połączeń. W sytuacji pojawienia się doniesień o nowych kampaniach malware, AionIQ® automatycznie sprawdzi, czy nasza infrastruktura nie stała się ich celem.

MACHINE LEARNING

Zastosowanie uczenia maszynowego uzupełnia zwyczajowo używane metody bazujące na sygnaturach, szukając zagrożeń w połączeniach, których niejednokrotnie nie da się sparametryzować. Za przykład może posłużyć mechanizm wykrywania Domain Generation Algorithms używanych w mechanizmach Command & control.

NDR View

NDR View to widok dedykowany do szybkiej i precyzyjnej analizy stanu bezpieczeństwa. Pozwala obserwować zdarzenia z poziomu konkretnych zasobów, użytkowników czy typów. Konsola daje możliwość ujęcia środowiska z perspektywy wszystkich zasobów, ale także szczegółowych danych, nawet do poziomu detali pojedynczych połączeń. Weryfikację incydentów ułatwia wbudowany algorytm szacujący poziomy ryzyka oraz odwołanie do frameworku MITRE ATT&CK®.



LASTINFOSEC®

Kompleksowa platforma threat intelligence

Wykrywaj zagrożenia dla Twojego systemu informatycznego płynące zarówno z zewnątrz, jak i od wewnątrz.

Skróć czas potrzebny na analizę wykrytych zagrożeń

Dzięki bibliotece zawierającej 6 mln IoC, ponad 5000 nowym markerom dodawanym każdego dnia oraz ponad 3000 różnym źródłom danych infrastruktura LASTINFOSEC® oferuje bogate i osadzone w kontekście dane threat intelligence.

LASTINFOSEC® ułatwia podejmowanie decyzji zespołom ds. bezpieczeństwa operacyjnego, znacząco skracając czas wymagany na analizę i reagowanie na zdarzenia, nie ingerując przy tym w procesy wewnętrzne.

LASTINFOSEC® korzysta ze zautomatyzowanych silników gromadzenia, analizy i korelacji danych, dzięki którym informacje na temat zagrożeń dostępne są na ogół 24 godziny wcześniej, niż w przypadku konkurencyjnych rozwiązań.

LASTINFOSEC® można w prosty i szybki sposób zintegrować dzięki eksportom do najnowszych standardów CTI (Stix v2, Stix v2.1, JSON itp.) oraz kompatybilnością z wiodącymi narzędziami analitycznymi (Splunk, OpenCTI itp.)

LASTINFOSEC® nieustannie inwentaryzuje i ocenia źródła danych z różnych kanałów: portali społecznościowych, specjalistycznych stron, darknetu oraz deep webu.

GATEWATCHER

Pełniejsze i bardziej przejrzyste spojrzenie na zagrożenia

Informacje dostarczane przez LASTINFOSEC® mogą być wykorzystywane przez całą organizację lub przez konkretne oddziały. Oferta obejmuje wdrożenie w ramach części technologii wykrywania, np. IDS lub EDR, narzędzi używanych przez zespoły SOC i CERT lub w całej organizacji w ramach platform threat intelligence. LASTINFOSEC® pozwala na proste zwiększenie skuteczności Twoich zabezpieczeń dzięki pełniejszemu i bardziej przejrzystemu spojrzeniu na zagrożenia. Wyszukiwanie zagrożeń możesz również zautomatyzować, dzięki czemu przyspieszysz wykrywanie.

Bezproblemowa integracja bez ingerencji w istniejące procesy

- Mniej fałszywych alarmów dzięki w pełni kwalifikowanemu i walidowanemu przepływowi danych.
- Format eksportu danych kompatybilny z istniejącymi rozwiązaniami cyberbezpieczeństwa.
- Szczegółowe alerty pozwalają Twoim zespołom skuteczniej reagować na zdarzenia.
- Analiza informacji ułatwia pracę zespołom SOC.
- Integracja z zewnętrznymi platformami threat intelligence, istniejącymi rozwiązaniami bezpieczeństwa sieci (IDS, IPS, NGFW, Sandbox, NDR) i punktów końcowych (EDR) oraz narzędziami do analizy SOC (SIEM, SOAR).

Platforma threat Intelligence

/ open source
oraz komercyjna

AIONBYTES®

Lokalny sandbox do analizy podejrzanych plików i linków

Umożliwia skuteczne przewidywanie przyszłych ataków oraz podejmowanie niezbędnych decyzji dotyczących bezpieczeństwa.

AIONBYTES® stanowi uzupełnienie Twojego systemu wykrywania, dzięki któremu:

- Możesz obserwować wpływ złośliwego oprogramowania na mutexy, rejestr, wywołania API oraz dostęp, zachowanie i artefakty systemu plików.
- Zrozumiesz, na czym polega cały cykl życia złośliwego programu: Dzięki obserwacji jego zachowań oraz tego, w jaki sposób łączy się z Internetem, symulując interakcje z programem, a także rejestrując zachowanie sieci.
- Identyfikuj techniki takie jak opóźnione wykonywanie, diagnostyka środowiska i weryfikacja interakcji z człowiekiem.
- Dane na temat złośliwego oprogramowania możesz udostępniać innym zabezpieczeniom, dzięki czemu obronisz się przed kolejnymi atakami.

Dedykowane, kontrolowane i chronione środowisko

AIONBYTES® oferuje bezpieczne środowisko, które uruchamia złośliwe oprogramowanie, a następnie dostarcza danych na temat zmian, które chce ono wprowadzić w systemie. W ciągu zaledwie kilku minut analitycy bezpieczeństwa otrzymują wstępną ocenę zagrożenia, jakie stanowi dane oprogramowanie lub shellcode, a także dane dotyczące jego zachowania.

5 silników analitycznych do oceny zagrożeń

AIONBYTES® dostarcza szczegółowych wyników z każdego silnika w oparciu o globalne statystyki, dzięki czemu możesz podejmować skuteczniejsze decyzje w obliczu zagrożenia.

ANALIZA STATYCZNA

Umożliwia szybkie sprawdzenie metadanych pliku.

ANALIZA DYNAMICZNA

Pozwala na ocenę zachowania pliku uruchomionego na maszynie wirtualnej.
Dane generowane podczas analizy mogą być eksportowane (jako zrzut pamięci czy pcap).

ANALIZA HEURYSTYCZNA

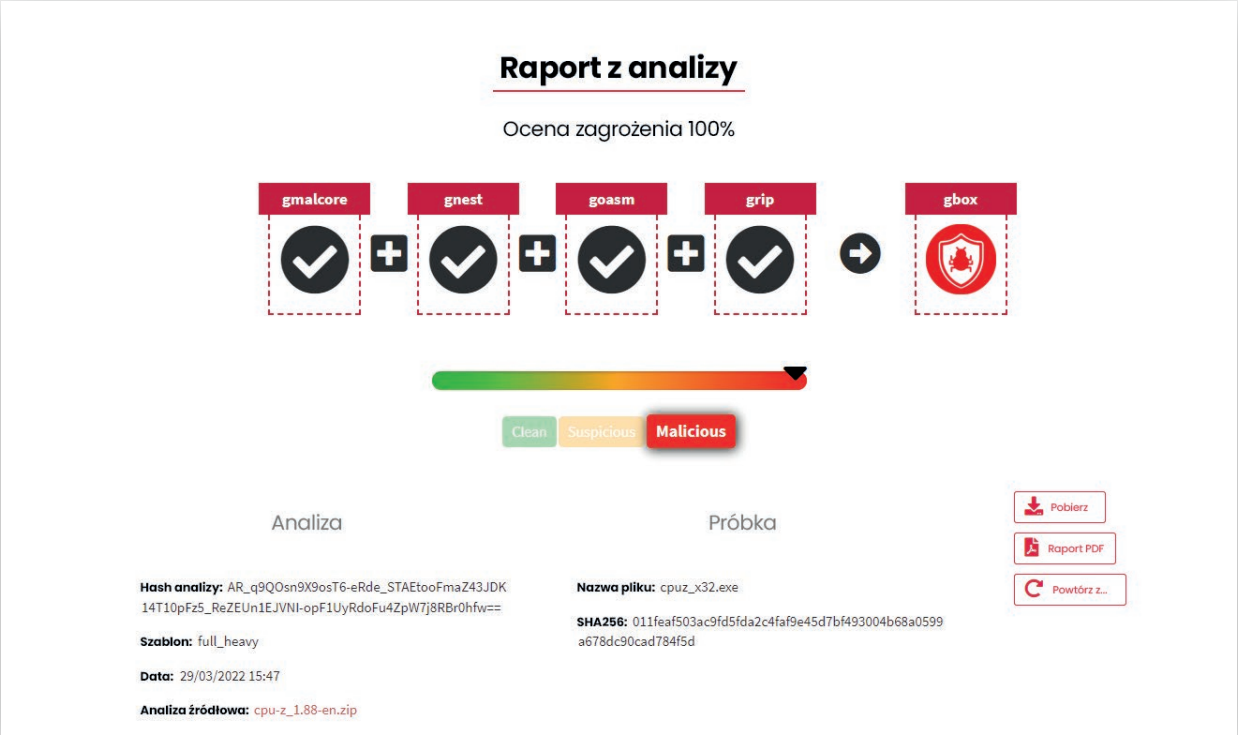
Oparta na 16 silnikach antymalware działających jednocześnie. Silniki te zostały wyselekcjonowane przez laboratorium Gatewatcher ze względu na ich komplementarność, skuteczność, używane technologie wykrywania oraz pochodzenie geopolityczne wykorzystywanych przez nie danych bezpieczeństwa.

ANALIZA SHELLCODE

Pozwala na identyfikację niektórych typów kodu i identyfikację wywołań systemowych.

DETEKTOR DGA

Wykrywa algorytmy generowania domen.

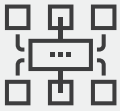


Dlaczego rozwiązania Gatewatcher?

Monitoring sieci to pierwszy i najważniejszy cel. Od wykrywania do analizy, z takim samym zaangażowaniem Gatewatcher opracowuje swoje rozwiązania.

Wspiera w kreowaniu polityki bezpieczeństwa dla systemu informatycznego

- Wykrywanie i analiza słabych punktów
- Wsparcie przy podejmowaniu decyzji
- Opracowanie planu działania



Ułatwia wykrywanie i gromadzenie danych o sieci

- Monitorowanie
- Audyty
- Ciągła analiza ruchu sieciowego

Automatyzuje analizę danych

- Ogranicza liczbę fałszywych alarmów
- Ocenia prawdo-podobieństwo wykorzystania podatności i jego wpływu na infrastrukturę

Twoje korzyści

INTUICYJNE NARZĘDZIA
...poprzez prosty i zwinny interfejs ułatwiający operacje w ramach SOC (Security Operations Center)

SKALOWALNA TECHNOLOGIA
...którą można dostosować do każdego środowiska.

PREWENCYJNE PODEJŚCIE
...automatyzujące przewidywanie zagrożeń i podatności zero-day.

ROZSZERZONA WIDOCZNOŚĆ
...wewnętrznego ruchu sieciowego organizacji.

Zaawansowane rozwiązania do wykrywania cyberzagrożeń.

Sprawdź nasze aktualne wydarzenia on-line
i zrób pierwszy krok w kierunku ochrony swojej firmy!

Chcesz dowiedzieć się więcej?
Skontaktuj się ze mną:

Mateusz Nowak
Product Manager Gatewatcher
795 518 758 / 32 893 11 19
gatewatcher@dagma.pl

GATEWATCHER

GATEWATCHER

DAGMA
BEZPIECZEŃSTWO IT

Dystrybutor rozwiązań
Gatewatcher w Polsce

DAGMA Bezpieczeństwo IT
ul. Bażantów 4/2, 40-668 Katowice

gatewatcher@dagma.pl
tel. +48 32 259 11 00