ОБЗОР

Nozomi Networks Platform

Единая интегрированная платформа для унифицированной видимости и безопасности OT, IoT и критической инфраструктуры

Поскольку подключение к сети и автоматизация онлайн-процессов стремительно распространяются, проблемы безопасности так же стремительно растут. Для многих компаний управление рисками и поддержка операционной эффективности начинаются с оценки уязвимостей и обнаружения угроз.

Глубокий, интеллектуальный анализ уязвимостей, сетевых аномалий, активных угроз и проблем промышленных процессов приводит к снижению рисков безопасности, оптимизации процессов и их улучшению, а также к быстрому устранению неисправностей в сложных средах OT/IoT. В этом вам поможет Nozomi Networks — решение для обеспечения видимости и кибербезопасности OT и IoT для различных промышленных процессов и критически важных инфраструктурных отраслей.

Методология платформы Nozomi Networks сосредоточена на фазах жизненного цикла реагирования на инциденты: видимость, выявление, реагирование (Visibility, Detection, Response).

Платформа предоставляет ключевые функции для поддержки типичных административных, сетевых задач и задач безопасности для каждой из описанных ниже фаз.

nozominetworks.bakotech.com
nozomi@bakotech.com

Видимость

Унифицированная видимость OT и IoT помогает предугадать потенциальные угрозы безопасности и надежности задолго до того, как они повлияют на рабочие процессы.

Первый шаг в достижении безопасности киберпространства — понимание того, что находится в вашей сети, а также предвидение, где могут возникнуть риски.
Nozomi Networks обеспечивает видимость всех ваших сетевых активов (проводных и беспроводных) и конечных точек с помощью детального сбора данных, который может обнаружить уязвимости и определить, на чем следует сосредоточить усилия по управлению рисками. Визуализируйте подключение устройств и схемы передачи трафика, чтобы способствовать аналитике и соблюдению соответствия стандартам. Прогнозируйте угрозы безопасности, прежде чем они повлияют на вашу работу, одновременно уменьшая риски и усилия по соблюдению соответствий.

Интерактивная визуализация сети.

Ключевые возможности платформы

Пассивное обнаружение активов

Выявление активов в средах OT и IoT может быть полностью пассивным благодаря непрерывному анализу зеркалированного трафика, чтобы не нарушать критически важные процессы и не генерировать дополнительный трафик.

Визуализация сети

Получите полный обзор коммуникаций устройств и схему трафика, чтобы создать визуальную карту, которая ускорит исследование и позволит быстро обнаруживать аномалии и инциденты.

База данных уязвимостей

Чтобы помочь определить риски и приоритеты установки исправлений, платформа Nozomi Networks поддерживает одну из наиболее полных баз данных известных уязвимостей, собранных командой исследователей и специалистов по безопасности по всему миру.

Workbooks

Инструкции с исправлениями помогут расставлять приоритеты для устранения уязвимостей, выделяя наиболее критические уязвимости конечных точек.

Asset Intelligence дополнение

Подписка на сервис Asset Intelligence помогает организациям оставаться в курсе новейших исследований по уязвимости, текущих уровней исправлений ОС и микропрограмм (прошивок), а также других нарушений безопасности.

Smart Polling дополнение

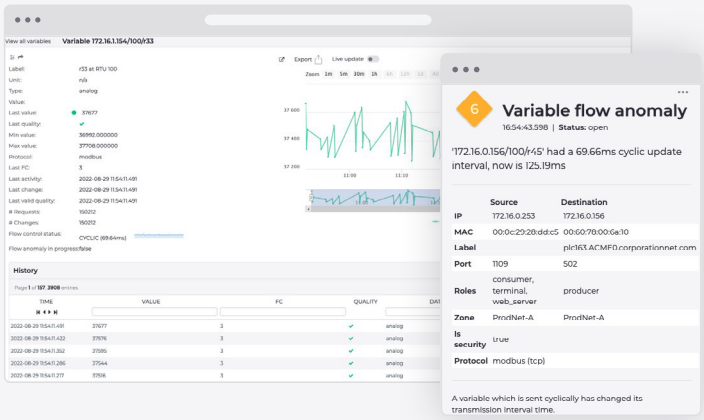
Эта функция точечного опроса активов активно проверяет устройства и собирает важную информацию о конечных точках для повышения безопасности. Параметры опроса можно настроить таким образом, чтобы минимально влиять на текущий трафик и устройства.

Обнаружение

Решение обеспечивает выявление аномалий OT и IoT, чтобы помочь диагностировать основные причины неожиданных изменений и отклонений от базового поведения.

Уменьшение рисков и предсказание потенциальных проблем не гарантирует устранения всех новых угроз. Для этого требуется непрерывный мониторинг процессов и трафика, который помогает выявлять и диагностировать угрозы, а также дает понимание аномалий технологических процессов.

Nozomi Networks использует свой механизм на базе искусственного интеллекта/машинного обучения для предоставления передовых отраслевых выводов и аналитики. Знания об угрозах, включающих множество сигнатур и индикаторов компрометации (IOC), позволят вам оставаться в курсе новейших атаках нулевого дня и тенденций программ-вымогателей.



Переменные процесса можно отслеживать на наличие аномалий, которые могут возникнуть из-за атаки, ошибки человека или потенциальной механической неисправности.

Ключевые возможности платформы

Мониторинг

Сравнивайте изменения в сетевом трафике и процессах в течение времени, чтобы выявить потенциальные угрозы и поддерживать максимальную эффективность промышленных процессов.

Пакеты содержимого (Content Packs)

Пакеты содержимого предлагают аналитику относительно распространенных проблем и новых угроз, таких как уязвимость Industroyer или соответствие стандарту IEC 62443.

Threat Intelligence дополнение

Находите больше угроз на большем количестве устройств благодаря возможностям обнаружения вторжений и поддержке широкого спектра промышленных устройств и протоколов. Анализ угроз поможет вам оставаться в курсе новых вредоносных программ и индикаторов компрометации (IOC), специфичных для промышленных процессов и устройств IoT.

Выявление аномалий

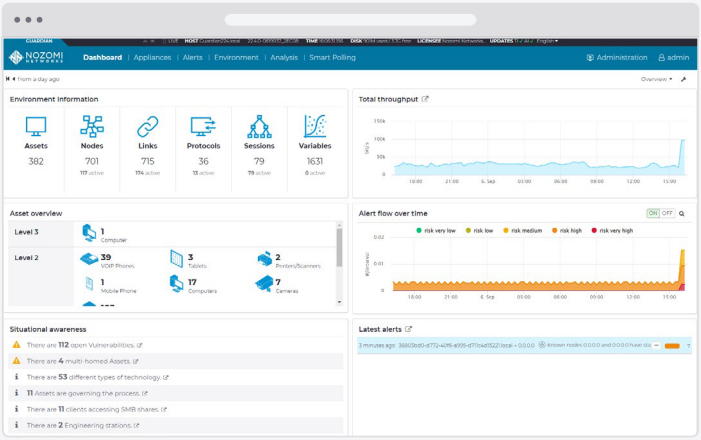
Система Nozomi Networks постепенно учится, чтобы помочь более качественно устранять ложные уведомления и получать более глубокое понимание тенденций процессов. Выйдите за рамки традиционных показателей обнаружения аномалий в сетевом трафике и перейдите к анализу тенденций переменных процессов и данных системы управления, чтобы разоблачить больше нарушений и расширить анализ корневых причин.

Реагирование

Действия на основе данных разведки и рекомендации исправления предоставляют вам информацию, необходимую для быстрого реагирования на критические нарушения безопасности OT и IoT, а также на проблемы управления процессами.

Когда возникает необходимость реагировать на нарушение безопасности или проблему управления процессами, нужна практическая информация для решения проблемы с минимальными затратами и влиянием на вашу работу. Nozomi Networks предоставляет вам всю необходимую информацию и инсайты для устранения проблем, углубления исследований и управления или координации ответной реакции. Платформа Nozomi собирает огромное количество данных с устройств и сетевого трафика по всей организации в течение определенного периода времени.

Эта задача может быть выполнена практически в неограниченном масштабе с помощью гибкой облачной платформы – Vantage. Удобный пользовательский интерфейс, панели оповещения, возможности запросов и инструменты для расследования инцидентов в платформе позволяют сделать собранные данные полезными и доступными для понимания.



Информационные панели предоставляют все важные для вас данные в одном месте. Вы можете настраивать данные панели в соответствии с вашими потребностями.

Ключевые возможности платформы

Машина времени

Функция Машина времени позволяет пользователям воспроизвести сетевые события во время инцидента, что дает возможность определить корневую причину и визуализировать влияние, чтобы уменьшить среднее время устранения неисправностей (MTTR).

Информационные панели и оповещения

Информационные панели Nozomi Networks предназначены для того, чтобы дать вам четкий и практический обзор событий, систем, активов, проблем безопасности и оповещений по всей организации. Фильтрация огромного объема информации позволяет командам администраторов экономить время и усилия, сосредотачиваясь на реальных проблемах. Создайте запросы по всей среде, чтобы быстро изолировать уязвимости, инциденты или определить и провести инвентаризацию активов.

Отчеты

Отчеты легко генерируются из готовых шаблонов, включающих данные по расследованию инцидентов или данные о соответствии. Запросы и отчеты могут быть добавлены в Content Packs или можно использовать существующие пакеты содержимого от Nozomi Networks и партнеров.

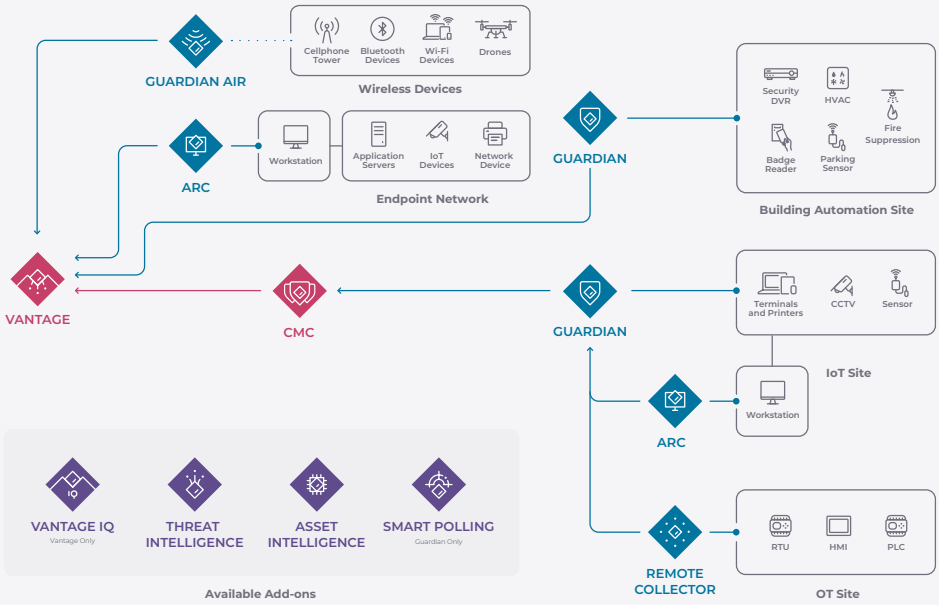
Плейбуки

Плейбуки критически важны для координации быстрой реакции на инцидент или сбой. Nozomi Networks позволяет вам импортировать или создавать собственные плейбуки безопасности для определения шагов восстановления для любого типа инцидента. Шаги можно настроить под конкретных администраторов или руководителей на основе типа или места возникновения инцидента. Следуйте описанным шагам плейбука, чтобы согласовать реагирование на инцидент с рабочим процессом и интегрировать его с системами тикетов.

Создайте собственное решение

Платформа Nozomi предлагает широкий спектр компонентов и формфакторов для гибкого развертывания и масштабирования в различных промышленных и корпоративных средах.

Выберите, как и что разворачивать локально и в облаке для максимальной эффективности.



Доступные дополнения

VANTAGE

SAAS

Nozomi Vantage — это решение SaaS, масштабирующее мониторинг безопасности и обеспечивающее обзор для крупных многосайтовых предприятий. В то же время оно предлагает преимущества, касающиеся стоимости и гибкости облачного решения. Vantage дает единую видимость и мониторинг безопасности для неограниченного количества узлов и систем для большого трафика и инфраструктуры активов. Это решение может упростить развертывание локальных сенсоров Guardian и уменьшить сложность управления несколькими устройствами CMC.

nozominetworks.com/products/vantage

CENTRAL MANAGEMENT CONSOLE

EDGE

PUBLIC CLOUD

Центральная консоль управления (CMC) Nozomi объединяет безопасность и видимость операционных технологий (OT) и интернет вещей (IoT) во всех сетях. Это облегчает мониторинг и расстановку приоритетов относительно уязвимых мест и рисков. Система помогает выявлять и нейтрализовать новые угрозы, а также быстро получать ответы на вопросы с помощью мощного инструмента запроса данных по любым операционным показателям.

nozominetworks.com/products/central-management-console

GUARDIAN

EDGE

PUBLIC CLOUD

Nozomi Guardian – это локальные сенсоры, которые собирают и анализируют ваши операционные данные. Они устраняют слепые зоны в вашей операционной среде, обеспечивая видимость активов, потока данных и сети для OT и IoT. Сенсоры Guardian обнаруживают киберугрозы, операционные угрозы и уязвимые места, обеспечивая ситуационную осведомленность, критическую для обеспечения безопасности и соответствия стандартам. Они эффективны для всех операционных систем/подсистем, включая промышленные контроллеры, датчики IoT, системы видеонаблюдения, системы автоматизации зданий и для специфических условий размещения.

nozominetworks.com/products/guardian

GUARDIAN AIR

ADD-ON

Nozomi Guardian Air – это первый в отрасли беспроводной сенсор для сред OT и IoT. Сенсор мониторит основные частоты передачи данных, обеспечивая видимость беспроводных активов, непрерывное обнаружение угроз и оценку уязвимости беспроводных сетей в среде OT и IoT. Его данные могут быть объединены в Vantage вместе с другими сетевыми данными для целостного представления вашей среды.

nozominetworks.com/products/guardian-air

ARC

EDGE

PUBLIC CLOUD

Nozomi Arc – это агенты для конечных точек, работающих на хостах Windows, Linux или macOS в сетях критической инфраструктуры. Теперь клиенты могут легко обнаруживать скомпрометированные хосты с вредоносным программным обеспечением, неавторизованными приложениями, незарегистрированными USB-накопителями и подозрительной активностью. Собранные данные можно передавать на Guardian или Vantage.

nozominetworks.com/products/arc

REMOTE COLLECTOR

ADD-ON

Nozomi Remote Collector – это сенсоры с низким потреблением ресурсов, которые собирают данные из ваших распределенных сетей и отправляют их на Guardian для анализа. Они улучшают обзор, одновременно сокращая расходы на развертывание.

VANTAGE IQ

ADD-ON

Nozomi Vantage IQ – это первый в области инструмент анализа и реагирования на базе искусственного интеллекта. Доступный как дополнение к Vantage. Vantage IQ имитирует знания опытных администраторов безопасности в крупных сетях значительно меньше. Он также автоматизирует трудоемкие задачи по пересмотру, соотношению и приоритетности множества данных сети, активов и оповещений.

nozominetworks.com/products/vantage-iq

SMART POLLING

ADD-ON

Smart Polling добавляет возможность фокусного активного опроса к пассивно выявленным активам Guardian, улучшая отслеживание активов, оценку уязвимости и мониторинг безопасности.

nozominetworks.com/products/smart-polling

ASSET INTELLIGENCE

ADD-ON

Сервис Asset Intelligence предоставляет регулярные обновления профилей устройств для более быстрого и более точного обнаружения аномалий. Это помогает сосредоточить усилия команд безопасности и сократить среднее время реагирования (MTTR).

nozominetworks.com/products/asset-intelligence

THREAT INTELLIGENCE

ADD-ON

Сервис Threat Intelligence обеспечивает постоянный поиск угроз и уязвимостей операционных технологий (OT) и интернет вещей (IoT). Он помогает вам следить за новыми угрозами и уязвимостями, а также сократить среднее время обнаружения (MTTD).

nozominetworks.com/products/threat-intelligence

Nozomi Networks защищает мировую критическую инфраструктуру от киберугроз. Платформа уникально сочетает видимость сети и конечных точек, выявление угроз и анализ с помощью ИИ для более быстрого и эффективного реагирования на инциденты. Благодаря решению Nozomi Networks, промышленные компании могут минимизировать риски и эффективно проводить мониторинг безопасности, одновременно достигая максимизации операционной устойчивости.

NOZOMI NETWORKS

nozominetworks.bakotech.com

nozomi@bakotech.com