ОГЛЯД

Nozomi Networks Platform

Єдина інтегрована платформа для уніфікованої видимості та безпеки OT, IoT та критичної інфраструктури

Оскільки підключення до мережі та автоматизація онлайн-процесів стрімко поширюються, проблеми безпеки так само стрімко зростають. Для багатьох компаній управління ризиками та підтримка операційної ефективності починаються з оцінки вразливостей та виявлення загроз.

Глибокий, інтелектуальний аналіз вразливостей, мережевих аномалій, активних загроз та проблем промислових процесів призводить до зниження ризиків безпеки, оптимізації процесів та їхнього покращення, а також швидкого усунення несправностей у складних середовищах OT/IoT. В цьому вам допоможе Nozomi Networks — рішення для забезпечення видимості та кібербезпеки OT та IoT для різноманітних промислових процесів та критично важливих інфраструктурних галузей.

Методологія платформи Nozomi Networks зосереджена на фазах життєвого циклу реагування на інциденти: Видимість, Виявлення, Реагування (Visibility, Detection, Response).

Платформа надає ключові функції для підтримки типових адміністративних, безпекових та мережевих завдань для кожної з описаних нижче фаз.

Видимість

Уніфікована видимість OT та IoT допомагає передбачити потенційні загрози безпеці та надійності задовго до того, як вони вплинуть на робочі процеси.

Перший крок у досягненні безпеки кіберпростору — це розуміння того, що є у вашій мережі, а також передбачення, де можуть виникнути ризики.

Nozomi Networks забезпечує видимість усіх ваших мережевих активів (дротових і бездротових) і кінцевих точок за допомогою детального збору даних, який може виявити вразливості та окреслити, на чому слід зосередити зусилля з управління ризиками. Візуалізуйте підключення пристроїв і схеми передачі трафіку, щоб сприяти аналітиці та дотриманню відповідності стандартам. Прогнозуйте загрози безпеці, перш ніж вони вплинуть на вашу роботу, одночасно зменшуючи ризики та зусилля щодо дотримання відповідностей.

Інтерактивна візуалізація вашої мережі.

Ключові можливості платформи

Пасивне виявлення активів

Виявлення активів в середовищах OT та IoT може бути повністю пасивним завдяки безперервному аналізу дзеркалізованого трафіку, щоб не порушувати критично важливі процеси та не генерувати додатковий трафік.

Візуалізація мережі

Отримайте повний огляд комунікацій пристроїв і схему трафіку, щоб створити візуальну карту, яка пришвидшить дослідження та дозволить швидко виявляти аномалії та інциденти.

База даних вразливостей

Щоб допомогти вам визначити ризики та пріоритети встановлення виправлень, платформа Nozomi Networks підтримує одну з найбільш повних баз даних відомих вразливостей, зібраних командою дослідників та спеціалістів з безпеки по всьому світу.

Workbooks

Інструкції з виправленнями допоможуть розставляти пріоритети для усунення вразливостей, виділяючи найбільш критичні вразливості кінцевих точок.

Asset Intelligence доповнення

Підписка на сервіс Asset Intelligence допомагає організаціям залишатися в курсі новітніх досліджень щодо вразливостей, поточних рівнів виправлень ОС і мікропрограм (прошивок), а також інших порушень безпеки.

Smart Polling доповнення

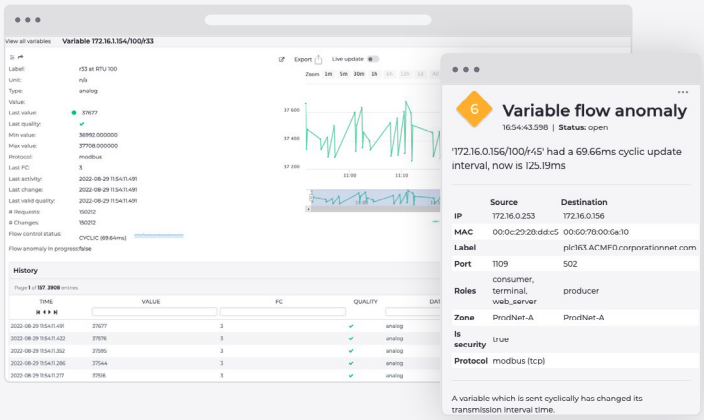
Ця функція точкового опитування активів активно перевіряє пристрої та збирає важливу інформацію про кінцеві точки для підвищення безпеки. Параметри опитування можна налаштувати такий спосіб, щоб мінімально впливати на наявний трафік і пристрої.

Виявлення

Рішення забезпечує виявлення аномалій OT та IoT, щоб допомогти вам діагностувати основні причини неочікуваних змін і відхилень від базової поведінки.

Зменшення ризиків і передбачення потенційних проблем не гарантує усунення всіх нових загроз. Для цього потрібен безперервний моніторинг процесів і трафіку, який допомагає виявляти та діагностувати загрози, а також дає розуміння аномалій технологічних процесів.

Nozomi Networks використовує свій механізм на базі штучного інтелекту / машинного навчання для надання передових галузевих висновків та аналітики. Знання про загрози, що охоплюють безліч сигнатур та індикаторів компрометації (IOC), дозволять вам залишатися обізнаними щодо найновіших атак нульового дня та тенденцій, пов'язаних з програмами-вимагачами.



Змінні процесу можна відстежувати на наявність аномалій, які можуть виникнути через атаку, помилку людини або потенційну механічну несправність.

Ключові можливості платформи

Моніторинг

Порівнюйте зміни в мережевому трафіку та в процесах протягом часу, щоб виявити потенційні загрози та підтримувати максимальну ефективність промислових процесів.

Пакети вмісту (Content Packs)

Пакети вмісту пропонують аналітику щодо поширених проблем і нових загроз, таких як вразливості Industroyer або відповідність стандарту IEC 62443.

Threat Intelligence доповнення

Знаходьте більше загроз на більшій кількості пристроїв завдяки можливостям виявлення вторгнень та підтримці найширшого спектра промислових пристроїв та протоколів. Аналіз загроз допоможе вам залишатися в курсі нових шкідливих програм та індикаторів компрометації (IOC), специфічних для промислових процесів та пристроїв IoT.

Виявлення аномалій

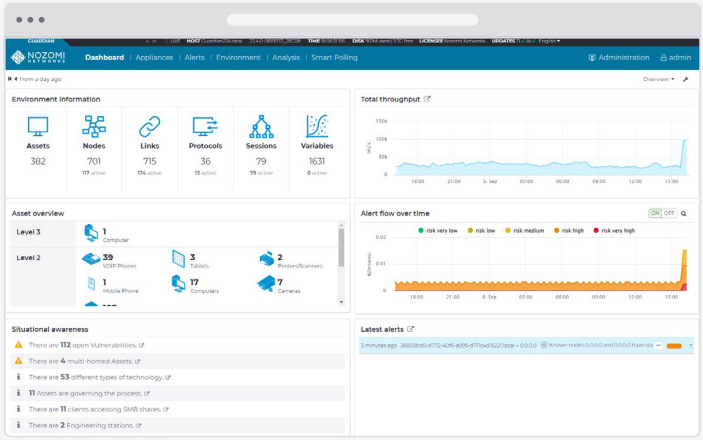
Система Nozomi Networks поступово навчається, щоб допомогти якісніше усувати хибні сповіщення та отримувати глибше розуміння тенденцій процесів. Вийдіть за рамки традиційних показників виявлення аномалій у мережевому трафіку та перейдіть до аналізу тенденцій змінних процесів та даних системи управління, щоб викрити більше порушень та розширити аналіз кореневих причин.

Реагування

Дії на основі даних розвідки та рекомендації виправлення надають вам інформацію, необхідну для швидкого реагування на критичні порушення безпеки OT і IoT, а також на проблеми з управлінням процесами.

Коли виникає необхідність реагувати на порушення безпеки або проблему керування процесами, вам потрібна практична інформація для розв'язання проблеми з мінімальними витратами та впливом на вашу роботу. Nozomi Networks надає вам всю необхідну інформацію та інсайти для усунення проблем, поглиблення досліджень та керування або координації відповідної реакції. Платформа Nozomi збирає величезну кількість даних з пристроїв і мережевого трафіку по всій організації протягом певного періоду часу.

Це завдання може бути виконане практично в необмеженому масштабі за допомогою гнучкої хмарної платформи — Vantage. Зручний користувацький інтерфейс, панелі оповіщення, можливості запитів та інструменти для розслідування інцидентів в платформі дозволяють зробити зібрані дані корисними та доступними для розуміння.



Інформаційні панелі надають всі важливі для вас дані в одному місці. Ви можете налаштовувати дані панелі відповідно до ваших потреб.

Ключові можливості платформи

Машина часу

Функція Машина часу дозволяє користувачам відтворити мережеві події під час інциденту, що допомагає визначити кореневу причину та візуалізувати вплив, щоб зменшити середній час усунення несправностей (MTTR).

Інформаційні панелі та оповіщення

Інформаційні панелі Nozomi Networks призначені для того, щоб надавати вам чіткий та практичний огляд подій, систем, активів, проблем безпеки та оповіщень по всій організації. Фільтрація величезного обсягу інформації дозволяє командам адміністраторів заощаджувати час і зусилля, зосереджуючись на реальних проблемах. Створіть запити по всьому середовищу, щоб швидко ізолювати вразливості, інциденти або визначити активи та провести їх інвентаризацію.

Звіти

Звіти легко генеруються з готових шаблонів, що містять дані про розслідування інцидентів або дані про відповідність. Запити та звіти можуть бути додані в Content Packs або також можна використовувати наявні пакети вмісту від Nozomi Networks та партнерів.

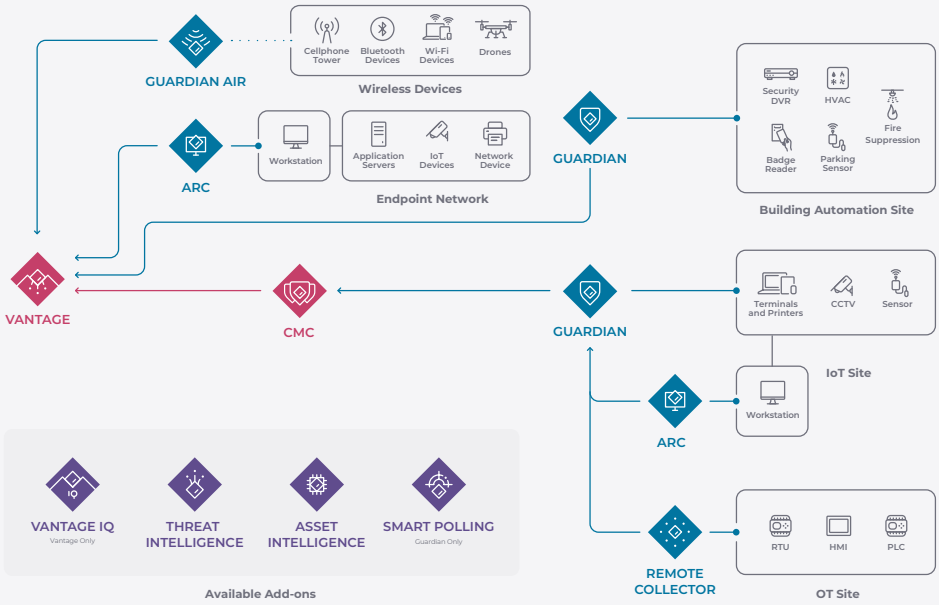
Плейбуки

Плейбуки є критично важливими для координації швидкої реакції на інцидент або збій. Nozomi Networks дозволяє вам імпортувати або створювати власні плейбуки безпеки для визначення кроків з відновлення для будь-якого типу інциденту. Кроки можна налаштувати під конкретних адміністраторів або керівників на основі типу або місця виникнення інциденту. Слідуйте описаним крокам плейбука, щоб узгодити реагування на інцидент із робочим процесом та інтегрувати його з системами тікетів.

Створіть власне рішення

Платформа Nozomi пропонує широкий спектр компонентів і формфакторів для гнучкого розгортання та масштабування в різноманітних промислових і корпоративних середовищах.

Оберіть, як і що розгортати локально та в хмарі для максимальної ефективності.



Доступні доповнення

VANTAGE

SAAS

Nozomi Vantage — це рішення SaaS, яке масштабує моніторинг безпеки та забезпечує огляд для великих багатосайтових підприємств. Водночас воно пропонує переваги, що стосуються вартості та гнучкості хмарного рішення. Vantage надає єдину видимість та моніторинг безпеки для необмеженої кількості вузлів і систем для великого трафіку та інфраструктури активів. Це рішення може спростити розгортання локальних сенсорів Guardian та зменшити складність керування кількома пристроями CMC.

nozominetworks.com/products/vantage

CENTRAL MANAGEMENT CONSOLE

EDGE

PUBLIC CLOUD

Центральна консоль управління (CMC) Nozomi об'єднує безпеку та видимість операційних технологій (OT) та інтернету речей (IoT) у всіх мережах. Це полегшує моніторинг та розставлення пріоритетів щодо вразливих місць і ризиків. Система допомагає виявляти та нейтралізувати нові загрози, а також швидко отримувати відповіді на запитання за допомогою потужного інструменту запиту даних за будь-якими операційними показниками.

nozominetworks.com/products/central-management-console

GUARDIAN

EDGE

PUBLIC CLOUD

Nozomi Guardian — це локальні сенсори, які збирають та аналізують ваші операційні дані. Вони усувають сліпі зони у вашому операційному середовищі, забезпечуючи видимість активів, потоку даних та мережі для середовищ OT та IoT. Сенсори Guardian виявляють кіберзагрози, операційні загрози та вразливі місця, забезпечуючи ситуаційну обізнаність, що є критичним для організації безпеки та відповідності стандартам. Вони ефективні для всіх операційних систем/підсистем, включно з промисловими контролерами, датчиками IoT, системами відеоспостереження, системами автоматизації будівель та для специфічних умов розміщення.

nozominetworks.com/products/guardian

GUARDIAN AIR

ADD-ON

Nozomi Guardian Air — це перший у галузі бездротовий сенсор для середовищ OT та IoT. Датчик моніторить основні частоти передачі даних, забезпечуючи видимість бездротових активів, безперервне виявлення загроз та оцінку вразливості бездротових мереж у вашому середовищі OT та IoT. Його дані можна об'єднати в Vantage разом з іншими мережевими даними для цілісного уявлення про ваше середовище.

nozominetworks.com/products/guardian-air

ARC

EDGE

PUBLIC CLOUD

Nozomi Arc — це агенти для кінцевих точок, які працюють на хостах Windows, Linux або macOS в мережах критичної інфраструктури. Тепер клієнти можуть легко виявляти скомпрометовані хости зі шкідливим програмним забезпеченням, неавторизованими програмами, незареєстрованими USB-накопичувачами та підозрілою активністю. Зібрані дані можна надсилати на Guardian або Vantage.

nozominetworks.com/products/arc

REMOTE COLLECTOR

ADD-ON

Nozomi Remote Collector — це сенсори з низьким споживанням ресурсів, які збирають дані з ваших розподілених мереж і надсилають їх на Guardian для аналізу. Вони покращують огляд, водночас скорочуючи витрати на розгортання.

VANTAGE IQ

ADD-ON

Nozomi Vantage IQ — це перший в галузі інструмент аналізу та реагування на базі штучного інтелекту. Доступний як доповнення до Vantage. Vantage IQ імітує знання досвідчених адміністраторів безпеки у великих мережах за значно меншу вартість. Він також автоматизує трудомісткі завдання з перегляду, співвідношення та пріоритетності величезної кількості даних мережі, активів та оповіщень.

nozominetworks.com/products/vantage-iq

SMART POLLING

ADD-ON

Smart Polling додає можливість фокусного активного опитування до пасивно виявлених активів Guardian, покращуючи відстеження активів, оцінку вразливості та моніторинг безпеки.

nozominetworks.com/products/smart-polling

ASSET INTELLIGENCE

ADD-ON

Сервіс Asset Intelligence надає регулярні оновлення профілів пристроїв для швидшого та точнішого виявлення аномалій. Він допомагає зосередити зусилля команд безпеки та скоротити середній час реагування (MTTR).

nozominetworks.com/products/asset-intelligence

THREAT INTELLIGENCE

ADD-ON

Сервіс Threat Intelligence забезпечує постійний пошук загроз і вразливостей операційних технологій (OT) та інтернету речей (IoT). Він допомагає вам стежити за новими загрозами та вразливостями, а також скоротити середній час виявлення (MTTD).

nozominetworks.com/products/threat-intelligence

Nozomi Networks захищає світову критичну інфраструктуру від кіберзагроз. Платформа унікально поєднує видимість мережі та кінцевих точок, виявлення загроз і аналіз за допомогою ШІ для швидшого й ефективнішого реагування на інциденти. Завдяки рішенню Nozomi Networks промислові компанії можуть мінімізувати ризики та ефективно проводити моніторинг безпеки, одночасно максимізуючи операційну стійкість.

NOZOMI NETWORKS

nozominetworks.bakotech.com

nozomi@bakotech.com