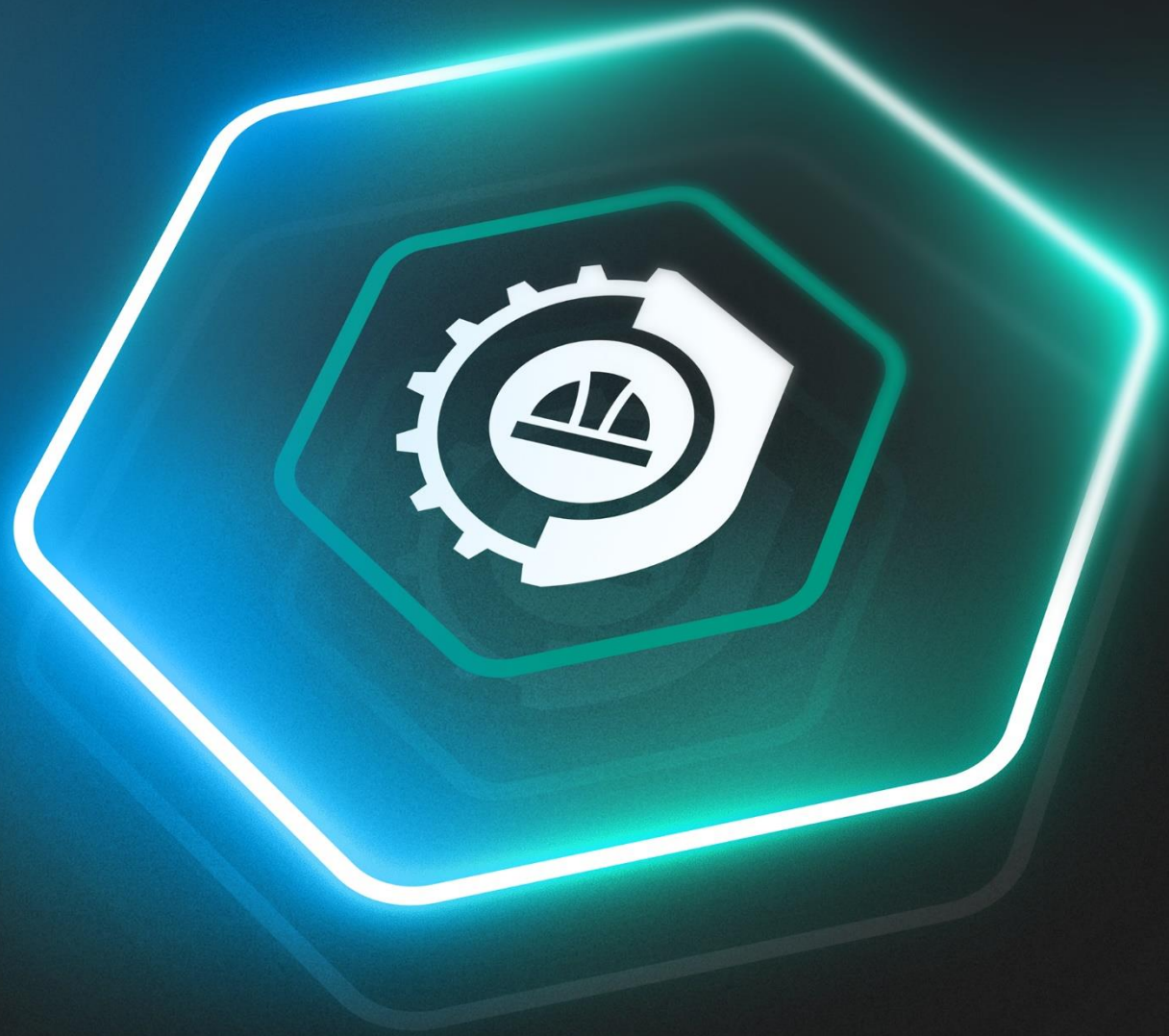
XDR-платформа Kaspersky Industrial CyberSecurity

Сплав технологий и экспертизы
для промышленной кибербезопасности

kaspersky

Kaspersky OT CyberSecurity



Три слагаемых Kaspersky OT CyberSecurity

Решения

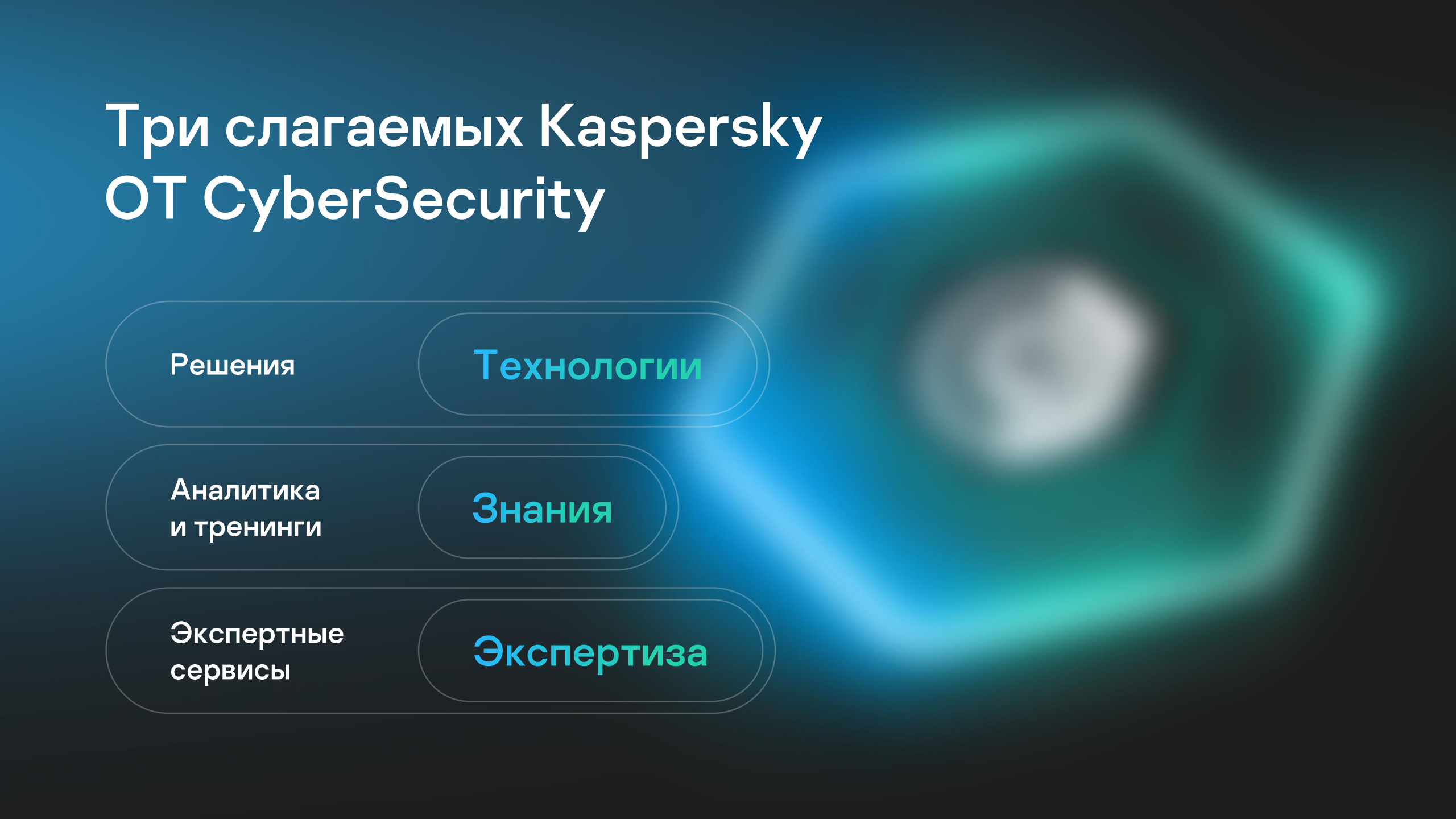
Технологии

Аналитика и тренинги

Знания

Экспертные сервисы

Экспертиза



Состав Kaspersky OT CyberSecurity

Знания

Аналитика об угрозах

- Kaspersky ICS Threat Intelligence

Повышение осведомленности

- Kaspersky Security Awareness

Тренинги для специалистов

- Kaspersky ICS CERT Training

Технологии

Основные

- Kaspersky Industrial CyberSecurity
- Kaspersky Unified Monitoring and Analysis Platform

Фокусные

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

Решения на базе KOS

- Kaspersky IoT Infrastructure Security
- Kaspersky Secure Remote Workspace

Экспертиза

Анализ защищенности

- Kaspersky ICS Security Assessment

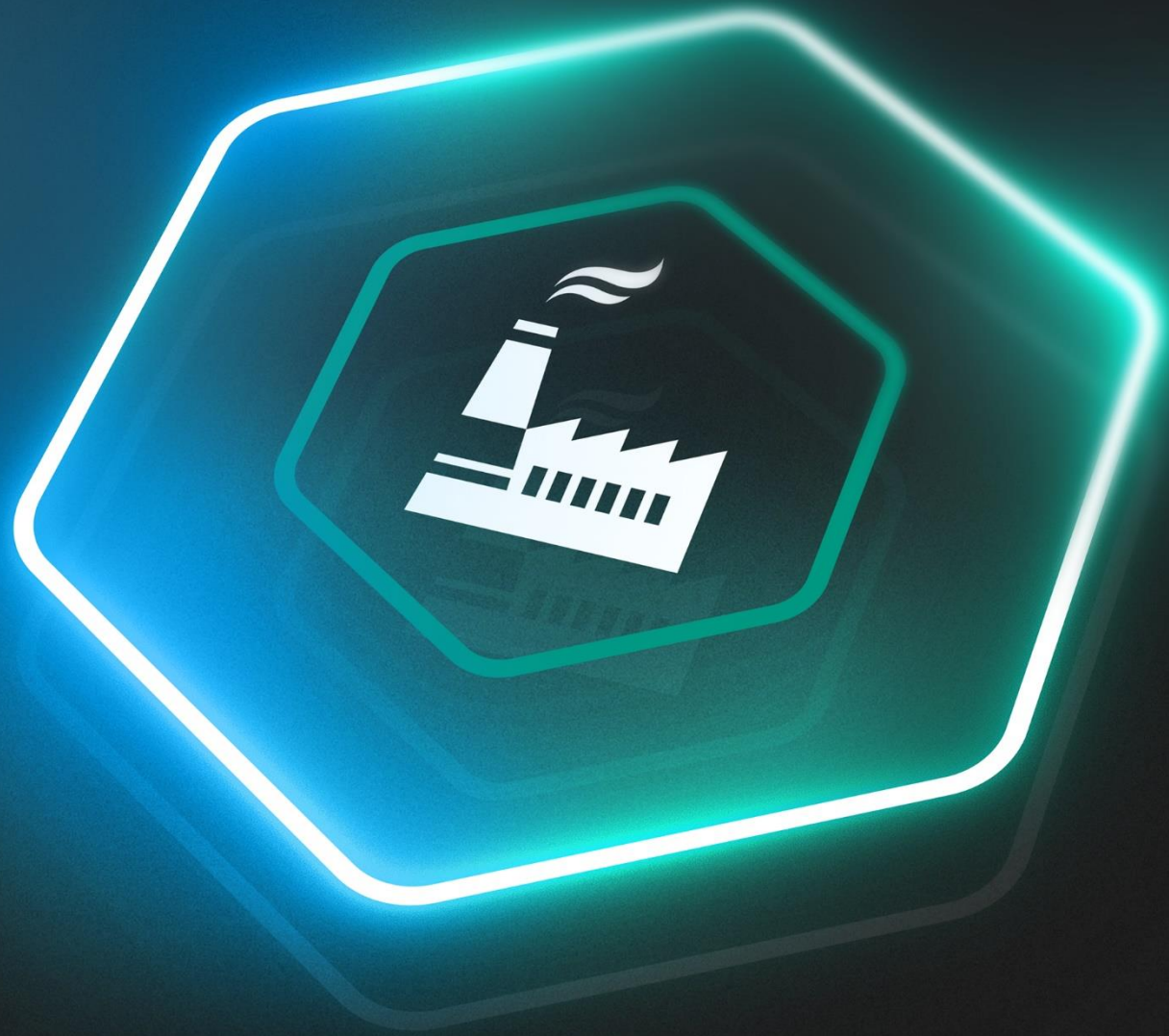
Управляемая защита

- Kaspersky Managed Detection and Response

Скорая помощь

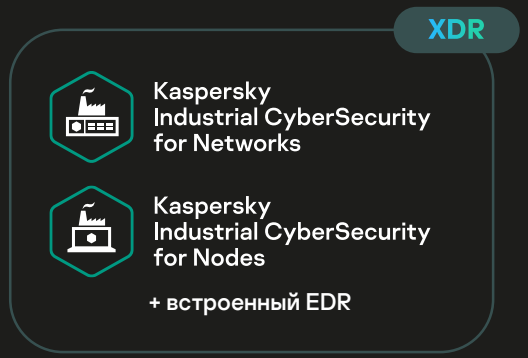
- Kaspersky Incident Response
- Kaspersky Industrial Emergency Kit

Kaspersky Industrial CyberSecurity



Kaspersky Industrial CyberSecurity

Промышленная XDR-платформа



KICS сегодня:

45 000+

Промышленных АРМ / серверов под защитой KICS for Nodes

300+

Клиентов по всему миру

350+

Промышленных сетей под защитой KICS for Networks

260

Количество проектов в 2021

Архитектура 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

Не просто обновление. Эволюция

Mission-critical functions		Become groundbreaking advantages with KICS for Networks
OT Visibility	• Список активов и коммуникаций, логическая карта сети; • Выявление аномалий тех. процесса; • Контроль целостности сети и обнаружение вторжений	• Аудит безопасности, оценка рисков, ситуационная осведомленность и отчеты; • Обнаружение уязвимостей промышленного оборудования; • Интеграция с KICS for Nodes (события EPP, обогащение сетевых событий, достоверная инвентаризация)
Asset management	• Пассивное обнаружение активов	• Активный опрос узлов; • Топологическая карта сети; • Плагин для централизованного мониторинга нескольких инсталляций продукта
Integration	• Интеграция по API со сторонними СЗИ	• Наличие встроенных коннекторов для интеграции с внешними системами; • Развитая экосистема решения для OT

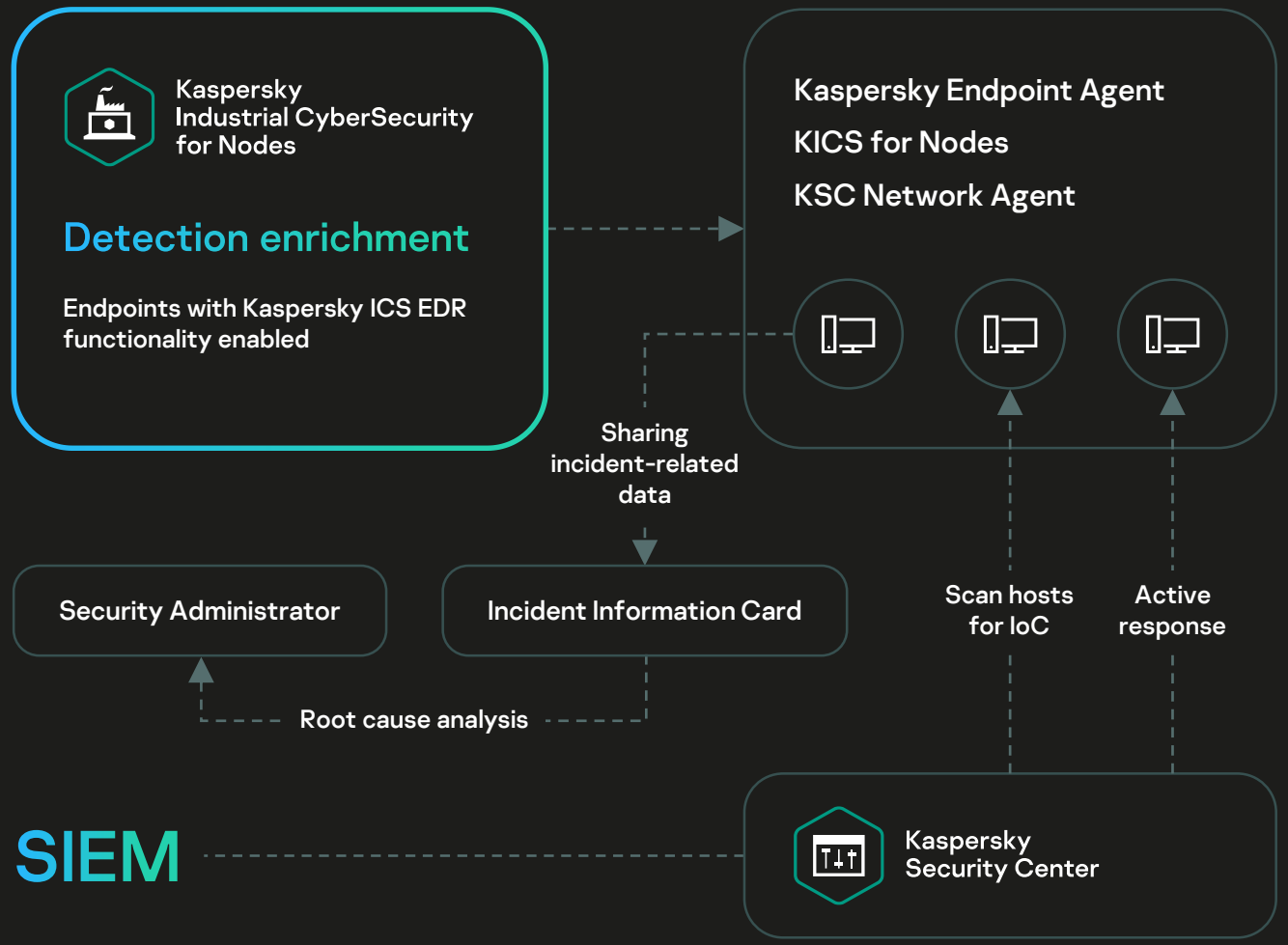
ICS Endpoint Detection and Response (EDR)

Ключевые возможности

Лидерский EDR от ЛК на базе KICS for Nodes для ICS

Большой набор сценариев реагирования на инцидент

Не требуется дополнительное оборудование!



Ключевые возможности

Автоматизированный и централизованный аудит

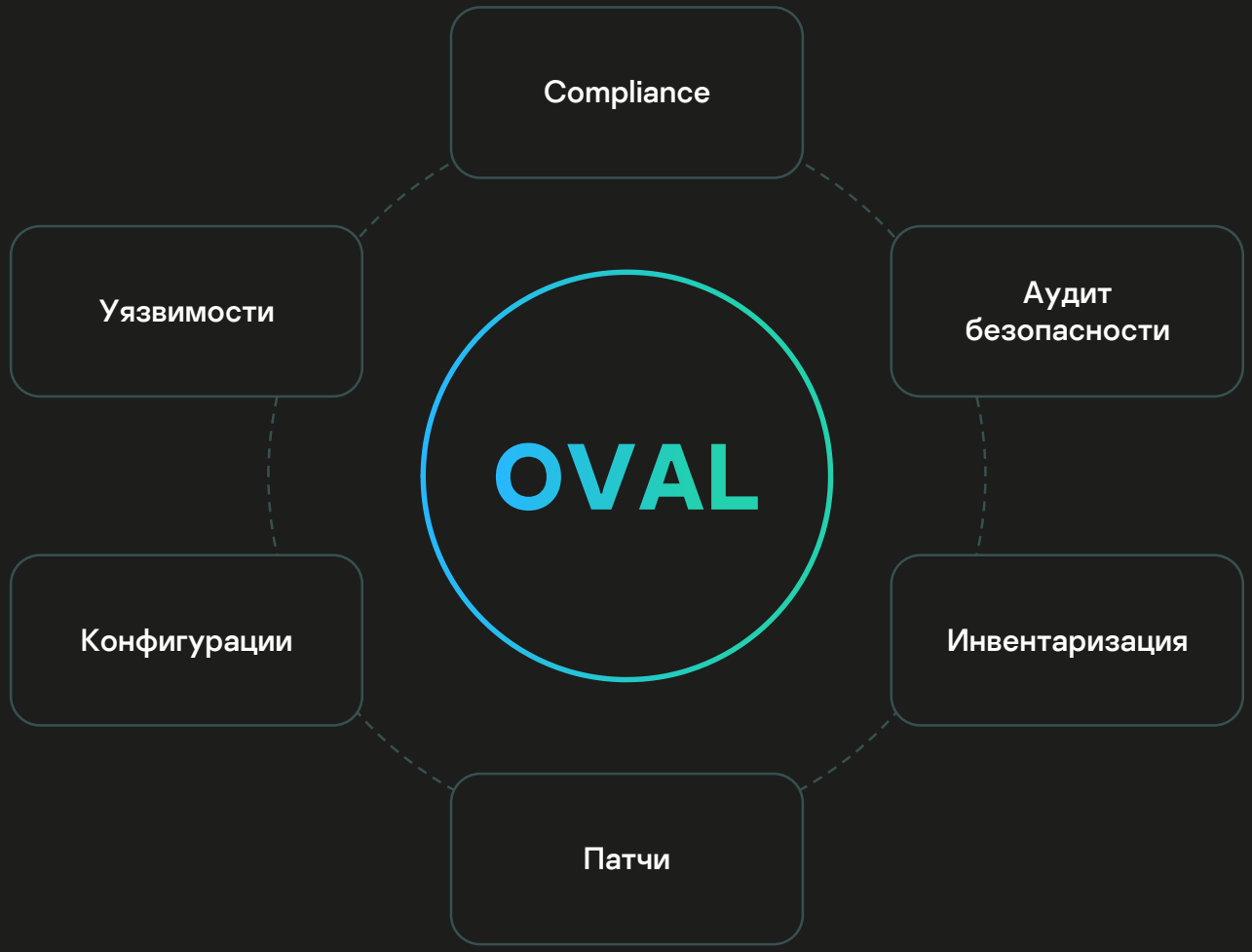
Используем стандарт в индустрии — OVAL

Проверка на соответствие приказам ФСТЭК

Встроенная база уязвимостей систем АСУ ТП от ICS Cert

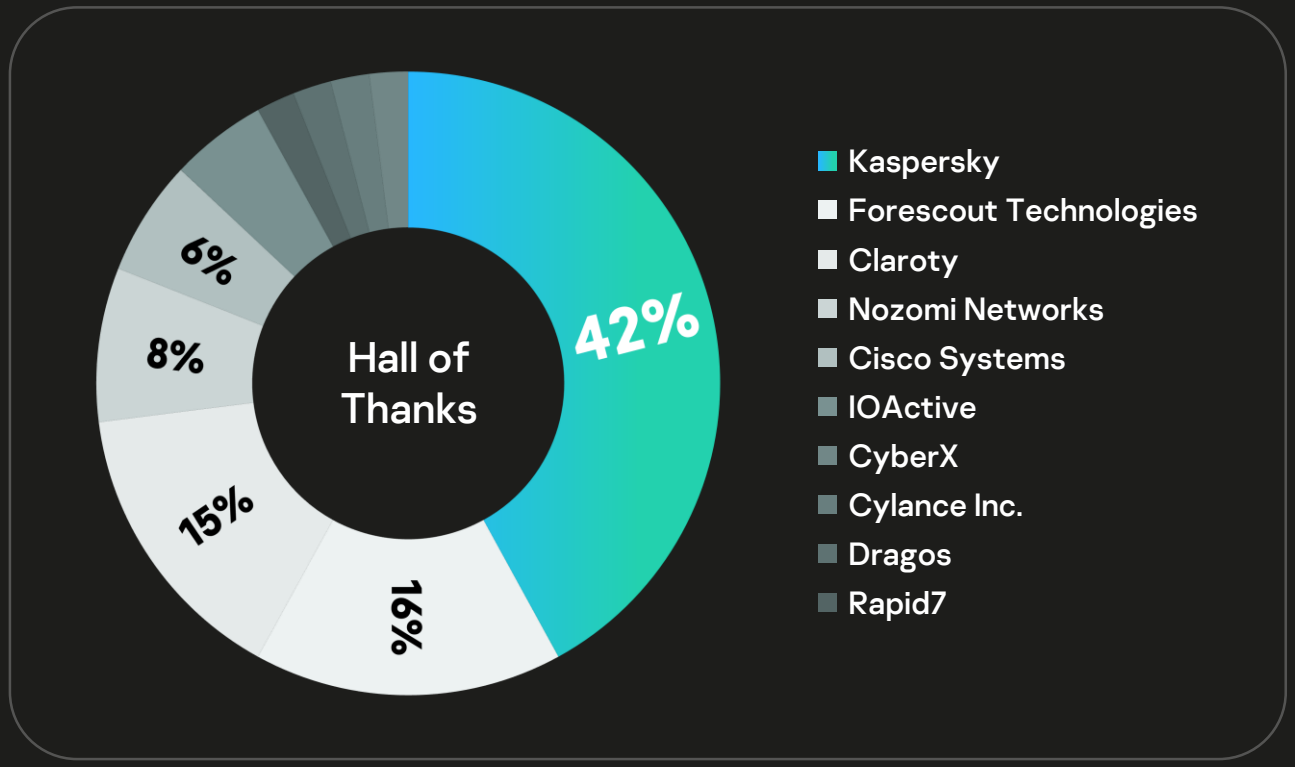
БДУ ФСТЭК, NIST, CIS и т.д.

Поддерживаем любые базы OVAL формата



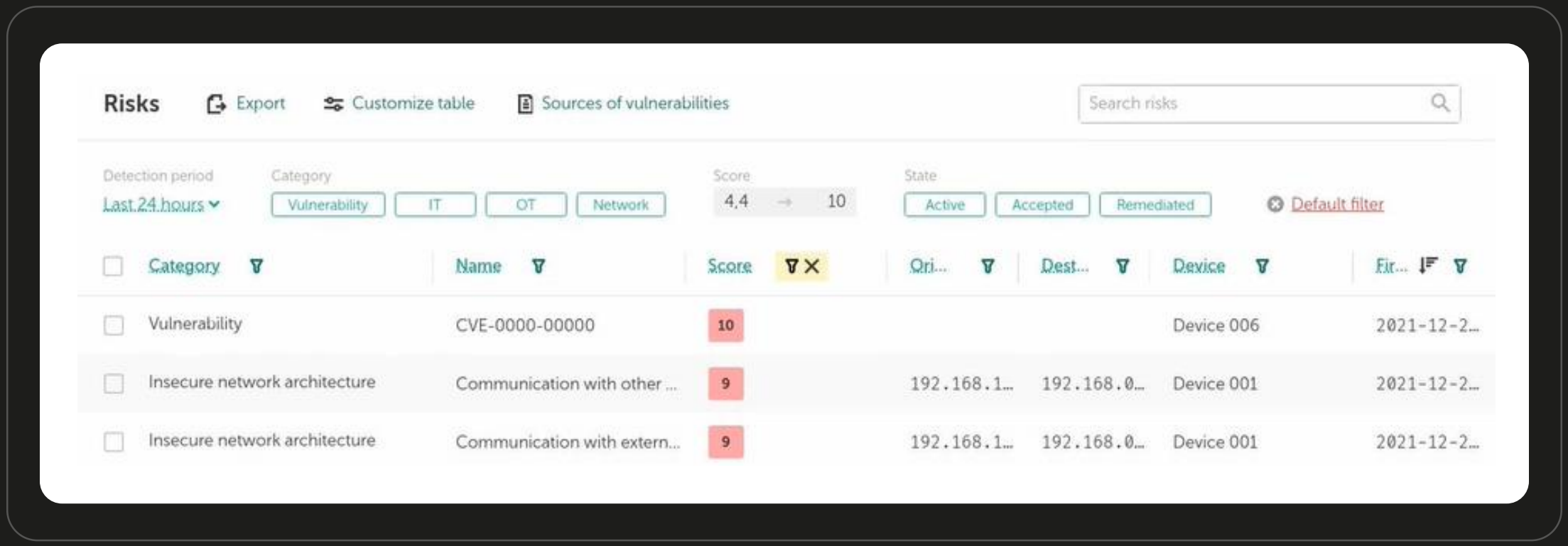
KICS for Networks
и KICS for Nodes
смогут определять уязвимости
в промышленном ПО
и оборудовании

Kaspersky — один из ведущих вендоров в Siemens “Hall of Thanks”

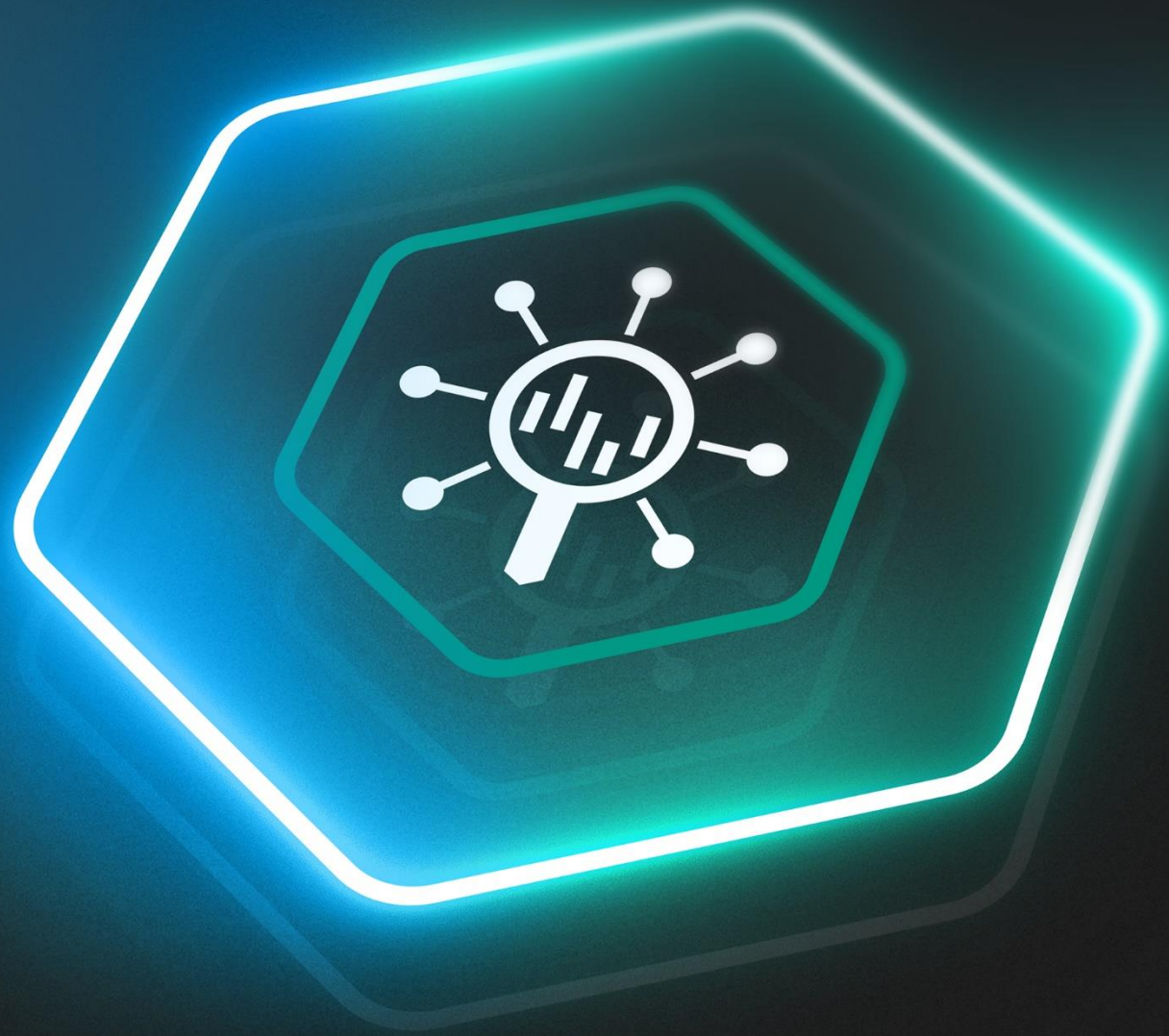


Пассивный анализ рисков

Инцидент | Что случилось? → **Риск** | Что может случиться?



Kaspersky Unified Monitoring and Analysis Platform

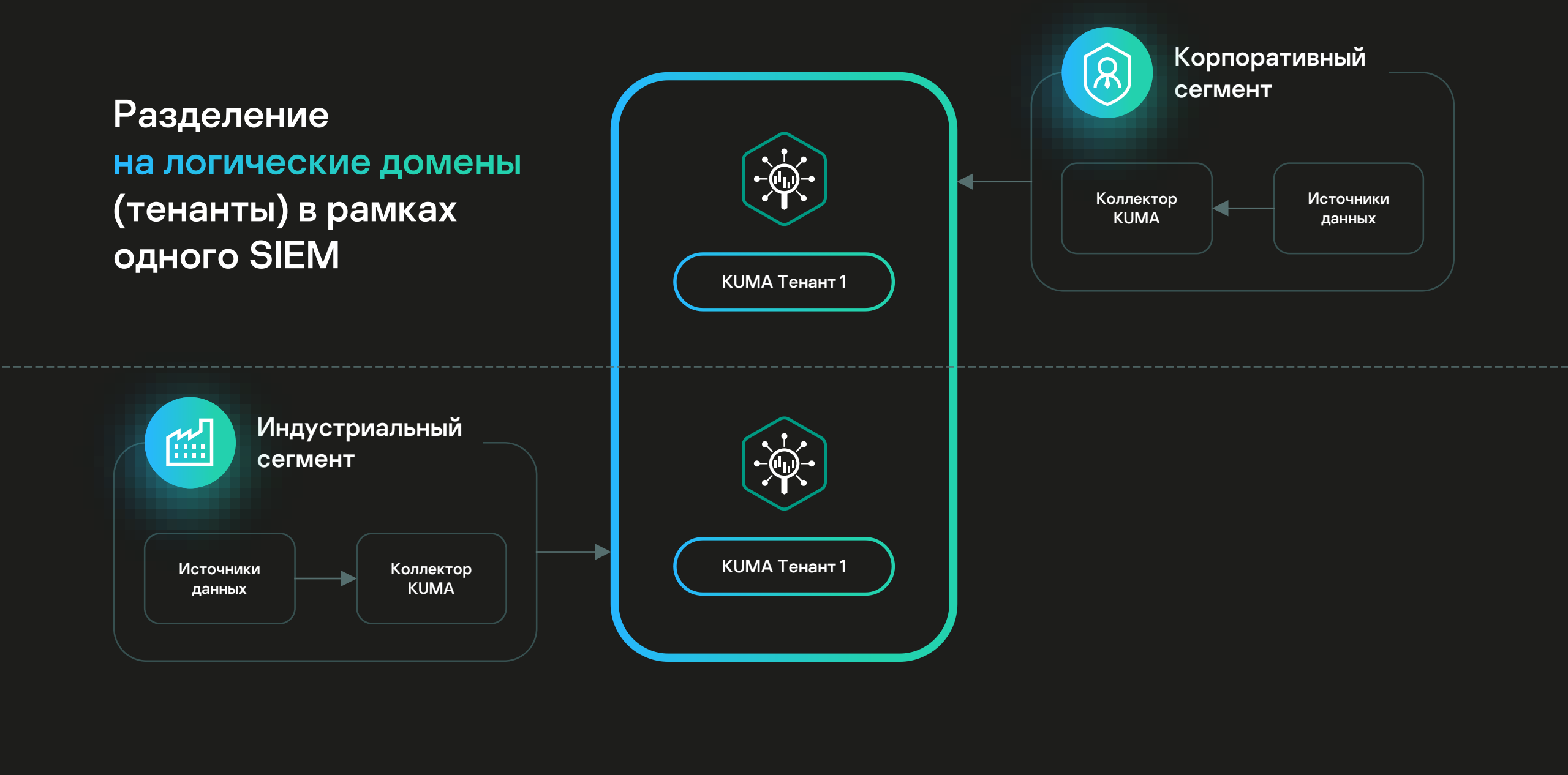


Цельное предложение для защиты OT и IT сред

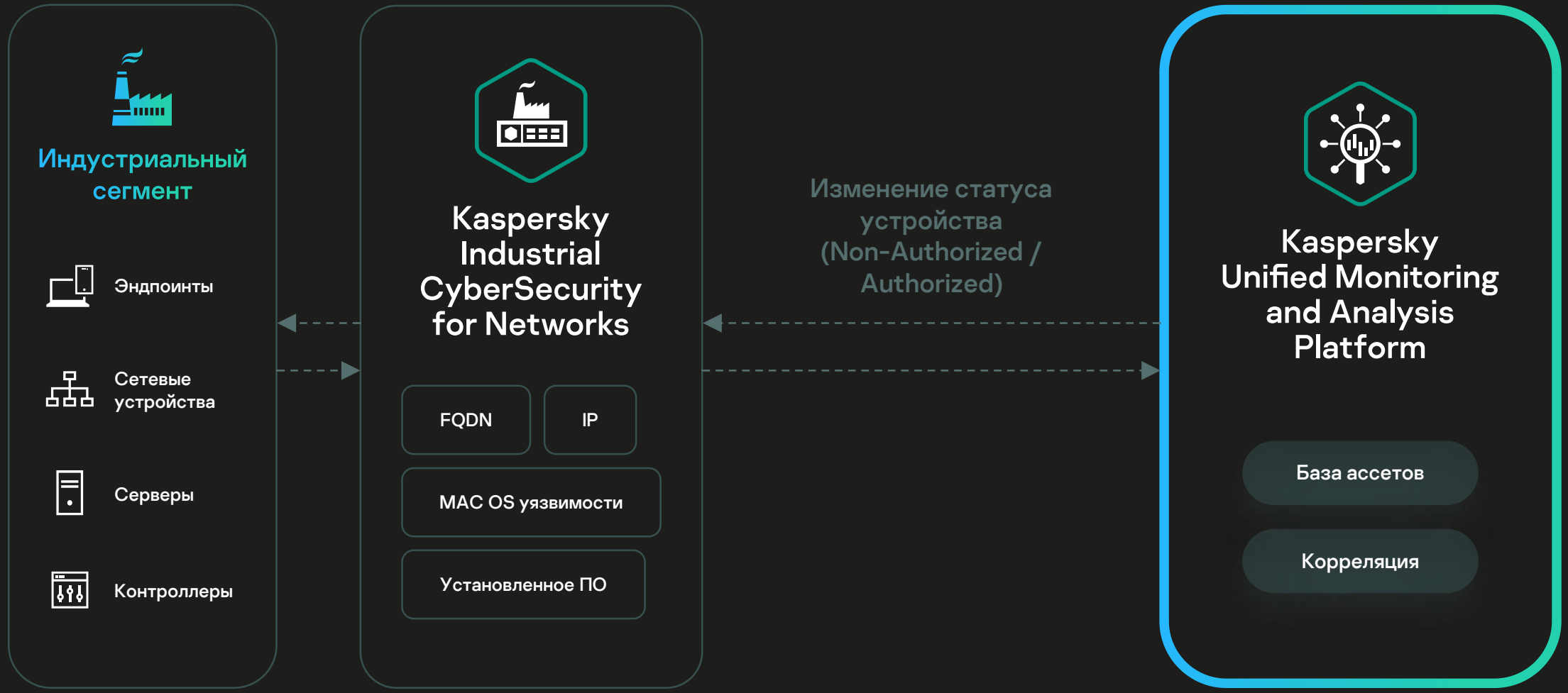
Разные сегменты, один SIEM

Разные сегменты, один SIEM

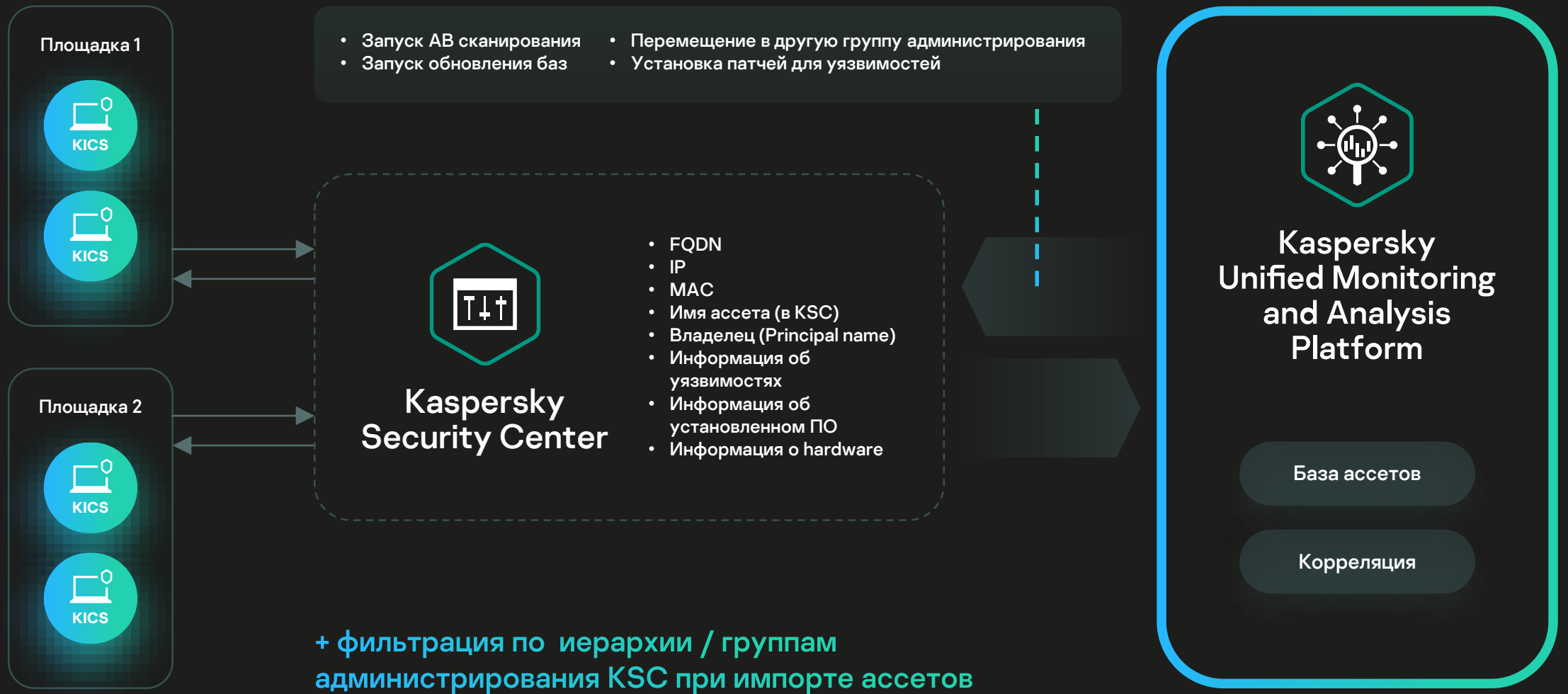
Разделение
на логические домены
(тенанты) в рамках
одного SIEM



Интеграция с KICS for Network



Инвентаризация информационных активов и базовое реагирование



+ фильтрация по иерархии / группам администрирования KSC при импорте ассетов

Потоковое обогащение событий

Решения

«Лаборатории Касперского»

Логи

Алерты

Телеметрия

+

Источники данных
передают «сырые» события

Приложения

АРМ

Сетевые СЗИ

Collector

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky CyberTrace

Kaspersky Threat Data Feeds

«Обогащение» событий

Correlator

Kaspersky Unified Monitoring and Analysis Platform

«Обогащенные» события

Обогащение событий по запросу

Запрос по индикатору

(вручную / авто)

Пример -URL: “example.com”)

Запрос по индикатору
(url, hash, domain, ip)

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Threat Lookup

Карточка инцидента

Имя: «Обнаружено взаимодействие с CnC сервером»
Описание:.....
Связанные события: .....
Связанные IP: 1.2.3.4, 2.3.4.5, ...
Связанные пользователи: i.Ivanov, a.petrov, ...
.....

“Обогащение” карточки инцидента данными из Kaspersky Threat lookup

Ответ на запрос

URL: «example.com»
first seen: “2016-08-10”
last seen:” 2020-03-01”
Связанные хэш-суммы вредоносных файлов MD5:”.....”
SHA-1: “.....”
SHA256:” ”
Связанные вредоносные URL: “....”
Связанные IP: 1.2.3.4, 2.3.4.5, ...

Источники
Threat Intelligence

Threat Intelligence — источники

- KSN
- Web crawlers
- BotFarms
- Spam traps
- Sensors
- Passive DNS
- Partners
- OSINT

Kaspersky SOC

GREAT
Kaspersky APT Research team

Kaspersky Red Team

Kaspersky ICS CERT

Kaspersky Threat Intelligence

Подробнее

Kaspersky ICS CERT

Первый индустриальный CERT в коммерческой организации

Более 30 экспертов в области исследования угроз и уязвимостей, расследования инцидентов и анализа защищенности АСУ ТП

Статус CVE Numbering Authority (CNA)

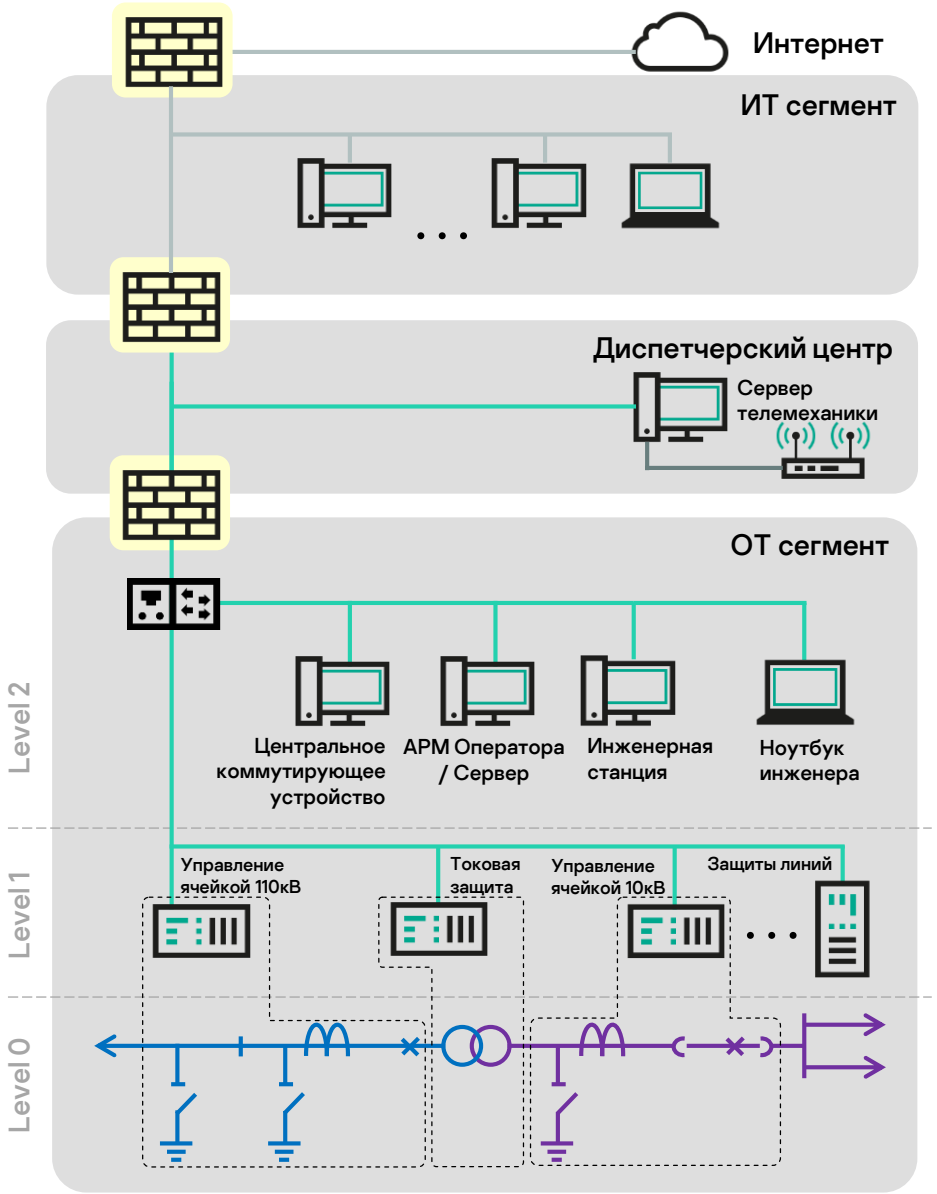
Обнаружили несколько сотен уязвимостей «нулевого дня» в компонентах АСУ ТП и IIoT

Членство в международных организациях:

ITU, IEEE, Global Platform®, enisa, ISO, FIRST, Industry IoT Consortium.

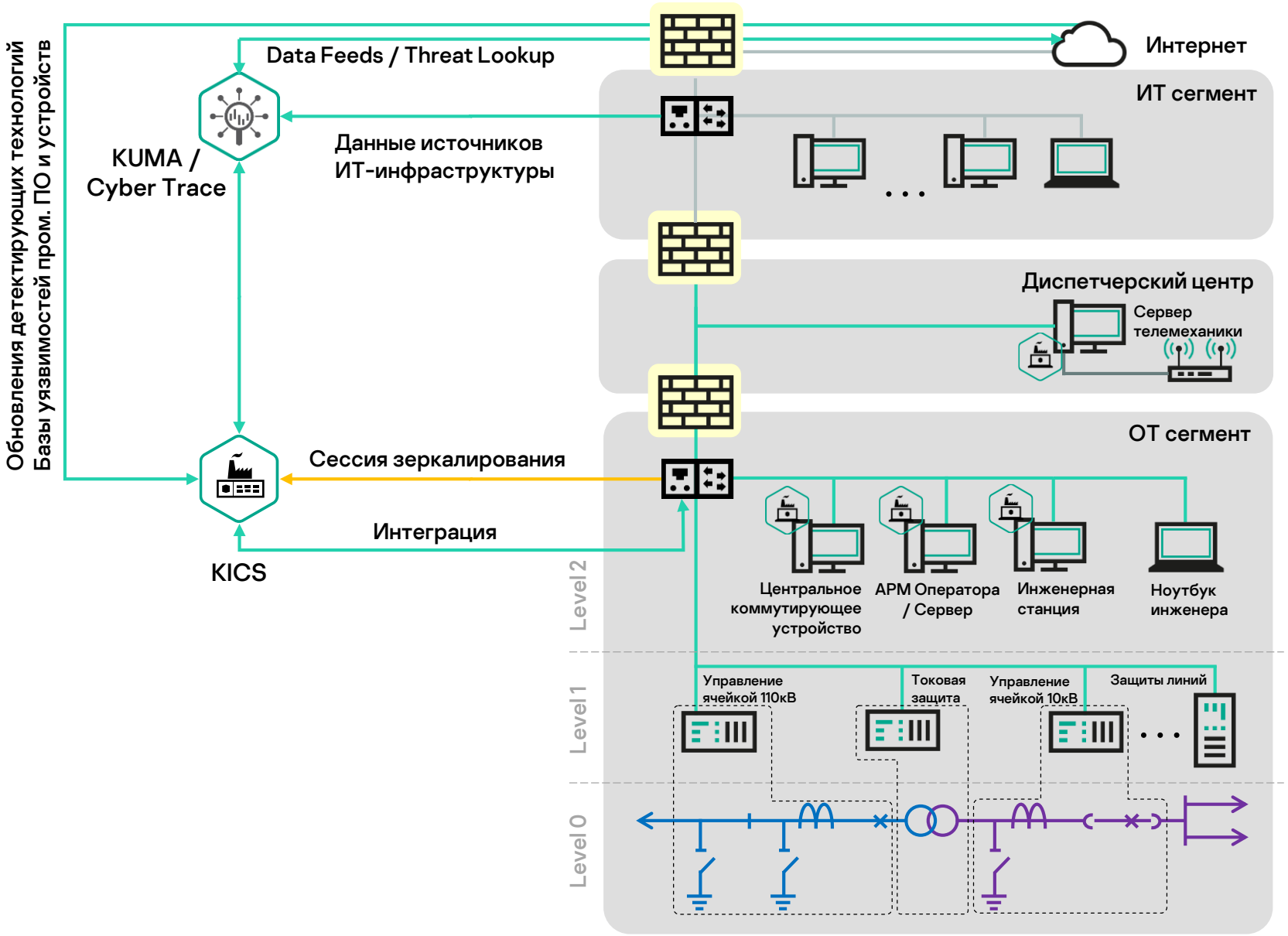
Описание демонстрационного стенда и сценария

Описание демонстрационного стенда и сценария

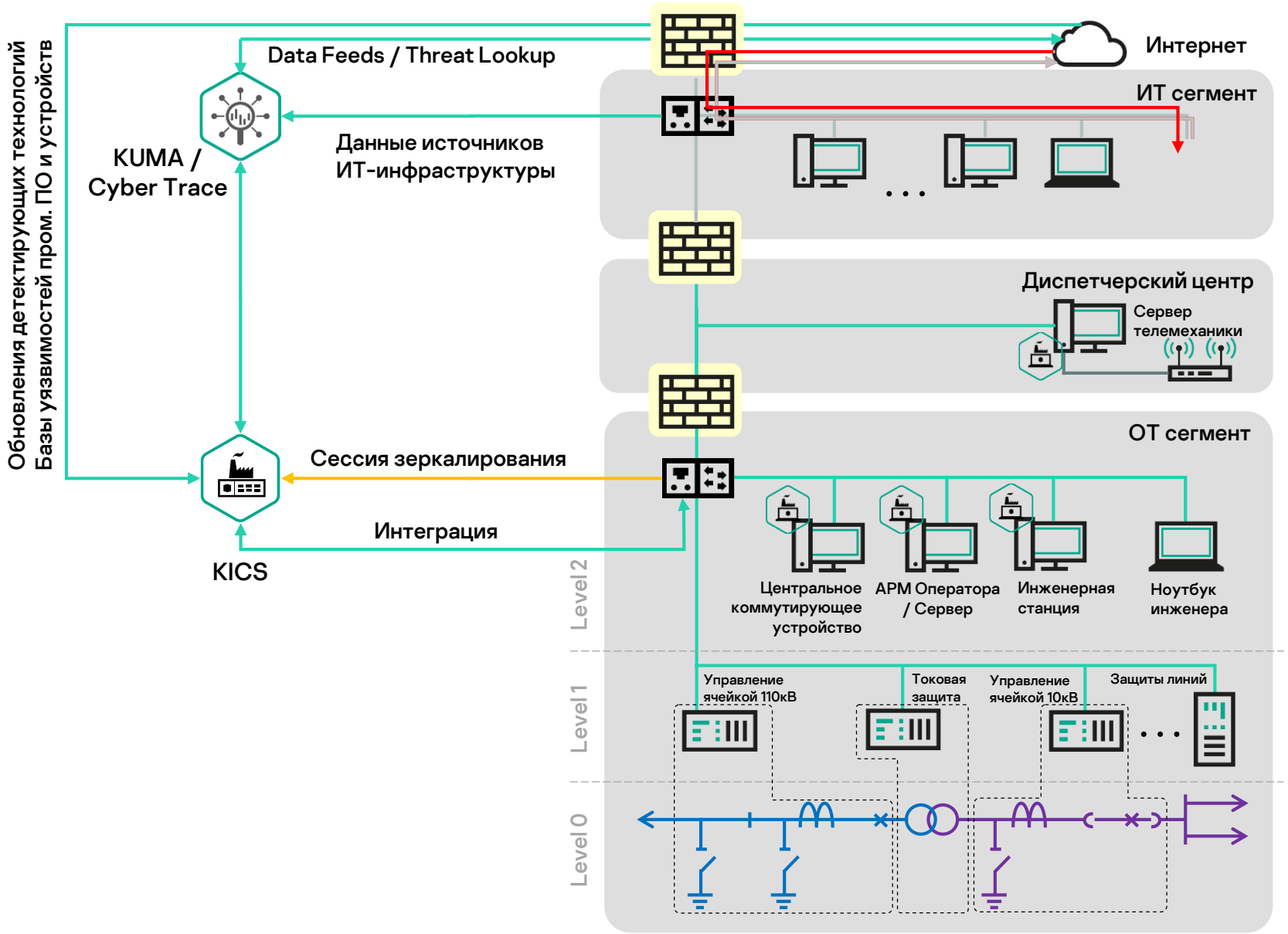


Демонстрационный стенд представляет собой симуляцию инфраструктуры объекта понижающей (трансформаторной) подстанции 110/10кВ

Описание демонстрационного стенда и сценария

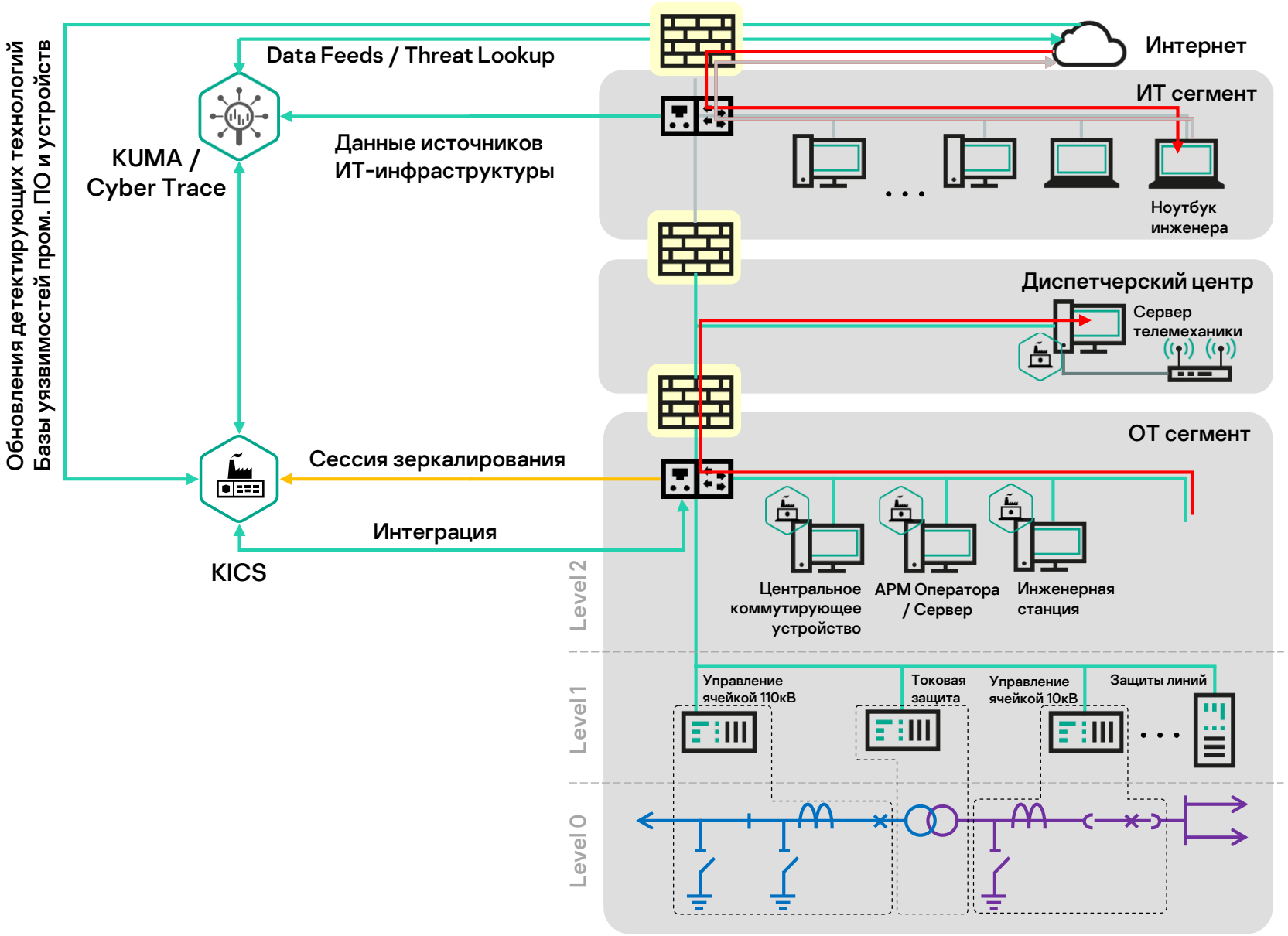


Описание демонстрационного стенда и сценария



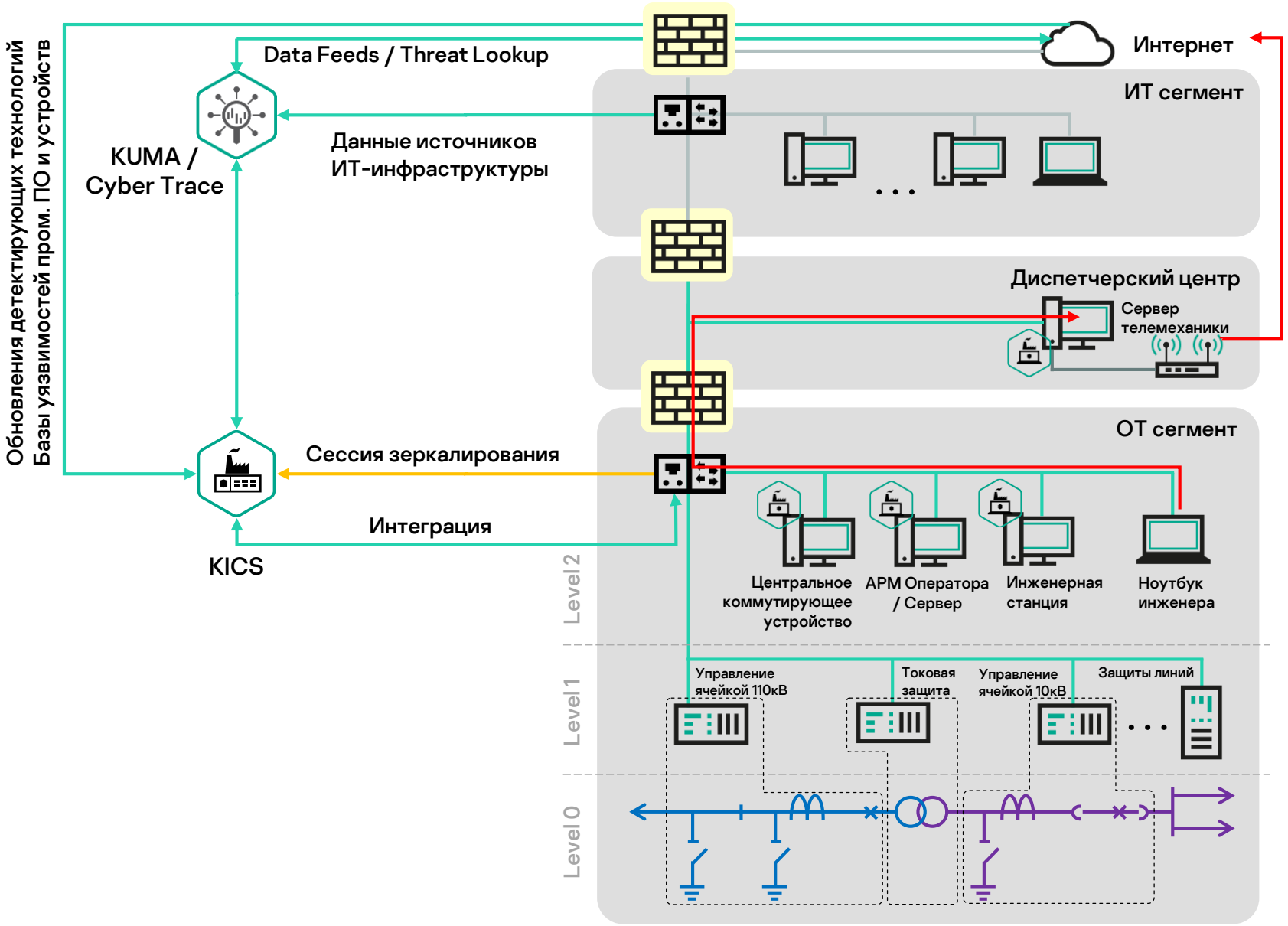
1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера

Описание демонстрационного стенда и сценария



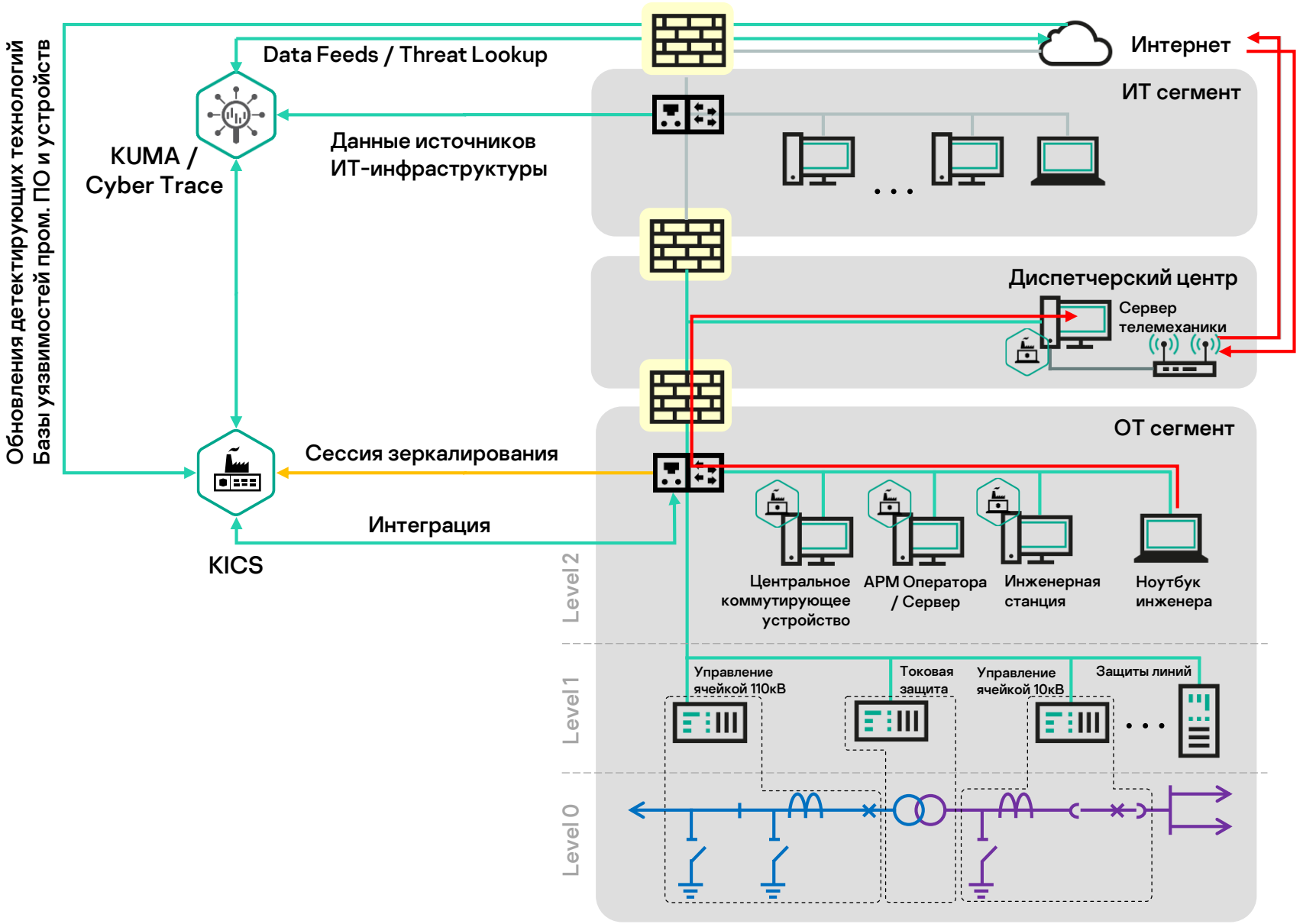
1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера
3. Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ

Описание демонстрационного стенда и сценария



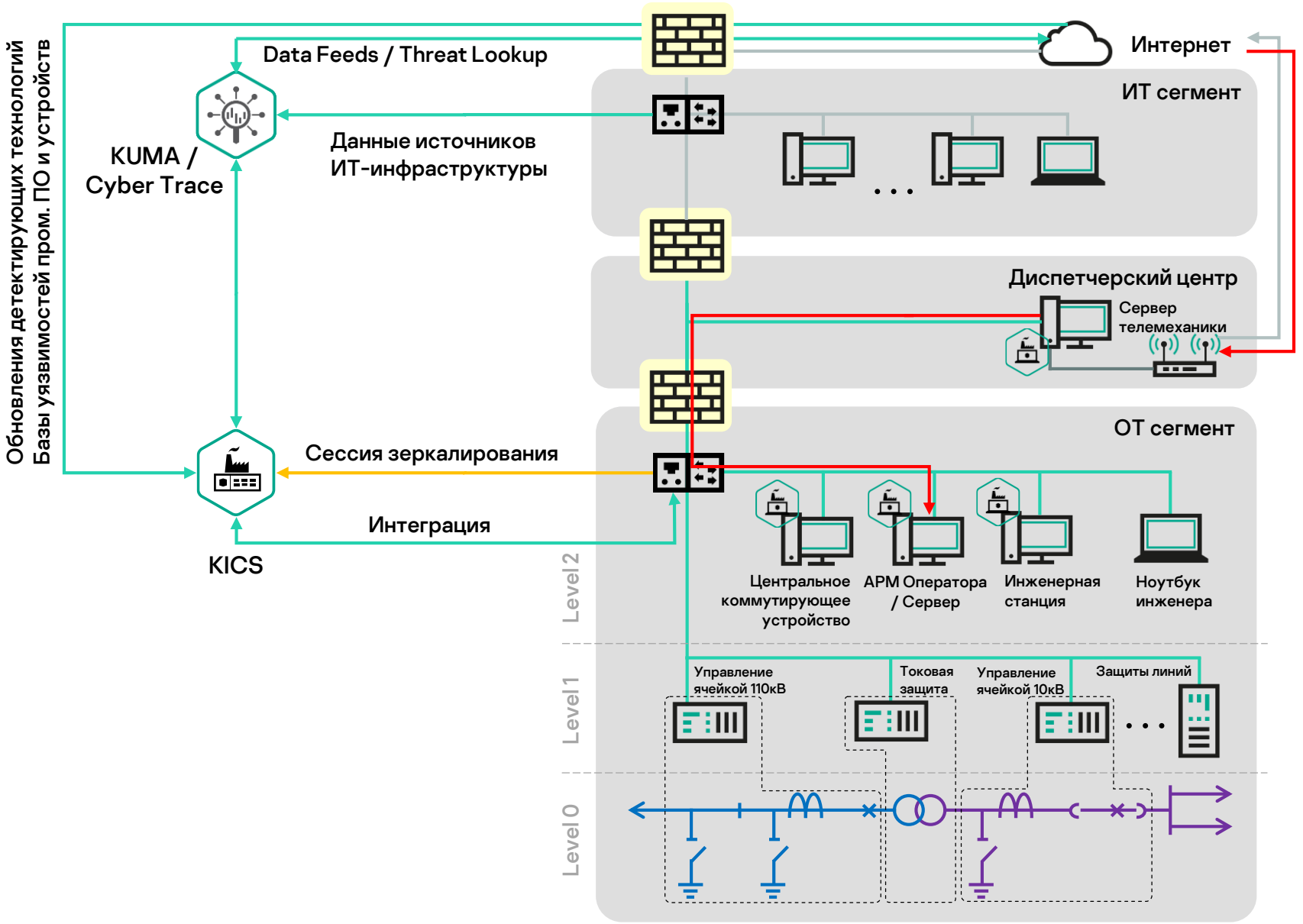
1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера
3. Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ
4. Активация 4G-модема удалённого обслуживания и подключение к недоверенному ресурсу

Описание демонстрационного стенда и сценария



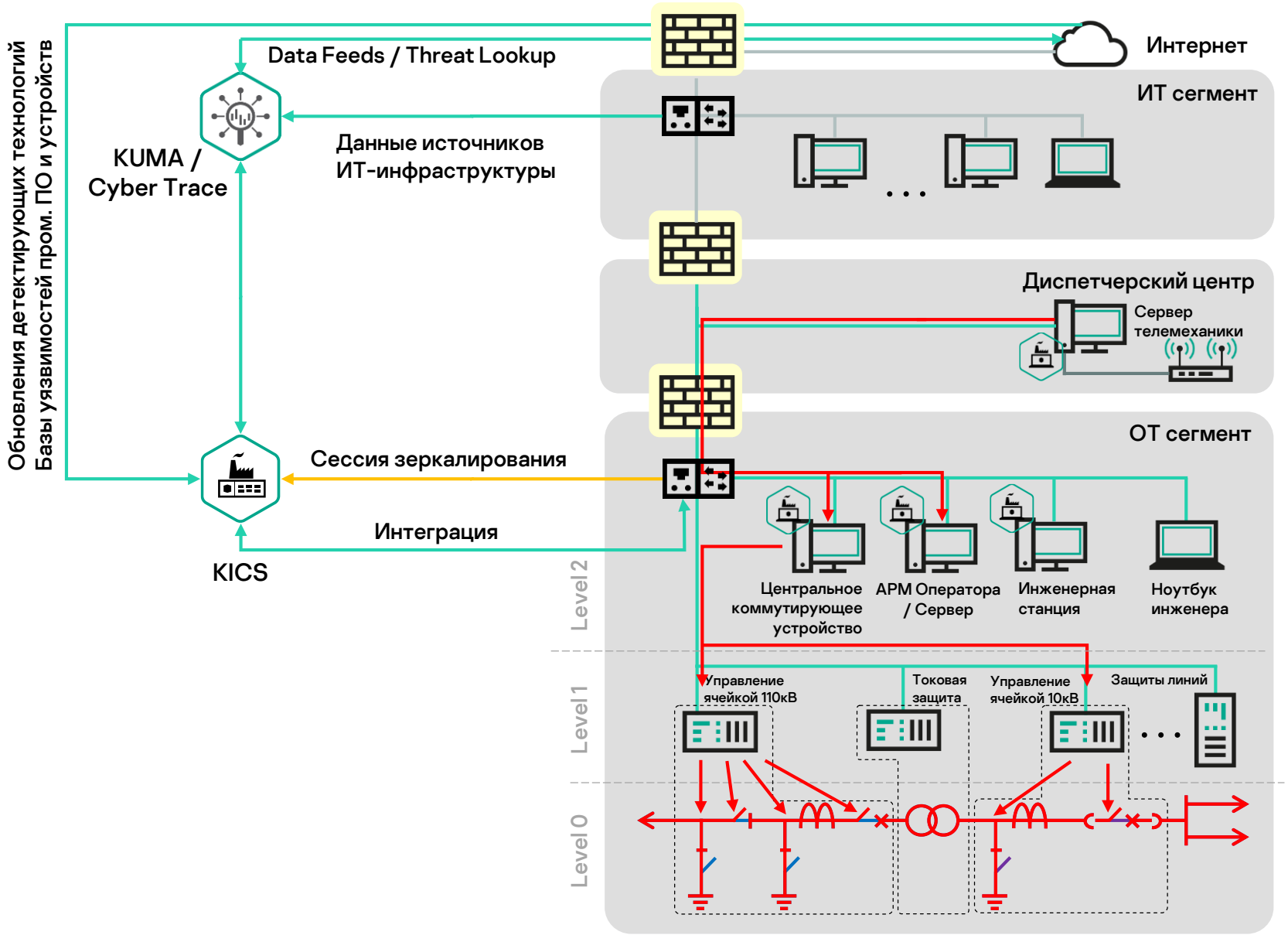
1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера
3. Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ
4. Активация 4G-модема удалённого обслуживания и подключение к недоверенному ресурсу
5. Загрузка и запуск вредоносного кода на сервере телемеханики
6. Подмена штатного клиента протокола МЭК 104 и блокирование удаленного доступа

Описание демонстрационного стенда и сценария



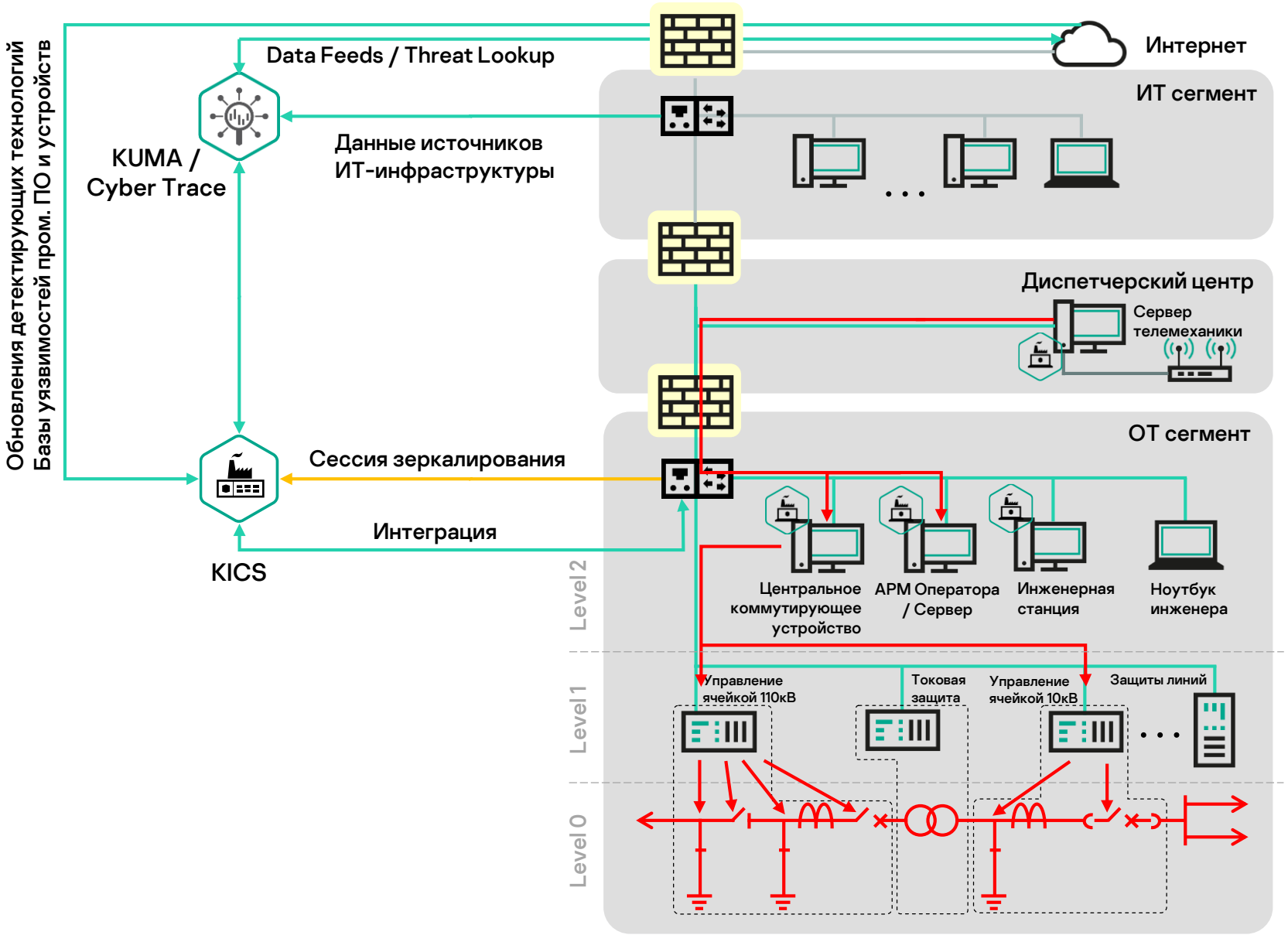
1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера
3. Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ
4. Активация 4G-модема удалённого обслуживания и подключение к недоверенному ресурсу
5. Загрузка и запуск вредоносного кода на сервере телемеханики
6. Подмена штатного клиента протокола МЭК 104 и блокирование удаленного доступа
7. Подмена мнемокадров и запрет локального управления на АРМ оператора

Описание демонстрационного стенда и сценария



1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера
3. Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ
4. Активация 4G-модема удалённого обслуживания и подключение к недоверенному ресурсу
5. Загрузка и запуск вредоносного кода на сервере телемеханики
6. Подмена штатного клиента протокола МЭК 104 и блокирование удаленного доступа
7. Подмена мнемокадров и запрет локального управления на АРМ оператора
8. Ретрансляция команд подменённого управления из Диспетчерского центра через ЦКУ на первичное оборудование подстанции

Описание демонстрационного стенда и сценария



1. Компрометация узла инженера и утечка данных о АСУ ТП
2. Загрузка скрипта целевой атаки на узел инженера
3. Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ
4. Активация 4G-модема удалённого обслуживания и подключение к недоверенному ресурсу
5. Загрузка и запуск вредоносного кода на сервере телемеханики
6. Подмена штатного клиента протокола МЭК 104 и блокирование удаленного доступа
7. Подмена мнемокадров и запрет локального управления на АРМ оператора
8. Ретрансляция команд подменённого управления из Диспетчерского центра через ЦКУ на первичное оборудование подстанции
9. Удаление первичных следов атаки. Схема разобрана, потребитель отключен

Спасибо!