

Еще больше XDR

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



kaspersky

## 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



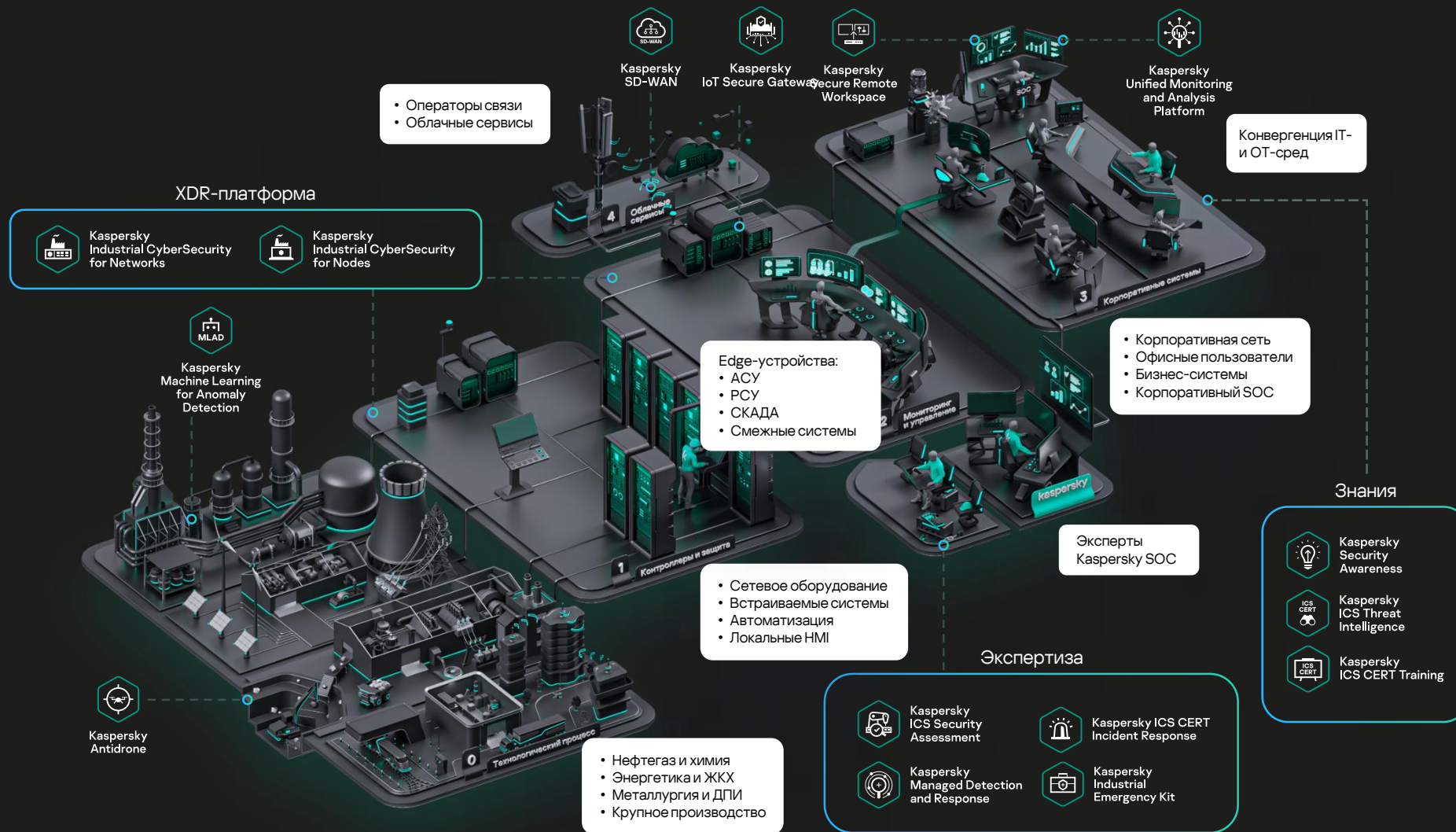
Kaspersky ICS CERT Incident Response



Kaspersky Industrial Emergency Kit

Набор экспертных сервисов для комплексной промышленной кибербезопасности

# Экосистема промышленной безопасности



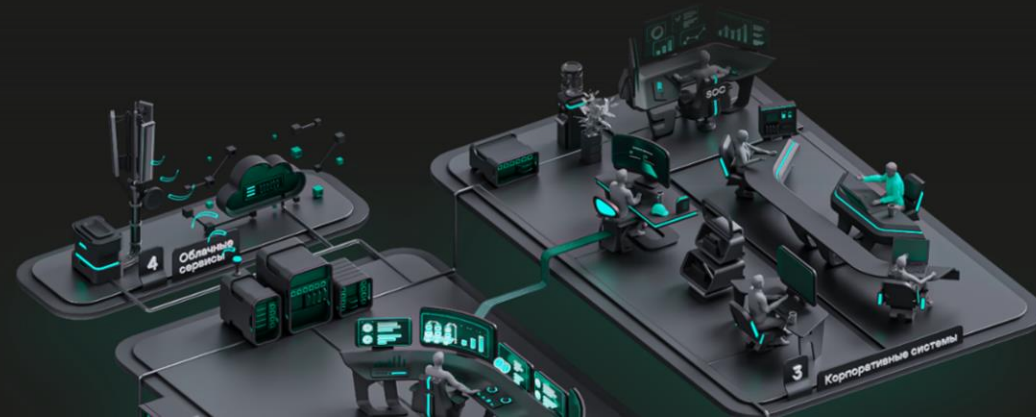


Сложность структуры сети, выработанная стратегия и уровень зрелости ИБ

Нативный  
ОТ XDR

Открытый  
ОТ XDR

Единый IT-  
ОТ 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

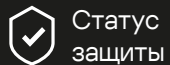


Комплексная защита корпоративной сети (IT XDR)



Единый граф расследования, плейбуки и управление инцидентами,  
благодаря платформе управления Kaspersky Single Management Platform





Статус защиты



Аудит безопасности



Сетевые коммуникации



Передача телеметрии хоста



Контроль оборудования



Реагирование на инциденты

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

- 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

The screenshot displays a network monitoring application interface. At the top, there are three tabs: 'Карта сетевых взаимодействий', 'Топологическая карта', and 'Сетевые сессии'. The 'Сетевые сессии' tab is active, showing a table of sessions. The table has columns for 'Статус', 'Сторона 1', 'Порт сторо...', and 'Сторо...'. Below the table, there are buttons for 'Показать связи', 'Скачать трафик', and 'Экспорт в CSV-файл'. A session card is overlaid on the right side of the screen, showing details for a session between IP addresses 172.17.0.200 and 172.17.0.220. The card includes a status bar with 'Показать связи', 'Скачать трафик', and 'Экспорт в CSV-файл'. The session details are as follows:

Статус	▶ Активна
Протокол передачи	TCP
Протокол приложений	Siemens SICAM SCC - взаимодействие с SICAM PAS
Текущая скорость	0 бит/с
Средняя скорость	8,4 кбит/с
Всего передано	18 КБ
Точки мониторинга	mp1
Начало	24.11.2023 11:22:34
Последнее взаимодействие	24.11.2023 11:22:51
Количество пакетов	62

The card also shows details for both sides of the session:

Сторона 1	
Устройство	SCADA_SERVER
Адрес	172.17.0.200
Порт	56519
Приложение	Loader for WinCC datamanager (V7.0 incl. SP3)

Сторона 2	
Устройство	SICAM-PAS
Адрес	172.17.0.220
Порт	10501
Приложение	Runtime protocol toolkit executable (V8.02)

# 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

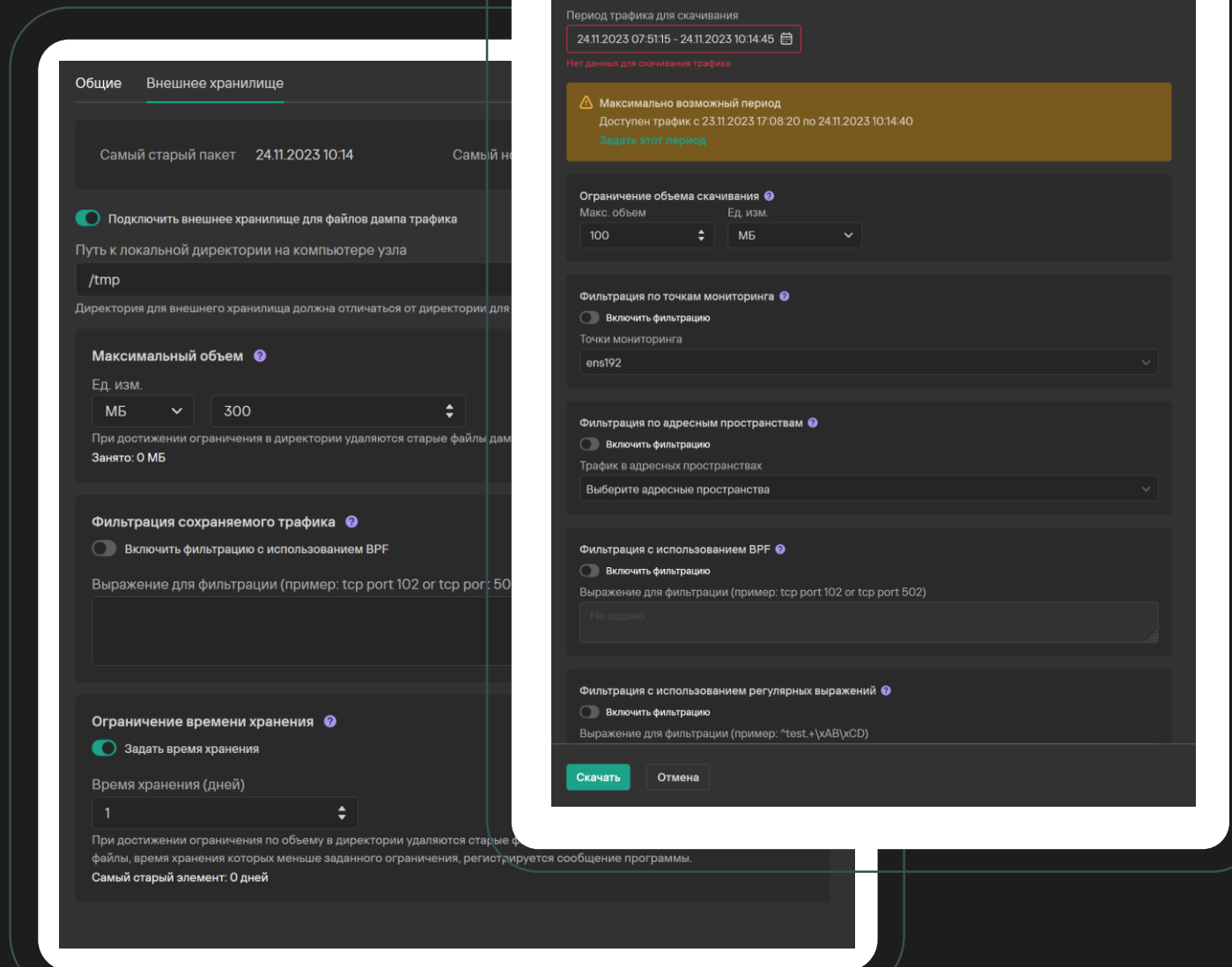
## Выгрузка трафика по запросу

Задание ограничений по объёму

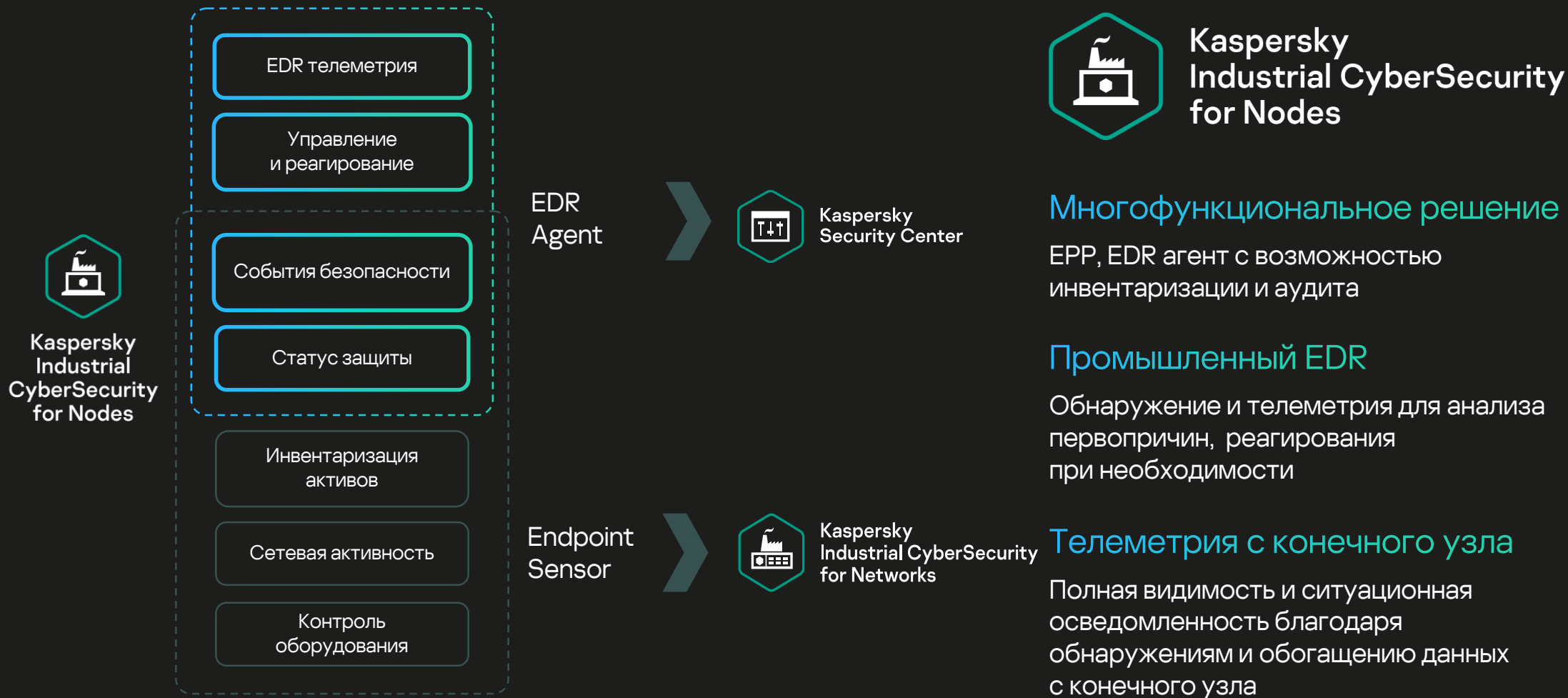
Применение BPF фильтров

Загрузка трафика для выделенного сегмента сети

Поиск по регулярным выражениям



# Новые XDR-сценарии



**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

Граф цепочки атаки на узле

Реагирование

Детальная карточка

The screenshot displays two main components of the KICS EDR interface. On the left is a 'Запуск процесса' (Process Launch) card, and on the right is a 'Граф цепочки атаки' (Attack Chain Graph) window.

**Запуск процесса (Process Launch Card):**

- Информация по процессу:** Дата и время: 01.01.2022 13:00:12. Параметры запуска: "C:\Users\Demo\AppData\Local\Temp\Industroyer\_104\_kit\starter.exe" C:\Users\Demo\AppData\Local\Temp\Industroyer\_104\_kit\104.dll configuration.ini. Системный идентификатор: 2832. Уровень целостности: Целостность системы. Имя пользователя: NT AUTHORITY\СИСТЕМА. Идентификатор входа: 00000000-000003e7. Login session type: Интерактивный. Пример привилегий пользователя: Нет.
- Файл запуска процесса:** Имя: C:\Users\Demo\AppData\Local\Temp\Industroyer\_104\_kit\104.dll. Размер: 136.7 KB. Хэш MD5: 66c67ebf254f29b925a8ae6a3163a1c. Хэш SHA256: b60f097b12087f2d809d4d945a9fe2e372fbae67a0e483237a2ced9f99b27e5. Создан: 21.11.2022 16:58:48. Изменен: 21.11.2022 16:58:48. Атрибуты: Системный, только для чтения. Digital signature organization: Microsoft Corporation. Signature check result: true. Создатель файла: NT AUTHORITY\СИСТЕМА. ZoneIdentifier: Local machine.
- Загрузка:** Веб-адрес: yandex.ru/search/?text=killchain. Программа: C:\Users\Demo\AppData\Local\Temp\Industroyer\_104\_kit\104.dll. Хэш MD5: 66c67ebf254f29b925a8ae6a3163a1c. Хэш SHA256: b60f097b12087f2d809d4d945a9fe2e372fbae67a0e483237a2ced9f99b27e5.

**Граф цепочки атаки (Attack Chain Graph):**

- Назван 'Обнаружен зараженный или возможно зараженный объект'.
- Показывает цепочку процессов: C:\Windows\PSEXESVC.exe → C:\Users\Demo\AppData\Local\Temp\autorun.exe → C:\Windows\System32\cmd.exe → C:\Windows\System32\powershell.exe → C:\Users\Demo\AppData\Local\Temp\starter.exe → C:\Users\Demo\AppData\Local\Temp\104.dll.
- Включает панель действий: 'Реагирование' (с выпадающим меню: 'Запретить запуск', 'Поместить на карантин', 'Изолировать устройство из сети'), 'Изменить статус', 'Экспорт', 'Показать связи', 'Загрузить трафик', 'Копировать детали'.
- Содержит таблицу 'Информация по детекту' с колонками: Имя, Дата и время, Путь, Размер, MD5, SHA256, Создан, Изменен, Атрибуты, Создатель файла.



# Аудит безопасности

## Аудит безопасности



SSH

### 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

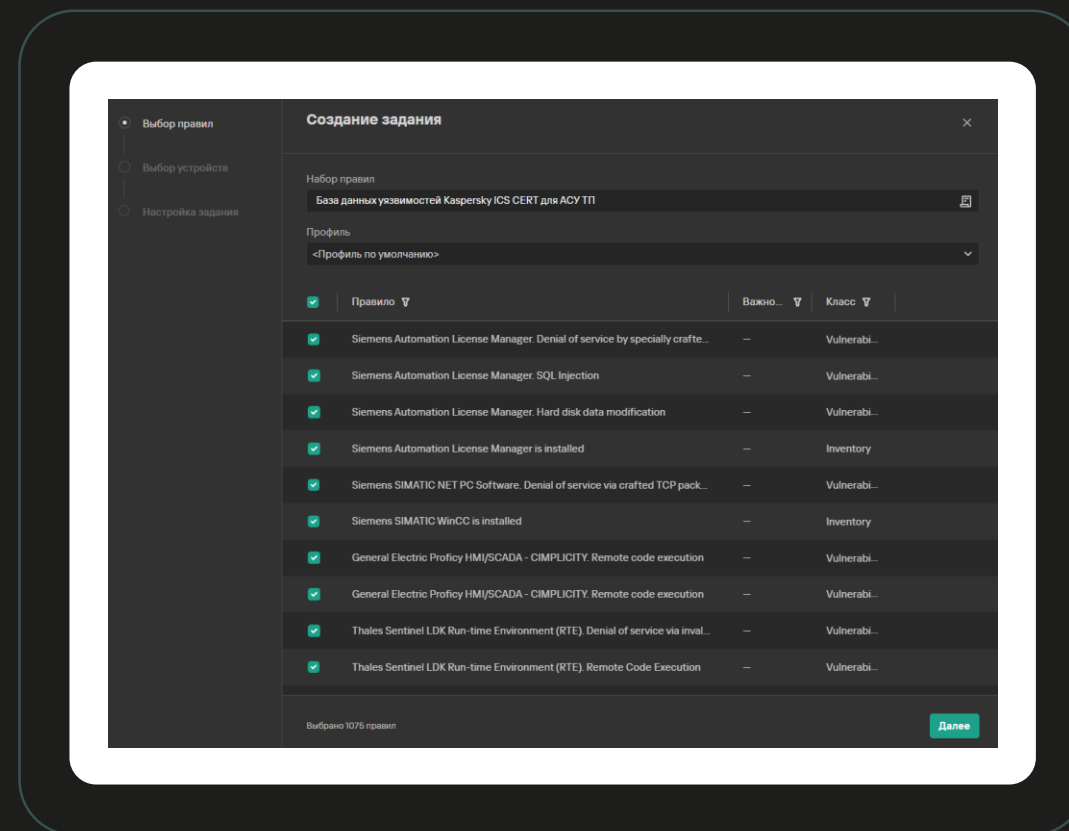
Ubuntu

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



## Редактор политик

**Минимальная длина пароля**

Применять при проверках

ID rule\_minimum\_password\_length

Важность **Высокая**

Класс Compliance

**Описание**

Эталонное значение: 8 знаков Этот параметр безопасности определяет минимальное количество символов, которое должно содержаться в пароле пользователя. Можно установить значение от 1 до 14, либо 0, если пароль не требуется. По умолчанию: 7 - на контроллерах домена. 0 - на автономных серверах. Примечание. По умолчанию рядовые члены домена используют конфигурацию своих контроллеров домена.

**Переменные**

Минимальная длина пароля

8

Сохранить Отмена

## Задачи аудита

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

## История запусков задачи

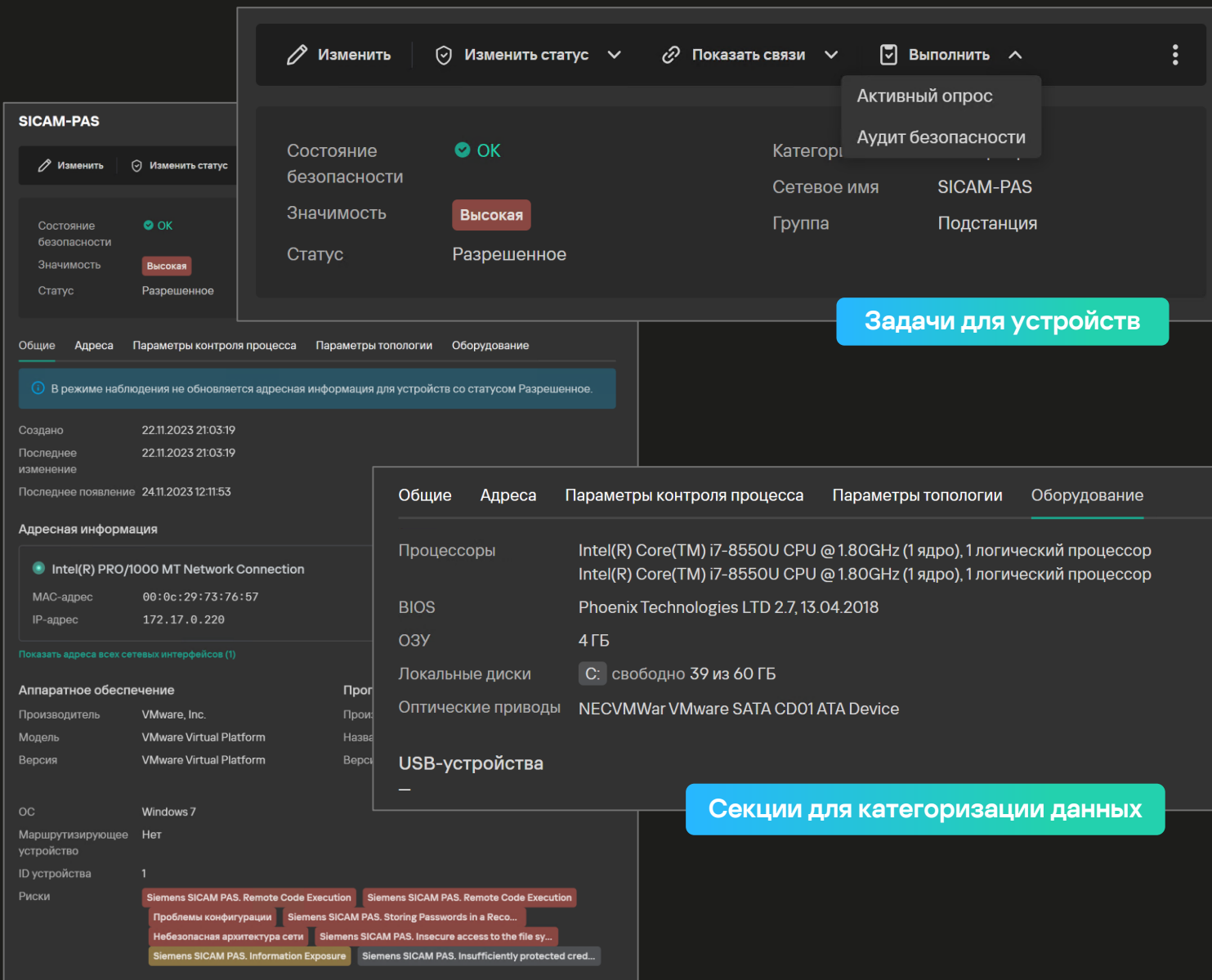
Поиск уязвимостей промышленного ПО (KL ICS CERT UPD)

Изменить Копировать Запустить Остановить Удалить

Параметры Правила 1077 / 1077 Устройства 5 Запуски 2

Запуск	Устройство	Статус	Начало	Завершение	Длительность...
Запуск задания 2		Выполняется	24.11.2023 11:54:13		
Сканирование 5	WinCCOA	Выполняется	24.11.2023 11:56:17		
Сканирование 4	KICS-WIN7	Выполняется	24.11.2023 11:56:50		
Сканирование 3	kics-winxpsp3	Ожидание			
Сканирование 2	KICS-WIN7-RU	Выполняется	24.11.2023 11:56:50		
Сканирование 1	KICS-WINSRV2016	Выполняется	24.11.2023 11:56:28		
Запуск задания 1		Завершено	16.11.2023 16:35:20	16.11.2023 16:38:52	00:03:32
Сканирование 5	WinCCOA	Завершено	16.11.2023 16:37:43	16.11.2023 16:38:22	00:00:39
Сканирование 4	KICS-WIN7	Завершено	16.11.2023 16:37:51	16.11.2023 16:38:22	00:00:30
Сканирование 3	kics-winxpsp3	Завершено	16.11.2023 16:38:07	16.11.2023 16:38:52	00:00:45
Сканирование 2	KICS-WIN7-RU	Завершено	16.11.2023 16:38:13	16.11.2023 16:38:52	00:00:39
Сканирование 1	KICS-WINSRV2016	Завершено	16.11.2023 16:37:02	16.11.2023 16:37:22	00:00:19

# Обновления продуктов KICS



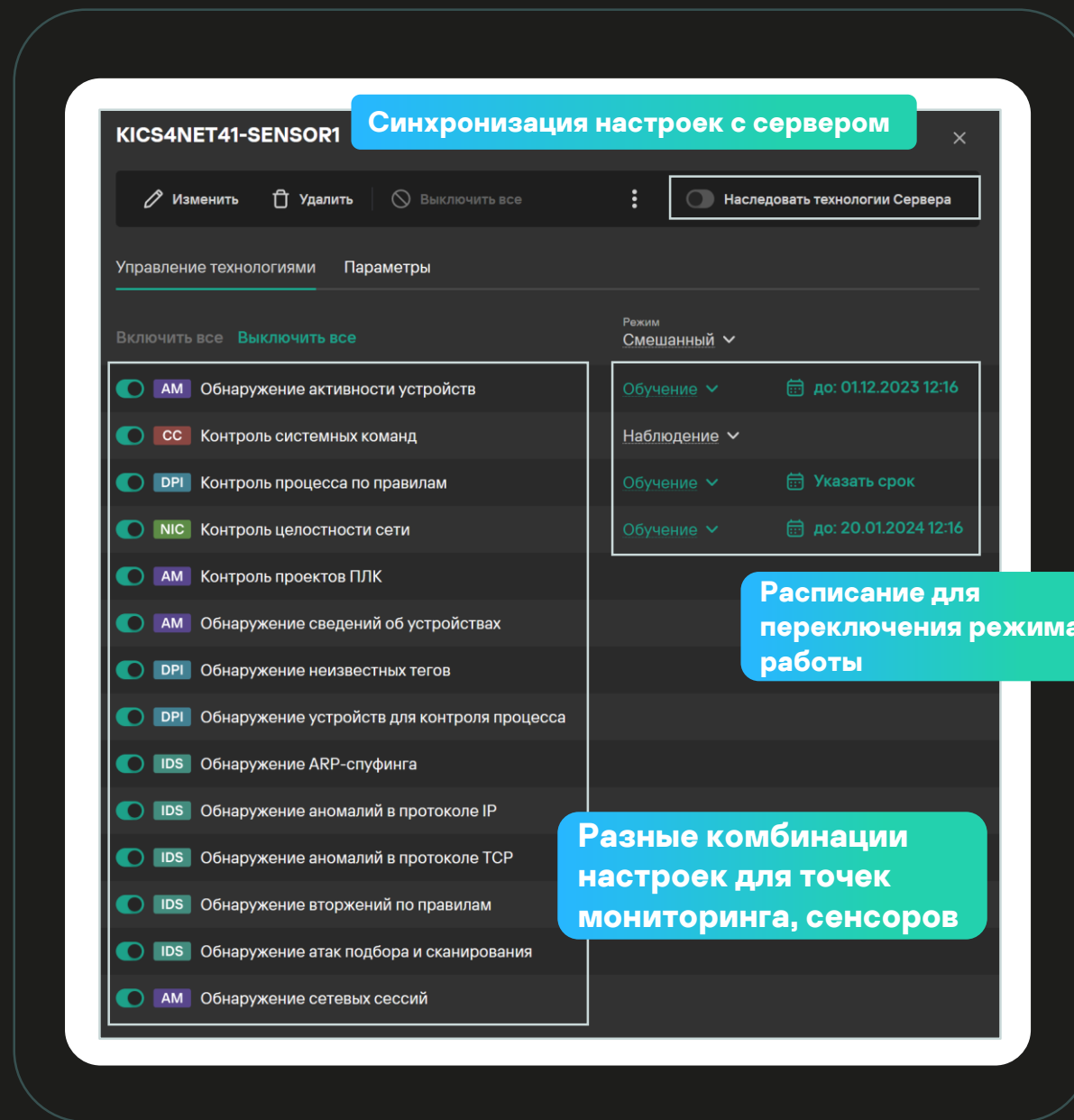
## Новый дизайн для удобного управления устройствами и событиями

- 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



## 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



## Контроль проекта ПЛК

Проверка целостности проекта ПЛК позволяет выявить попытки изменения технологического процесса

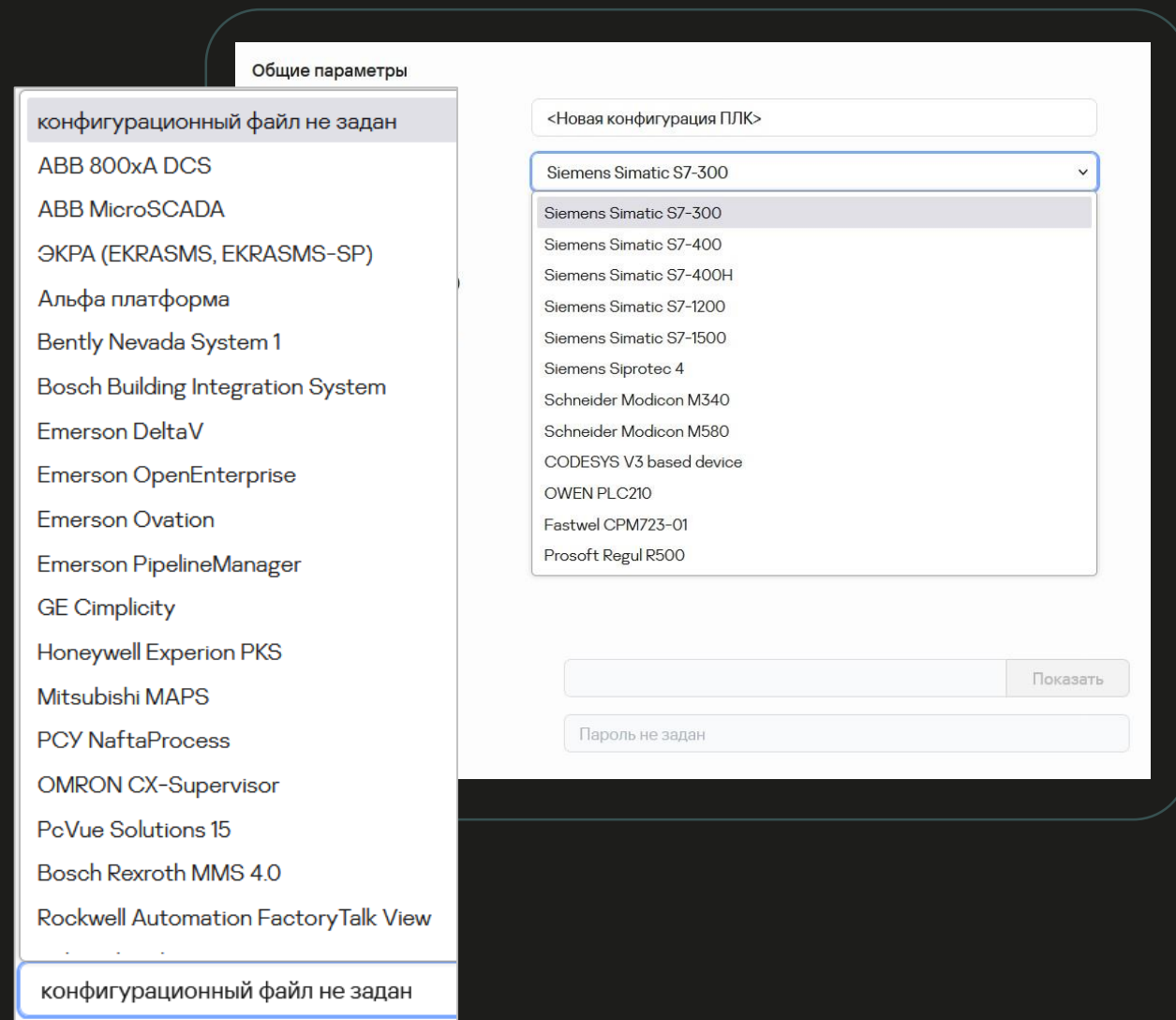
## Сертификация и тестирование с системами автоматизации

- 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

Управление сетевым экраном

Общие | Приложения (входящие соединения) | Приложения (исходящие соединения) | Порты (входящие соединения) | Порты (исходящие соединения)

### Интеграция с брандмауэром Windows

- Отслеживать статус работы брандмауэра Windows  
Программа только отслеживает статус работы брандмауэра Windows.
- Контролировать работу брандмауэра Windows  
Программа контролирует работу брандмауэра Windows в соответствии с параметрами ниже.

### Входящие соединения

Действие для входящих соединений:

Правил для приложений: (2 / 0 / 2)  
(разрешающих/блокирующих/всего)

Правил для портов: (2 / 0 / 2)  
(разрешающих/блокирующих/всего)

### Исходящие соединения

Действие для исходящих соединений:

Правил для приложений: (4 / 0 / 4)  
(разрешающих/блокирующих/всего)

Правил для портов: (2 / 0 / 2)  
(разрешающих/блокирующих/всего)

### Дополнительно

- Разрешить ICMP-соединения

Параметр регулирует входящие и исходящие ICMP-соединения по протоколам ICMPv4 и ICMPv6.



Антивирус

Контроль запускаемых приложений

Контроль устройств

Контроль целостности файлов

Защита от шифрования сетевых папок

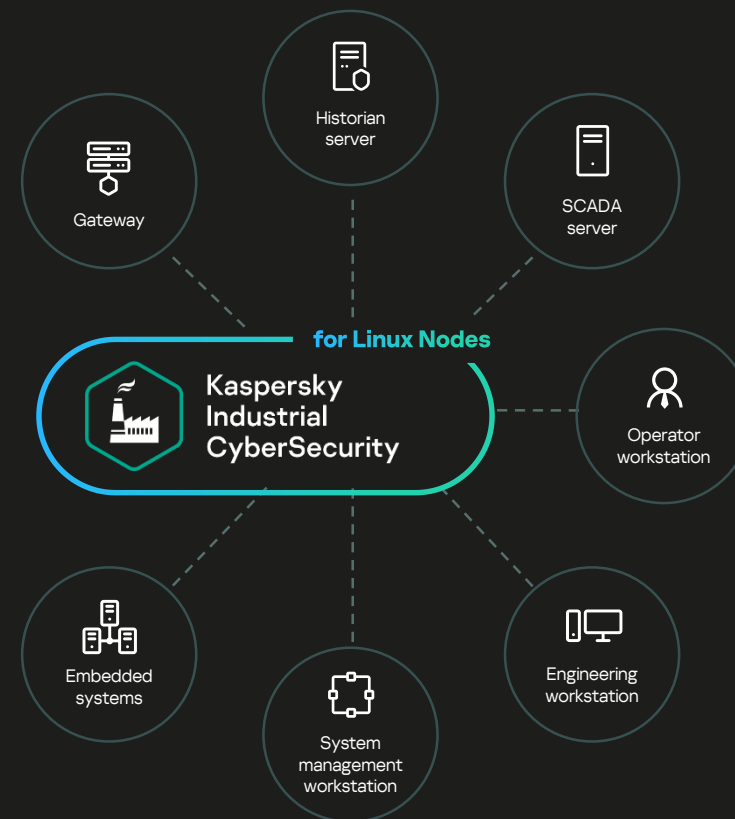
Анализ поведения

Защита от сетевых угроз

Управление Firewall

Сенсор телеметрии (Интеграция с KICS for Networks)

## Industrial Endpoint Protection



## 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

Workstation

Server

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



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

