Platforma Nozomi Networks

Zintegrowana platforma, zapewniająca jednolitą widoczność i bezpieczeństwo w środowiskach OT, IoT oraz infrastrukturze krytycznej.

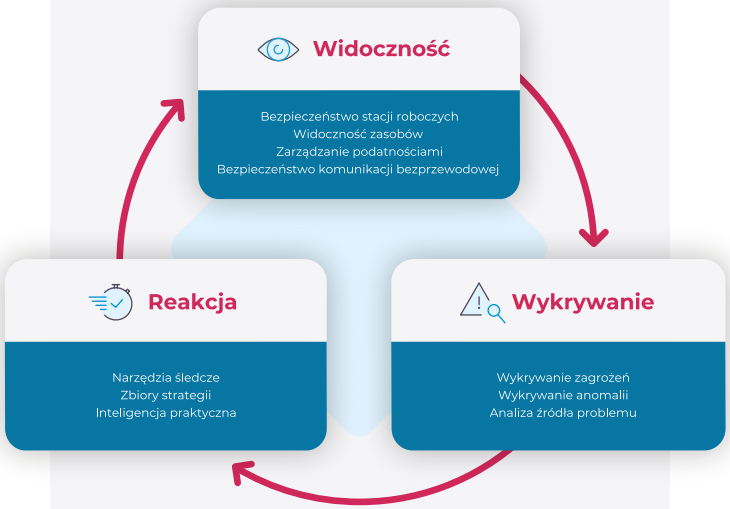
W miarę wzrostu skali połączeń i automatyzacji procesów online, zwiększają się również obawy dotyczące bezpieczeństwa. Dla wielu organizacji zarządzanie ryzykiem i utrzymanie efektywności operacyjnej zaczyna się od oceny podatności i wykrywania zagrożeń.

Głęboka, inteligentna analiza podatności, anomalii sieciowych, aktywnych zagrożeń oraz problemów związanych z procesami przemysłowymi to mniejsze ryzyko naruszenia bezpieczeństwa, optymalizacja procesów oraz szybsze usuwanie problemów w złożonych środowiskach OT/IoT.

Nozomi Networks jest Twoim partnerem w zakresie widoczności OT i IoT oraz rozwiązań cyberbezpieczeństwa dla zróżnicowanych procesów przemysłowych i sektora usług krytycznych.

Metodologia platformy Nozomi Networks koncentruje się wokół cyklu reagowania na incydenty, składającego się z 3 faz: widoczności, wykrywania i reakcji.

Oferuje ona kluczowe funkcje wspierające typowe zadania administracyjne, związane z bezpieczeństwem oraz siecią dla każdej z opisanych faz.



Widoczność

Jednolita widoczność OT i IoT pozwala przewidzieć potencjalne zagrożenia dla bezpieczeństwa i niezawodności długo przed tym, zanim będą miały realny wpływ na operacje.

Pierwszym etapem dojrzałości cyberbezpieczeństwa jest zrozumienie, co znajduje się w Twojej sieci i przewidzenie, gdzie mogą pojawić się ryzyka.

Nozomi Networks zapewnia widoczność wszystkich Twoich zasobów sieciowych (przewodowych i bezprzewodowych) oraz urządzeń końcowych za pomocą „głębokiego” zbierania danych, które może ujawnić podatności i wskazać, gdzie skoncentrować wysiłki w zakresie zarządzania ryzykiem. Wizualizacja połączeń i wzorców ruchu ułatwia weryfikację oraz prace związane z zapewnieniem zgodności. Przewidywanie zagrożeń bezpieczeństwa pozwala zredukować ryzyko oraz czas wymaganych analiz, zanim wpłyną one na Twoje operacje.

Network View zapewnia interaktywną wizualizację połączeń w Twojej sieci.

Główne funkcje platformy

Pasywne odkrywanie zasobów

Odkrywanie zasobów w środowiskach OT i IoT może być całkowicie pasywne i opierać się na obserwacji odzwierciedlonego ruchu, aby nie zakłócać krytycznych procesów, wyzwalać alarmów lub generować dodatkowego ruchu.

Baza danych podatności

Aby pomóc identyfikować ryzyka i priorytety w zakresie utrzymania ruchu urządzeń, zarządzamy jedną z najbardziej obszernych baz danych znanych podatności, pochodzącą od badaczy i organów bezpieczeństwa na całym świecie.

Inteligencja zasobów [Asset Intelligence] DODATEK

Subskrypcja Asset Intelligence zapewnia organizacjom dostęp do najnowszych badań luk w zabezpieczeniach, aktualnych poziomów poprawek systemu operacyjnego i oprogramowania układowego oraz najnowszych informacji o naruszeniach bezpieczeństwa.

Wizualizacja sieci

Uzyskaj kompletny widok urządzeń komunikacyjnych i wzorców ruchu, aby zbudować mapę wizualizacji, która może przyspieszyć badania i pozwoli szybko zidentyfikować anomalie i incydenty.

Notatniki [Workbooks]

Notatniki priorytetyzują wysiłki naprawcze, podkreślając najważniejsze podatności urządzeń końcowych.

Inteligentne odpytywanie [Smart Polling] DODATEK

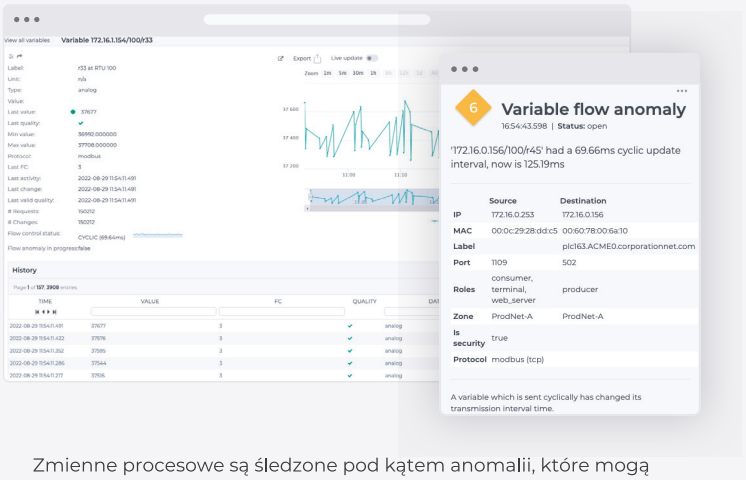
Ta funkcja proaktywnie sprawdza urządzenia i gromadzi krytyczne informacje o punktach końcowych w celu zwiększenia bezpieczeństwa. Parametry odpytywania mogą być ustawione tak, aby minimalnie wpływać na istniejący ruch i urządzenia poniżej progów alarmowych. Do odpytywania wykorzystywane są natywne protokoły komunikacyjne urządzeń.

Wykrywanie

Wychodzimy poza wykrywanie anomalii w OT i IoT, aby pomóc Ci zdiagnozować przyczyny nieoczekiwanych zmian procesowych i odstępstw od zachowania bazowego.

Zmniejszenie ryzyka i przewidywanie potencjalnych problemów nie gwarantuje, że wyeliminujesz każde nowe zagrożenie. Ciągłe monitorowanie procesów i ruchu jest kluczowe dla identyfikowania i diagnozowania zagrożeń lub zrozumienia ich anomalii.

Nozomi Networks stosuje własny silnik sztucznej inteligencji/uczenia maszynowego, aby dostarczać wiodące w branży informacje i analizy.
Dzięki pozyskanym przez nas danym będziesz na bieżąco z najnowszymi sygnaturami i wskaźnikami kompromitacji (IOC) najnowszych ataków zero-day i trendów ransomware.



Zmienne procesowe są śledzone pod kątem anomalii, które mogą wynikać z ataku, błędu ludzkiego lub potencjalnej awarii mechanicznej.

Główne funkcje platformy

Monitorowanie

Porównaj ruch sieciowy i trendy procesowe w czasie, aby zidentyfikować potencjalne zagrożenia i utrzymać procesy przemysłowe na najwyższym poziomie efektywności.

Inteligencja zagrożeń [Threat Intelligence] DODATEK

Wykrywaj więcej zagrożeń dzięki naszym narzędziom, ułatwiającym identyfikację włamań, obsługę najszerszego zakresu urządzeń przemysłowych i protokołów komunikacyjnych. Inteligencja zagrożeń zapewnia najnowszą wiedzę o złośliwym oprogramowaniu, IOC (wskaźnikach kompromitacji) specyficznych dla procesów przemysłowych... i urządzeń IoT. Nasz kanał informacyjny jest również dostępny w otwartym formacie do użytku w innych platformach bezpieczeństwa.

Pakiety treści

Dzięki pakietom treści otrzymasz wgląd w typowe problemy i pojawiające się zagrożenia, takie jak luki w zabezpieczeniach Industroyer2 lub zgodność z IEC 62443.

Wykrywanie anomalii

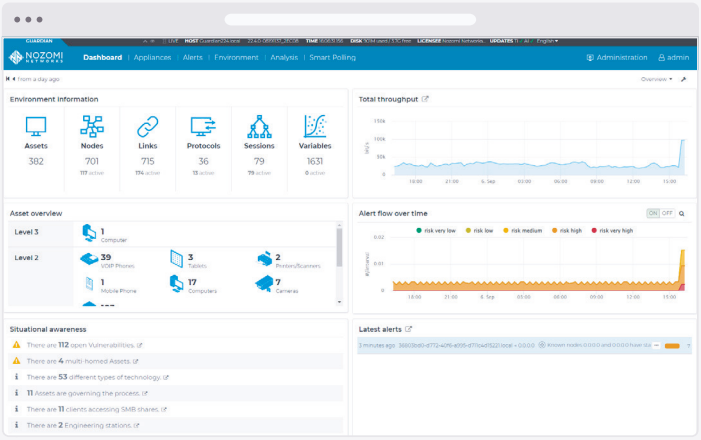
Wyuczone w ramach twojej sieci mechanizmy pomagają wyeliminować fałszywe alarmy i zapewniają głębszy wgląd w trendy procesowe. Wyjdź poza tradycyjne wskaźniki wykrywania anomalii w ruchu sieciowym i zbuduj linię trendów zmiennych procesowych i danych systemu sterowania, aby zidentyfikować szerszy kontekst i dokonać trafniejszej analizy źródeł problemów.

Reagowanie

Praktyczna inteligencja i ukierunkowane środki zaradcze zapewniają wgląd, potrzebny do przyspieszenia reakcji na krytyczne naruszenia bezpieczeństwa OT i IoT oraz problemy z kontrolą procesów.

Gdy nadchodzi czas, by zareagować na naruszenie bezpieczeństwa lub problem z kontrolą procesu, potrzebujesz praktycznych informacji, niezbędnych do rozwiązania problemu przy minimalnym koszcie i wpływie na Twoje operacje. Nozomi Networks dostarcza wszystkich informacji oraz wglądu, koniecznego, by usuwać problemy, zagłębiać się w dalsze badania oraz kierować lub koordynować odpowiednią reakcję. Platforma Nozomi Networks agreguje ogromną ilość danych z urządzeń i ruchu sieciowego w całej organizacji.

Dzięki elastycznej ofercie chmury Vantage, skala agregowanych informacji może być niemal nieskończona. Udostępnienie tych danych, ich użyteczność i dostępność pod wieloma różnymi kątami to moc interfejsu użytkownika platformy, pulpitów nawigacyjnych, alertów, możliwości kreowania zapytań i narzędzi śledczych.



Konfigurowalne pulpity nawigacyjne dostarczają ważnych danych w jednym miejscu.

Główne funkcje platformy

Wehikuł czasu [Time Machine]

Wehikuł czasu pozwala użytkownikom odtwarzać zdarzenia sieciowe wokół incydentu, aby pomóc w izolacji przyczyny i wizualizacji wpływu, zmniejszając średni czas naprawy (MTTR).

Tablice i alerty

Tablice i alerty Nozomi Networks zostały zaprojektowane w ten sposób, by umożliwić Ci obserwowanie zdarzeń, systemów, zasobów, problemów z bezpieczeństwem i alarmów w całej organizacji w przystępny sposób. Filtrowanie dużej ilości informacji przy zachowaniu ich pełnego uporządkowania i dostępności oszczędza czas i wysiłek zespołów administracyjnych, które mogą skupić się na realnych problemach. Dodatkowo zapewnia łatwe budowanie zapytań, aby szybko izolować podatności, incydenty lub identyfikować i inwentaryzować zasoby.

Raporty

Raporty są generowane dla gotowych, powtarzalnych działań śledczych lub zapewnienia zgodności. Zapytania i raporty można dołączyć do pakietów treści lub korzystać z tych istniejących, oferowanych przez Nozomi Networks i partnerów.

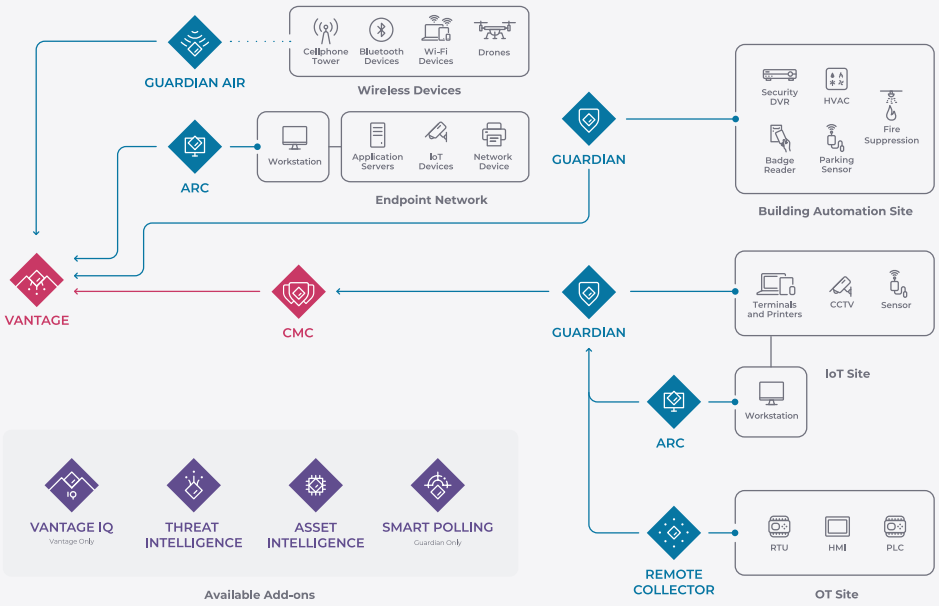
Przewodniki [Playbooks]

Przewodniki są kluczowe dla koordynowania szybkiej reakcji na incydent lub awarię. Nozomi Networks umożliwia importowanie lub projektowanie własnych przewodników bezpieczeństwa, ułatwiających identyfikację kroków naprawczych dla każdego typu incydentu. Etapy można dostosowywać, uwzględniając określonych administratorów lub kierowników wykonawczych, w zależności od typu incydentu lub lokalizacji. Śledzenie kroków przewodnika pozwala koordynować reakcję na incydent jako workflow i zintegrować ją z systemami zgłoszeń.

Zbuduj swoje rozwiązanie

Platforma Nozomi Networks zapewnia szeroki zakres komponentów i form do elastycznego wdrożenia i skalowania w zakresie środowisk przemysłowych i korporacyjnych.

Sam możesz wybrać, co i jak wdrażać w lokalnych i chmurowych środowiskach dla maksymalnej wydajności.



VANTAGE

SAAS

Nozomi Vantage to rozwiązanie typu SaaS, które skaluje monitorowanie bezpieczeństwa i widoczność dla dużych przedsiębiorstw z wieloma lokalizacjami, oferując jednocześnie korzyści finansowe i elastyczność rozwiązania hostowanego w chmurze. Zapewnia ujednoliconą widoczność i monitorowanie bezpieczeństwa nieograniczonej liczby węzłów oraz systemów dla dużych wolumenów ruchu i zasobów. Może uprościć wdrażanie lokalnych czujników Guardian i zmniejsza złożoność zarządzania wieloma urządzeniami CMC.
nozominetworks.com/products/vantage

CENTRAL MANAGEMENT CONSOLE

EDGE

PUBLIC CLOUD

Nozomi Central Management Console (CMC) łączy bezpieczeństwo OT i IoT oraz widoczność w sieciach, ułatwiając monitorowanie oraz priorytetyzowanie podatności i czynników ryzyka. Pomaga wykrywać i przerywać pojawiające się zagrożenia oraz szybko docierać do dodatkowych informacji za pomocą zaawansowanych zapytań, dotyczących dowolnych danych operacyjnych.
nozominetworks.com/products/central-management-console

GUARDIAN

EDGE

PUBLIC CLOUD

Czujniki Nozomi Guardian to czujniki on-site, które zbierają i analizują Twoje dane operacyjne. Eliminują martwe punkty w środowisku operacyjnym, dzięki widoczności zasobów, przepływom danych i sieci dla środowisk OT i IoT. Czujniki Guardian wykrywają zagrożenia cybernetyczne i operacyjne, a także luki w zabezpieczeniach, zapewniając świadomość sytuacyjną, która jest kluczowa dla zapewnienia bezpieczeństwa i zgodności. Są skuteczne dla wszystkich systemów/podsystemów operacyjnych, w tym sterowników przemysłowych, czujników IoT, kamer CCTV, systemów automatyki budynkowej i środowisk o wzmocnionej konstrukcji.
nozominetworks.com/products/guardian

GUARDIAN AIR

ADD-ON

Nozomi Guardian Air to pierwszy na rynku bezprzewodowy czujnik dla środowisk OT i IoT. Monitoruje dominujące częstotliwości komunikacji, aby zapewnić widoczność aktywów, ciągłe wykrywanie zagrożeń i ocenę podatności sieci bezprzewodowych w Twoim środowisku. Jego dane mogą być agregowane do Vantage wraz z innymi danymi sieciowymi po to, by umożliwić holistyczne monitorowanie Twojego środowiska.
nozominetworks.com/products/guardian-air

ARC

EDGE

PUBLIC CLOUD

Nozomi Arc to czujniki instalowane na urządzeniach końcowych, które działają w systemach Windows, Linux lub macOS, w sieciach o kluczowym znaczeniu. Pozwalają łatwo identyfikować skompromitowane hosty ze złośliwym oprogramowaniem, aplikacje szpiegujące, nieautoryzowane napędy USB czy podejrzane aktywności użytkowników. Zebrane dane mogą być wysyłane zarówno do Guardiana, jak i chmury Vantage.
nozominetworks.com/products/arc

REMOTE COLLECTOR

ADD-ON

Kolektory zdalne (Remote collector) to niskonakładowe czujniki, które zbierają dane z Twoich rozproszonych lokalizacji i wysyłają je do Guardiana w celu analizy. Poprawiają widoczność i redukują koszty wdrożenia.

VANTAGE IQ

ADD-ON

Nozomi Vantage IQ to pierwszy w branży silnik analizy i reagowania, oparty na zasadach sztucznej inteligencji, dostępny jako dodatek do chmury Vantage. Vantage IQ naśladuje wiedzę ekspercką z obszaru bezpieczeństwa, aby zautomatyzować żmudne zadania przeglądania, korelacji i priorytetyzacji ogromnych ilości danych sieciowych, zasobów i alertów. Asystent Vantage IQ jako część chmury Vantage, umożliwia zespołom łatwe tworzenie zapytań na podstawie słów kluczowych w celu uzyskania głębszego wglądu w to, co dzieje się w sieci.
nozominetworks.com/products/vantage-iq

SMART POLLING

ADD-ON

Smart Polling dodaje aktywne odpytywanie do pasywnego odkrywania zasobów, zwiększając śledzenie aktywów, ocenę podatności i monitorowanie bezpieczeństwa.
nozominetworks.com/products/smart-polling

ASSET INTELLIGENCE

ADD-ON

Usługa Asset Intelligence zapewnia regularne aktualizacje profili w celu szybszego i dokładniejszego wykrywania anomalii. Pomaga skoncentrować wysiłki i skrócić średni czas reakcji (MTTR).
nozominetworks.com/products/asset-intelligence

THREAT INTELLIGENCE

ADD-ON

Usługa Threat Intelligence zapewnia bieżącą analizę zagrożeń i luk w zabezpieczeniach OT i IoT. Pomaga być na bieżąco z pojawiającymi się zagrożeniami i nowymi podatnościami oraz skrócić średni czas wykrywania (MTTD).
nozominetworks.com/products/threat-intelligence

Nozomi Networks chroni krytyczną infrastrukturę przed zagrożeniami cybernetycznymi. Nasza platforma w unikalny sposób łączy widoczność sieci i punktów końcowych, wykrywanie zagrożeń oraz analizę opartą na sztucznej inteligencji w celu szybszej i skuteczniejszej reakcji na incydenty. Nasi klienci z całego świata polegają na nas, aby zminimalizować ryzyko i złożoność, jednocześnie maksymalizując odporność operacyjną.

NOZOMI NETWORKS

nozominetworks.com