Kaspersky Industrial Cybersecurity Conference 2023

OT XDR — новейший подход к промышленной кибербезопасности

Антон Иванов
CTO

kaspersky

Современные ИБ-реалии

Ежегодно

Усложняется ландшафт угроз, киберпреступники совершенствуют свои методы

Расширяется поверхность атаки и количество точек входа злоумышленников

Усиливаются требования регуляторов, особенно в отношении обеспечения защиты КИИ

Добавилось

Наступила эра хактивизма и целевой киберагрессии

Больше лазеек из-за ухода ИБ-вендоров, изменение целей киберпреступников и связанных с этим тактик и техник

Началась активная фаза импортонезависимости

АСУ в 2023

- Рост интереса хактивистов к системам автоматизации
- Увеличение числа APT-угроз в промышленном сегменте
- 31,9%* компьютеров АСУ в России были атакованы ВПО в H1 2023 года.

- Атаки для сбора всевозможного рода информации, например, связанных с развитием промышленных секторов экономики.
- Атаки с целью закрепиться на «черный день», а также с целью нанесения прямого ущерба
- Главные факторы активности атакующих — геополитическая напряженность

Необходимость соответствовать требованиям регулирующих органов побуждают организации к внедрению специализированных средств киберзащиты промышленных инфраструктур.

Kaspersky ICS CERT, сентябрь 2023 г.

Устойчивое развитие промышленных предприятий и объектов КИИ

Сегодня как никогда важен выбор надежного партнера, который обладает экспертизой на стыке промышленной и корпоративной кибербезопасности и готов предложить полный арсенал расширенных защитных технологий

Единая концепция промышленной кибербезопасности Kaspersky OT CyberSecurity

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 (OT XDR)

- 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 Secure Remote Workspace
- Kaspersky IoT Secure Gateway
- 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

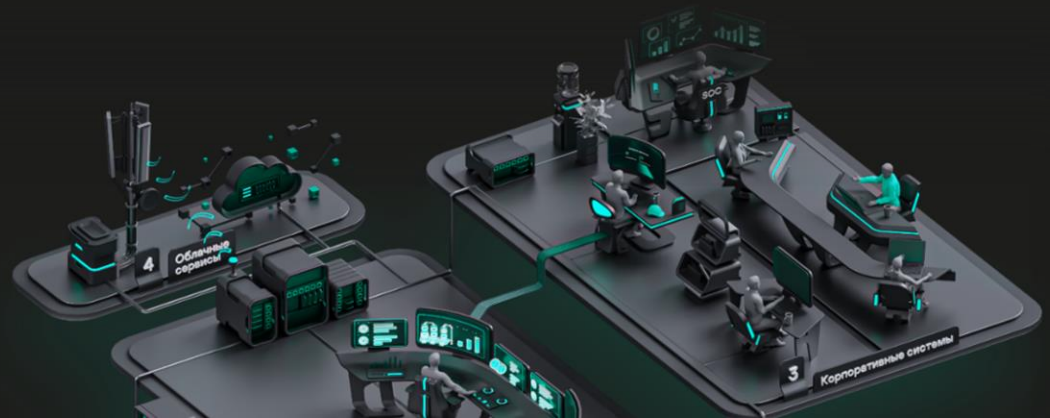
- Kaspersky Incident Response
- Kaspersky Industrial Emergency Kit

Набор экспертных сервисов для комплексной промышленной кибербезопасности

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			●

Архитектура промышленной нативной OT XDR-платформа

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

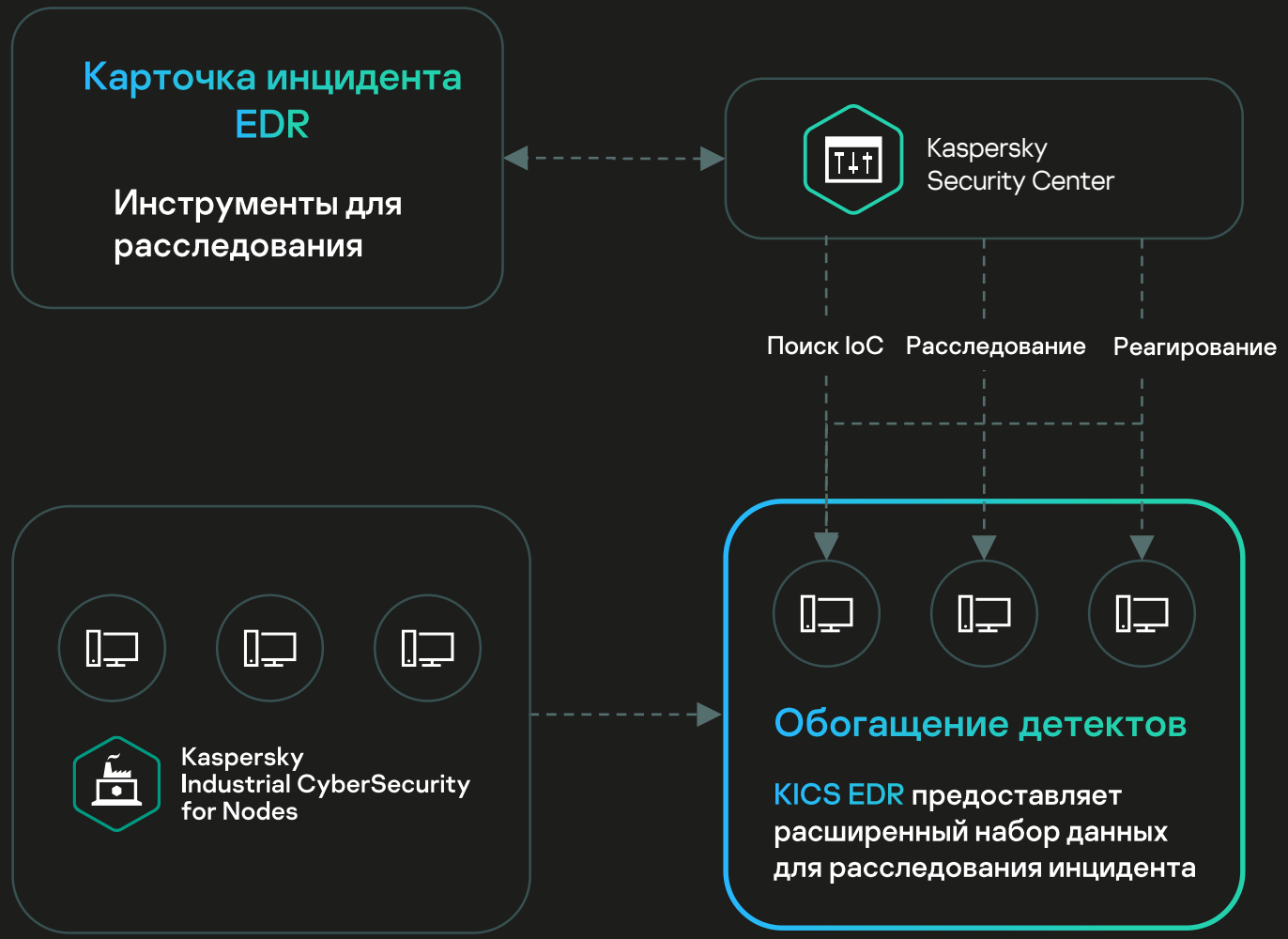
Реагирование на инциденты

Ключевые преимущества

Лидерский EDR от ЛК на базе KICS for Nodes для ICS

Большой набор сценариев реагирования на инцидент

Не требуется дополнительное оборудование!



Направления развития в 2023 году

Работа с инцидентами

- Агрегация и корреляция всех событий с узлов и сети в одном окне KICS for Networks
- Обогащение событий контекстом для быстрого расследования инцидентов
- Цепочка атаки для событий с узлов сети
- Реагирование для предотвращения дальнейшего распространения угрозы

Аудит безопасности

- Централизованный аудит безопасности на базе KICS for Networks
- Защищенное хранилище учетных данных для автоматизации задач аудита
- Расширяемые базы с контентом: уязвимости АСУ ТП, контроль конфигураций, комплаенс
- Открытый формат правил (OVAL)

Linux

- Активное развитие KICS for Linux Nodes, сертификация и поддержка отечественных дистрибутивов
- Поддержка KSC Linux (паритет фич с Windows версией в 2024)

Расширение NTA функциональности

- Отображение сессий для полной видимости сетевой активности
- Возможность сохранения и выгрузки трафика по сессиям для детального исследования
- Детектирование аномалий в сети по статистическим правилам

Возможности по анализу сетевого трафика (Network Traffic Analysis)

Технологии KICS

Экспертиза и технологии KATA

NTA

Kaspersky Industrial CyberSecurity

for Networks

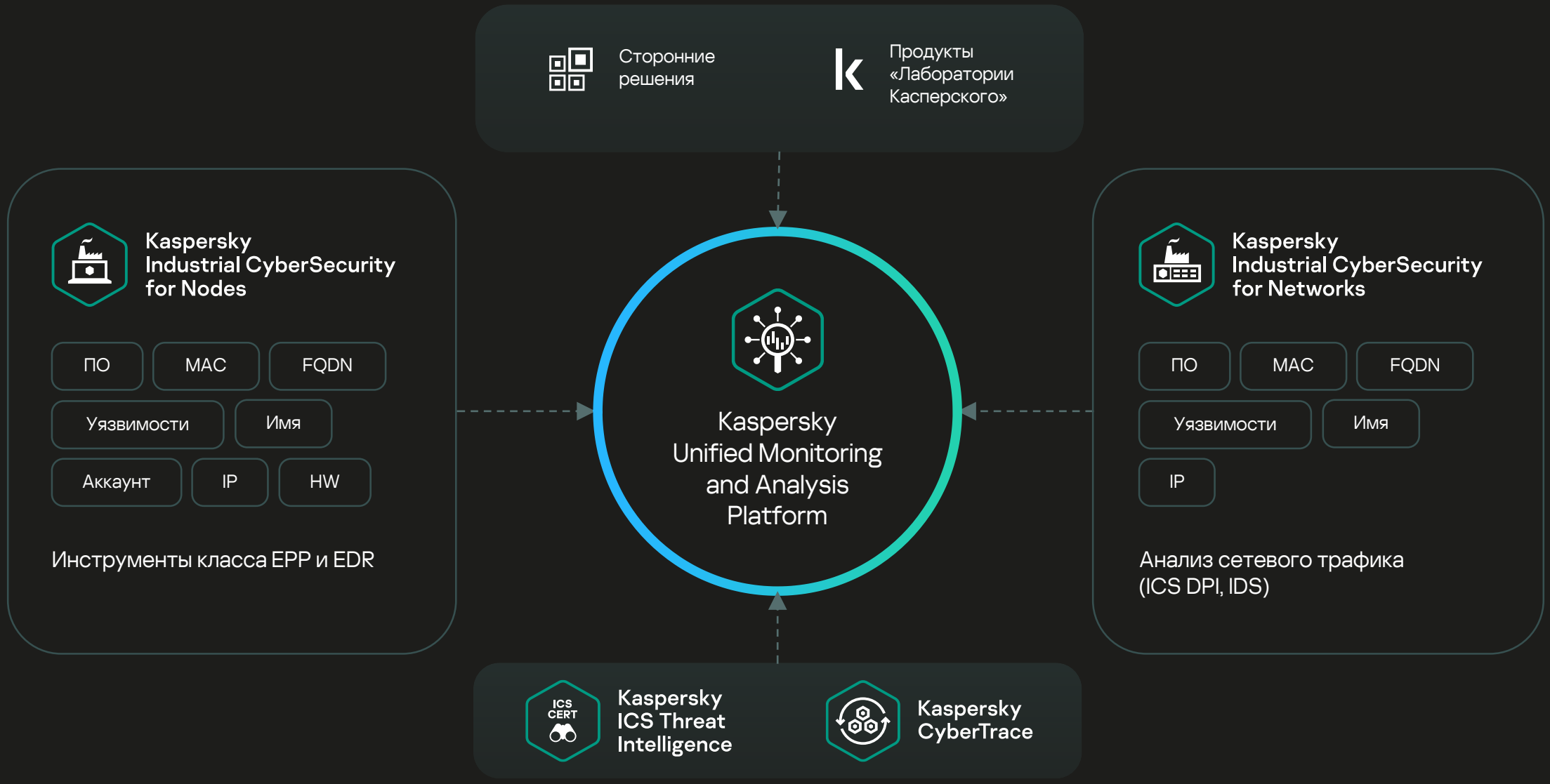
\+

Kaspersky Anti Targeted Attack Platform

=

Kaspersky Network Traffic Analysis

Состав открытой OT XDR-платформы



Всестороннее понимание угроз и уязвимостей

Kaspersky ICS Threat Intelligence

Kaspersky ICS Malware Data Feed

Регулярно обновляемый поток данных об актуальных угрозах для систем АСУ ТП, позволяющий упростить и автоматизировать обнаружение и расследование атак. Основан на телеметрии с более чем 1 млн узлов, относящихся к АСУ ТП

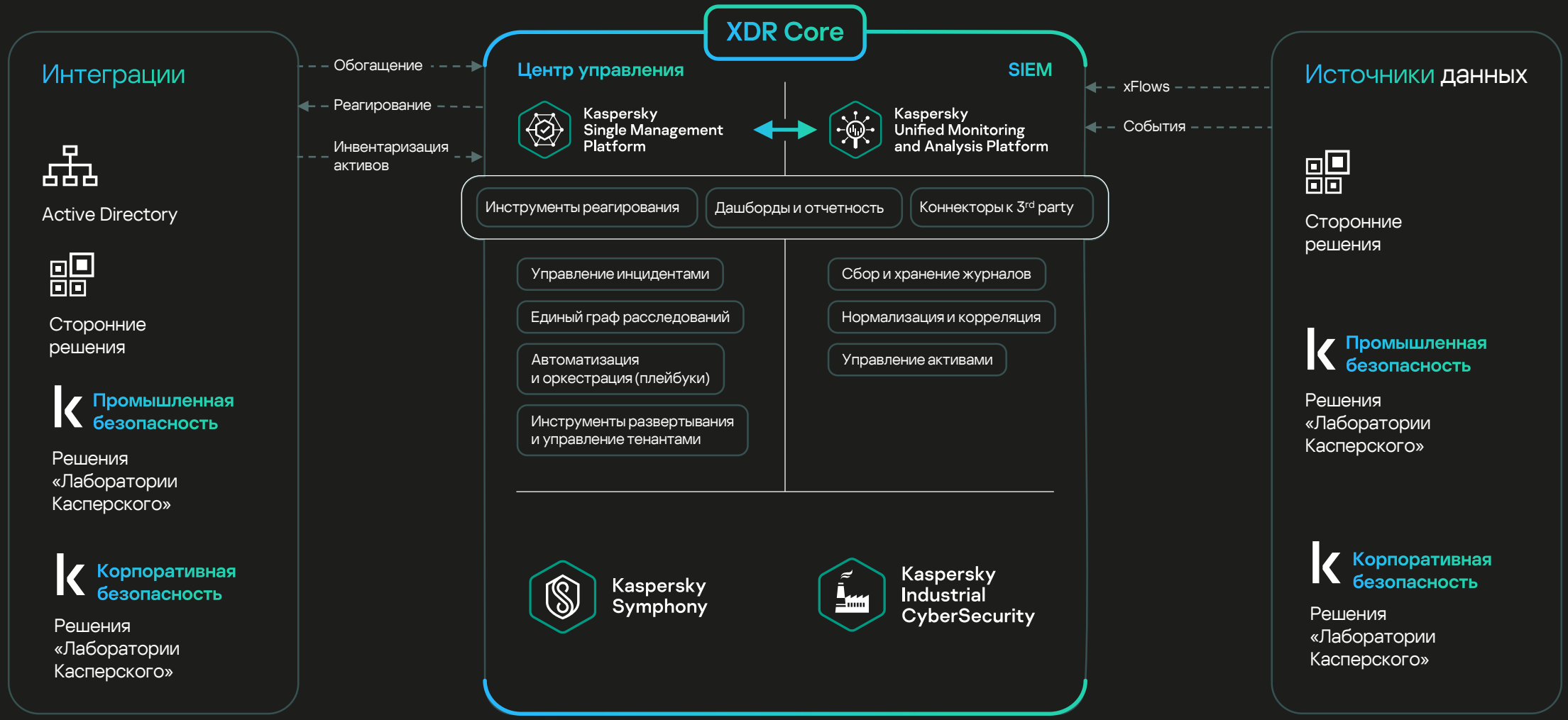
Kaspersky ICS Threat Intelligence Reporting

Отчеты и оповещения о кибератаках на промышленные предприятия и об уязвимостях в промышленном ПО и оборудовании, а также регулярные обзоры угроз для систем промышленной автоматизации, доступные через web-портал или API

Kaspersky ICS Vulnerability Data Feed

Регулярно обновляемый поток проверенных и уточненных данных об уязвимостях в ПО и оборудовании для АСУ ТП в машиночитаемом формате

Архитектура единой IT-OT XDR-платформы

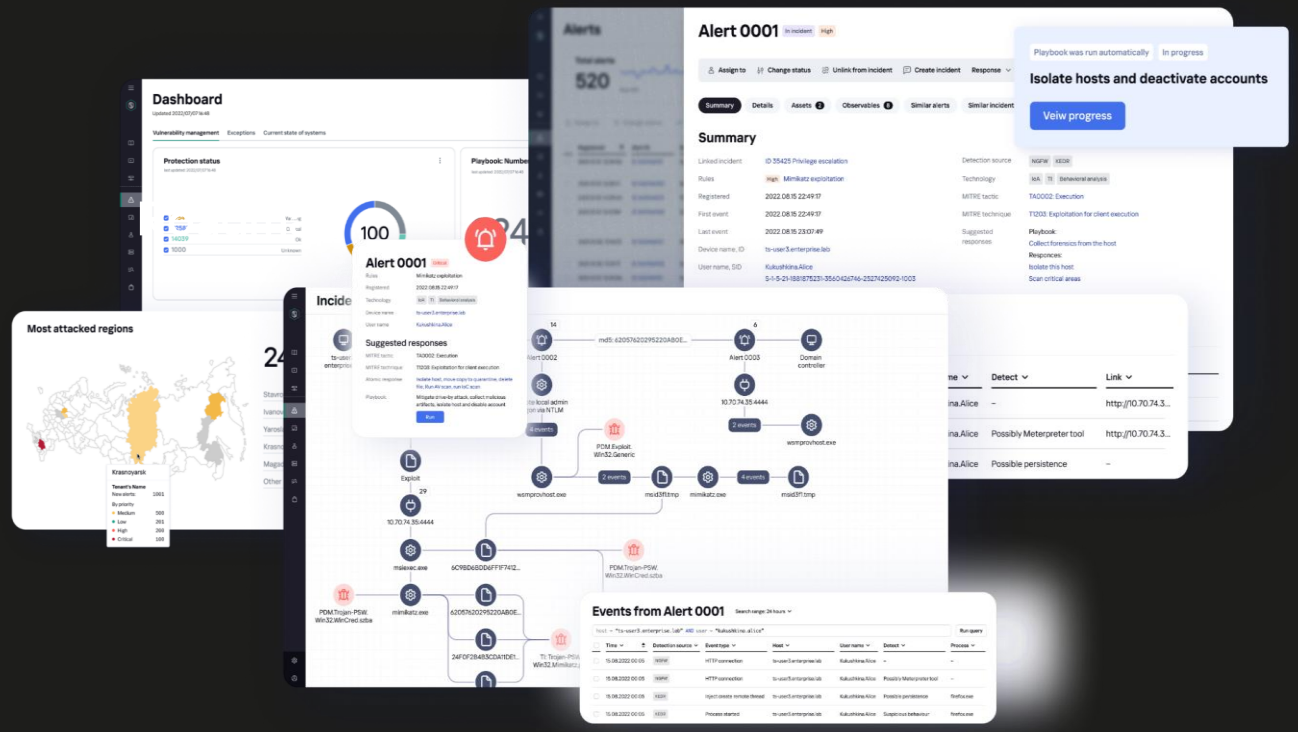


Единая консоль для работы со сложными инцидентами

Централизованное реагирование через ручные и автоматические плейбуки

Кросс-продуктовые сценарии реагирования на базе доступных интеграций

Граф расследования с обогащением контекста и применением сценариев реагирования



Описание сценария атаки

1

Компрометация узла инженера и утечка данных о АСУ ТП

2

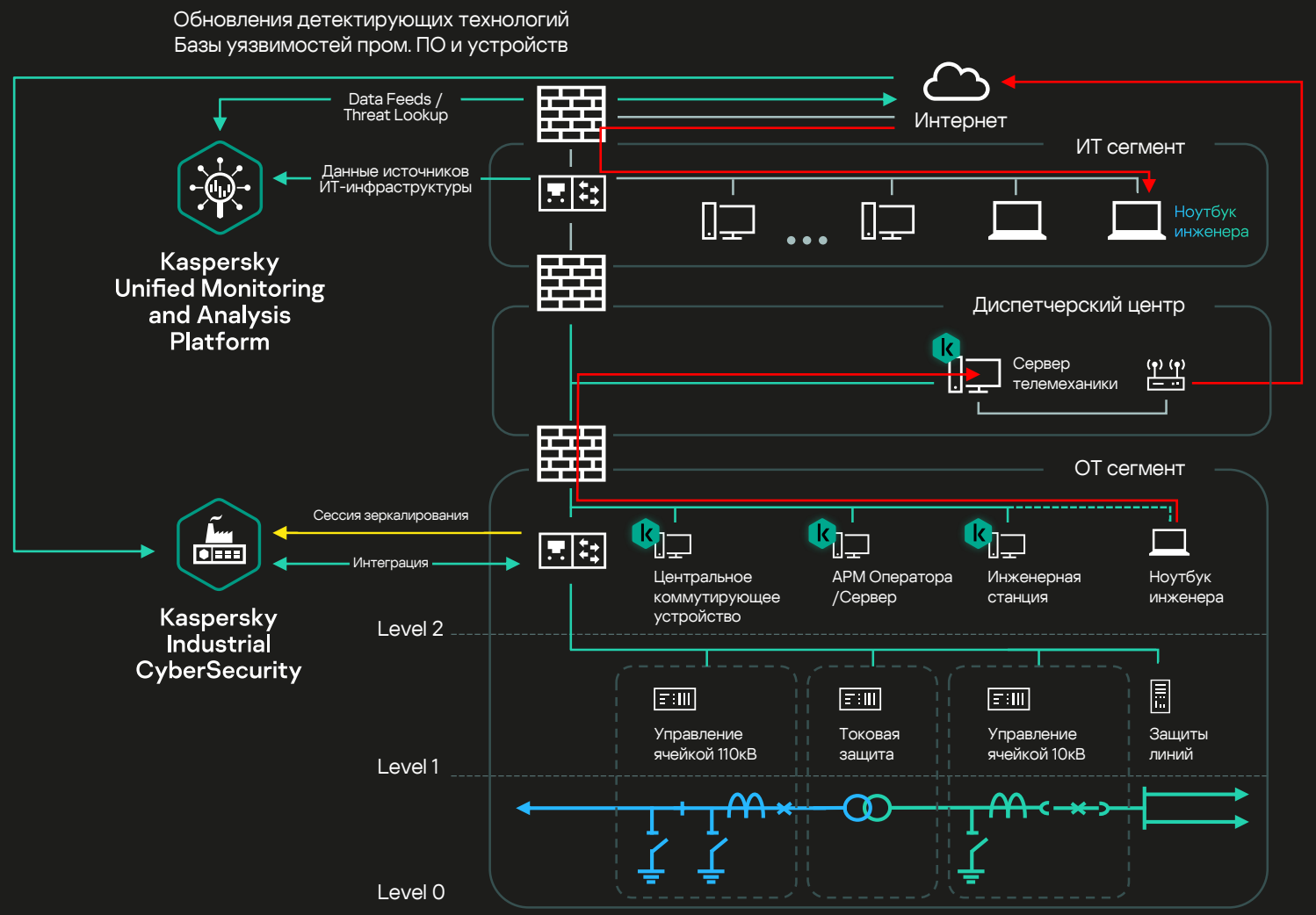
Загрузка скрипта целевой атаки на узел инженера

3

Загрузка скрипта целевой атаки на сервер телемеханики в ДЦ

4

Активация 4G-модема удалённого обслуживания и подключение к недоверенному ресурсу



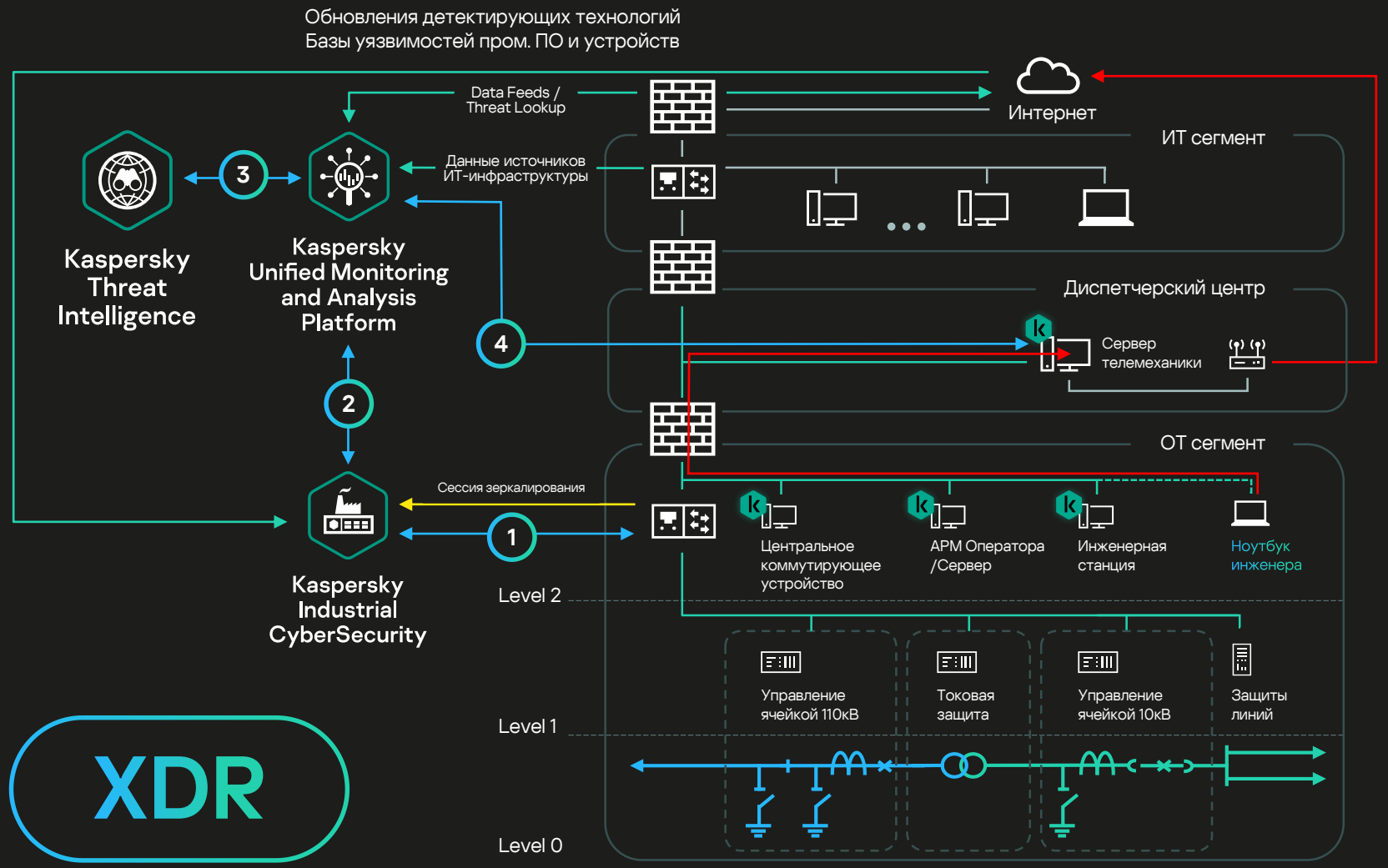
Описание сценария атаки (Detection)

1. Alert о подключение процесса к недоверенному ресурсу наружу

2. Передача Alert в XDR

3. Проверка данных о внешнем IP адресе связанным с Alert

4. Корреляция на XDR: Alert + TI данные. Обработка алерта от KICS + TI = завершение вредоносного процесса

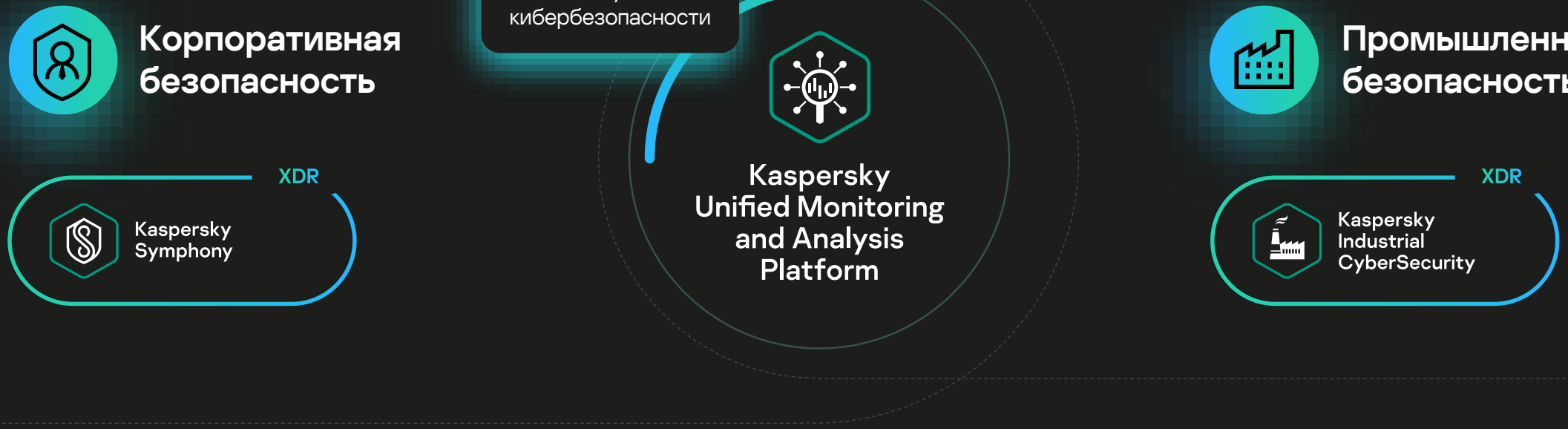


Цельное предложение Kaspersky для защиты OT и IT сред и дальнейшее развитие

SASE Secure Access Service Edge

Zero Trust
- Контроль доступа к ресурсам и данным
- Запрет на несанкционированные действия

\+ Кибериммунный модуль Zero Trust на базе KOS



Партнер по кибербезопасности, которому можно доверять

Глобальное присутствие, опыт и знания мирового уровня

Высокий статус в индустрии безопасности IT/OT-систем

Более 100 сертификатов о совместимости с решениями вендоров АСУ ТП

Доказанная эффективность технологий и соответствие стандартам

ICS CERT

Собственное международное подразделение ICS CERT

Клиенты по всему миру

Kaspersky Industrial Cybersecurity Conference 2023

Спасибо!

kaspersky