XDR-платформа для обеспечения комплексной безопасности промышленных предприятий

Kaspersky Industrial CyberSecurity

kaspersky активируй будущее

Атаки вредоносного ПО

В первом квартале 2025 года пострадавшими организациями или ответственными должностными лицами было публично подтверждено 118 инцидентов кибербезопасности, причем 52,5% этих инцидентов пришлись на производственный сектор.

Kaspersky ICS CERT,
июнь 2025 г.

Подробнее

Ландшафт угроз для промышленных систем

Новая реальность для владельцев и операторов промышленных объектов формируется под воздействием ряда факторов, включая растущий интерес хактивистов к системам автоматизации, высокие регуляторные требования, конвергенцию IT и OT и увеличение разнообразия кибератак в промышленном секторе (в первом квартале 2025 года решения «Лаборатории Касперского» заблокировали на системах промышленной автоматизации вредоносные программы из 11 679 различных семейств).

Распространение цифровых технологий, обычно воспринимаемое как позитивное явление, стирает границы между IT- и OT-средами. Эти границы раньше служили защитой OT-сред от киберпреступников. Один-единственный флеш-накопитель, попавший в среду АСУ ТП, может серьезно повлиять на ключевые бизнес-процессы компании, а мотивированная хакерская группа способна проникнуть в OT-сеть, нанести серьезный ущерб и/или похитить ценные данные. На фоне того, что стандарты автоматизации постепенно переходят от рекомендательных норм к законодательным требованиям, а потребность в обмене передовыми практиками и управлении рисками постоянно растет, обеспечение кибербезопасности промышленных предприятий становится все более трудной задачей.

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

Нефтегазовая отрасль и химическая промышленность

Цифровизация процессов разведки, добычи, транспортировки и переработки — ключевой фактор конкурентоспособности для этих компаний — подразумевает интеграцию IIoT, дронов и роботов, внедрение решений на базе 5G, блокчейна и виртуальной реальности, что расширяет ландшафт угроз, связанных с возможными вредоносными действиями.

Критически важные производственные объекты

Стремясь повысить рентабельность, эти предприятия внедряют передовые технологии и системы связи, переходят в облако и исследуют сценарии конвергенции IT и OT — все это делает их мишенями для новейших и постоянно меняющихся угроз.

Горнодобывающая и металлургическая промышленность

Этой отрасли, лежащей в основе критически важного производства национального масштаба, приходится находить баланс между затратами и преимуществами автоматизации и цифровых технологий. Будучи лакомым куском для хактивистов и профессиональных злоумышленников, отрасль не может позволить себе экономить на кибербезопасности.

Энергетика и коммунальные сети

Цифровые и передовые технологии играют ключевую роль в энергетическом переходе при сохранении традиционной инфраструктуры, по-прежнему лежащей в основе большинства энергетических объектов. Однако применение этих технологий сопряжено с наибольшим риском и требует дополнительных усилий по обеспечению кибербезопасности.

Среди основных целей APT атак будут:

Владельцы и операторы объектов критической инфраструктуры

Стратегически важные организации в нефтегазовой отрасли, химической промышленности, энергетике и секторе коммунальных услуг потенциально могут столкнуться с гораздо более серьезными последствиями при вмешательстве в их операционную деятельность

Критически важные производственные объекты

От отдельного завода до предприятий национального и международного масштаба — деятельность этих компаний, в том числе работающих в металлургии, горнодобывающей промышленности, сельском хозяйстве и глобальном производственном секторе, сопряжена с высоким уровнем риска, и в случае инцидента они могут нести значительные затраты

Число атак на промышленные системы, особенно на АСУ ТП и SCADA, продолжает расти. При этом традиционные защитные решения все менее эффективны против современных киберугроз, нацеленных на промышленные среды. Они могут оказать негативное влияние на работу конечных узлов и технологического процесса в целом. Поэтому нужно выбирать проверенные специализированные решения для промышленной инфраструктуры. В этих условиях «Лаборатория Касперского» предлагает комплексный подход к защите предприятий в данных отраслях. Ознакомьтесь с историями успеха наших клиентов, аналитикой по ландшафту угроз и специальными предложениями для конкретных сценариев на нашем сайте.

Сегодня как никогда важен выбор надежного партнера, который обладает экспертизой на пересечении промышленной и корпоративной кибербезопасности и готов предложить полный спектр передовых технологий защиты.

Узнайте больше об APT- и финансовых атаках на промышленные предприятия в начале 2025 года

Подробнее

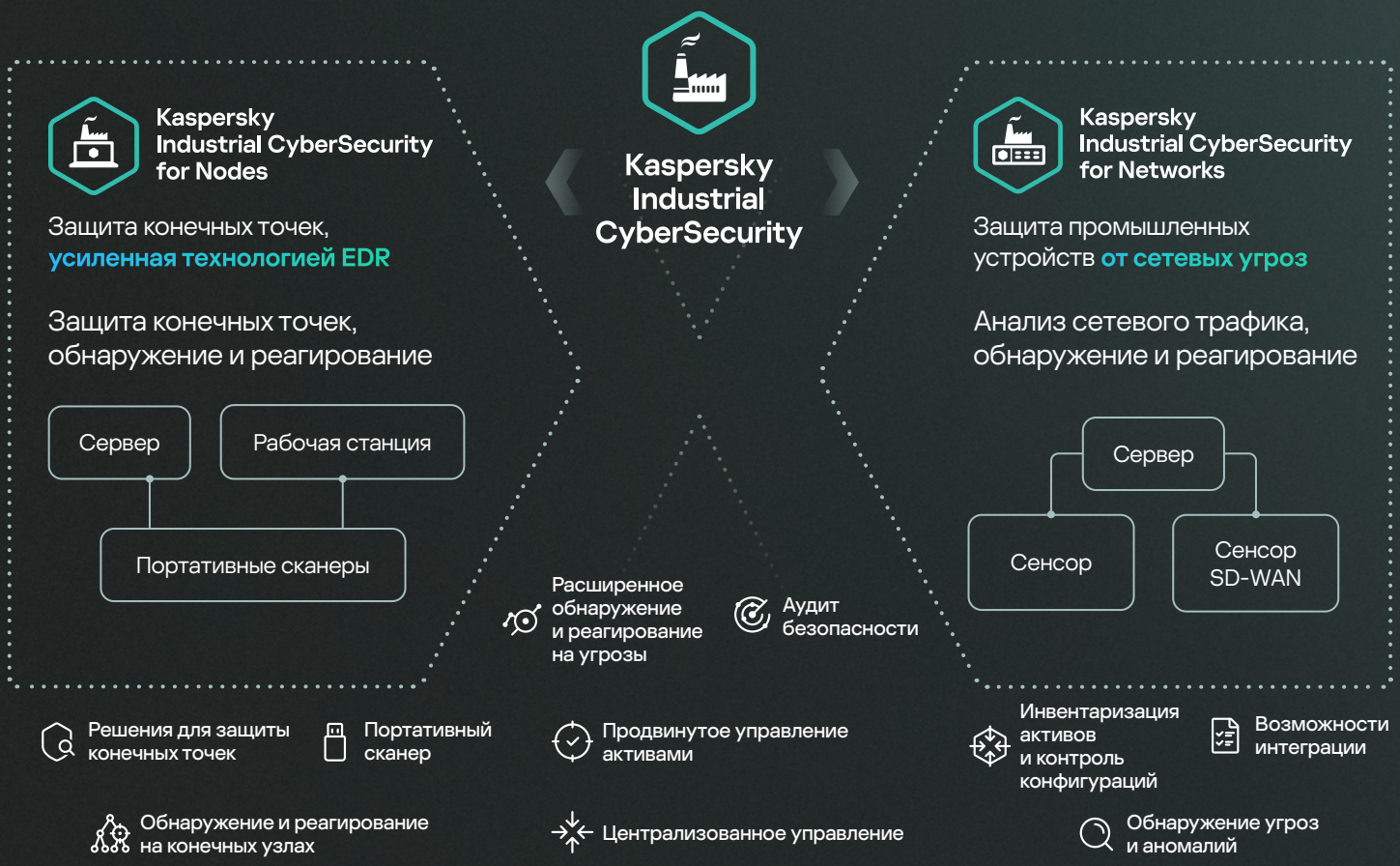
Передовые технологии защиты АСУ ТП

Разрыв между IT- и OT-средами, который раньше защищал OT-среду от киберпреступников, продолжает стремительно сокращаться — именно поэтому владельцам и операторам киберфизических систем сегодня необходимо комплексное защитное решение уровня предприятия от единого поставщика для обеспечения безопасности критической инфраструктуры. **Kaspersky Industrial CyberSecurity (KICS)** — специализированная XDR-платформа, включающая компоненты KICS for Networks и KICS for Nodes и обеспечивающая защиту систем промышленной автоматизации и сетевой инфраструктуры.

KICS for Networks — это решение для промышленных сетей, сочетающее технологии анализа трафика, обнаружения и реагирования на угрозы. Совместимо с системами промышленной автоматизации. **KICS for Nodes** — это решение для защиты конечных узлов в промышленной среде, которое обнаруживает угрозы и обеспечивает возможность своевременного реагирования. Для распределенных или автономных систем под управлением ОС Linux или Windows. Portable Scanner — версия решения, предназначенная для защиты автономного оборудования и устройств подрядчиков без необходимости установки.

Вместе эти компоненты образуют XDR-платформу KICS, которая обеспечивает централизованную инвентаризацию активов, управление рисками и аудит, позволяя масштабировать защиту для разнородной и распределенной инфраструктуры через единую платформу с полным графом инцидентов, аналитикой и другими возможностями.

XDR-платформа KICS позволяет пользователям видеть общую картину с широким контекстом: цепочку инцидентов на уровне сети и конечных точек, точные параметры активов, карты сетевых взаимодействий и топологии сетей даже для сегментов, для которых зеркалирование трафика пока невозможно, и многое другое.



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

SPAN

Сетевое оборудование

Kaspersky Industrial CyberSecurity for Networks

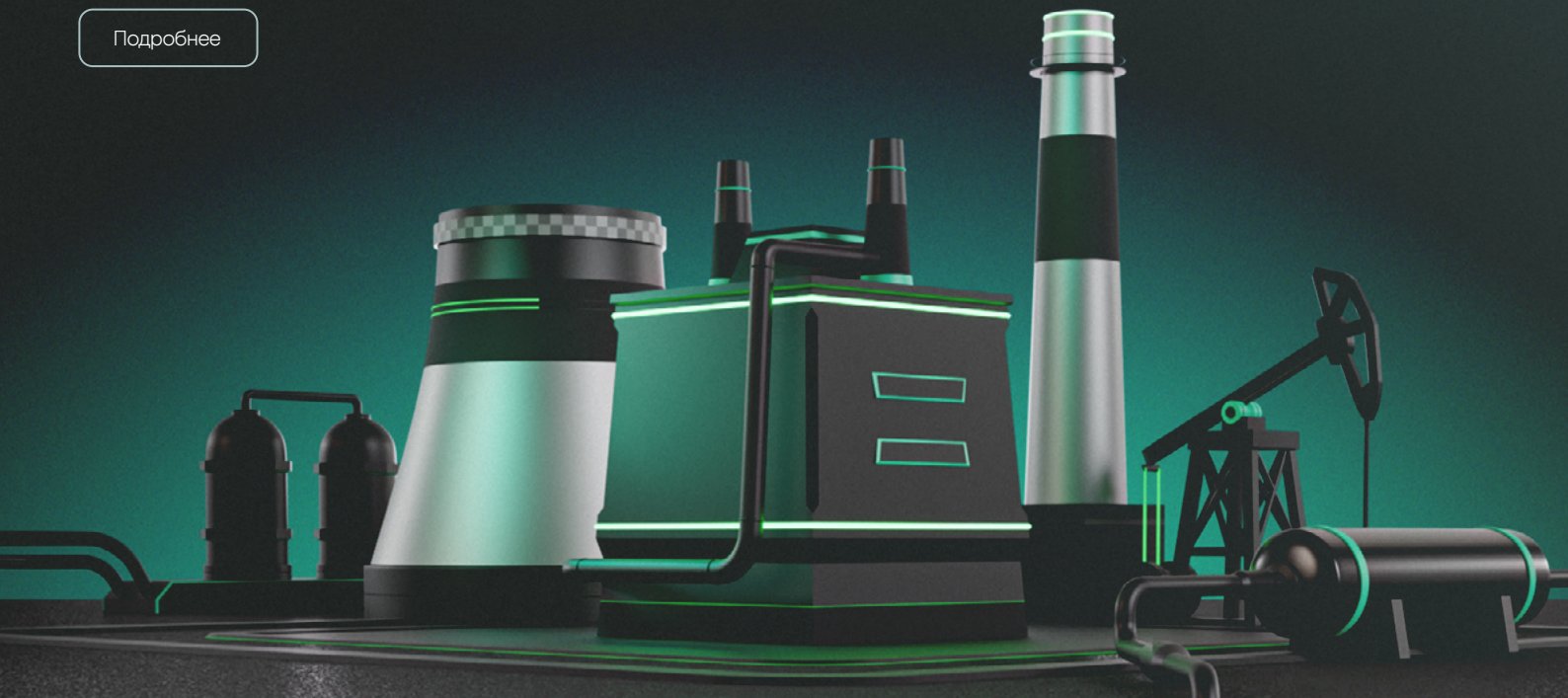
- Контроллер присоединения (BCU)
- Интеллектуальное электронное устройство (IED)
- Программируемые логические контроллеры (ПЛК)
- Релейная и противоаварийная защита (ПАЗ)

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) — это инновационная система, которая использует методы машинного обучения (искусственного интеллекта) для одновременного наблюдения за большим количеством показателей телеметрии и выявления отклонений в работе промышленных объектов до того, как эти отклонения станут представлять угрозу для производства.

Подробнее

Isolated Nodes (ручная проверка с помощью KICS Portable Scanner)



Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

Решение для мониторинга промышленной сети и анализа трафика. Обеспечивает глубокий анализ пакетов (DPI) проприетарных промышленных протоколов. Поставляется в виде программного обеспечения или виртуального устройства безопасности.

KICS for Networks выявляет аномалии и вторжения в АСУ ТП на ранней стадии, обнаруживает события безопасности в сети и на узлах (kill chain и телеметрия EDR), а также обеспечивает принятие необходимых мер для предотвращения негативного влияния на технологический процесс.

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

Инвентаризация активов и контроль конфигураций

Обнаружение активов
Сбор информации об устройствах в сети и их конфигурации, уязвимостях и рисках безопасности

Видимость сети
Мониторинг трафика, построение карт топологии сетей и контроль состояния сети во времени для обеспечения полной прозрачности

Инструменты анализа трафика
Отслеживание и анализ сетевых сессий с возможностью детального экспорта и хранения данных трафика

Преимущества

- Поддержка широкого набора OT-протоколов, устройств и сетевых атак «из коробки»
- Встроенные наборы правил для аудита безопасности и анализа уязвимостей
- Удобный интерфейс и отчеты
- Полная осведомленность о рисках в распределенной инфраструктуре
- Сбор трафика из различных источников: собственных сетевых сенсоров, сенсоров SD-WAN, агентов на конечных точках и портативного сканера

Возможности интеграций

Платформа решений
Раскройте весь потенциал решений «Лаборатории Касперского» благодаря единому кросс-продуктовому подходу к кибербезопасности и интеграции со следующими решениями:

- Kaspersky Machine Learning for Anomaly Detection (MLAD)
  Подробнее
- Kaspersky Software-Defined Wide Area Network (SD-WAN)
  Подробнее

Интеграция со сторонними решениями
Бесшовная совместимость с многочисленными внешними средствами и платформами обеспечения кибербезопасности

Обнаружение сетевых угроз и аномалий

Обнаружение вторжений
Сигнатурное обнаружение и статистический анализатор для выявления попыток подбора пароля или сканирования

Контроль целостности сети
Обучение системы нормальным сетевым взаимодействиям и оповещение о каждом отклонении

Обнаружение аномалий
Выявление аномалий на уровне пакетов и протоколов. Обнаружение аномалий в технологическом процессе при интеграции с Kaspersky MLAD

Deep Packet Inspection (DPI) для промышленных протоколов
Контроль технологического процесса путем разбора системных команд и технологических параметров в сетевом трафике

Корреляция событий
Соотнесение событий информационной безопасности с классификацией MITRE и единой цепочкой атаки (kill chain)

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**.

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

KICS for Nodes

Kaspersky Industrial CyberSecurity for Nodes

Испытанное сертифицированное решение промышленного класса для защиты рабочих мест, обнаружения угроз и реагирования на них. Легкое, совместимое и стабильное решение для Linux, Windows и автономных систем.

KICS for Nodes обеспечивает защиту каждой конечной точки в современных цифровых, управляемых и распределенных системах автоматизации. Решение собирает данные телеметрии, давая ясное и подробное визуальное представление о распространении инцидента по рабочим станциям, серверам, шлюзам и другим конечным узлам, благодаря чему администраторы системы автоматизации могут быть уверены, что инцидент полностью устранен и не повторится.

Защиты конечных точек

Предотвращение угроз в режиме реального времени
Настраиваемые и запускаемые по требованию проверки съемных носителей и критических областей для предотвращения срабатывания эксплойтов и защиты файлов

Локальный контроль активности
Функции контроля устройств и Wi-Fi Обеспечение целостности проектов ПЛК для полной прозрачности локальной активности

Контроль активности в сети
Управление межсетевыми экранами хостов и блокировка сетевых сессий для защиты от сетевых угроз

Мониторинг системы
Проверка целостности файлов, контроль доступа к реестру и выявление угроз в системных журналах для обеспечения безопасности ОС

Обнаружение и реагирование на конечных точках

Обнаружение
Проверка на наличие индикаторов компрометации (IoC), расширенные возможности мониторинга и отчетности

Реагирование
Запрет запуска, карантин/удаление файлов, запуск/завершение процессов, изоляция сетей и многое другое

- Узлы Windows
- Портативный сканер
- Узлы Linux
- Агент аудита

Портативный сканер

Сканер вредоносного ПО
Антивирусная проверка автономного оборудования и всех компьютеров, ввозимых на промышленный объект

OVAL-сканирование
Обеспечение выполнения политики кибербезопасности на автономных устройствах с помощью ручной проверки на наличие уязвимостей и соответствие требованиям

Сбор и анализ сетевых пакетов
Захват и анализ сетевого трафика для обеспечения полной видимости даже в изолированной инфраструктуре

Инвентаризация узлов
Сбор полной информации об аппаратном и программном обеспечении с помощью безагентского решения

Преимущества

- Незначительное влияние на защищаемые устройства, что помогает сохранить максимальную производительность систем
- Совместимость со старыми ОС и оборудованием
- Базовые настройки безопасности, а также расширенные параметры для защиты узлов от любых типов угроз
- Модульное развертывание и настройки без влияния на технологический процесс
- Поддержка ПЛК: Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4; Schneider Electric Modicon M340, M580; устройства на базе CODESYS V3; Fastwel CPM723-01
- Гибкие варианты лицензирования — от 1 месяца до 5 лет
- Проверенные и эффективные пресеты конфигурации для самых популярных АСУ ТП

- Шлюз
- Сервер Historian
- Сервер SCADA
- Рабочее место оператора
- Встраиваемые системы
- Рабочая станция управления системой
- Рабочая станция инженера

Платформа KICS и другие возможности

Единая система обеспечения кибербезопасности для промышленного и корпоративного сегментов вашего предприятия

Специализированная XDR-платформа для защиты промышленных инфраструктур

Базовые компоненты Kaspersky Industrial CyberSecurity — KICS for Networks и KICS for Nodes — изначально спроектированы для бесшовной совместной работы в рамках нашей платформы, обеспечивая целостный и согласованный пользовательский опыт. При совместном приобретении они формируют нативную XDR-платформу, предоставляющую дополнительную ценную кросс-продуктовую функциональность.

Продвинутое управление активами

- Сбор данных об оборудовании
- Инвентаризация пользователей и приложений
- Обнаружение изменений в конфигурации

Аудит безопасности

- Сканирование уязвимостей
- Соответствие стандартам
- Контроль конфигураций

Расширенное обнаружение и реагирование на угрозы

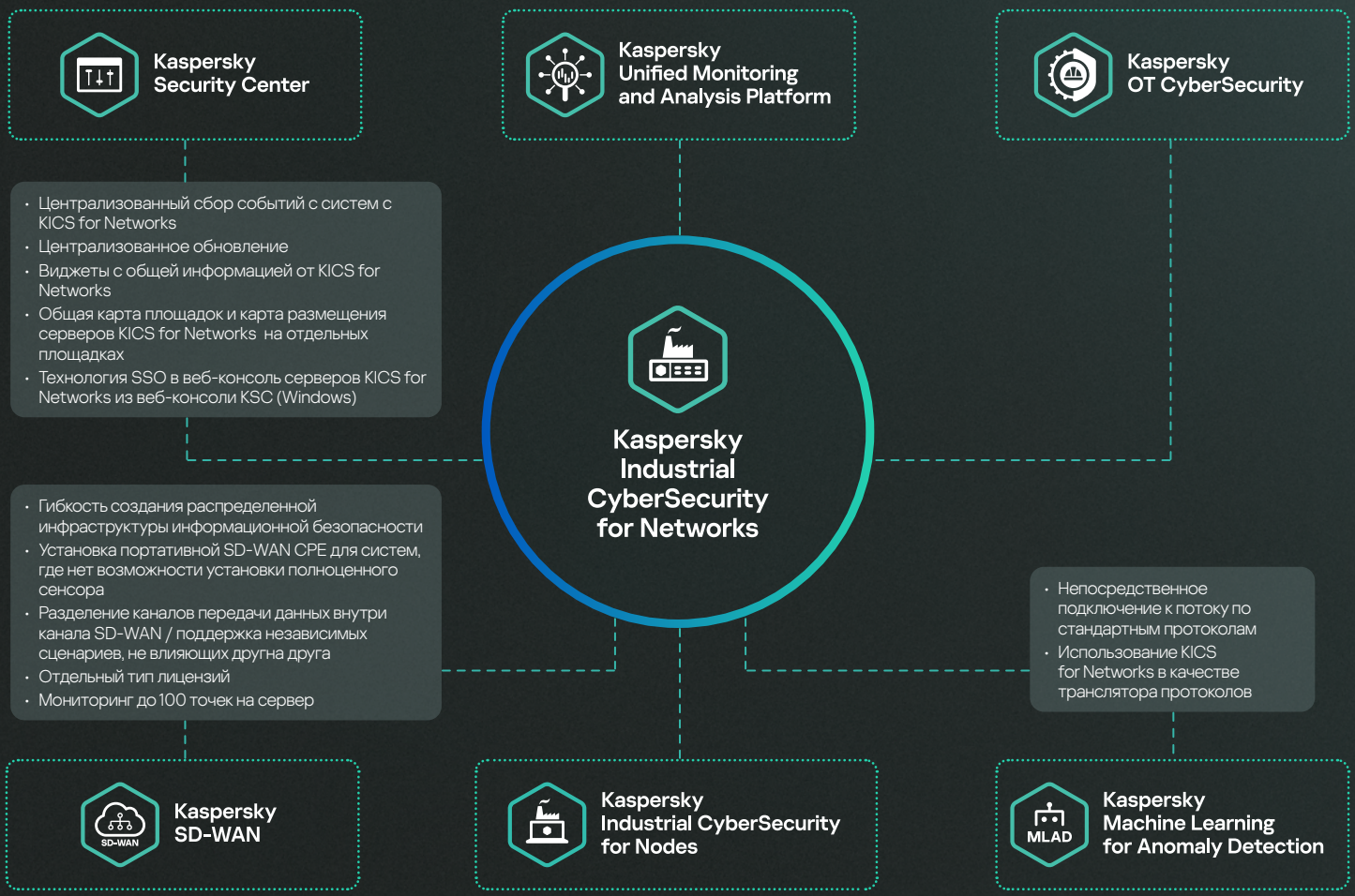
- Единая цепочка событий
- Обогащение инцидентов
- Предотвращение запуска объектов
- Изоляция файлов и хоста
- Интеграция с межсетевыми экранами

Единая киберзащита промышленного и корпоративного сегментов одного предприятия

Расширьте возможности ваших EDR-решений с помощью механизма корреляции, автоматического реагирования и коннекторов к сторонним системам — дополните платформу KICS решением Kaspersky XDR Core, чтобы получить доступ к следующим возможностям:

Комплексный мониторинг и корреляция событий информационной безопасности (SIEM), интеграция с различными системами

Обогащение и управление данными Threat Intelligence



28 лет опыта мирового уровня и петабайты данных об угрозах

ICS CERT

ICS CERT — наше международное подразделение по исследованию безопасности OT- и IoT-сред

Доказанная компетентность в области IT/OT-безопасности, подтвержденная многочисленными наградами и достижениями

Более 200 сертификатов совместимости с решениями производителей систем автоматизации

Доказанная эффективность технологий и соответствие стандартам и требованиям

Клиенты по всему миру

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее