Платформа XDR для обеспечения комплексной безопасности промышленных предприятий

Kaspersky Industrial CyberSecurity

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Угрозы на компьютеры АСУ

По данным Kaspersky ICS CERT, 31,9% компьютеров АСУ в России были атакованы вредоносным программным обеспечением в первом полугодии 2023 года.

Kaspersky ICS CERT, сентябрь 2023 г.

Подробнее

Среди основных целей APT атак:

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

Узнать больше о техниках, тактиках и процедурах атак на промышленные компании на примере имплантов для удаленного доступа

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 — новая реальность 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

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 АСУ ТП и SCADA, продолжает расти. При этом традиционные решения не способны защитить промышленные среды от новых киберугроз.

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.

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.

Взаимодействие компонентов платформы:

- Статус защиты
- Аудит безопасности
- Сетевые коммуникации
- Передача телеметрии хоста
- Контроль оборудования
- Реагирование на инциденты

Передовые технологии защиты АСУ ТП

Kaspersky Industrial CyberSecurity (KICS) — это специализированная промышленная XDR-платформа, разработанная для комплексной защиты основных компонентов систем автоматизации и управления производством на всех уровнях. Благодаря отличной 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

Защита конечных точек, усиленная технологией EDR

- Сервер
- Рабочая станция
- Портативные сканеры

Kaspersky Industrial CyberSecurity

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

Kaspersky Industrial CyberSecurity for Networks

Защита промышленных устройств от сетевых угроз

- Сервер
- Сенсор

Ответные действия

- Изоляция хоста
- Запрет запуска
- Карантин

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
- Шлюз АСУ ТП

Коммутатор

Зеркалирование / SPAN

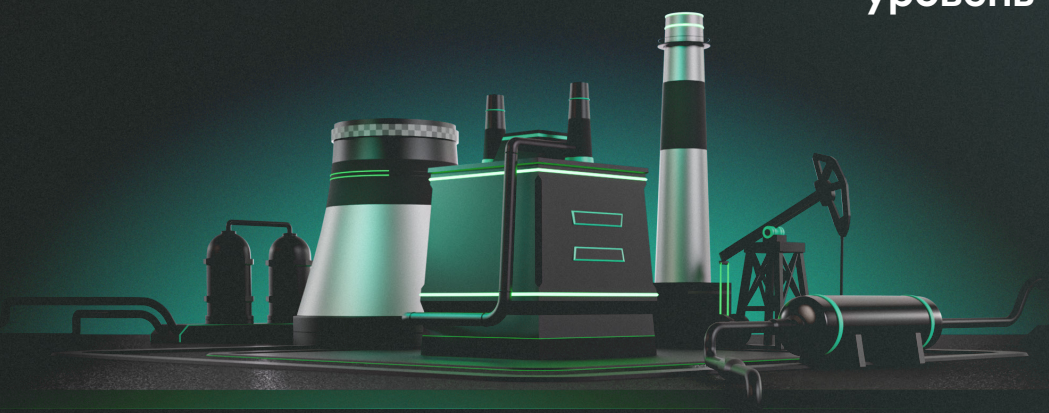
Kaspersky Industrial CyberSecurity for Networks

- Контроллер присоединения (BCU)
- Интеллектуальное электронное устройство (IED)
- Программируемые логические контроллеры (PLC)
- Релейная и противоаварийная защита
- Автономные подсистемы (ручная проверка с помощью KICS Portable Scanner)

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.

Физический уровень



Подробнее

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.

KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранних этапах, демонстрирует развитие атаки как по сети, так и на узлах (EDR киллчейн и телеметрию), позволяет выполнять ответные действия на уровне узлов и сетевого оборудования.

Работая на предупреждение инцидентов, решение помогает обнаружить и ранжировать риски на основе данных об уязвимостях, сетевых соединениях и важности различных активов.

Обнаружение устройств

Идентификация и учет устройств в промышленной сети

Deep Packet Inspection (DPI)

Анализ параметров технологического процесса 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

Обмен данными об обнаруженных активах или событиях безопасности благодаря интеграции через API

Централизованный аудит узлов промышленной сети

KICS for Networks осуществляет централизованный аудит узлов промышленной сети: агентский (при помощи KICS for Nodes) и безагентский аудит конечных точек и сетевого оборудования на предмет уязвимостей и соответствия требованиям ИБ при помощи формата OVAL* и XCCDF**.

- Обновляемые базы уязвимостей промышленного оборудования Kaspersky ICS CERT
- Поддержка базы данных уязвимостей ФСТЭК
- Проверка на соответствие приказам ФСТЭК
- Отчеты для одного узла или единый общий отчет по всем аудитам сети
- Защищенное хранилище учетных записей для всех узлов сети
- Редактор правил для создания пользовательских политик

* Open Vulnerability and Assessment Language (OVAL) (открытый язык описания и оценки уязвимостей).
** The Extensible Configuration Checklist Description Format (XCCDF) (расширяемый формат описания контрольных листов настроек).

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.

KICS for Nodes Portable Scanner — портативная версия решения, не требующая установки. Подходит для регулярного сканирования изолированных подсистем и оборудования, а также гостевых устройств, на которые невозможно поставить полнофункциональное решение.

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

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
- 34 семейства 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

Проверка целостности:

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200
- Schneider Electric Modicon M340, M580
- Устройства на базе CODESYS V3
- ОВЕН ПЛК210
- Fastwel CPM723-01
- Прософт-Системы Regul R500
- Siemens серии SIPROTEC 4

Аудит

Комплексный аудит безопасности уязвимостей и соответствие требованиям на базе открытого стандарта OVAL

Преимущества интеграции с KUMA

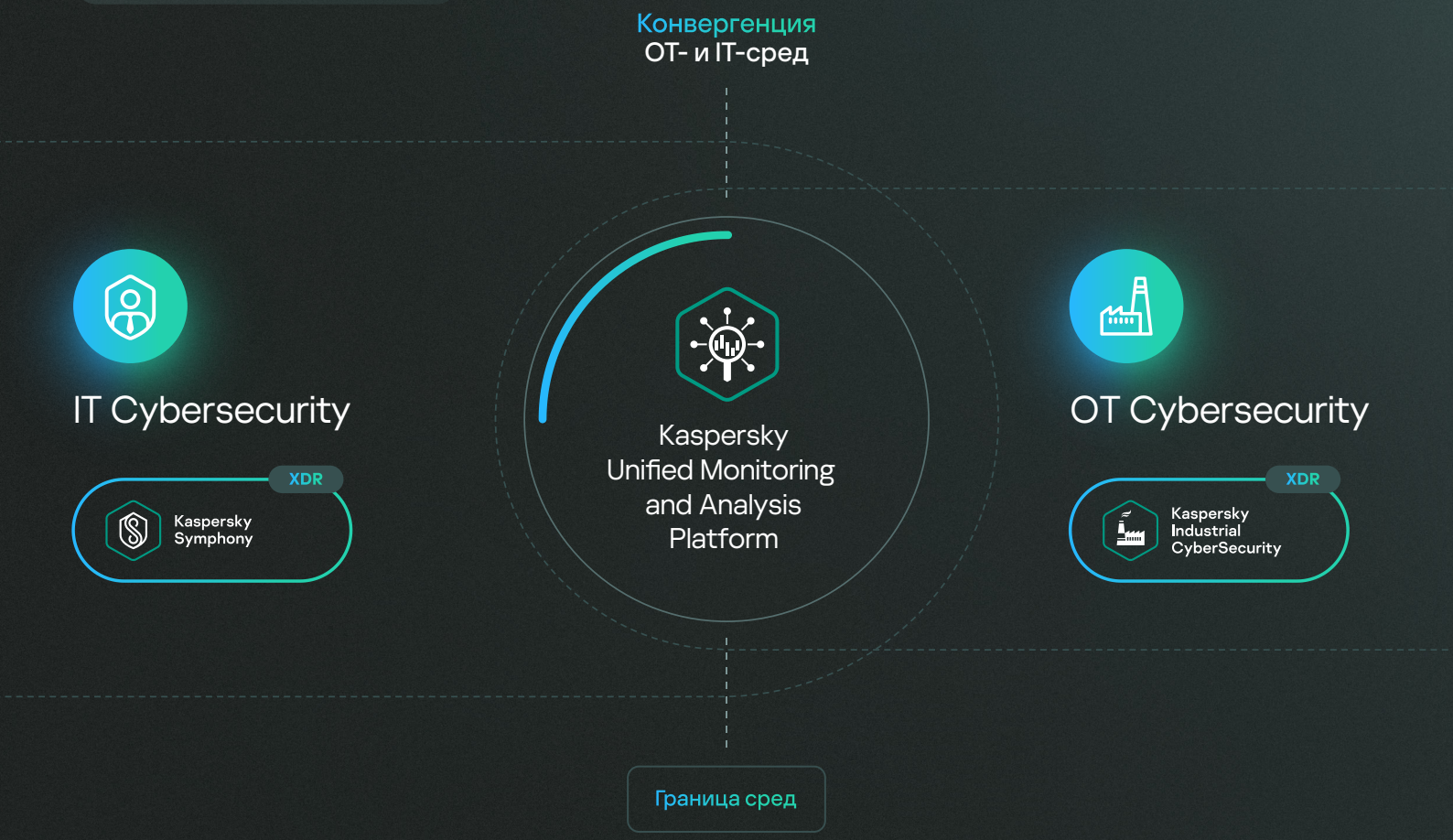
- Цельное предложение для защиты OT- и IT-сред
- Унифицированные правила детектирования, единая база активов, кросс-сценарии для двух сегментов (OT и IT)
- Поддержка разделения на логические домены (тенанты) в рамках одного SIEM
- Инвентаризация информационных активов и базовое реагирование
- Потоковое 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 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 100 сертификатов о совместимости с решениями вендоров АСУ ТП

Доказанная эффективность технологий и соответствие стандартам

ICS CERT

Собственное международное подразделение Kaspersky ICS CERT

Клиенты по всему миру

РОСАТОМ · НОРНИКЕЛЬ · ЕвроХим · НЛМК · TATNEFT · РОССЕТИ · alperia · PacificLight · КазМунайГаз

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Kaspersky Industrial CyberSecurity

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее