Почему промышленная кибербезопасности стала приоритетом. Опыт Лаборатории Касперского

kaspersky

Исторические особенности систем АСУ ТП

Мир в себе

- Изолированность от бизнес-сетей (метод топора)
- Хаотичное развитие без единого плана
- Устаревшее ПО как системного, так и прикладного уровня
- Непонимание бизнесом ландшафта угроз
- Скептицизм по отношению к информационной безопасности промышленных сетей
- Большой объем неснижаемых остатков ЗИП

Новые бизнес-процессы

- Сбор данных в реальном времени о состоянии оборудования и его элементов для минимизации остатков ЗИП
- Интеграции ИС АСУ ТП с ИС республиканских операторов, системами ТОиР и ERP
- Желание понимать структуру систем АСУ ТП и контролировать происходящее в них для снижения рисков
- Требования регуляторов (п.п. РК 832, закон 121 КР, п.П. РУ ПП-167, 187-ФЗ РФ)

Привлекательность промышленности для атакующих

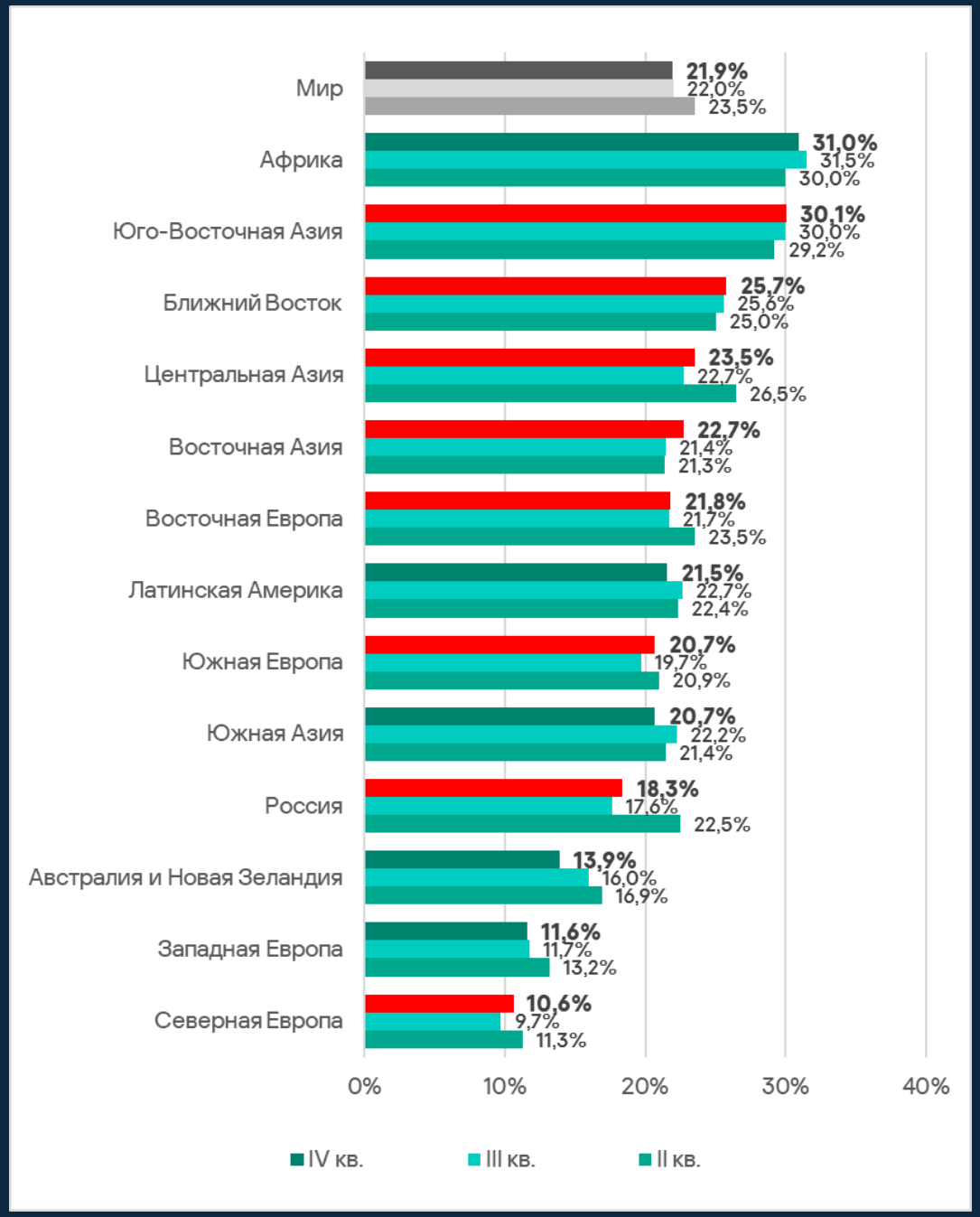
Риски

- В условиях экономической нестабильности промышленность становится привлекательной целью для злоумышленников
- Отсутствие системного подхода превращает индустриальные сети в легкую добычу
- Человеческий фактор играет все большую роль
- Убытки от атак вирусов-вымогателей, а также от выходя из строя сложного оборудования исчисляются 8-значными цифрами
- Шанс техногенных катастроф и человеческих жертв в результате успешных атак

Динамика роста атак на промышленные объекты

Географический ландшафт угроз

- На конец 2024 года каждый пятый компьютер АСУ был атакован
- Наибольшее количество атак зафиксировано в Африке (31%)
- Наименьшее в Северной Европе (10,6%)
- В Центральной Азии было атаковано 23,5% всего парка компьютеров
- Рост количества атак за 4 квартал 2024 года по региону Центральной Азии +0,8%



Системы водоподготовки

- Увеличение злоумышленниками уставок подачи гидроксида натрия в 100 раз, что могло вызвать массовый летальный исход или серьезный вред здоровью у потребителей
- Причиной являлось отсутствие системного подхода к обеспечению информационной безопасности объекта критической важности, в том числе одинаковые пароли как для удаленного доступа к технологической сети через TeamViewer, так и к системам АСУ ТП
- Масштабная авария предотвращена бдительным дежурным персоналом в силу низкой квалификации атакующих

Ядерные объекты

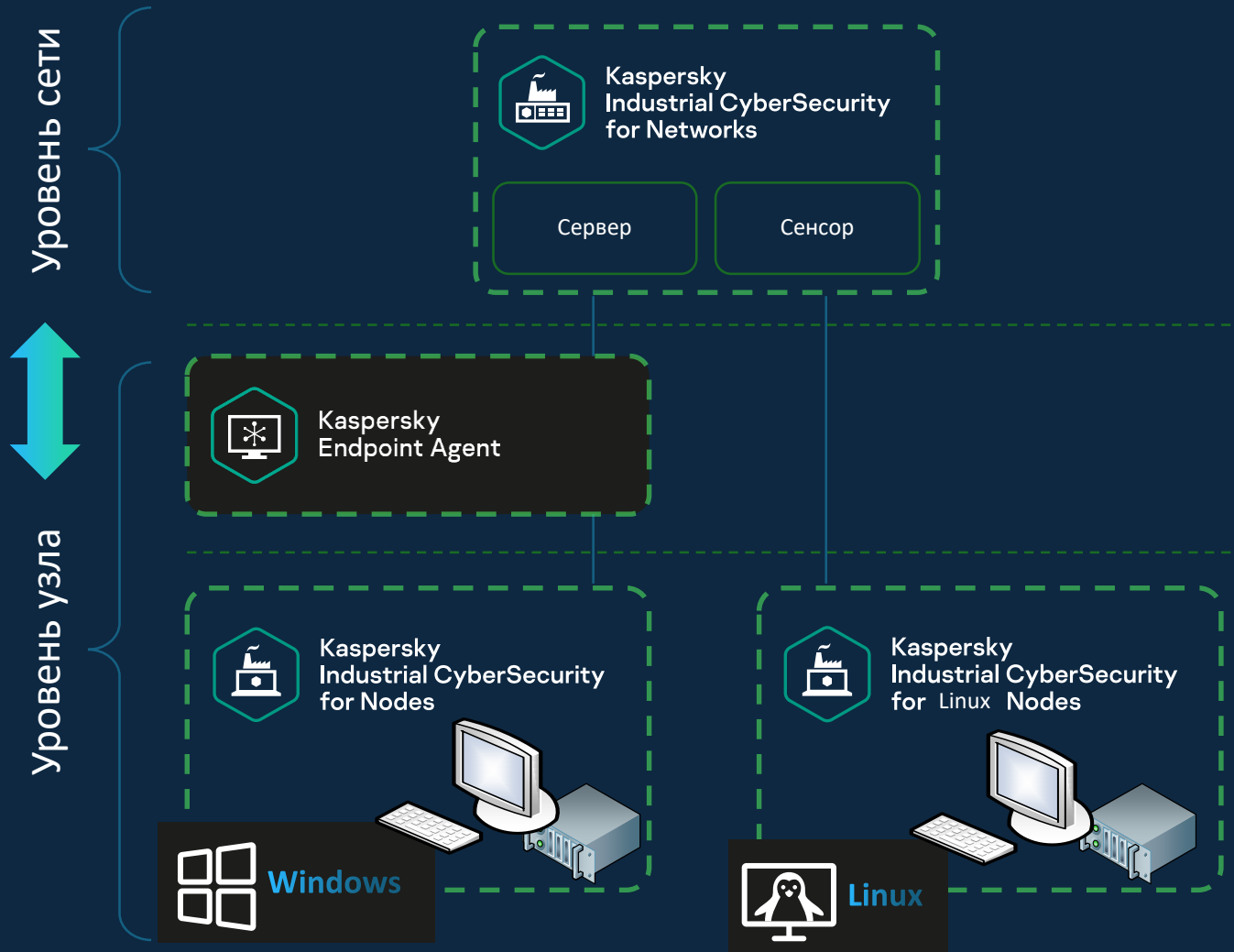
- Подмена данных межконтроллерного обмена для выведения урановых центрифуг на закритические значения, и их последующее разрушение
- Распространение через портативные носители в изолированной сети
- Незаметность для неспециализированных систем ИБ
- Атака завершилась успехом

Специализированные решения для защиты АСУ ТП

Kaspersky Industrial CyberSecurity

kaspersky

Архитектура платформы KICS и основные функции



Управление активами, событиями и рисками

- Инвентаризация сети
- Анализ промышленных протоколов (IDS, DPI)
- Обнаружение атак в сетевом трафике
- Контроль конфигурации оборудования

EDR агент

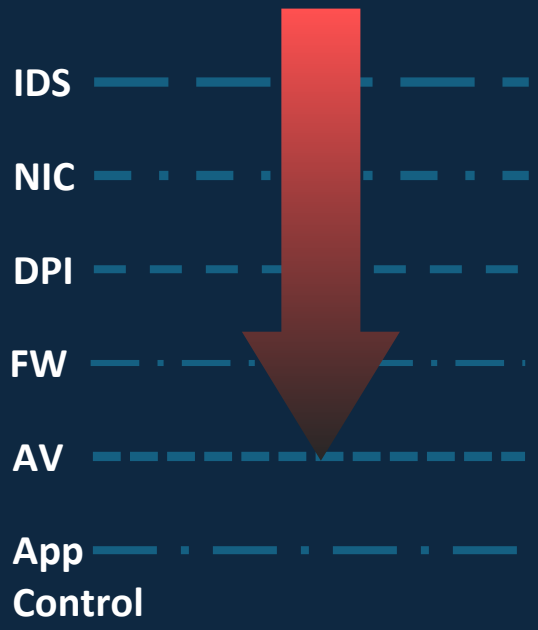
- Сведения об узле
- Обнаружение и телеметрия для анализа первопричин
- Реагирование

Обнаружение и реагирование на уровне конечных узлов

- Антивирус
- Контроль запуска ПО
- Контроль подключения устройств
- Защита узла от сетевых угроз
- Контроль целостности ПО и файлов
- и многое другое

Kaspersky Industrial CyberSecurity

Эшелонированная защита



Учет особенностей АСУ ТП

- Работа на слабом железе, ограничение потребляемых ресурсов узла
- Поддержка устаревших ОС (с Windows XP SP2)
- Неблокирующий режим для всех компонентов
- Подтвержденная совместимость с промышленным ПО
- Перезагрузка при установке/обновлении/удалении не требуется
- Обновление баз в изолированных средах

Использование особенностей АСУ ТП

Обучение

Наблюдение

KICS for Nodes: функции

Windows

Антивирус

Контроль запускаемых приложений

Автоматический белый список

Контроль устройств

Мониторинг файловых операций

Анализ журналов Windows на предмет нарушений

Мониторинг доступа к реестру

Контроль целостности проектов в ПЛК

Защита от сетевых угроз

Управление Брандмауэром

Защита от эксплойтов

Интеграция с KICS for Networks

Поддержка ОС

20+ десктопных версий Windows, начиная с WinXP SP2

15+ серверных версий Windows, начиная с Windows Server 2003

15+ встраиваемых версий Windows, начиная с Windows XP Embedded SP2 WEPOS

70+ дистрибутивов Linux

KICS for Nodes: Портативный сканер

Применение:

- Автономные узлы
- Узлы с устаревшим железом и ОС (от Windows 2000 SP4)
- Узлы, на которые нельзя ставить антивирус (станки с ЧПУ)
- Ноутбуки подрядчиков перед допуском к работам

Антивирус:

- Без установки и изменений на проверяемом узле
- Режимы: лечить/удалять или «только информировать»
- Регулируемая нагрузка на CPU (%, не более)
- На каждую проверку каждого узла на флэш-накопителе создается отдельная папка:
  - Отчет о сканировании
  - Подозрительные файлы в запароленном архиве

Захват сетевых пакетов:

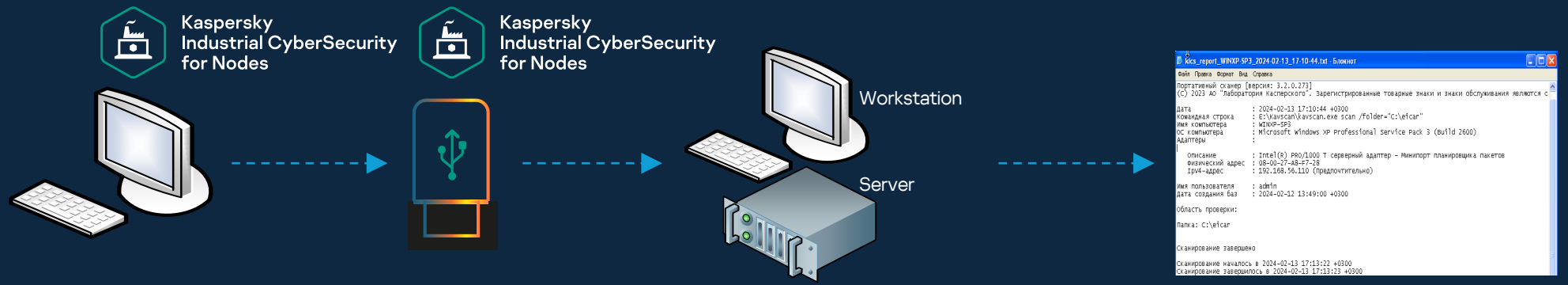
- Для передачи на анализ в KICS for Networks

Инвентаризация узла:

- Сбор данных о ПО и оборудовании на узле

Аудит безопасности:

- OVAL-сканирование
- Использование встроенных и пользовательских баз OVAL-описаний, БДУ ФСТЭК России



Узел с установленным KICS for Nodes с лицензией KICS Portable

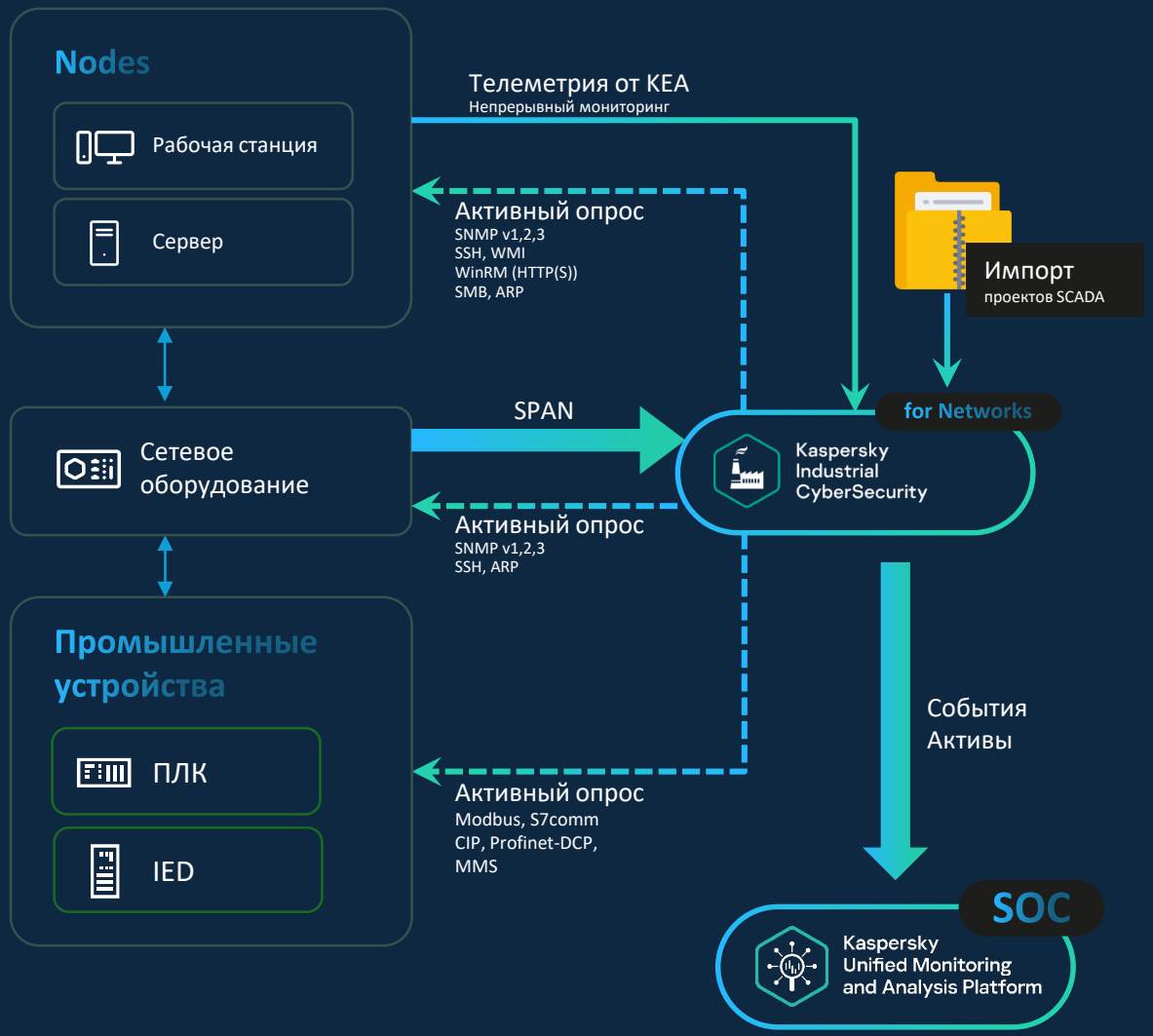
USB флэш-накопитель

Сканирование узлов один за другим из командной строки одним флэш-накопителем

Анализ отчетов и подозрительных файлов

Инвентаризация устройств и сессий

Kaspersky
Industrial CyberSecurity
for Networks



Методы инвентаризации сети

1. Пассивный мониторинг (копия трафика)
2. Телеметрия с агента (KEA, KICS for Linux Nodes) на узле
3. Активный опрос
   - АРМ, серверов, ПЛК и др. – сбор информации об устройстве
   - Сетевое оборудование (по SNMP) – получение данных о топологии подключений
4. Импорт конфигураций SCADA / DSC / PLC проектов – узлы и теги

Поддержка

50+ промышленных протоколов (теги и команды)

35+ ИТ-протоколов

100+ промышленных устройств

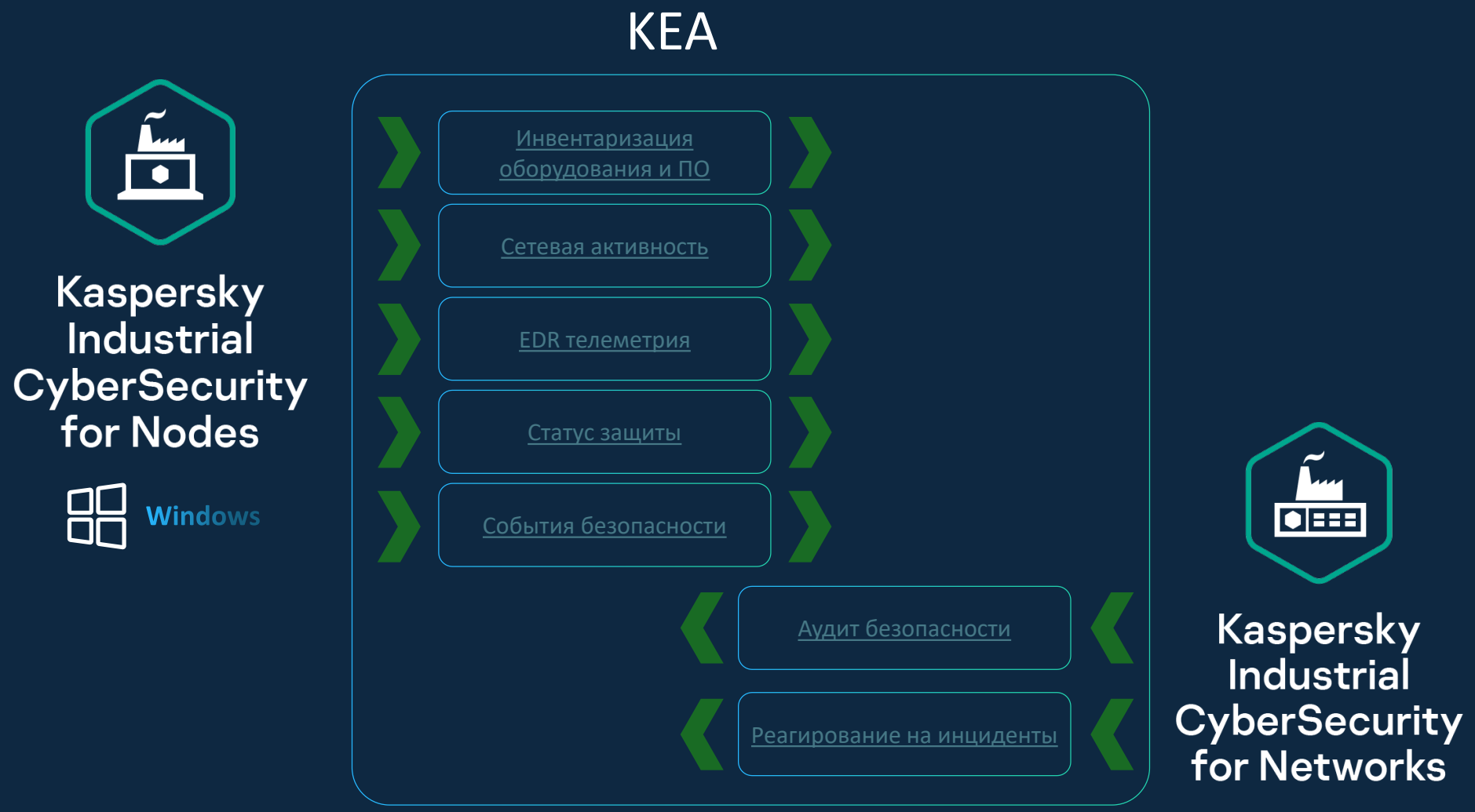
5k+ сигнатур кибератак, включая специальные сигнатуры для АСУТП от Kaspersky ICS CERT

Централизованная система аудита узлов промышленной сети

Ключевые преимущества

- Аудит выполнения требований безопасности для узлов на Windows, Linux и сетевого оборудования
- Встроенная база уязвимостей для промышленного ПО от Kaspersky ICS CERT
- Контроль конфигурации устройств (Win/Linux, ПЛК, сетевые устройства)
- Отчёты, результаты аудита и история проверок доступны в одном месте

Kaspersky Endpoint Agent



Отчеты

- Инвентаризация ОТ активов
- Анализ коммуникаций
- Отчет по рискам и инцидентам
- Генерация отчета
  за произвольный период времени и
  расписанию
- Рассылка отчетов на почту

Kaspersky Industrial CyberSecurity

Лицензирование

Простой способ: заполнить опросный лист
https://box.kaspersky.com/d/9c58d3bee371480bb477/

Сложный способ

Kaspersky Industrial CyberSecurity for Nodes

- Срок: 1, 2, 3 года (поддержка и обновление)
- Количество защищаемых узлов
- Тип защищаемых узлов: Workstation – для пользовательских версий ОС, Server – для всего остального
- С EDR или без EDR
- Тип лицензии: новая, продление, crossgrade
- Техподдержка Enterprise и обновления всегда включены

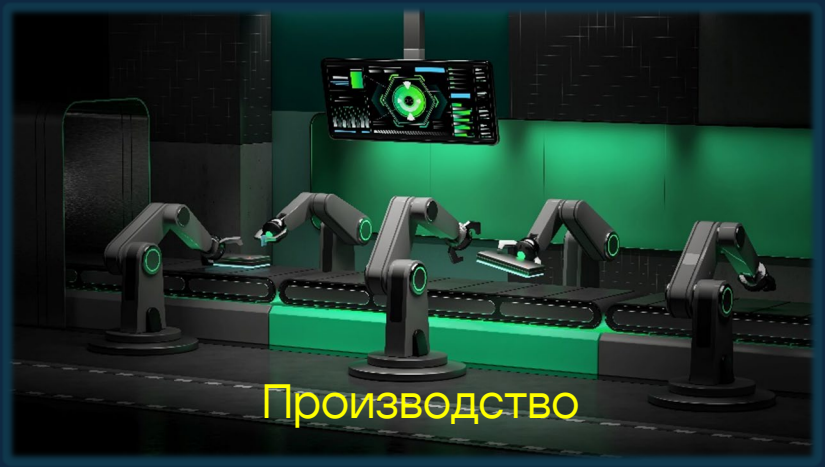
Kaspersky Industrial CyberSecurity for Networks

- Срок: 1, 2, 3 года (поддержка и обновление) + бессрочная (для первой инсталляции)
- Количество серверов и сенсоров
- С активным опросом и аудитом безопасности или без них
- Тип лицензии: новая, продление, crossgrade
- Техподдержка Enterprise и обновления всегда включены

Особые виды лицензий:

- Portable scanner – по числу проверяемых узлов, срок: 1, 2, 3 года
- Certified Media Pack

Регуляторный хаб



- **Автоподбор нормативных документов:** поможем понять, что необходимо именно вашему бизнесу для соответствия законодательству
- **Интерактивная база знаний:** покажем взаимосвязь между документами, подберем необходимую информацию, чтобы вам не пришлось изучать десятки страниц законов, приказов и т. д.
- **Практические ИБ-советы:** подберем решения для обеспечения информационной безопасности с учетом требований законодательства

Получить набор мер

Полезные ссылки

KICS for Networks. Видео с обзором решения
https://box.kaspersky.com/f/9a924f698b56405a93ce

Сертификаты совместимости с промышленными вендорами
https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity/certification

Жизненный цикл решений
https://support.kaspersky.ru/corporate/lifecycle

Сертификаты государственных регуляторов
https://support.kaspersky.ru/common/certificates

Истории успеха
https://www.kaspersky.ru/enterprise-security/industrial-cybersecurity#stories

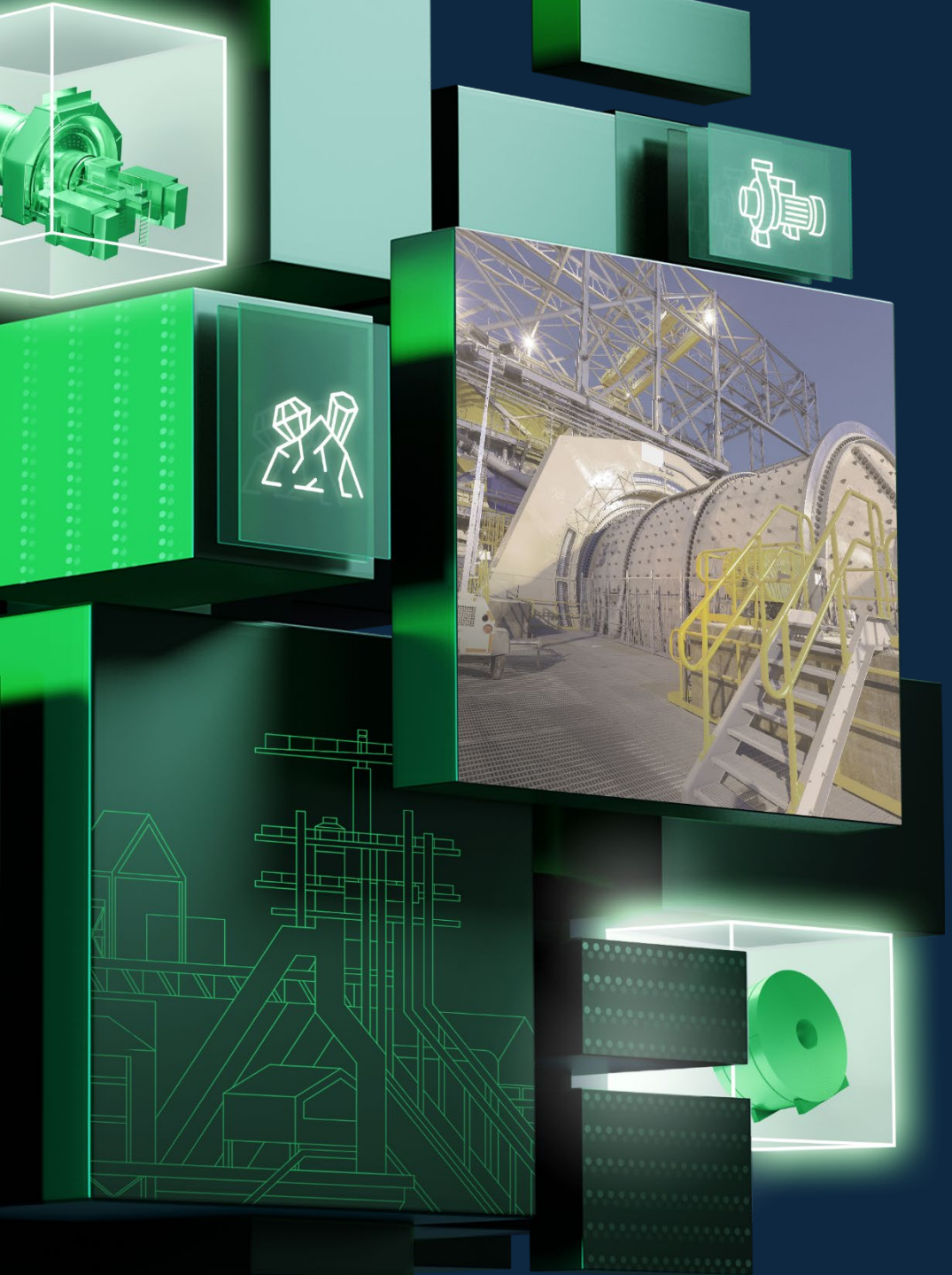
Регуляторный хаб
https://regulhub.kaspersky.ru

Отчеты Kaspersky ICS Cert
https://ics-cert.kaspersky.ru/

Онлайн справка по продуктам
https://support.kaspersky.com/help

Сертифицированные партнеры
https://locator.kaspersky.com

Kaspersky Threat Intelligence Portal
https://opentip.kaspersky.com



Спасибо!