AIONIQ®

Analiza behawioralna i mapowanie dla zaawansowanej analizy sieci

GATEWATCHER

Wykrywanie zaawansowanych cyberzagrożeń: nowe wyzwanie dla organizacji

Konsekwencje finansowe cyberataku są w stanie na długi czas osłabić Twoją organizację.

Wzrost liczby zagrożeń sprawia, że ocena poziomu ich krytyczności staje się dla analityków bezpieczeństwa coraz trudniejsza.

Atak ukierunkowany, który nie został odpowiednio szybko wykryty, potrafi spowodować poważne szkody w infrastrukturze informatycznej.

Niewykrywalność i złożoność współczesnych ataków utrudnia ich wykrycie i skuteczne unieszkodliwienie.

$3,86 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]

Aioniq®: mapowanie i analiza behawioralna cyberzagrożeń pozwala na sprawniejsze wykrywanie i zwiększa widoczność ataków ukierunkowanych

- **Wykrywanie zagrożeń, nawet w zaszyfrowanej sieci.** Aioniq® to platforma NDR wykorzystująca uczenie maszynowe do identyfikowania wszystkich typów zagrożeń wewnątrz Twojej infrastruktury, nawet jeżeli ruch sieciowy jest zaszyfrowany.
- **Mapowanie wszystkich zasobów systemu informatycznego.** Aioniq® to jedyna platforma NDR umożliwiająca mapowanie wszystkich zasobów IT w sposób całkowicie pasywny i bezagentowy, dzięki czemu zapewnia wykrywanie zaawansowanych ataków na ruchu wschód-zachód.
- **Lepsza widoczność ukrytych zagrożeń.** Aioniq® umożliwia tworzenie typologii metadanych o unikalnym poziomie szczegółowości, dzięki czemu optymalizuje czas potrzebny na analizę zdarzenia.
- **Modelowanie ryzyka dla poszczególnych zasobów i użytkowników.** Aioniq® to jedyna platforma NDR zdolna do modelowania poziomu ryzyka w oparciu o typ zdarzenia, zasób i użytkownika, z widokiem Mitre Att&ck agregującym alerty według poziomu ryzyka.

Aioniq® to nowa platforma network detection and response (NDR), umożliwiająca identyfikację szkodliwych aktywności i anomalii ruchu w oparciu o mapowanie zasobów infrastruktury IT.

Łącząc powyższe funkcje z analizą wszystkich operacji, nawet gdy ruch sieciowy jest zaszyfrowany, rozwiązanie gwarantuje 360 -stopniowe modelowanie zagrożeń dla każdego połączenia pomiędzy zasobami a użytkownikami, oferując niezrównanie wysoki poziom wykrywania i widoczności.

Aioniq® to rozwiązanie wysoce granularne i skalowalne, które nieustannie dopasowuje się do znanych i nieznanych zagrożeń takich jak ataki ransomware, APT i zero-day, dzięki czemu oferuje skuteczną i spersonalizowaną ochronę.

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

Korzyści dla użytkownika

PLATFORMA SOFTWARE'OWA ODPORNA NA CYBERATAKI

Aioniq® został zaprojektowany zgodnie z podejściem „Security by design", dlatego opiera się na systemie operacyjnym o podwyższonym bezpieczeństwie, dzięki czemu gwarantuje wysoką odporność na ataki.

NATYCHMIASTOWA I SKUTECZNA OCHRONA

Aioniq® nie wymaga dodatkowego sprzętu i nie wiąże się z ukrytymi kosztami. Platforma wykrywa zagrożenia już od samego początku fazy audytu, bez wpływu na środowisko produkcyjne.

WYSOKA INTEROPERACYJNOŚĆ Z ISTNIEJĄCYMI ZASOBAMI

Aioniq® to otwarta platforma umożliwiająca zautomatyzowaną odpowiedź na ataki dzięki integracji z większością dostępnych na rynku narzędzi bezpieczeństwa takich jak EDR, SIEM i SOAR.

OFERTA, KTÓRA ŁĄCZY WYDAJNOŚĆ I SKALOWALNOŚĆ

Aioniq® dostosowuje się do zagrożeń i specyfiki Twojej organizacji dzięki skalowalnemu systemowi wykrywania oraz możliwości implementacji On-prem lub w chmurze.

GRANULARNY I ELASTYCZNY SYSTEM

Aioniq® dostępny jest w ramach kilku różnych pakietów dostosowanych do potrzeb infrastruktury bezpieczeństwa i obecnie wykorzystywanych technologii, dzięki czemu oferuje idealnie dopasowaną ochronę.

ZOPTYMALIZOWANA WYDAJNOŚĆ DLA TWOJEGO Security Operation Center

Aioniq® ułatwia pracę analitykom zajmującym się badaniem zdarzeń i analizą krytyczności alertów dzięki metadanym i mapowaniu z wizualizacją chronologiczną zgodną z frameworkiem MITRE ATT&CK.

Zastosowania

Wykrywanie:
Skuteczne wykorzystanie uczenia maszynowego.
W odróżnieniu od modelu wykrywania opartego jedynie na SI, Aioniq® cechuje wieloczynnikowe podejście, na które składa się analiza statyczna, dynamiczna i algorytmiczna w zależności od typu zagrożenia, co umożliwia identyfikację taktyk, technik i procedur każdego cyberataku.

- Wykrywanie Cobalt Strike Beacon w kontekście ataków DGA
- Wykrywanie nieprawidłowości nawet w sieciach z szyfrowaniem ruchu
- Wykrywanie algorytmów zaciemniania kodu używanych w atakach lateralnych

Polowanie:
Reagowanie na pierwsze oznaki ukierunkowanego ataku.
Aioniq® to jedyne rozwiązanie na rynku zdolne do ochrony przed wszystkimi etapami cyberataku oraz identyfikacji użytych technik, dzięki czemu hakerzy nie są w stanie się przed nim ukryć.

- Dogłębna analiza typów metadanych, sesji, protokołów i działań użytkowników
- Oparte na UEBA zarządzanie interakcjami zasobów pozwala skoncentrować się na najważniejszych zagrożeniach
- Analiza post-mortem wszystkich metadanych przy pomocy wskaźników nowej generacji naruszeń (IoC)

Reakcja na zdarzenia:
Skuteczna interoperacyjność z Twoimi narzędziami umożliwia natychmiastową reakcję na ataki.
Aioniq® to otwarte rozwiązanie umożliwiające szybką i łatwą integrację z większością narzędzi bezpieczeństwa dzięki obszernemu katalogowi API, co pozwala na natychmiastową odpowiedź na cyberataki.

- Szybkie tworzenie własnych plików sygnatur w celu dostosowania się do infrastruktury
- Automatyzacja scenariuszy SOAR w celu odpowiadania na zdarzenia
- Szeroki wybór API EDR umożliwia szybkie i zautomatyzowane reagowanie

Analiza post-mortem:
Wyjątkowa widoczność gwarantuje lepszą odporność na ataki. Aioniq® mapuje zasoby informatyczne oraz jest w stanie skorelować je z każdym użytkownikiem w celu oceny zagrożenia, dzięki czemu oferuje możliwość analizy post-mortem przebiegu każdego ataku.

- Gromadzenie rozbudowanych metadanych pozwala na dokładną analizę każdego ataku
- Szybkie aktualizacje dzięki łączności z różnymi platformami Threat Intelligence dostępnymi na rynku
- Interaktywny interfejs graficzny pozwala na ustalenie czasu i propagacji każdego ataku