Платформа XDR для обеспечения комплексной безопасности промышленных предприятий

Kaspersky Industrial CyberSecurity

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Угрозы на компьютеры АСУ

По данным Kaspersky ICS CERT 39,2% компьютеров АСУ ТП в России были атакованы вредоносным программным обеспечением во втором полугодии 2022 года и их количество постоянно растет.

Kaspersky ICS CERT, март 2023 г.

Подробнее

Киберугрозы для АСУ и промышленных предприятий

Рост интереса хактивистов к системам автоматизации, увеличение числа APT-угроз в промышленном сегменте, уход зарубежных вендоров с российского рынка, ослабление уровня защищенности, новые регуляторные требования — 2022 год был богат на события кибербезопасности. Он доставил много проблем для владельцев и операторов промышленных инфраструктур.

Наиболее значимые изменения в ландшафте угроз для промышленных предприятий и OT-инфраструктур будут теперь определяться, прежде всего, геополитическими и связанными с ними макроэкономическими факторами, и в скором будущем мы увидим смещение отраслевого фокуса активности APT.

По данным Kaspersky ICS CERT, в числе мишеней атак все чаще будут встречаться организации **из следующих секторов экономики:**

Сельское хозяйство, производство удобрений, сельхозтехники и продуктов питания

Ввиду маячащих продовольственных кризисов и переделов продовольственных рынков

Логистика и транспорт (включая транспорт энергоресурсов)

Ввиду начавшихся глобальных перестроений логистических цепочек

Энергетика, добыча и обработка полезных ископаемых, цветная и черная металлургия, химическая промышленность, судостроение, приборо- и станкостроение

Поскольку доступность продукции этих компаний и их технологий входят в фундамент экономической безопасности стран и политических альянсов

Хайтек-компании, фармацевтика и производство медицинского оборудования

Поскольку они необходимы для обеспечения технологической независимости

Среди основных целей APT будет прослеживаться и традиционный фокус на:

Критическая инфраструктура

Атаки с целью закрепиться на «черный день», а в некоторых случаях и с целью нанесения прямого ущерба

Госучреждения

Атаки для сбора всевозможного рода информации об инициативах и проектах государства, связанных с развитием промышленных секторов экономики

Предприятия ВПК

Главные факторы активности атакующих — геополитическая напряженность

Устойчивое развитие промышленных предприятий и объектов критической инфраструктуры напрямую зависит от стабильности производственных и бизнес-процессов и защиты важных активов. В эпоху четвертой промышленной революции число атак на промышленные системы, в частности на системы АСУ ТП и SCADA, продолжает расти. При этом традиционные решения не способны защитить промышленные среды от новых киберугроз. Постоянно меняющаяся ИБ-реальность и необходимость соответствовать требованиям регулирующих органов побуждают организации к внедрению специализированных средств киберзащиты промышленных инфраструктур.

Именно поэтому сегодня как никогда важен выбор надежного партнера, который обладает экспертизой на стыке промышленной и корпоративной кибербезопасности и готов предложить полный арсенал расширенных защитных технологий.

Узнать больше о киберугрозах для АСУ и промышленных предприятий в 2023 году

Подробнее

Передовые технологии защиты АСУ ТП

Благодаря единой XDR платформе Kaspersky Industrial CyberSecurity ИБ-специалист видит общую картину того, что происходит в технологической сети: серии инцидентов в сети на уровне рабочих мест, точные параметры активов, карты сетевых коммуникаций даже для сегментов, для которых зеркалирование трафика пока невозможно, и многое другое.

Kaspersky Industrial CyberSecurity (KICS) — это специализированная промышленная XDR-платформа, разработанная для комплексной защиты основных компонентов систем автоматизации и управления производством на всех уровнях. Благодаря безупречной интеграции компонентов платформы друг с другом вы сможете централизованно контролировать все разрозненные промышленные сети, рабочие места и системы автоматизации. Это способствует повышению осведомленности о ситуации и более эффективному противодействию сложным угрозам.

XDR-платформа состоит из двух взаимодополняющих компонентов. KICS for Nodes защищает промышленные рабочие места, в то время как KICS for Networks следит за безопасностью промышленных сетей. Пассивный мониторинг помогает собирать данные не перегружая сеть и без нежелательного воздействия на чувствительные компоненты АСУ ТП. Возможность активного опроса сети позволяет быстро и точно собирать данные о топологии сетей и настройках. Функция аудита рабочих мест помогает гарантировать соблюдение политик безопасности, включая безопасность текущих настроек, и организацию процесса выявления и митигации уязвимостей.

Kaspersky Industrial CyberSecurity for Nodes

Инструменты класса EPP и EDR

Предназначено для защиты рабочих станций и серверов в рамках промышленной сети и усиливается встроенной EDR-функциональностью для работы со сложными инцидентами

- Сервер
- Портативные сканеры
- Рабочая станция

Kaspersky Industrial CyberSecurity

- Единая консоль
- Нативная интеграция
- Кросс-продуктовые сценарии
- Общий kill-chain
- Управление рисками и активами

Kaspersky Industrial CyberSecurity for Networks

Анализ трафика ICS DPI и IDS

Предназначено для анализа трафика на уровне промышленных протоколов для выявления сложных киберугроз и реагирования на них

- Сервер
- Сенсор

Точки применения платформы

Конвергенция OT- и IT-сред

DMZ / GTW

IT-среда

OT-среда

Kaspersky Industrial CyberSecurity for Nodes

- Рабочая станция оператора
- Сервер SCADA
- Рабочая станция инженера

Коммутатор

Зазеркаливание / SPAN

Kaspersky Industrial CyberSecurity for Networks

- Контроллер присоединения (BCU)
- Интеллектуальное электронное устройство (IED)
- Контроллеры Реле
- Программируемые логические контроллеры (PLC)

Kaspersky Machine Learning for Anomaly Detection

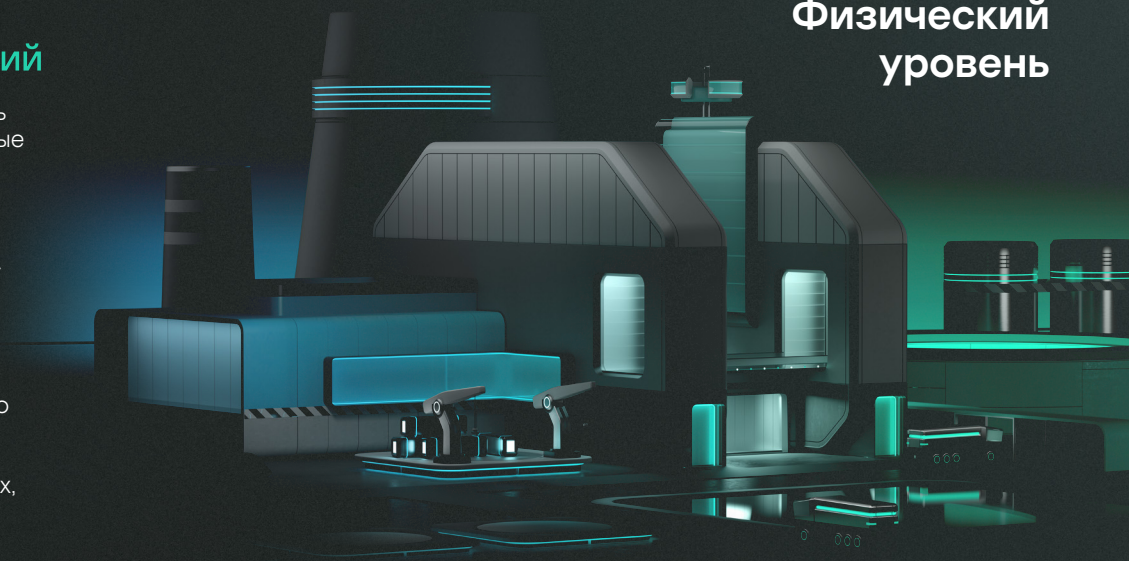
MLAD

Система раннего обнаружения аномалий

Решение помогает предотвратить отказы, аварии, незапланированные простои промышленного оборудования, выявив признаки проблемы и аномалии задолго до того, как они повлияют на работу предприятия. Kaspersky MLAD использует нейронные сети, машинное обучение, диагностические правила и интегрируется с KICS for Networks для более эффективного обнаружения отклонений в технологическом процессе или в работе оборудования, связанных, в том числе, с действиями киберпреступников.

Подробнее

Физический уровень



Защищается с помощью продуктов «Лаборатории Касперского»

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Решение для мониторинга промышленной сети и анализа трафика на уровне проприетарных протоколов, поставляемое в виде программного продукта или виртуального устройства, подключаемого к АСУ ТП.

KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранних этапах и предоставляет необходимую информацию для предотвращения ущерба технологическим процессам.

Преимущества

Обнаружение устройств

Пассивная идентификация и учет устройств в промышленной сети

Deep Packet Inspection (DPI)

Анализ телеметрии технологических параметров практически в режиме реального времени

Контроль целостности сети

Обнаружение несанкционированных узлов и соединений

Система обнаружения вторжений

Оповещения о вредоносной активности в сети и признаках эксплуатации уязвимостей

Контроль команд

Проверка команд, передаваемых по промышленным протоколам

Поддержка внешних систем

Обнаружение угроз внешними системами благодаря интеграции через API

Использование машинного обучения для обнаружения аномалий (Kaspersky MLAD)

Позволяет выявлять аномалии в цифровых и физических процессах с помощью телеметрии в режиме реального времени и обработки исторических данных (рекуррентная нейронная сеть)

Обнаружение уязвимостей

Обновляемая база уязвимостей промышленного оборудования

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

KICS for Nodes обеспечивает защиту рабочих мест в рамках промышленной сети. Решение поставляется в виде программного обеспечения для компьютеров с встроенной ICS EDR функциональностью.

- Контроль запуска программ
- Антивирус
- Контроль подключаемых USB-устройств
- Проверка целостности файлов/папок и проектов ПЛК
- Защита от шифрования
- Анализ логов ОС
- Аудит безопасности
- Выявление уязвимостей
- Защита от сетевых атак
- Базовые EDR-сценарии: инструменты расследования и реагирования

Преимущества

Производительность

Незначительно влияние на защищаемые устройства, что помогает сохранить максимальную производительность систем

Широкое покрытие

- Все Windows, начиная с XP SP2 и Server 2003 SP1
- Портативный сканер
- Более 30 ОС на базе Linux

Расширенная защита

- Защита от вредоносного ПО, шифрования и эксплойтов
- Анализ журналов
- Управление сетевым экраном
- Встроенная технология ICS EDR

Модульная архитектура

С гибкими возможностями и настройкой без влияния на технологический процесс

Поддержка различных устройств

На базе операционных систем семейств Windows и Linux

Аудит

Комплексный аудит уязвимостей и соответствие требованиям

Преимущества интеграции с KUMA

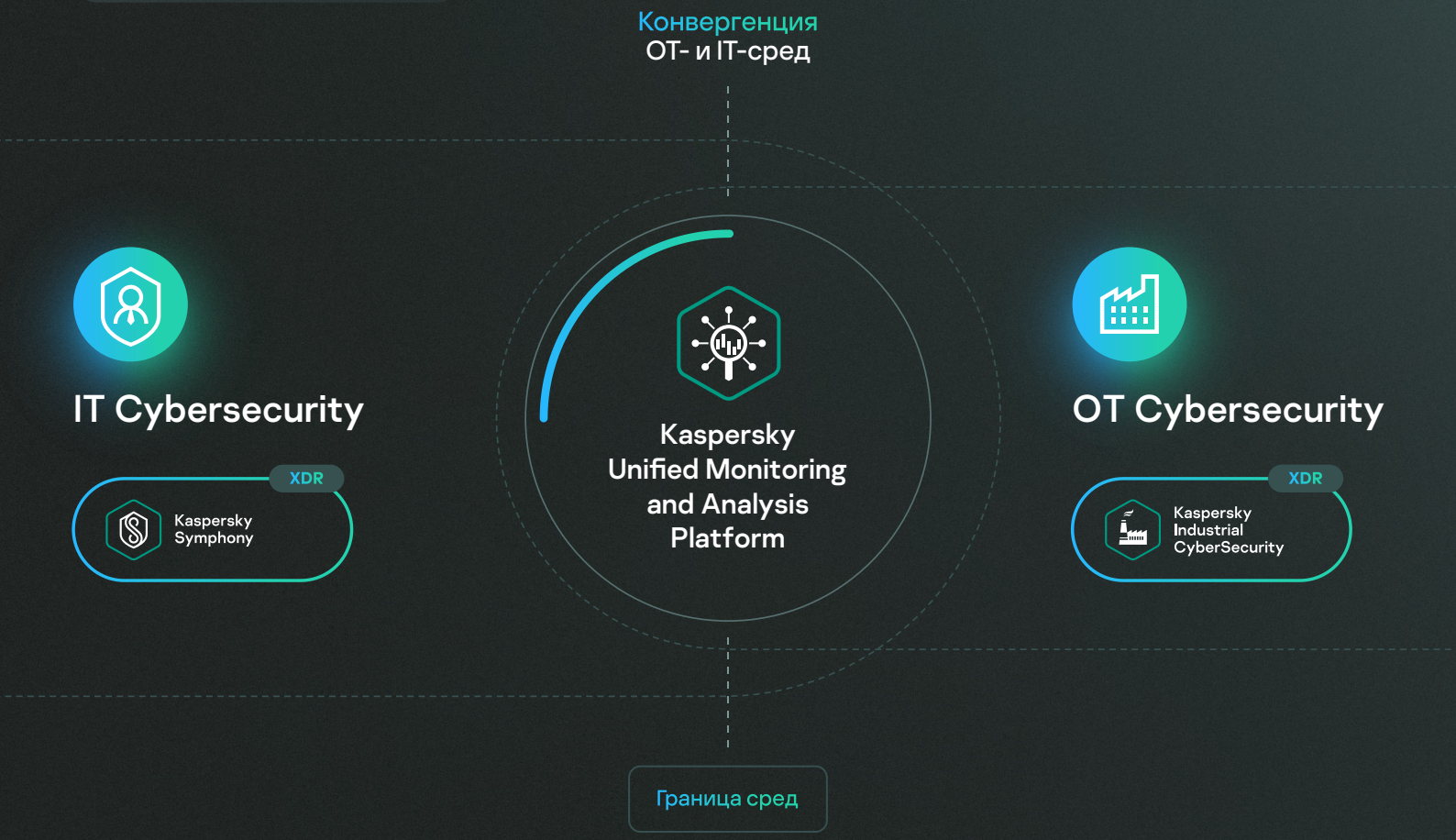
- Цельное предложение для защиты OT- и IT-сред
- Унифицированные правила детектирования, единая база активов, кросс-сценарии для двух сегментов (OT и IT)
- Поддержка разделения на логические домены (тенанты) в рамках одного SIEM
- Инвентаризация информационных активов и базовое реагирование
- Потоковое обогащение событий и обогащение событий по запросу
- Поддержка сценариев реагирования

Единая киберзащита промышленного и корпоративного сегментов одного предприятия

Число атак на промышленные системы, в частности на системы АСУ ТП и SCADA, продолжает расти. Именно поэтому сегодня как никогда важен выбор надежного партнера, который обладает экспертизой на пересечении промышленной и корпоративной кибербезопасности и готов предложить комплексный подход, способный обезопасить промышленную и корпоративную среду от актуальных киберугроз.

Благодаря тесной интеграции с SIEM-системой Kaspersky Unified Monitoring and Analysis Platform (KUMA) платформа Kaspersky Industrial CyberSecurity позволяет реализовывать больше сценариев взаимодействия с решениями сторонних поставщиков и расширить действия по расследованию и реагированию.
Это также позволяет защищать бизнес не только в промышленной среде, но и в той части, где промышленная среда пересекается с корпоративной, тесно взаимодействуя с корпоративной XDR-платформой Kaspersky Symphony XDR.

Подробнее



Глобальное присутствие, опыт и знания мирового уровня

Высокий статус в индустрии безопасности IT-/OT-систем

Более 80 сертификатов о совместимости с решениями вендоров АСУ ТП

Доказанная эффективность технологий и соответствие стандартам

ICS CERT

Собственное международное подразделение ICS CERT

Клиенты по всему миру

РОСАТОМ, НОРНИКЕЛЬ, Северсталь, KAMAZ, TATNEFT, РОССЕТИ, НЛМК, alperia, PacificLight, КазМунайГаз

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Networks

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее