Информационная безопасность в АСУ ТП

Борис Дорошенко

Инженер предпродажной поддержки,
Лаборатория Касперского

kaspersky

Архитектура платформы KICS и основные функции

Управление активами, событиями и рисками

АУД.1 УКФ.3 АУД.5 СОВ.1 СОВ.2 ЗИС.35

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

EDR агент

АУД.1 ИНЦ.3 ИНЦ.4

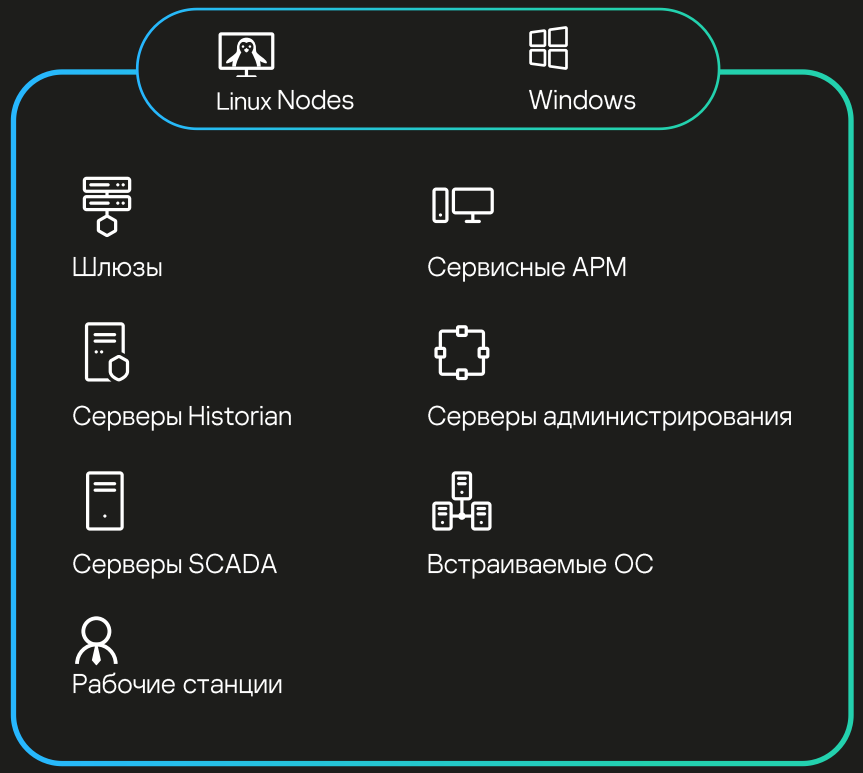
- Сведения об узле
- Обнаружение и телеметрия для анализа первопричин
- Реагирование

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

KICS for Nodes: Особенности применения в АСУ ТП



Ключевые преимущества

Kaspersky Industrial CyberSecurity for Nodes

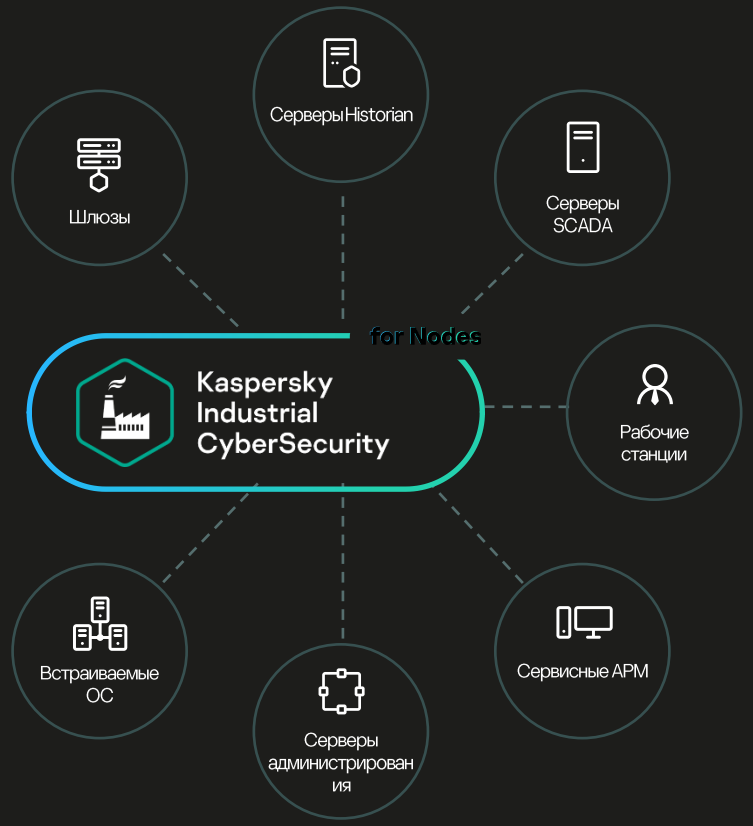
- Совместимость с промышленным ПО
- Работа на слабом устаревшем оборудовании
- Поддержка устаревших ОС (с Windows XP SP2)
- Неблокирующий режим для всех компонентов
- Перезагрузка при установке/обновлении не требуется
- Обновление баз в изолированных средах
- Модульная архитектура для гибкой установки и настройки
- Настройка ограничений потребляемых ресурсов
- Наличие сертификатов ФСТЭК и ФСБ

KICS for Nodes: модули

Windows Nodes

- АВЗ.1, АВЗ.3 — Антивирус
- ЗИС.23, ОПС.1, УКФ.3, ОПС.2 — Контроль запускаемых приложений (Автоматический белый список ПО)
- ЗНИ.5, ЗНИ.7 — Контроль устройств (Автоматический белый список носителей)
- ЗИС.13, ОЦЛ.1, ОЦЛ.2 — Мониторинг файловых операций
- ОЦЛ.1 — Мониторинг доступа к реестру
- ЗИС.13 — Защита от шифрования сетевых папок
- АУД.2 — Защита от эксплойтов
- ЗИС.35 — Защита от сетевых угроз
- АУД.7 — Анализ журналов Windows на предмет нарушений
- УПД.14, ЗИС.35 — Управление Брандмауэром
- ОЦЛ.1 — Контроль целостности проектов в ПЛК
- Интеграция с KICS for Networks
- ИНЦ.1, ИНЦ.6, АУД.4, АУД.7 — Журнал событий на узле
- АУД.6 — Функции самозащиты

Защита рабочих станций и серверов

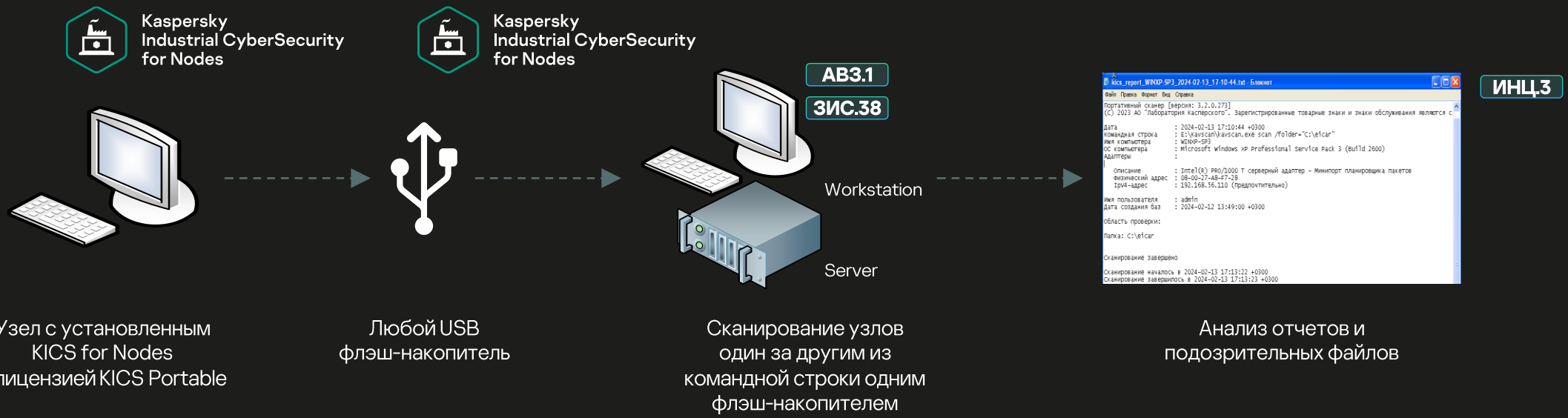


KICS for Nodes: Портативный сканер

Решает задачи:

- Сканирование автономных систем
- Сканирование систем, в которых использование антивирусного программного обеспечения запрещено из-за рисков совместимости или нарушения целостности
- Позволяет проводить проверку безопасности ноутбуков гостей или субподрядчиков перед выполнением работ в АСУ ТП

- Не требует 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



Узел с установленным KICS for Nodes с лицензией KICS Portable

Любой USB флэш-накопитель

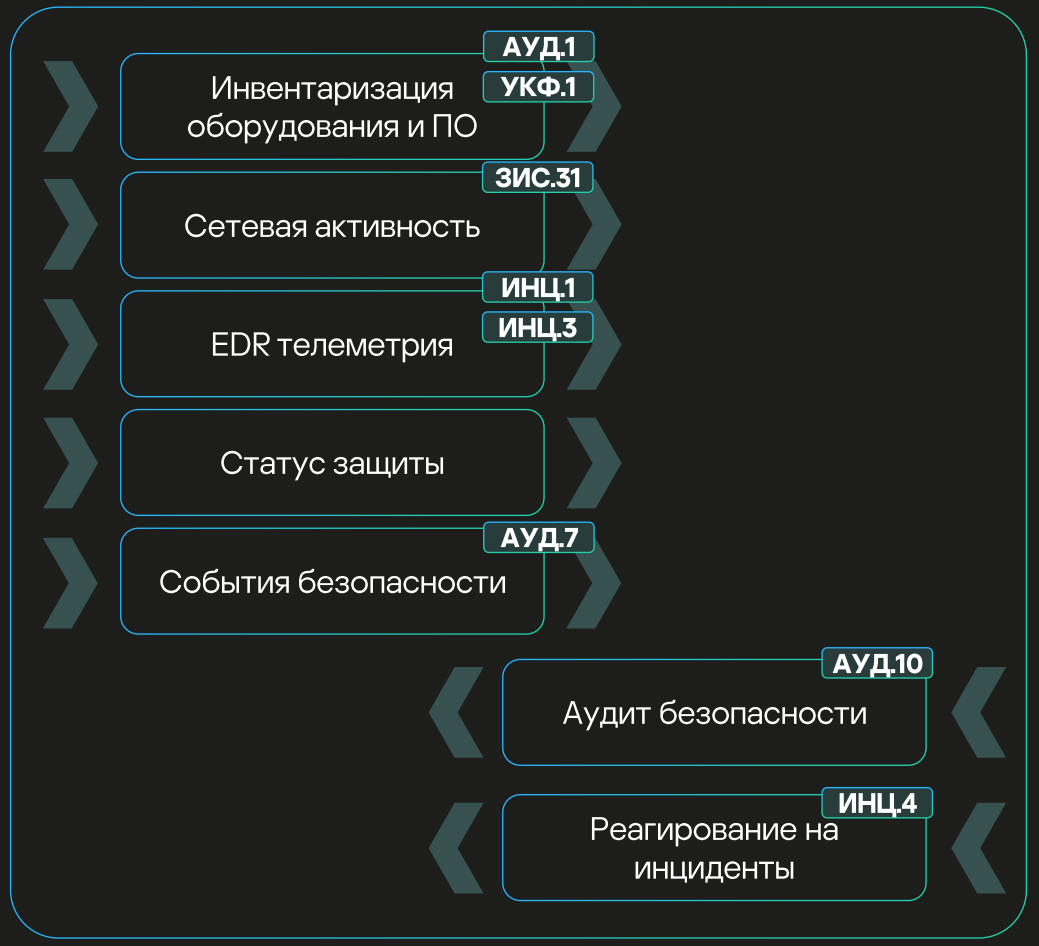
Сканирование узлов один за другим из командной строки одним флэш-накопителем

Анализ отчетов и подозрительных файлов

Kaspersky Endpoint Agent

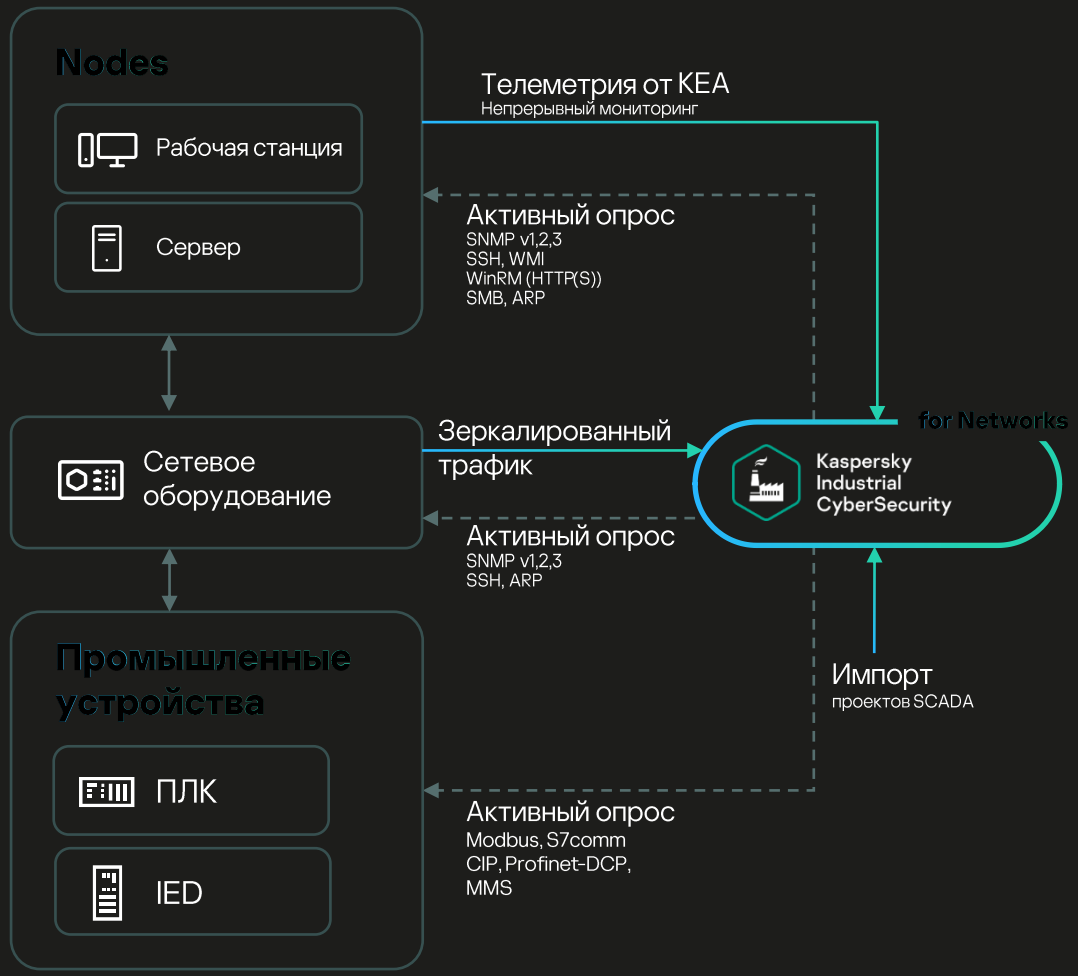
Kaspersky Industrial CyberSecurity for Nodes

Windows



Kaspersky Industrial CyberSecurity for Networks

Инвентаризация устройств и сессий



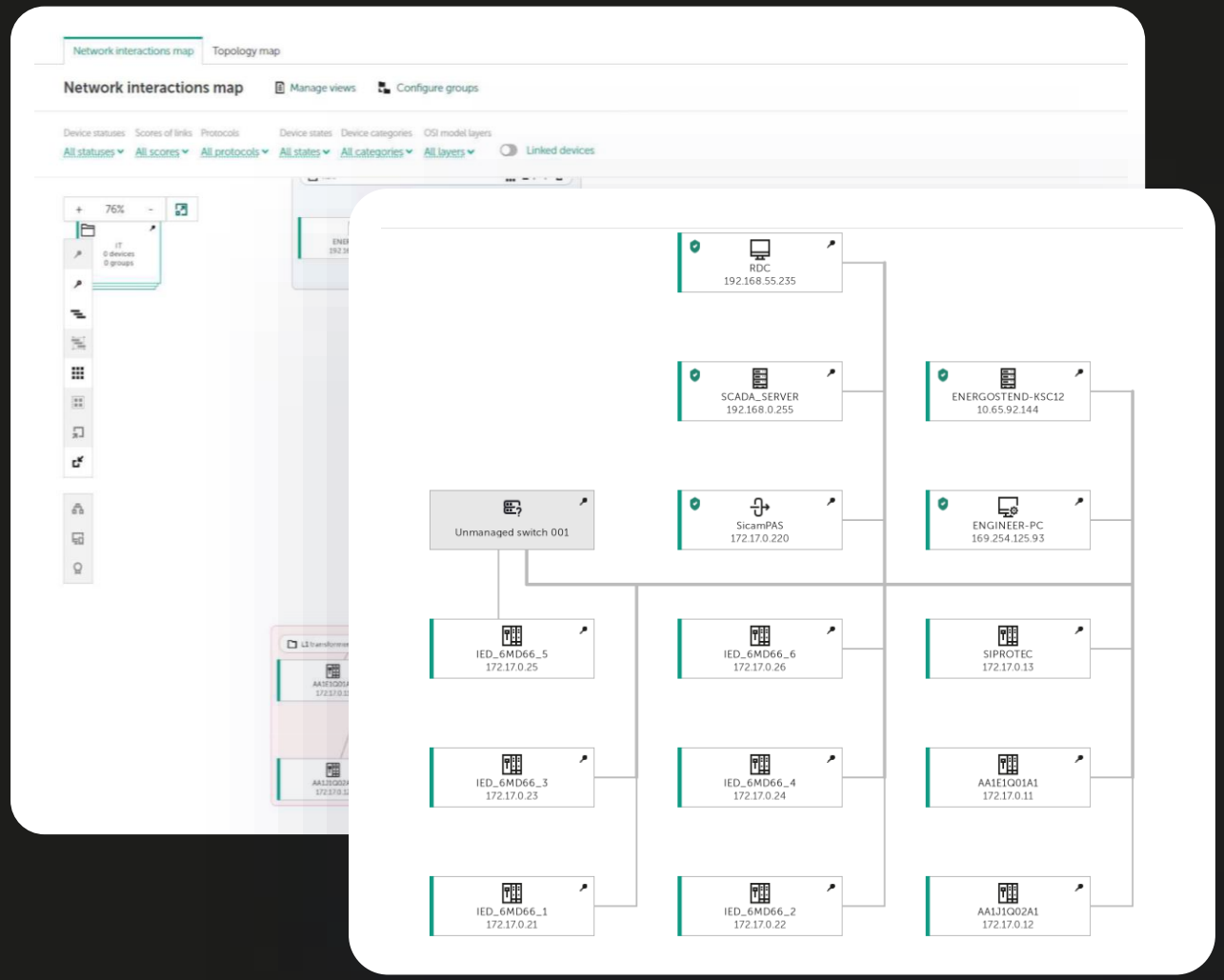
Методы инвентаризации сети

1. Пассивный мониторинг (копия трафика) ЗИС.28 ЗИС.29 ЗИС.35
2. Телеметрия с агента (KEA) на узле ЗИС.31
3. Активный опрос
4. Импорт конфигураций SCADA / DSC / PLC проектов

Ключевые преимущества

- Автоматическая инвентаризация и категоризация устройств, анализ рисков и аудит безопасности АУД.1
- Комбинированный подход к инвентаризации активов
- Инвентаризация без SPAN сессии
- Автоматическое определение метода активного опроса по категории устройства: только протоколы и порты, поддерживаемые устройством

Визуализация сети



Карта сетевых коммуникаций

УПД.14
- Карта показывает логическое взаимодействие между узлами в сети

ИНЦ.3
- Позволяет визуализировать взаимосвязи, указать протоколы взаимодействия, количество переданного трафика
- Имеет инструменты по автоматическому расположению узлов, распределению на группы, фильтрации для скрытия устройств или протоколов

УКФ.2
- Обладает историческими данными, набор данных для показа на карте можно выбрать на временной шкале

Топологическая карта сети

- Карта физических подключений с ортогональными линками и шинами данных
- Позволяет точно определить к какому порту коммутатора подключено устройство
- Строится автоматически за счёт активного опроса узлов и сетевого оборудования
- Есть ручное редактирование

Анализ сетевых сессий

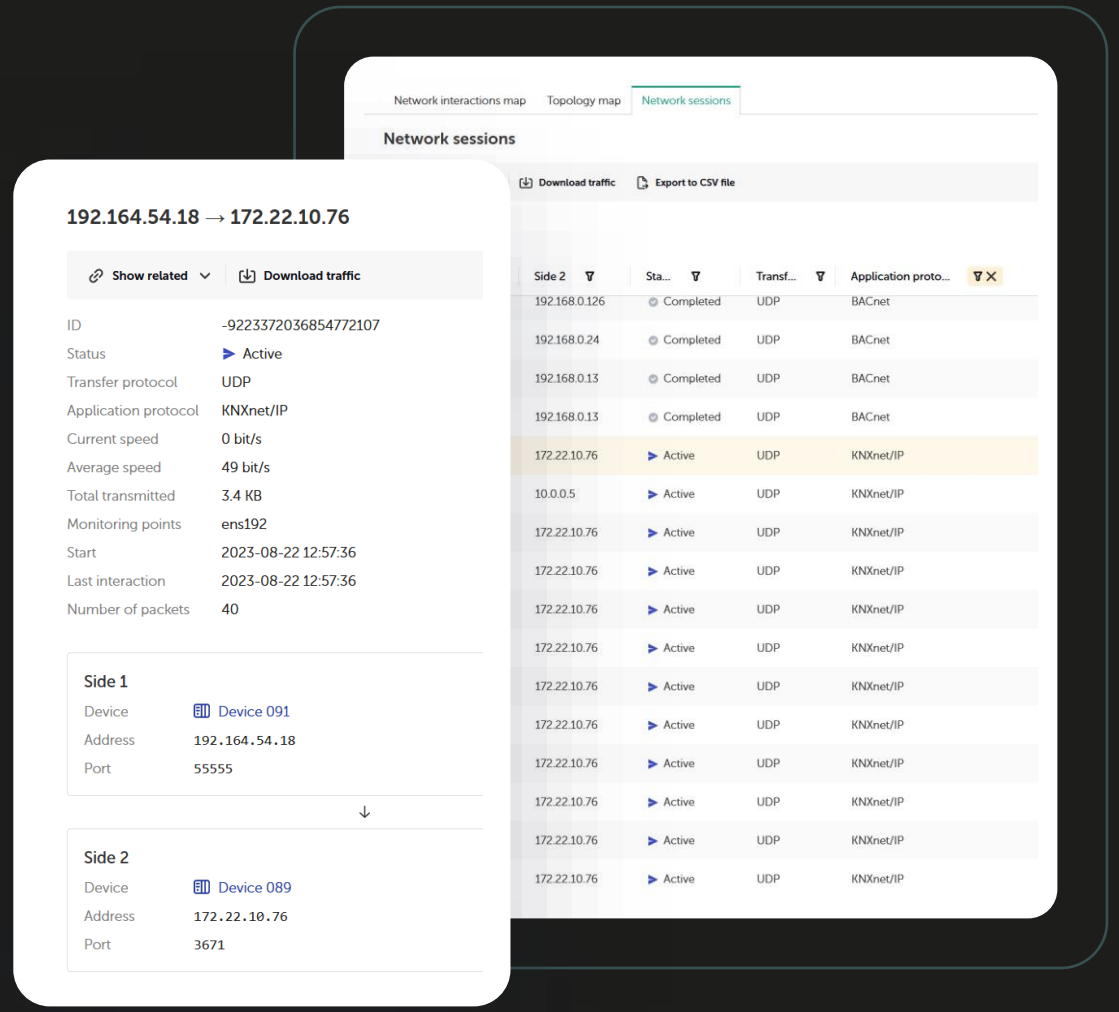
Сетевые сессии

ЗИС.28
ЗИС.29
ЗИС.35

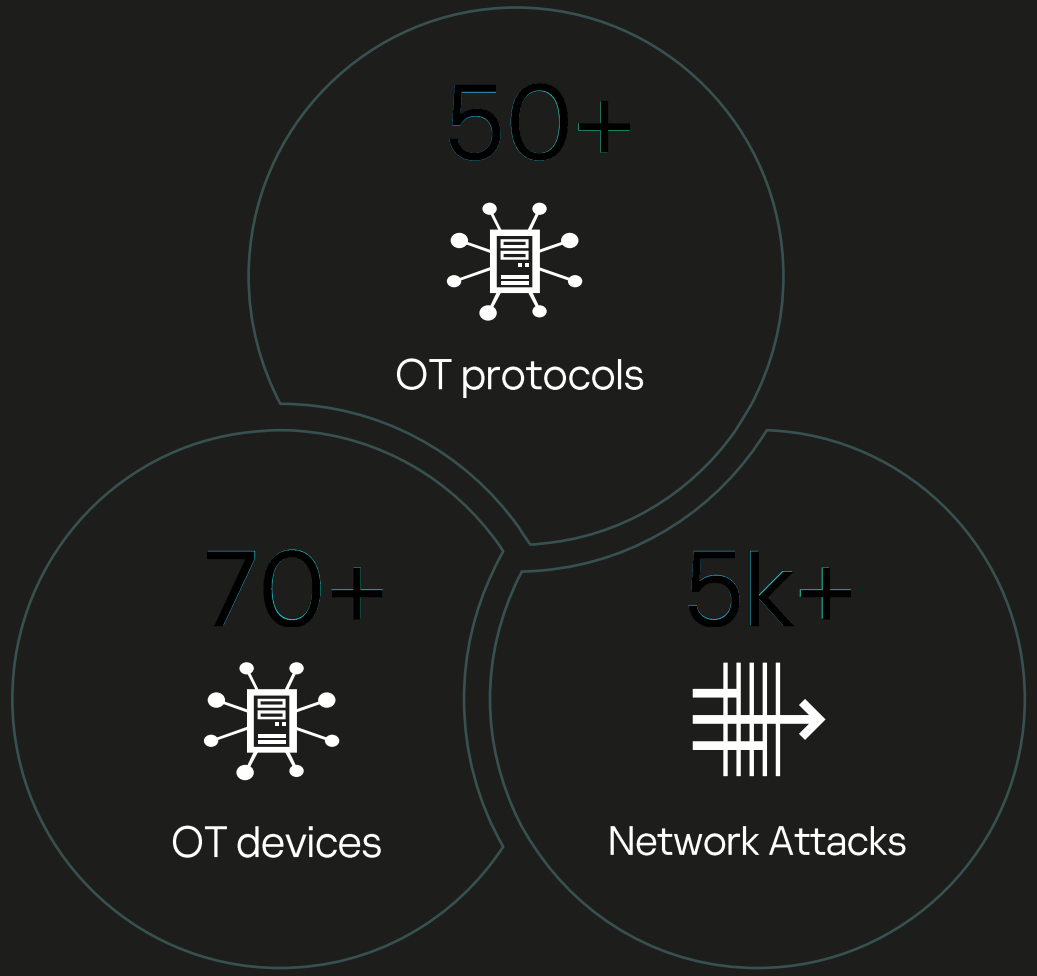
- Статус сессий (Активная / Закрытая)
- Направление коммуникаций
- Транспортный и прикладной уровень протоколов
- Статистика по сессиям (скорость, объем)

ИНЦ.3
ИНЦ.6

- Хранение и выгрузка трафика для выбранных сессии



Поддержка промышленных устройств и протоколов



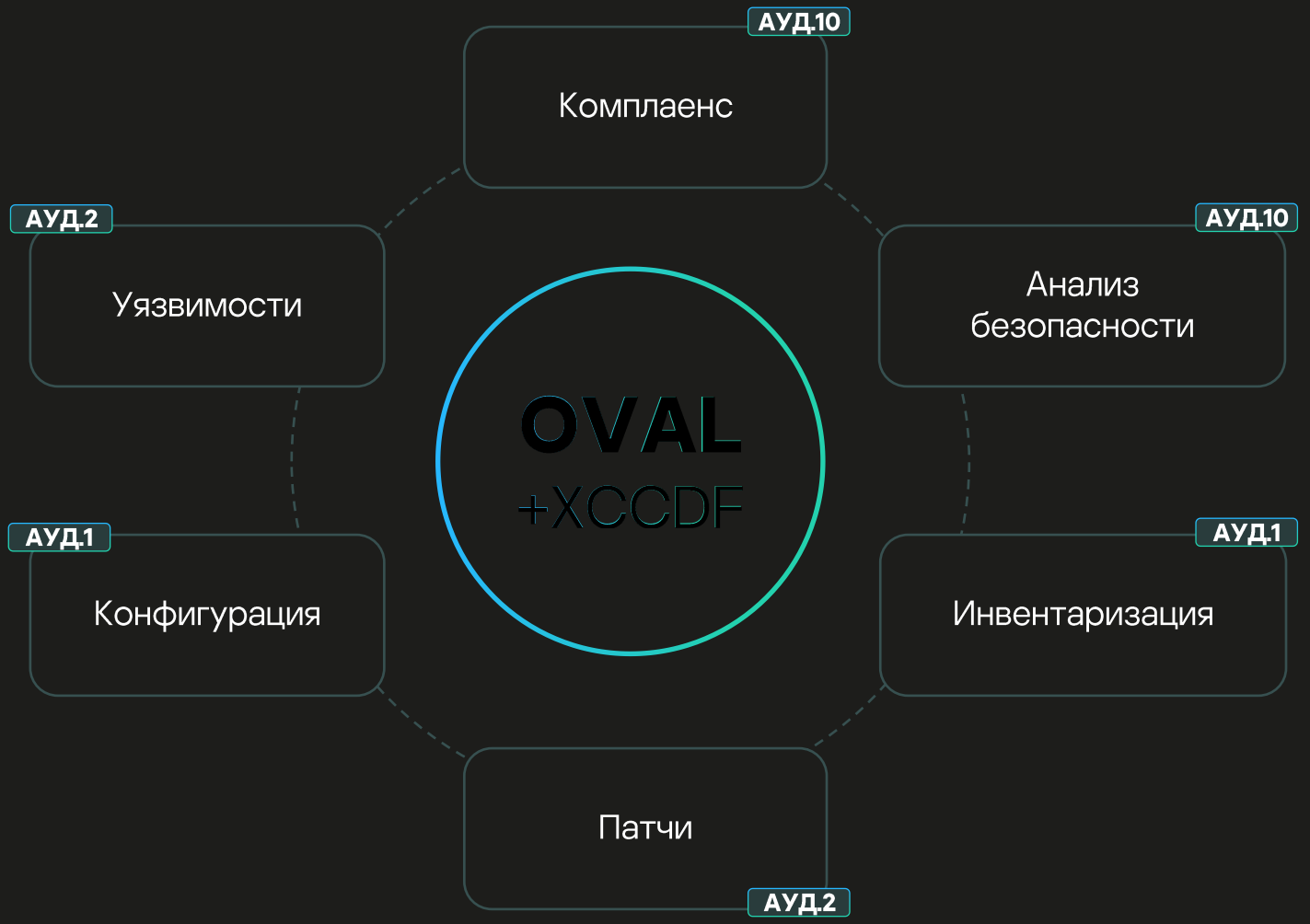
АУД.5

- Глубокая проверка пакетов для протоколов OT
- Поддержка новых устройств и протоколов предоставляется с обновлениями, без переустановки продукта и не в качестве дополнительного экспертного пакета
- Автоматическое определение и отслеживание значений тегов, автоматическая генерация правил процесса, готовых к включению
- Импорт SCADA-проектов для ввода информации об активах и тегах

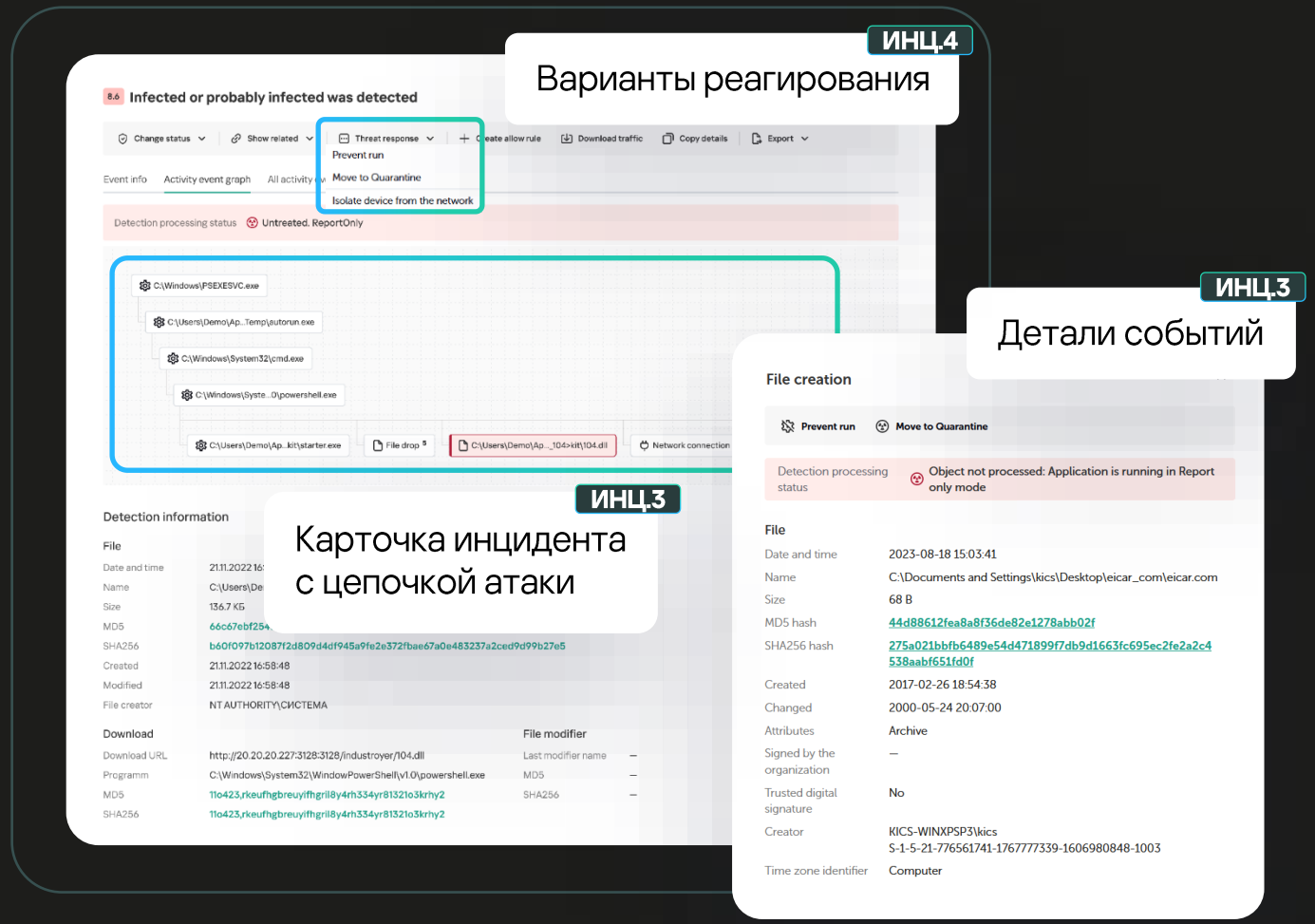
Централизованная система аудита узлов промышленной сети

Ключевые преимущества

- Аудит безопасности для узлов на Windows, Linux и сетевого оборудования
- Встроенная база уязвимостей для промышленного ПО от Kaspersky ICS CERT
- Поддержка сторонних и пользовательских баз
- Отчёты, результаты аудита и история проверок доступны в одном месте



KICS XDR: телеметрия с узла, обнаружение и реагирования



Нативный XDR

для расследования инцидентов и реагирования на них

- **АУД.4** **АУД.7** **ИНЦ.6** KICS for Networks – единая консоль для хранения и просмотра событий в сети и на конечных узлах
- **ИНЦ.3** Построение цепочки атаки по телеметрии с конечного узла
- **ИНЦ.4** Возможность точечного реагирования: отправить файл на карантин, запретить запуск, изолировать узел

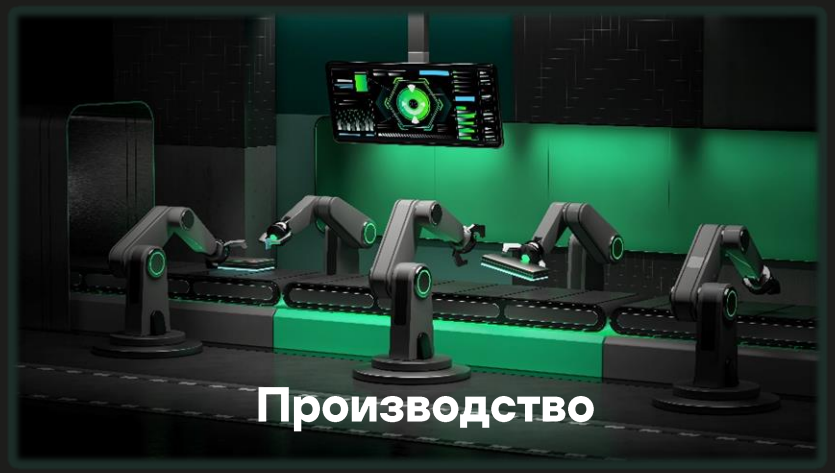
Отчеты

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

Сертификаты ФСТЭК и ФСБ

Решение	ФСТЭК России	ФСБ России
KICS for Networks	Сертификат соответствия №4027 - Требования к СОВ - Профиль защиты СОВ уровня сети 4 класса - 4 уровень доверия	Сертификат соответствия №СФ/СЗИ-0685 - Средство обнаружения атак класса В
KICS for Nodes	Сертификат соответствия №3907 - Требования к САВЗ - Требования к средствам контроля СМНИ - Профиль защиты САВЗ типа В 2 класса - Профиль защиты СКСМНИ 2 класса - 2 уровень доверия	Сертификат соответствия №СФ/СЗИ-0695 - антивирусное средство класса В2
KICS for Linux Nodes	Сертификат соответствия №3907 - Требования к САВЗ - Профиль защиты САВЗ типа В 2 класса - 2 уровень доверия	Сертификат соответствия №СФ/СЗИ-0617 - антивирусное средство класса В2

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/

Регуляторный хаб
https://regulhub.kaspersky.ru

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

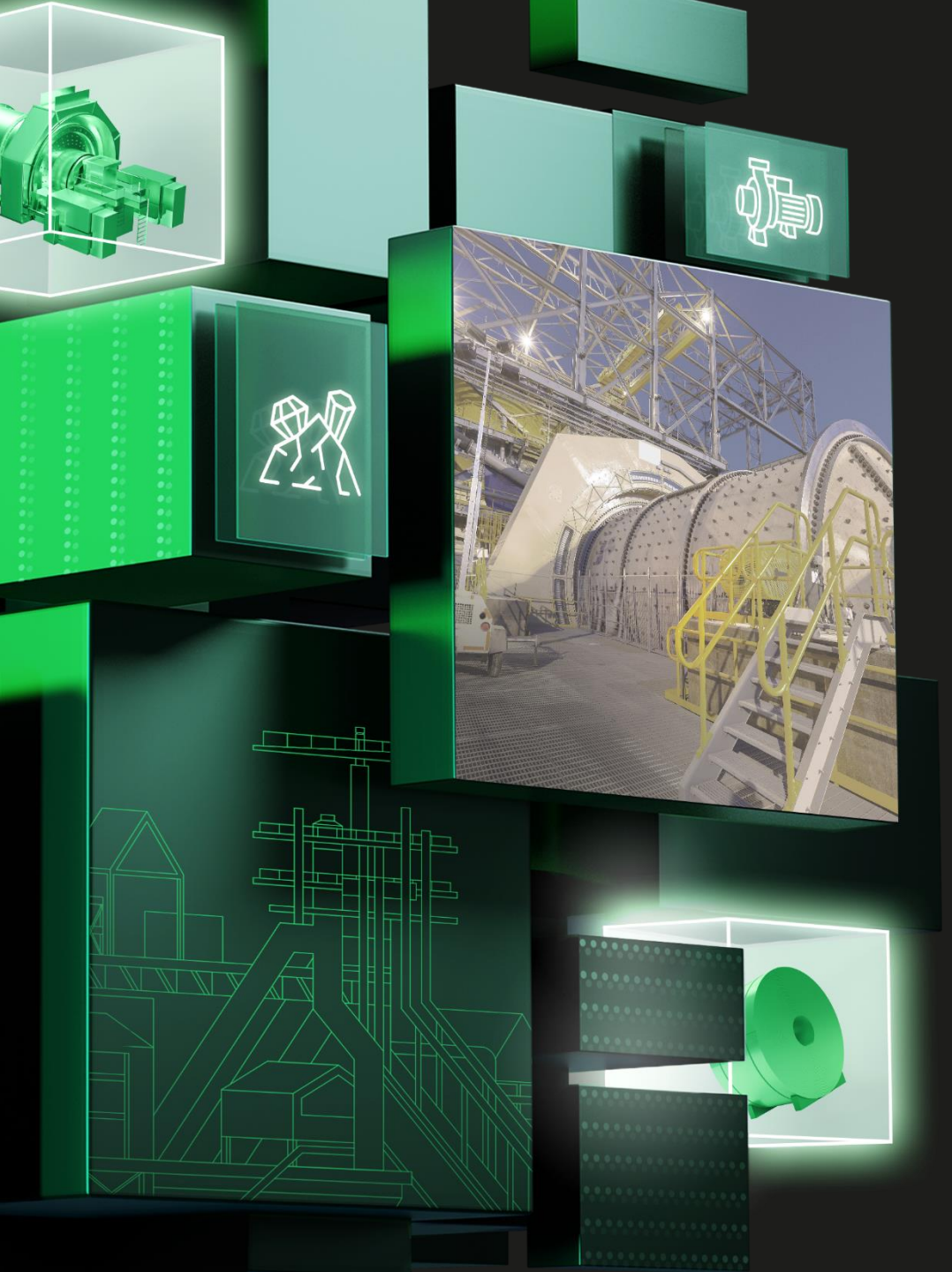
Отчеты Kaspersky ICS Cert
https://ics-cert.kaspersky.ru/

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

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

Сертификаты ФСТЭК и ФСБ
https://support.kaspersky.ru/common/certificates

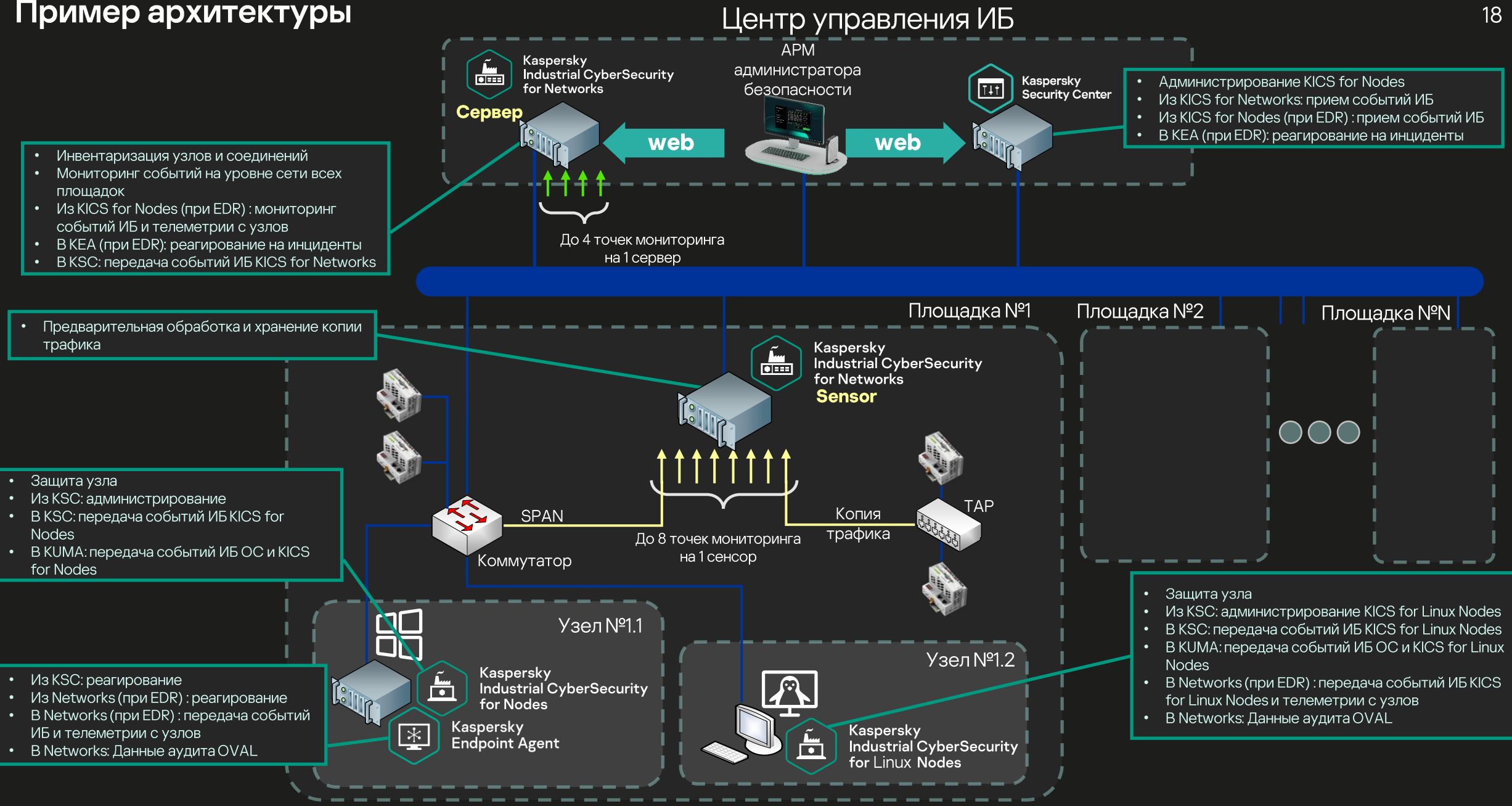
Сертифицированные партнеры
https://locator.kaspersky.com



Спасибо!

boris.doroshenko@kaspersky.com

Пример архитектуры



- Инвентаризация узлов и соединений
- Мониторинг событий на уровне сети всех площадок
- Из KICS for Nodes (при EDR) : мониторинг событий ИБ и телеметрии с узлов
- В KEA (при EDR): реагирование на инциденты
- В KSC: передача событий ИБ KICS for Networks

- Администрирование KICS for Nodes
- Из KICS for Networks: прием событий ИБ
- Из KICS for Nodes (при EDR) : прием событий ИБ
- В KEA (при EDR): реагирование на инциденты

- Предварительная обработка и хранение копии трафика

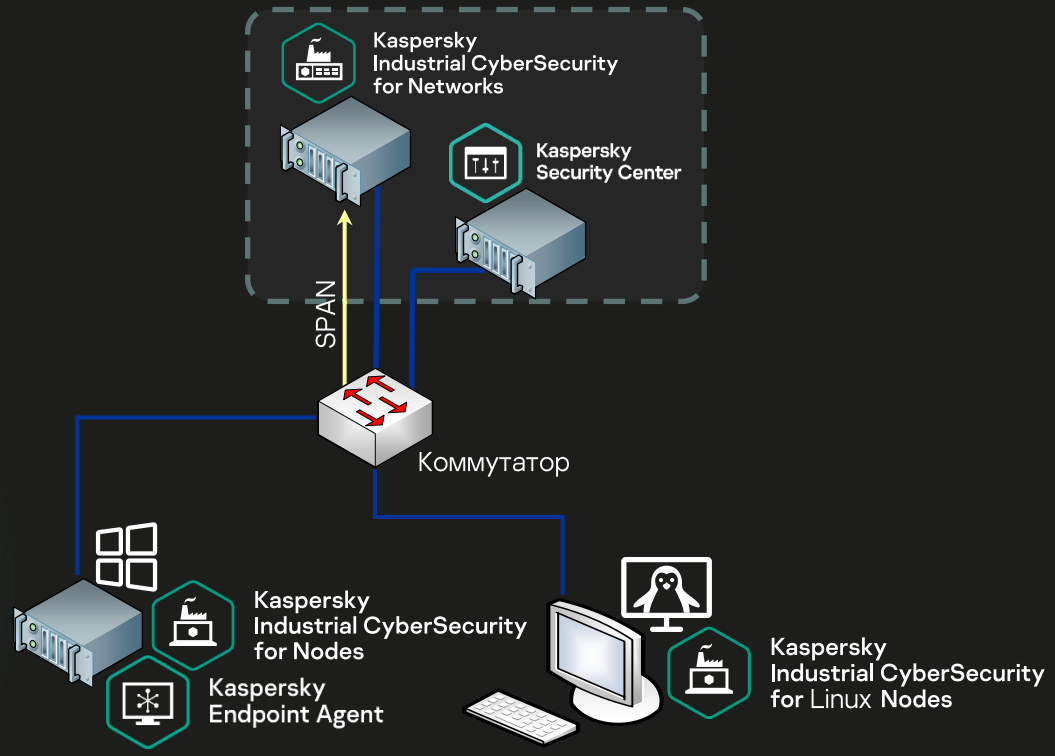
- Защита узла
- Из KSC: администрирование
- В KSC: передача событий ИБ KICS for Nodes
- В KUMA: передача событий ИБ ОС и KICS for Nodes

- Из KSC: реагирование
- Из Networks (при EDR) : реагирование
- В Networks (при EDR) : передача событий ИБ и телеметрии с узлов
- В Networks: Данные аудита OVAL

- Защита узла
- Из KSC: администрирование KICS for Linux Nodes
- В KSC: передача событий ИБ KICS for Linux Nodes
- В KUMA: передача событий ИБ ОС и KICS for Linux Nodes
- В Networks (при EDR) : передача событий ИБ KICS for Linux Nodes и телеметрии с узлов
- В Networks: Данные аудита OVAL

Варианты защиты узлов

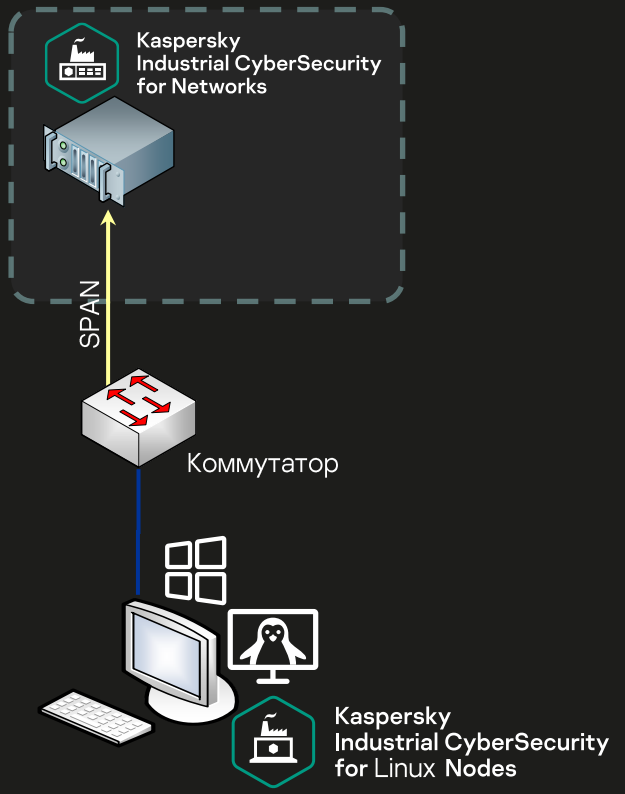
Центр управления ИБ



- Администрирование KICS for Nodes и KEA
- Защита узла (антивирус, контроль запуска ПО и др.)
- Выявление сетевых угроз
- Передача информации об узле в KICS for Networks
- Аудит безопасности
- EDR: Передача событий и телеметрии в KICS for Networks
- EDR: Реагирование из KICS for Networks

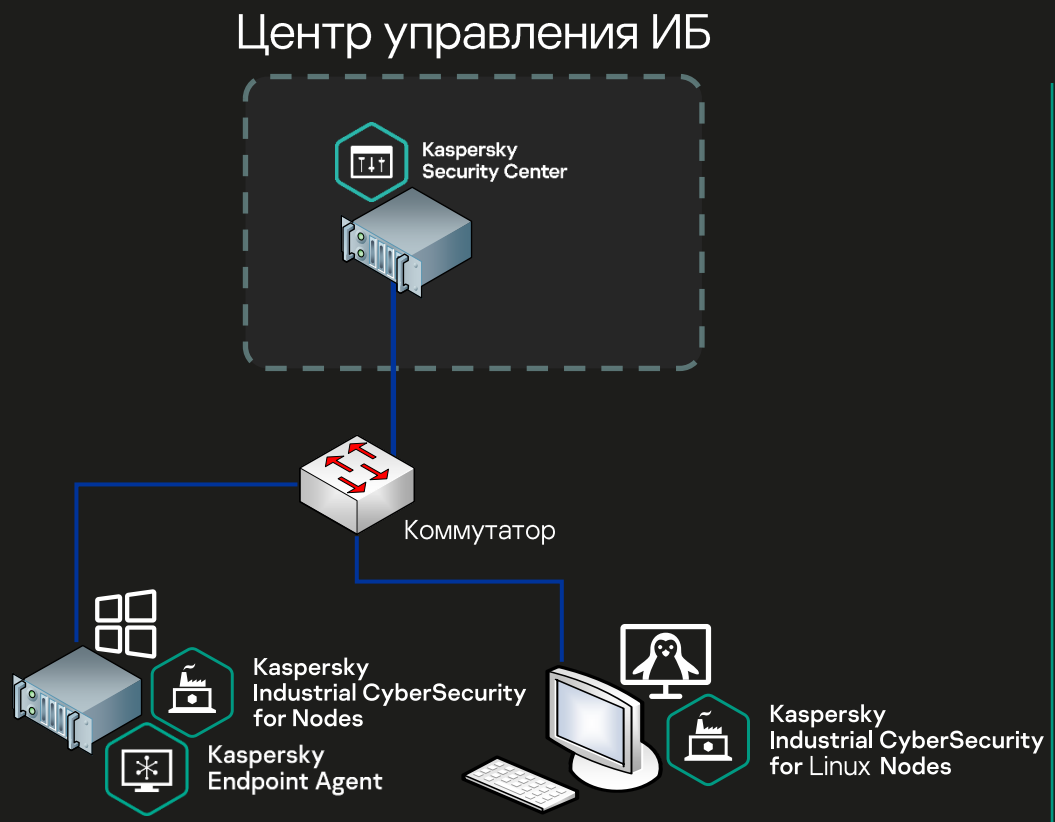
- Администрирование KICS for Linux Nodes
- Защита узла (антивирус, контроль запуска ПО и др.)
- Выявление сетевых угроз
- Передача информации об узле в KICS for Networks
- Аудит безопасности
- EDR: Передача событий и телеметрии в KICS for Networks

Центр управления ИБ

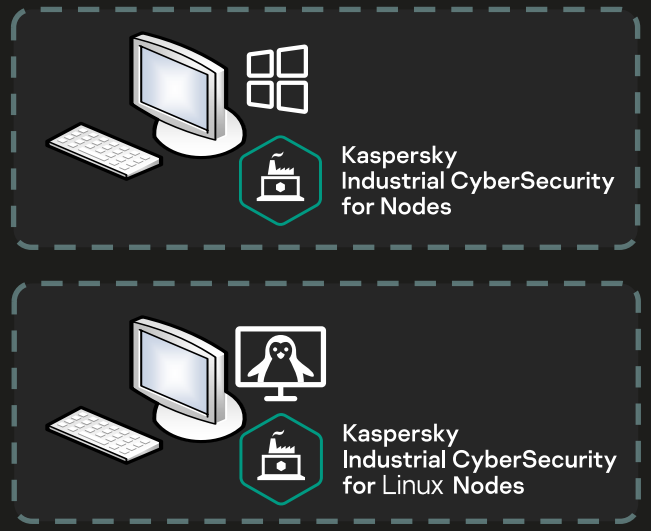


- Защита узла (антивирус, контроль запуска ПО и др.)
- Выявление сетевых угроз

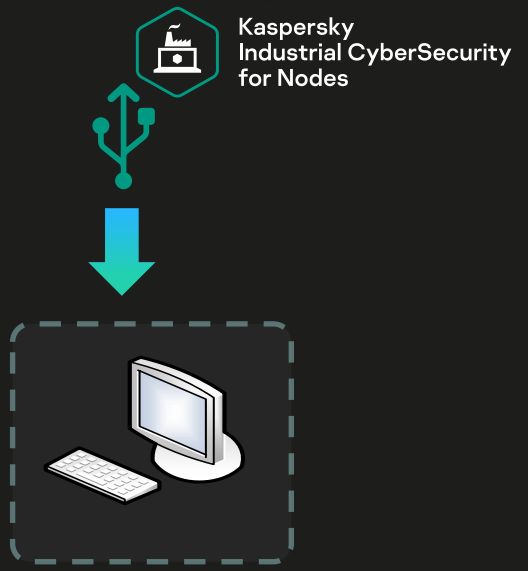
Варианты защиты узлов



- Администрирование KICS for Nodes и KEA
- Защита узла (антивирус, контроль запуска ПО и др.)
- Передача событий в KSC



- Защита узла (антивирус, контроль запуска ПО и др.)



- Антивирусное сканирование