Еще больше XDR

Обновление промышленной XDR-платформы **Kaspersky Industrial CyberSecurity**

kaspersky

Единая концепция промышленной безопасности

Знания

Аналитика об угрозах

- Kaspersky ICS Threat Intelligence

Повышение осведомленности

- Kaspersky Security Awareness

Тренинги для специалистов

- Kaspersky ICS CERT Training

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Технологии

Основные

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Unified Monitoring and Analysis Platform

Фокусные

- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN
- Kaspersky Antidrone

Решения на базе KasperskyOS

- Kaspersky IoT Secure Gateway
- Kaspersky Secure Remote Workspace
- Kaspersky Automotive Secure Gateway

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

Экспертиза

Анализ защищенности

- Kaspersky ICS Security Assessment

Управляемая защита

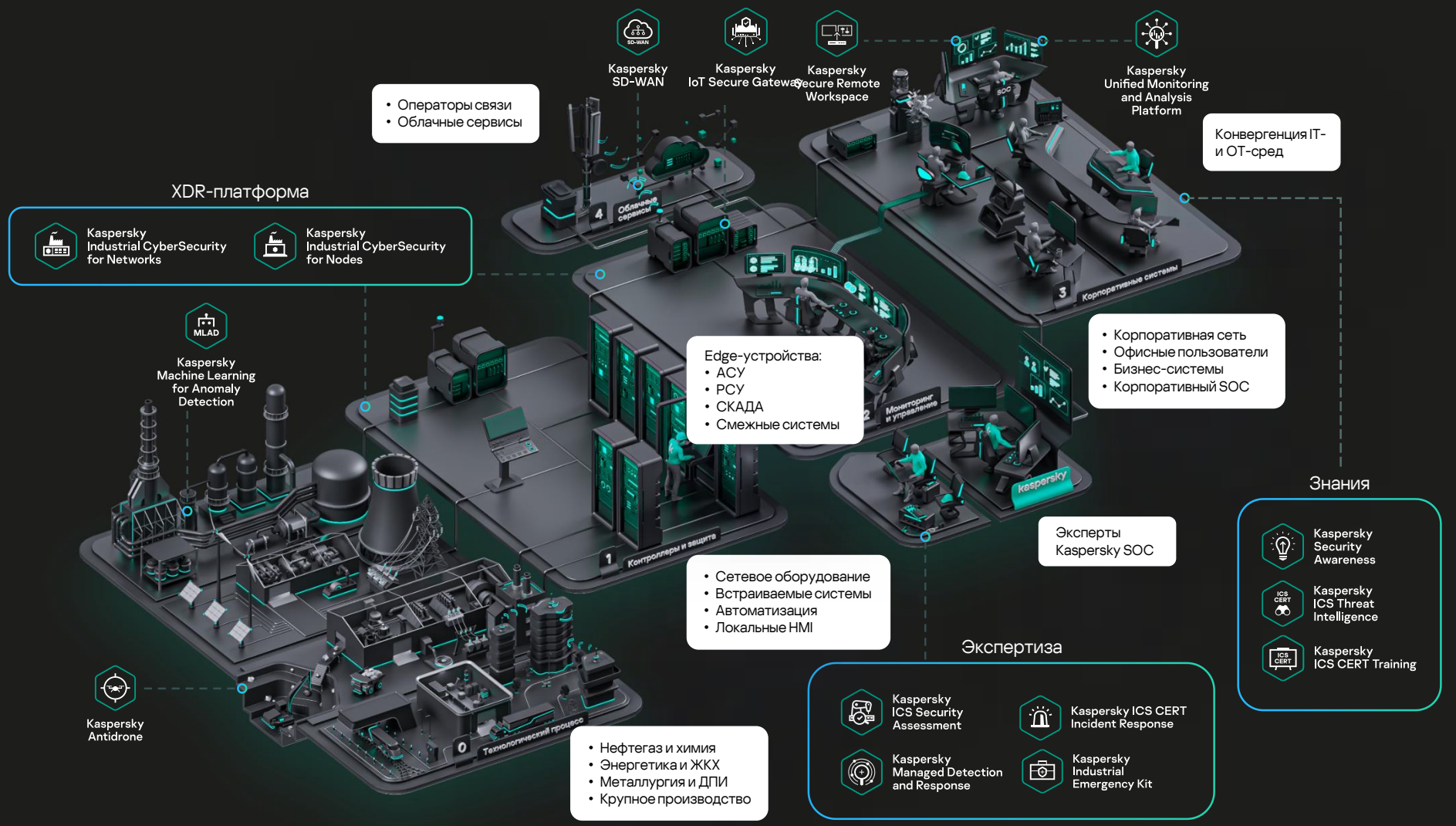
- Kaspersky Managed Detection and Response

Скорая помощь

- Kaspersky ICS CERT Incident Response
- Kaspersky Industrial Emergency Kit

Набор экспертных сервисов для комплексной промышленной кибербезопасности

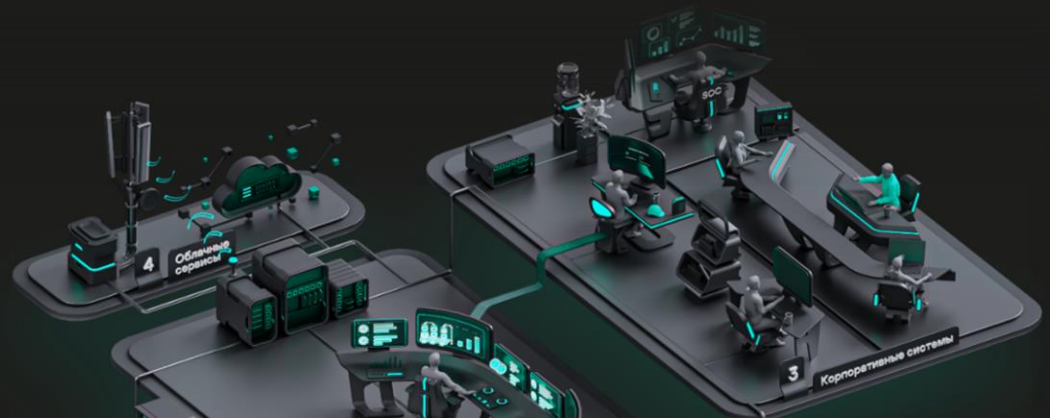
Экосистема промышленной безопасности



Гибкий подход к OT XDR

Сложность структуры сети, выработанная стратегия и уровень зрелости ИБ

Нативный OT XDR	Открытый OT XDR	Единый IT-OT XDR



Функциональное сравнение OT XDR

Kaspersky OT XDR	Нативный OT XDR	Открытый OT XDR	Единый IT-OT XDR
Состав	Kaspersky Industrial CyberSecurity	Kaspersky Industrial CyberSecurity + KUMA	Kaspersky Industrial CyberSecurity + Kaspersky Symphony XDR
Защита инфраструктуры конечных точек в промышленной сети (KICS for Nodes + EDR)	●	●	●
Мониторинг промышленной сети и анализ трафика (KICS for Networks)	●	●	●
Комплексный мониторинг и корреляция событий ИБ (SIEM), встроенный модуль ГосСОПКА, интеграция с различными ИБ-системами		●	●
Управление аналитическими данными о киберугрозах		●	●
Комплексная защита корпоративной сети (IT XDR)			●
Единый граф расследования, плейбуки и управление инцидентами, благодаря платформе управления Kaspersky Single Management Platform			●

Сценарии OT XDR-платформы

Kaspersky Industrial CyberSecurity for Nodes

Инструменты класса
EPP и EDR, аудит

- Сервер
- Рабочая станция
- Портативные сканеры

Kaspersky Industrial CyberSecurity

- Единая консоль
- Нативная интеграция
- Кросс-продуктовые сценарии
- Общий kill-chain

Управление рисками и активами

- Пассивное обнаружение компонентов и уязвимостей OT
- Дополнительный активный опрос, ориентированная на риск ситуационная осведомленность и отчетность

Kaspersky Industrial CyberSecurity for Networks

Анализ сетевого трафика
(ICS DPI, IDS)

- Сервер
- Сенсор

Статус защиты

Аудит безопасности

Сетевые коммуникации

Передача телеметрии хоста

Контроль оборудования

Реагирование на инциденты

Почему XDR важен для промышленности

Показывает скрытые угрозы, аномалии, уязвимости и попытки вторжений задолго до того, как это стало опасным

Сертифицировано вендорами АСУ ТП и регуляторами

Не влияет на технологический процесс, исключает недопустимый ущерб

Помогает управлять сложной распределенной инфраструктурой автоматизации и реагировать на инциденты

Преимущества

Аудит узлов, опрос сетевых устройств, централизованное управление рисками, политиками безопасности и активами на всех уровнях АСУ

Непревзойденная прозрачность при расследовании нарушений. Визуализация развития инцидента в сети и на узлах

Полное покрытие инфраструктуры АСУ. Защита Linux, Windows, изолированных или приносимых компьютеров, обнаружение сетевых аномалий и угроз

Kaspersky Industrial CyberSecurity XDR-платформа

Нативная XDR-платформа для комплексной защиты предприятий всех отраслей промышленности

Обновление платформы

1. Усиление NTA-функциональности
2. Новые XDR-сценарии
3. Аудит безопасности
4. Обновления продуктов KICS

Усиление NTA-функциональности

Сетевые сессии

Сетевые сессии

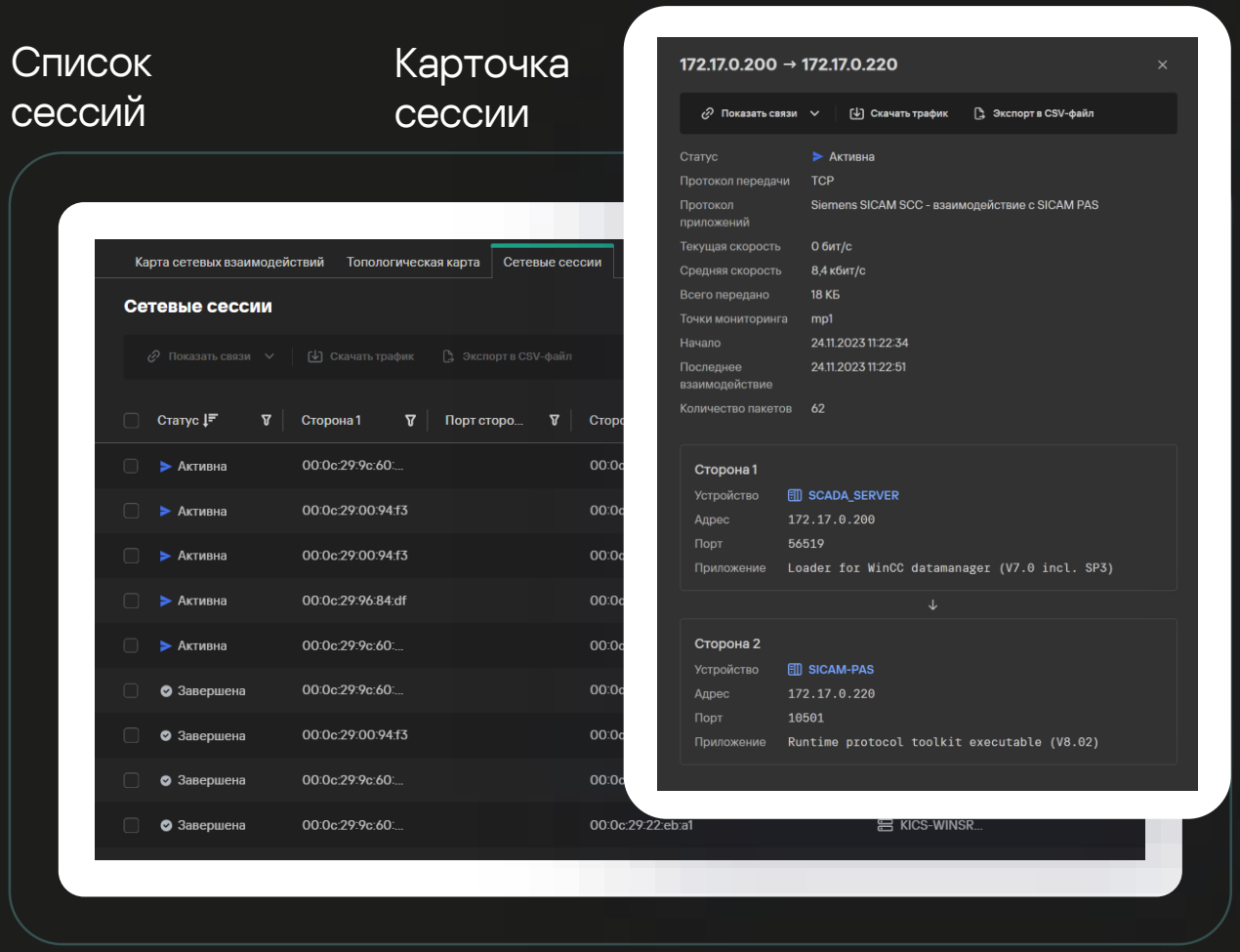
- Статус сессии (Активна/Завершена)
- Направление
- Транспортный протокол и L7 протокол
- Статистика (скорость, объем данных и т.п.)

Сценарии

- Сбор статистики по сессиям протокола
- Регистрация периода активности сессий
- Выгрузка трафика для выбранных сессий

Список сессий

Карточка сессии



Хранение и выгрузка трафика

Хранение сырого трафика

Встроенное локальное хранилище на Сервере и Сенсоре

Подключение внешнего хранилища для хранения больших объемов трафика

Задание ограничений по объёму

Фильтрация трафика, отправляемого в хранилище

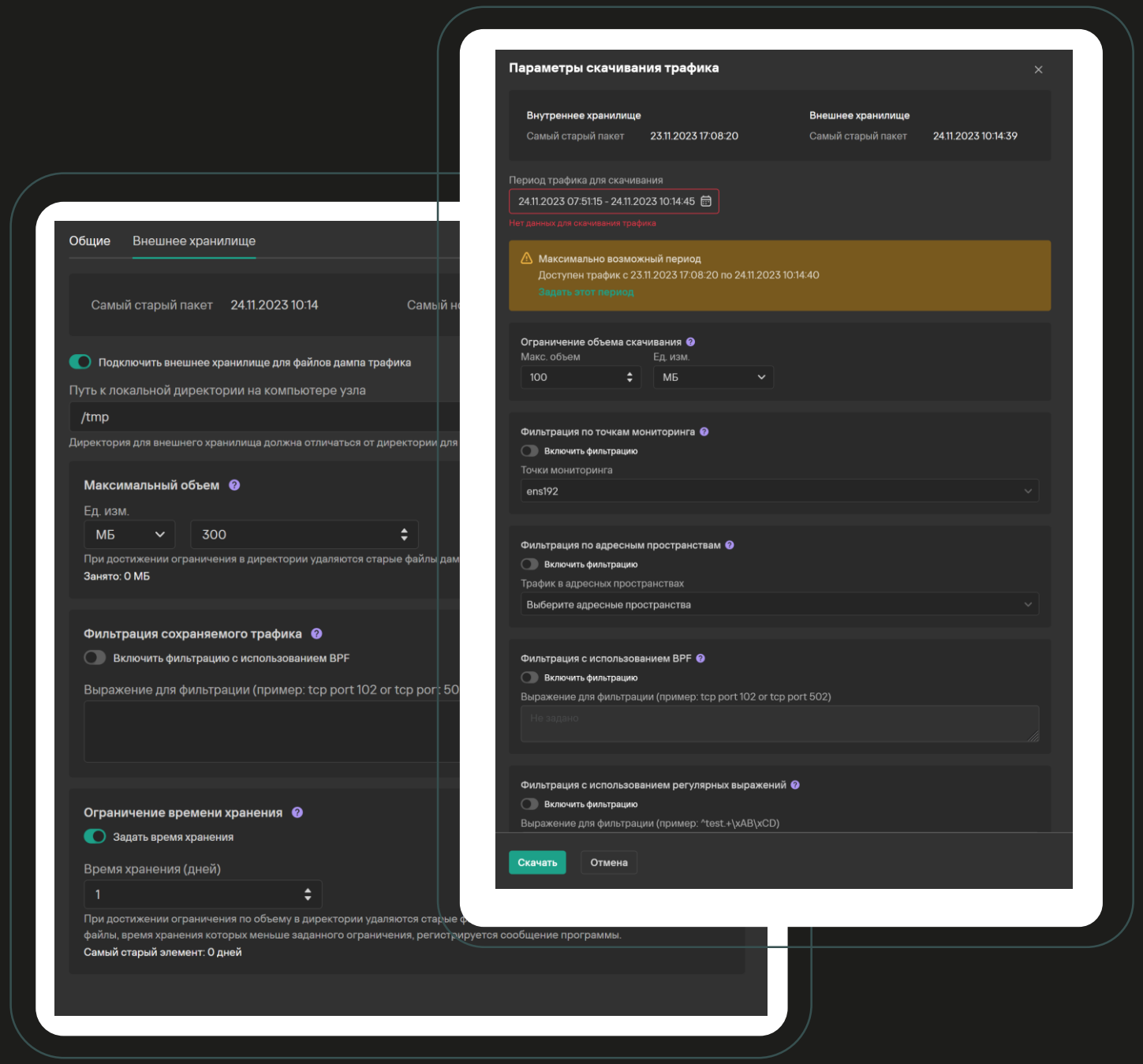
Выгрузка трафика по запросу

Задание ограничений по объему

Применение BPF фильтров

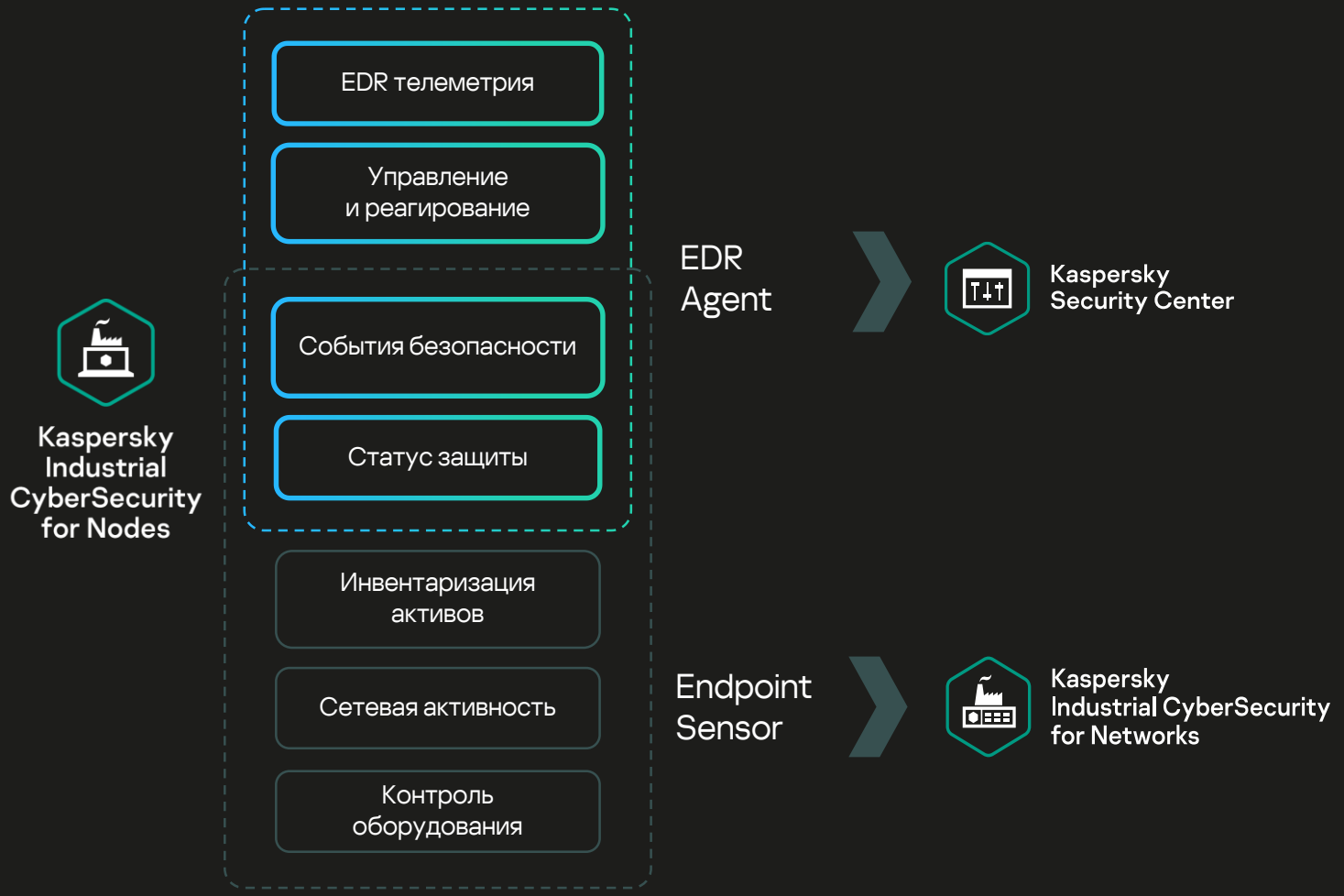
Загрузка трафика для выделенного сегмента сети

Поиск по регулярным выражениям



Новые XDR-сценарии

Функции узлового сенсора



Kaspersky Industrial CyberSecurity for Nodes

Многофункциональное решение

EPP, EDR агент с возможностью инвентаризации и аудита

Промышленный EDR

Обнаружение и телеметрия для анализа первопричин, реагирования при необходимости

Телеметрия с конечного узла

Полная видимость и ситуационная осведомленность благодаря обнаружениям и обогащению данных с конечного узла

Развитие XDR возможностей, интеграция с KICS EDR

KICS for Networks —
единая точка для сбора всех событий с промышленных узлов сети и из трафика

Индикаторы компрометации для всех алертов позволяют быстро расследовать угрозу и найти другие скомпрометированные узлы в сети

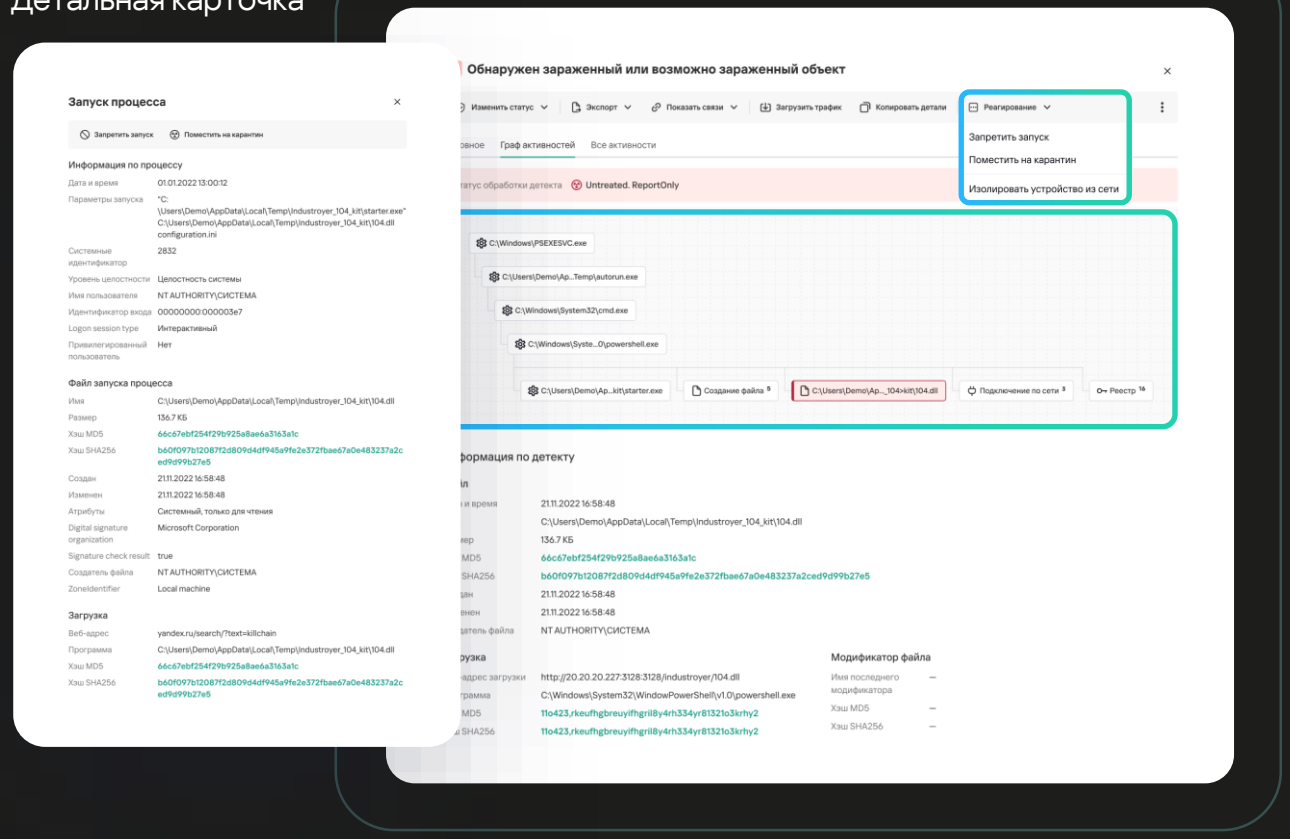
Базовые меры реагирования позволяют экстренно предотвратить развитие атаки в технологической сети

Сетевые и узловые алерты отображены в едином списке событий, скоррелированы в инциденты в виде цепочки атаки с графом для расследования точки проникновения в систему

Детальная карточка

Граф цепочки атаки на узле

Реагирование



Аудит безопасности

Аудит безопасности

Удаленный

Настройка рабочих станций и серверов:

Настройки безопасности Linux

Конфигурация сетевых устройств:

Активное сетевое оборудование

Агент (KICS for Nodes)

Настройка рабочих станций и серверов:

Настройки безопасности Windows

Уязвимости:

Инвентаризация промышленного ПО и обнаружение уязвимостей

Ключевые преимущества

Аудит безопасности для узлов на Windows, Linux и сетевого оборудования

Открытый язык описаний Open Vulnerability and Assessment Language (OVAL)

Полнофункциональный редактор для проверок и параметров безопасности

Встроенная база уязвимостей для промышленного ПО от Kaspersky ICS CERT

Задачи для одного узла или групповые, запускаемые вручную или по расписанию

Поддержка сторонних и пользовательских баз OVAL

Отчёты, результаты аудита и история проверок доступны в одном месте

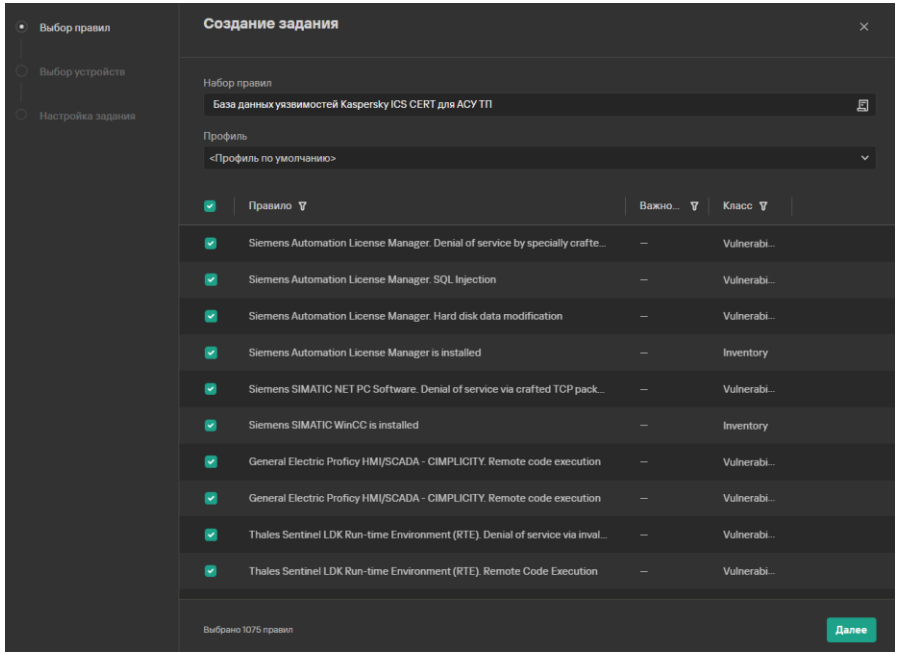
Защищённое хранилище секретов для безагентского аудита

Конфигурации безопасности из коробки

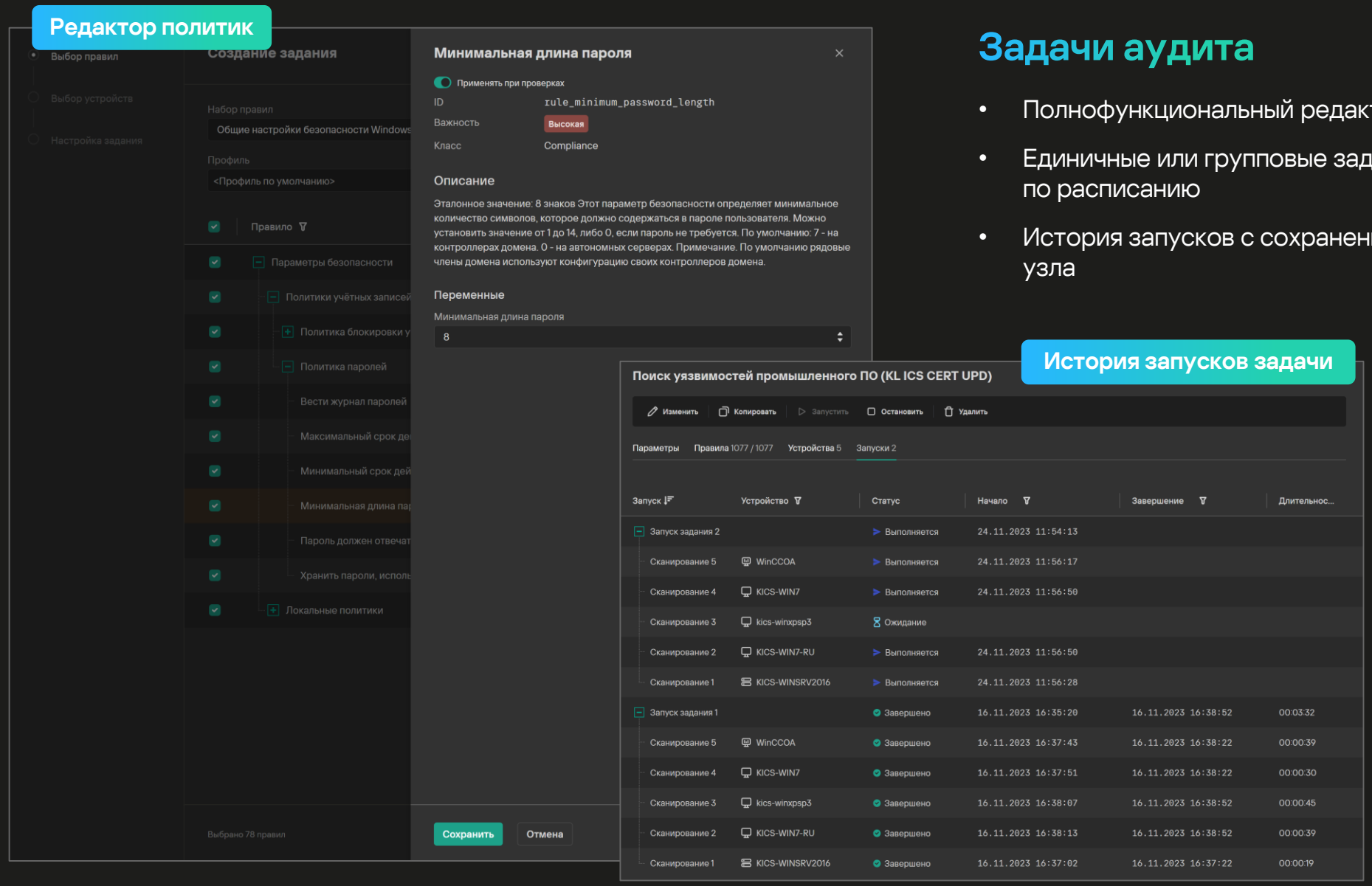
Kaspersky ICS CERT уязвимости АСУ ТП	Windows XP/7/8.1/10/11	Windows Server 2012/2012 R2/2016/2019/2022
Debian	Red Hat Enterprise Linux, CentOS, Oracle Linux	Ubuntu
SUSE Linux Enterprise, openSUSE	Маршрутизаторы и коммутаторы Cisco, Fortigate	

Новые конфигурации будут доставляться в рамках обновления баз продукта

Большой выбор систем АСУ ТП для поиска уязвимостей



Задачи аудита безопасности

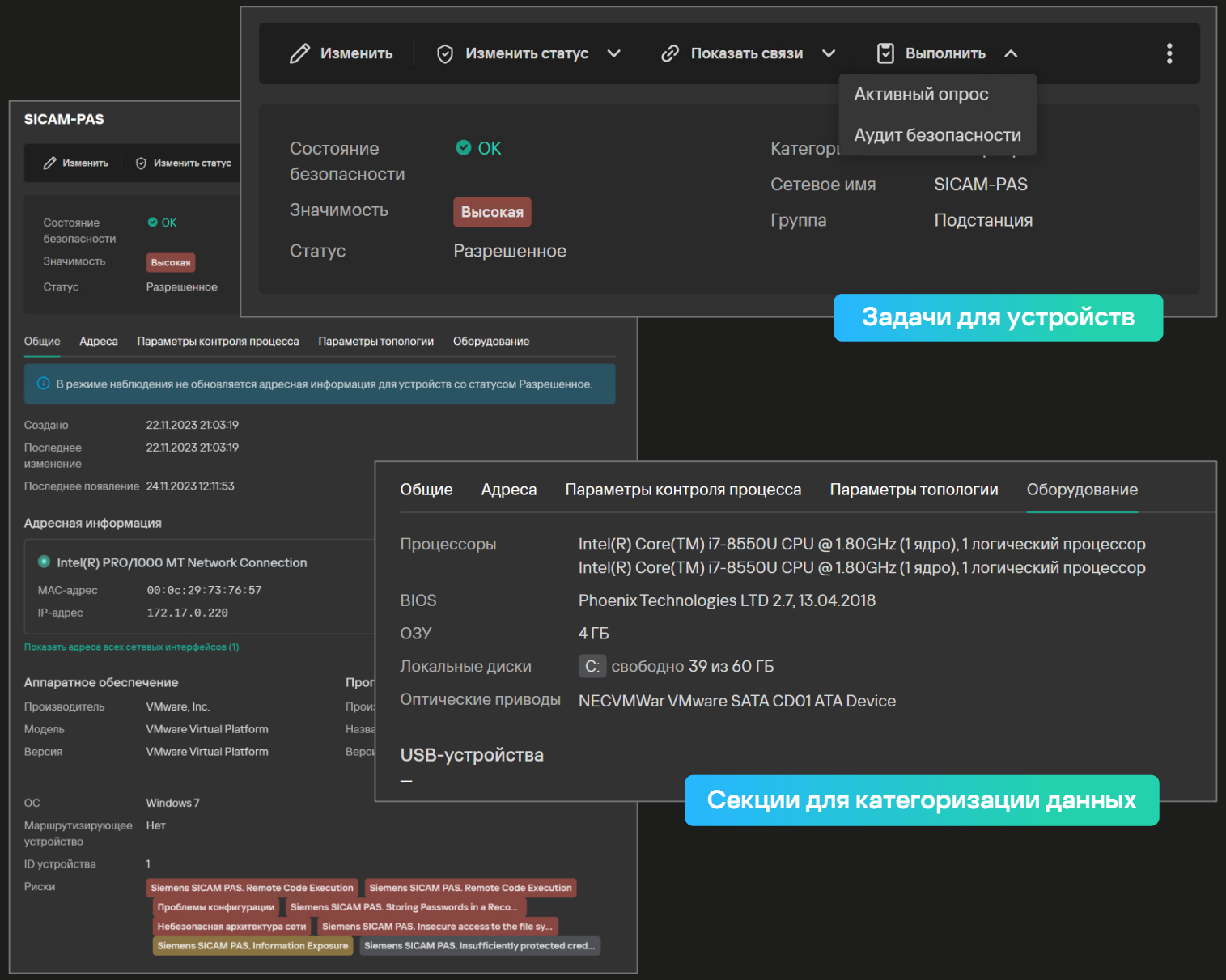


Задачи аудита

- Полнофункциональный редактор задач
- Единичные или групповые задачи, запускаемые вручную или по расписанию
- История запусков с сохранением результатов для каждого узла

Обновления продуктов KICS

Новый дизайн карточек устройств и событий



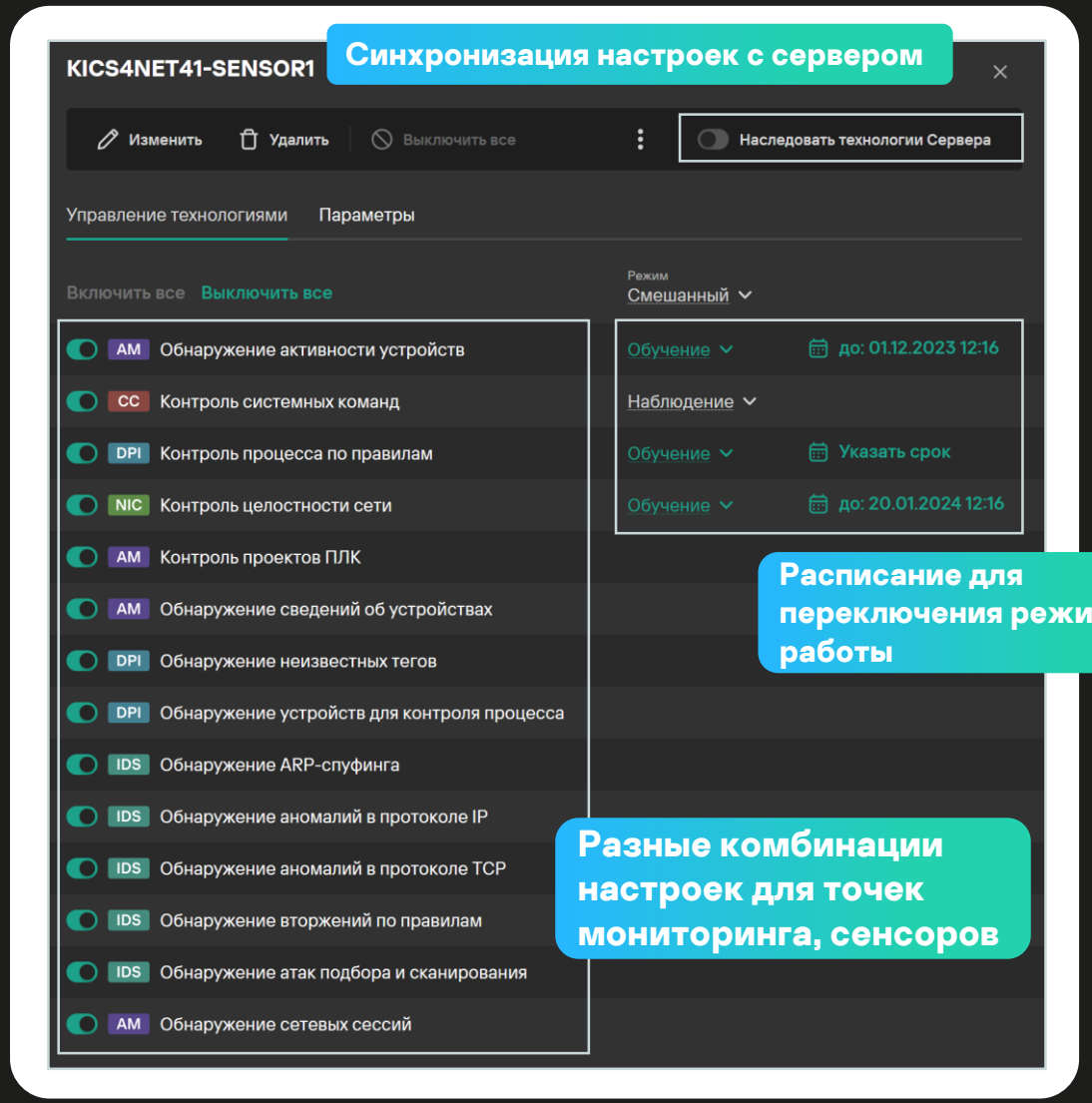
Новый дизайн для удобного управления устройствами и событиями

- Оптимизация пространства, больше информации в карточке
- Данные в карточке разбиты по секциям
- Множество инструментов для работы с событиями и устройствами
- Создание задач по активному опросу, аудиту устройств

Гранулярное обучение

Упрощённый подход к внедрению, настройке и расширению системы

- Автоматический перевод системы из режима обучения в режим мониторинга и по расписанию
- Гибкость настройки режима работы для сервера, сенсоров, точек мониторинга – доступны разные комбинации
- Расширение системы можно выполнить полностью безударно для действующей инсталляции – точки мониторинга, сенсоры можно добавлять на лету, устанавливать независимые от основной системы режимы работы



Обновление KICS for Nodes

Контроль проекта ПЛК

Проверка целостности проекта ПЛК позволяет выявить попытки изменения технологического процесса

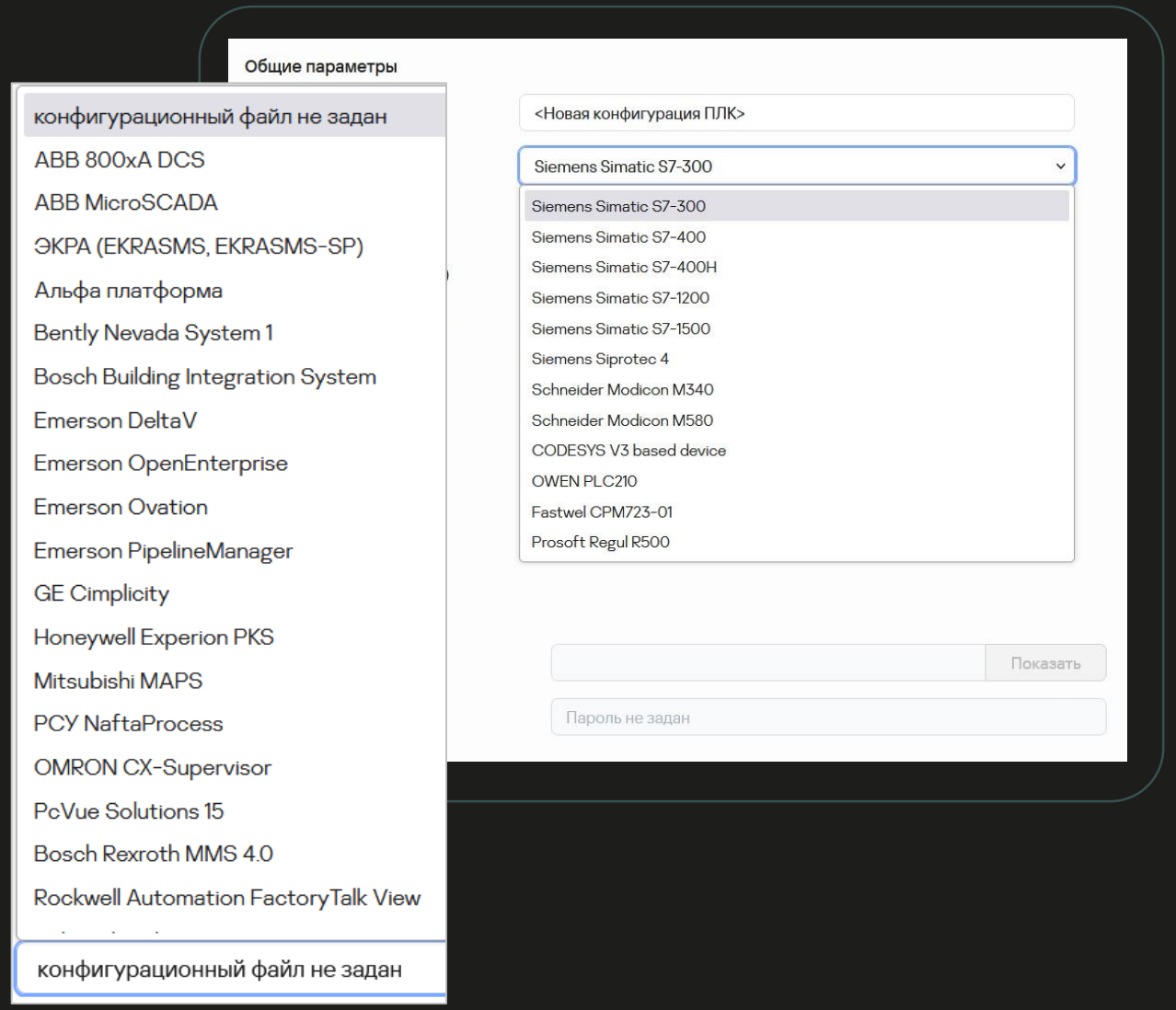
Сертификация и тестирование с системами автоматизации

- Взаимодействие с крупнейшими вендорами АСУ ТП
- Проверка совместимости и корректной работы
- Проработка совместных архитектур с системами АСУ ТП

Рекомендованные настройки под разные системы

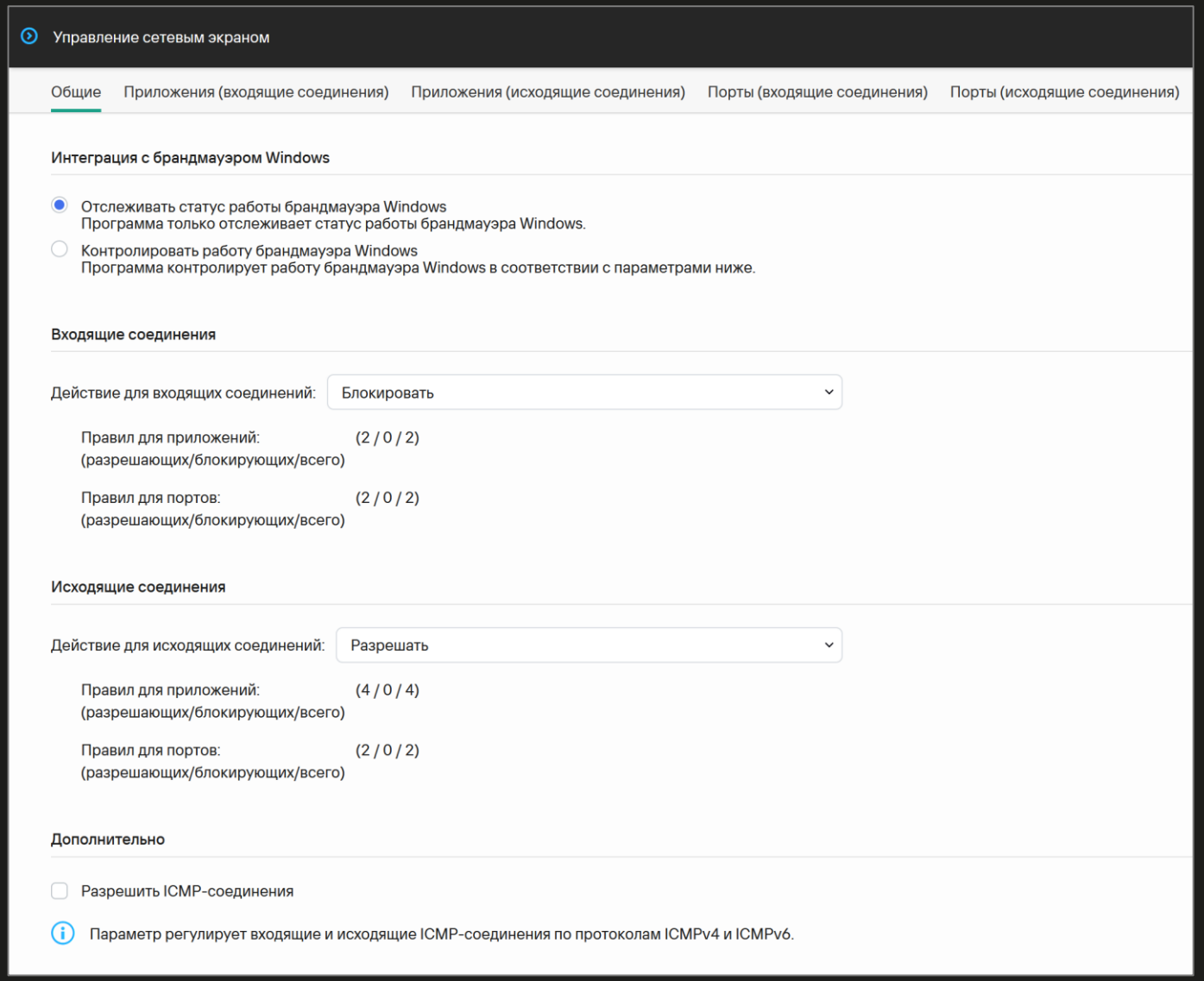
Из коробки предоставляются пред-настроенные политики с доверенной зоной под различные системы

- Экспертиза на базе совместных испытаний
- Общие гайды по внедрению
- Поддержка и внедрение экспертами с опытом работы в индустрии



Обновление контроля активности сети

- Детектирование MAC spoofing
- Настройка интеграции с сетевым экраном – мониторинг работы или управление
- Правила для исходящих соединений
- Создание разрешающих и запрещающих правил для приложений



KICS for Linux Nodes

Linux Nodes

Антивирус

Контроль запускаемых приложений

Контроль устройств

Контроль целостности файлов

Защита от шифрования сетевых папок

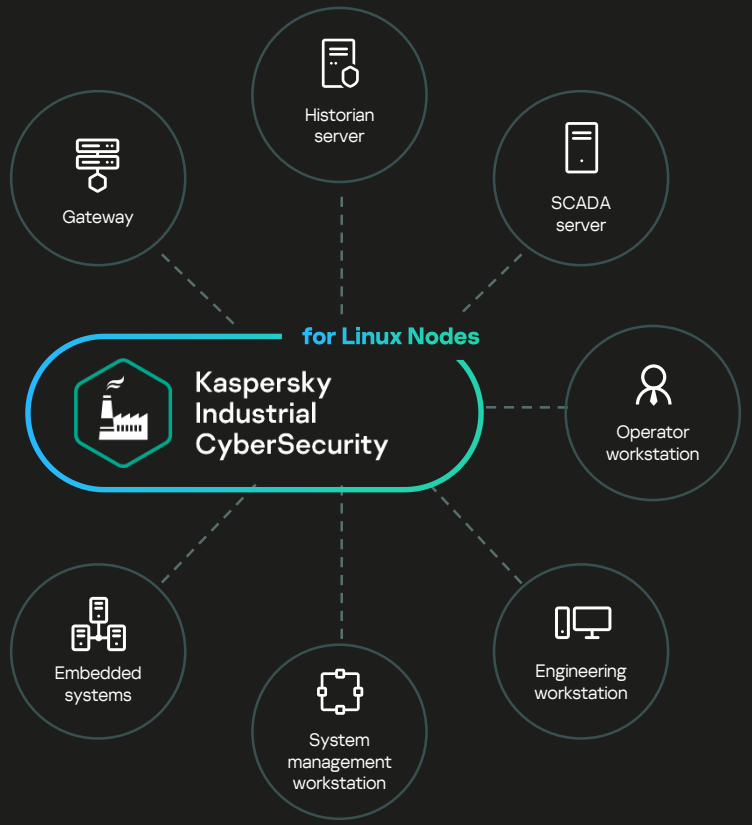
Анализ поведения

Защита от сетевых угроз

Управление Firewall

Сенсор телеметрии (Интеграция с KICS for Networks)

Industrial Endpoint Protection



KICS for Nodes. Портативный сканер

Решает задачи:

- Сканирование или защита автономных систем
- Сканирование или защита 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 на месте

- Преобразуйте флэш-накопитель в портативный сканер KICS for Nodes
- Используйте этот портативный инструмент на нескольких узлах ICS, даже с устаревшей ОС
- Подход, не требующий установки и не влияющий на работу технологического узла
- Режимы блокировки или «только уведомлять»
- Отчеты для всех хостов, хранящиеся на портативном накопителе сканера

KICS for Nodes с KICS Portable лицензией

Любой USB флэш-накопитель

- Защита от копирования
- Работа с командной строкой
- Не требует установки

- Сканирование узла, не позволяющего установить какое-либо дополнительное ПО

- Отчет о сканировании сохраняется на флэш-накопитель.
- Сканирование узлов один за другим одним флэш-накопителем

Спасибо!

Kaspersky Industrial
CyberSecurity

kaspersky