Сплав технологий и экспертизы для промышленной кибербезопасности

Переход от антивируса и системы обнаружения вторжений к технологии XDR в АСУ ТП

kaspersky

Современные реалии

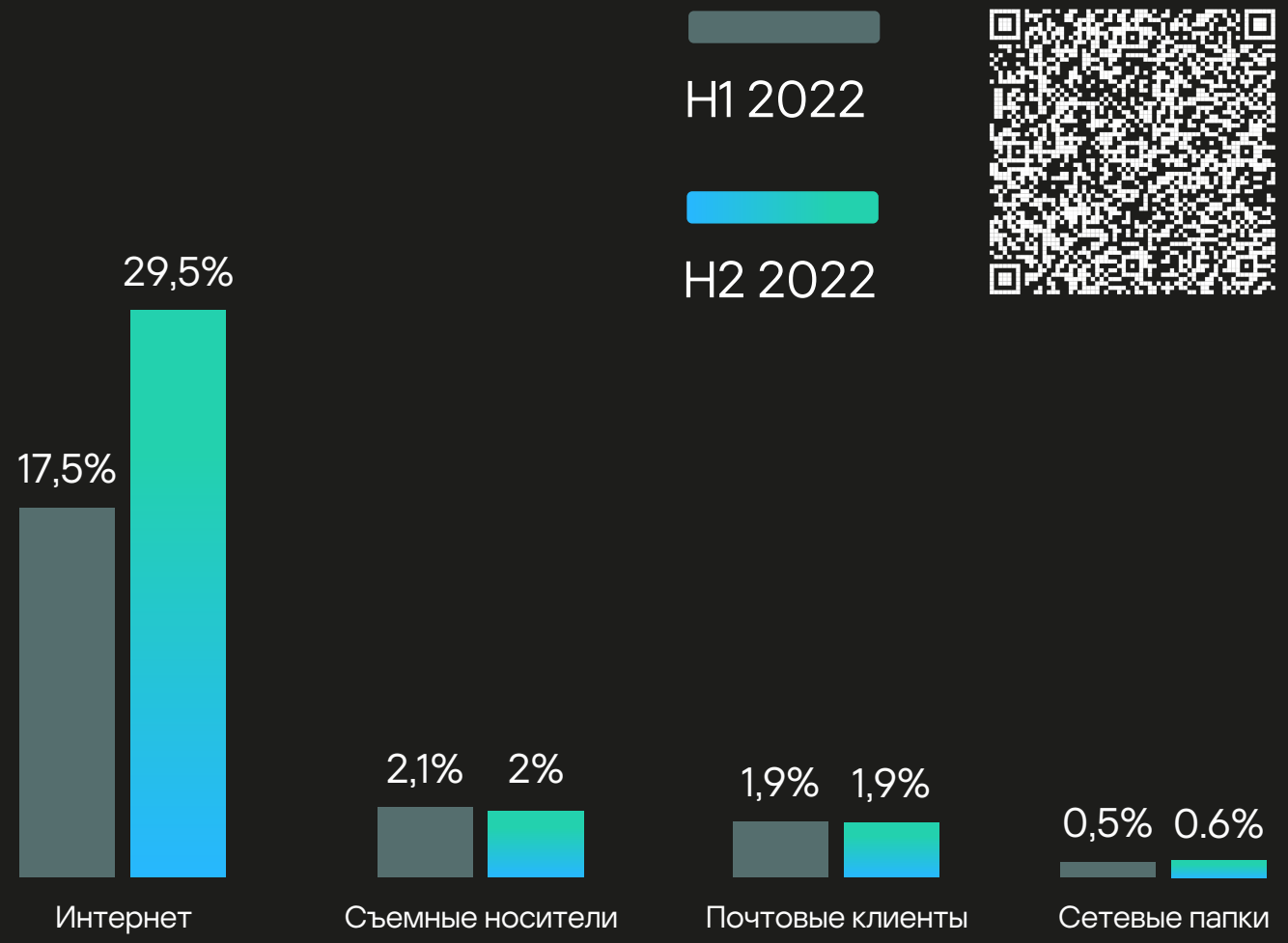
Уход зарубежных вендоров АСУ ТП и ИБ с российского рынка

Низкий уровень осведомленности персонала об угрозах ИБ в АСУ ТП

Повышенный уровень киберагрессии в отношении российских промышленных предприятий

Ослабление уровня защищенности корпоративной инфраструктуры и сопряжения с OT-средой

В H2 2022 в России отмечено самое значительное изменение процента атакованных компьютеров в АСУ среди всех стран. Этот показатель увеличился на 9 п.п. и составил 39,2%



В начале пути

Kaspersky Industrial CyberSecurity for Nodes

- Защита от вредоносного ПО с минимальным влиянием на систему
- Контроль целостности ПЛК
- Противодействие шифровальщикам
- Контроль приложений и устройств

Kaspersky Industrial CyberSecurity for Networks

- Обнаружение в трафике передаваемых технологических параметров и их отклонений (промышленный DPI)
- Обнаружение отклонений от базовых параметров в сетевых коммуникациях
- Скоринг рисков событий и узлов
- Инвентаризация активов, включая данные об уязвимостях и состоянии узлов

Архитектура интегрированных решений

Kaspersky
Industrial CyberSecurity
for Nodes

Инструменты класса
EPP и 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

Kaspersky OT CyberSecurity

Средство обнаружения и реагирования на сложные атаки

Единая концепция промышленной кибербезопасности

Технологии

Полный арсенал защитных решений, протестированных вендорами АСУ ТП

Знания

Достоверная аналитика угроз в АСУ ТП и специальные тренинги

Экспертиза

Набор экспертных сервисов для комплексной промышленной кибербезопасности

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 for Nodes
- Kaspersky Industrial CyberSecurity for Networks

Фокусные

- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN
- Kaspersky Antidrone
- Kaspersky Unified Monitoring and Analysis Platform

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

Это специализированное решение для мониторинга сети АСУ ТП и защиты конечных узлов промышленной среды. Представляет собой специализированную промышленную платформу класса XDR.

Подробнее

Полная информация о продукте и больше преимуществ

Ключевые преимущества

Признание

Более 10 лет активного присутствия в сфере. Признана компанией года на рынке промышленной кибер-безопасности (Frost and Sullivan, 2020)

Совместимость

Более чем 80 сертификатов о совместимости с решениями вендоров АСУ ТП

Сертификация

Продукты разработаны с учетом соответствия требованиям 187-ФЗ о защите КИИ и сертифицированы ФСТЭК и ФСБ России

Специализированная защита

Продукты не влияют на технологический процесс и работают в распределенных и изолированных сетях

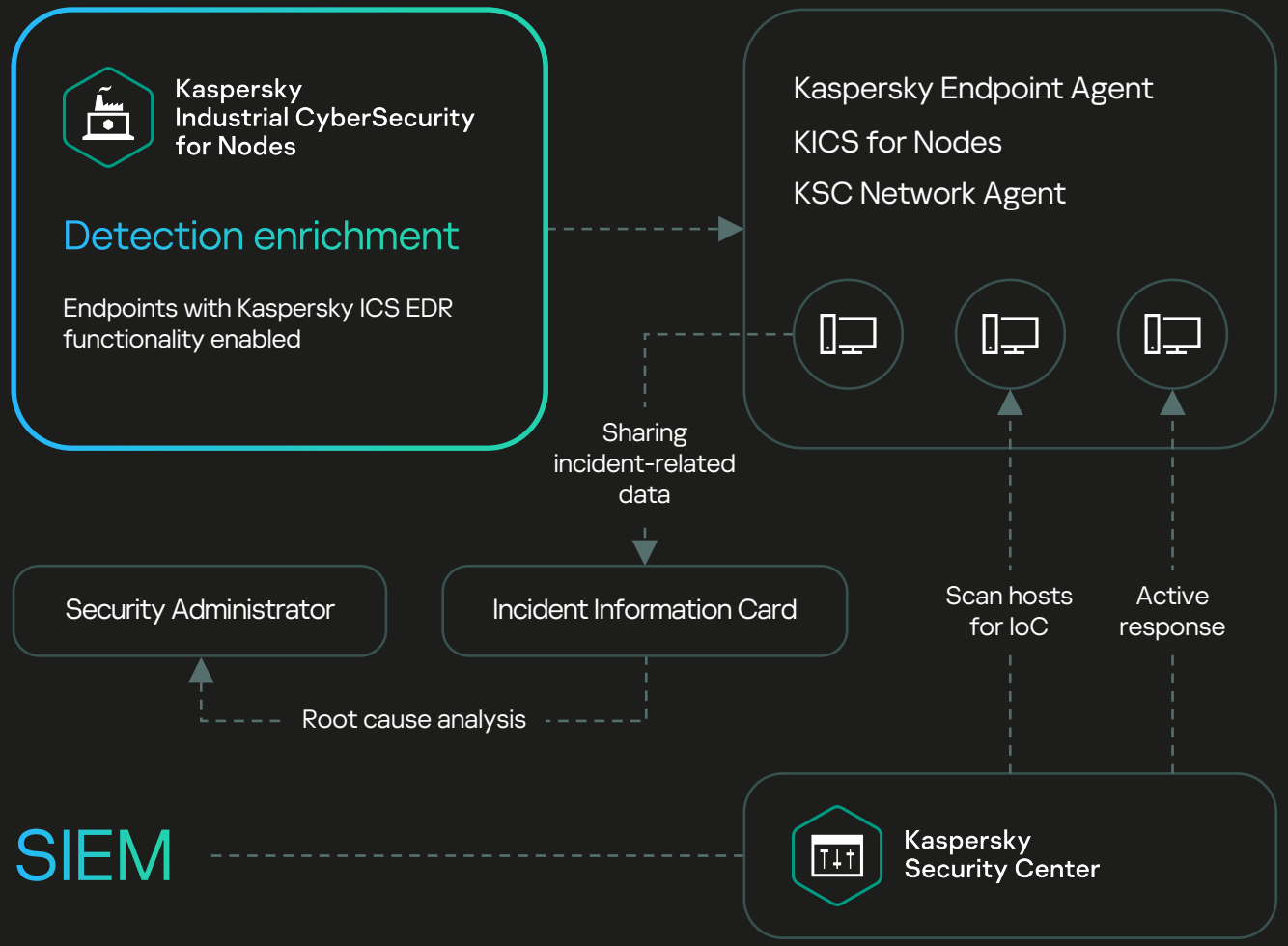
ICS Endpoint Detection and Response (EDR)

Ключевые возможности

Лидерский EDR от ЛК на базе KICS for Nodes для АСУ ТП

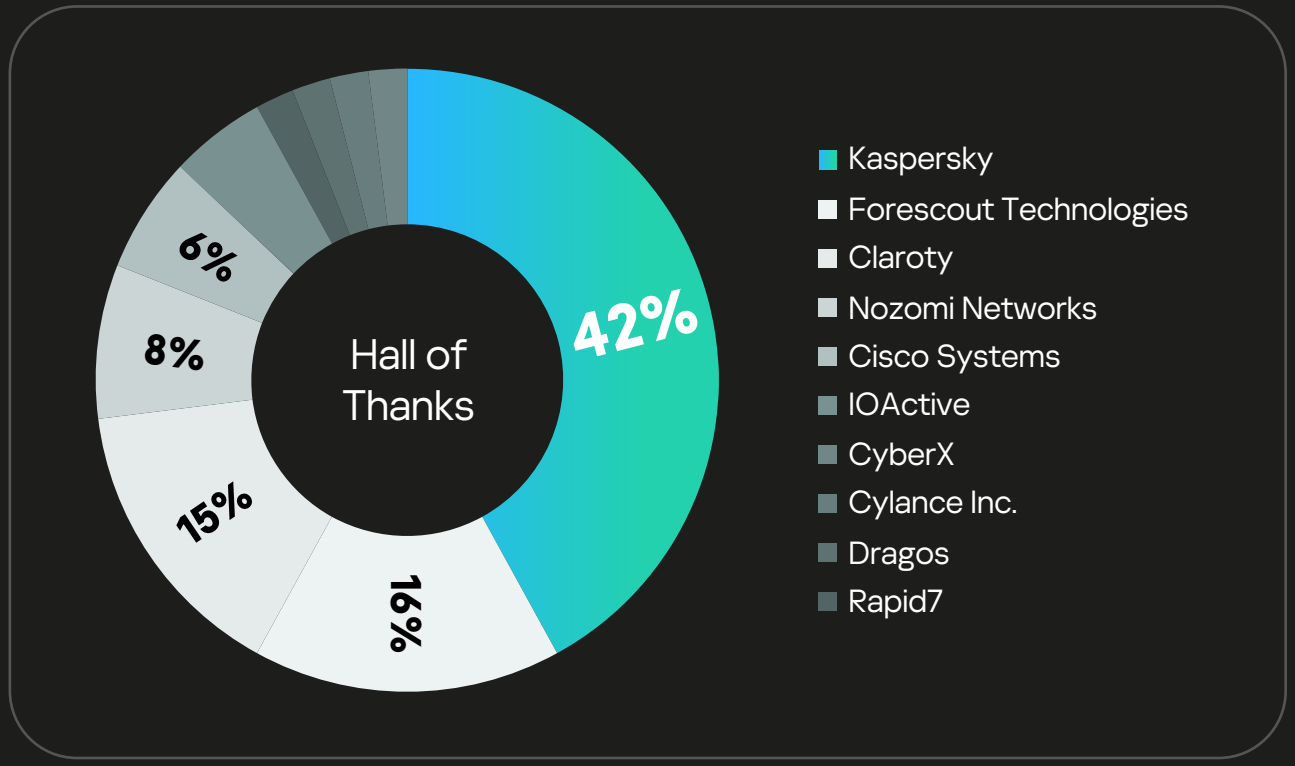
Большой набор сценариев реагирования на инцидент

Не требуется дополнительное оборудование!



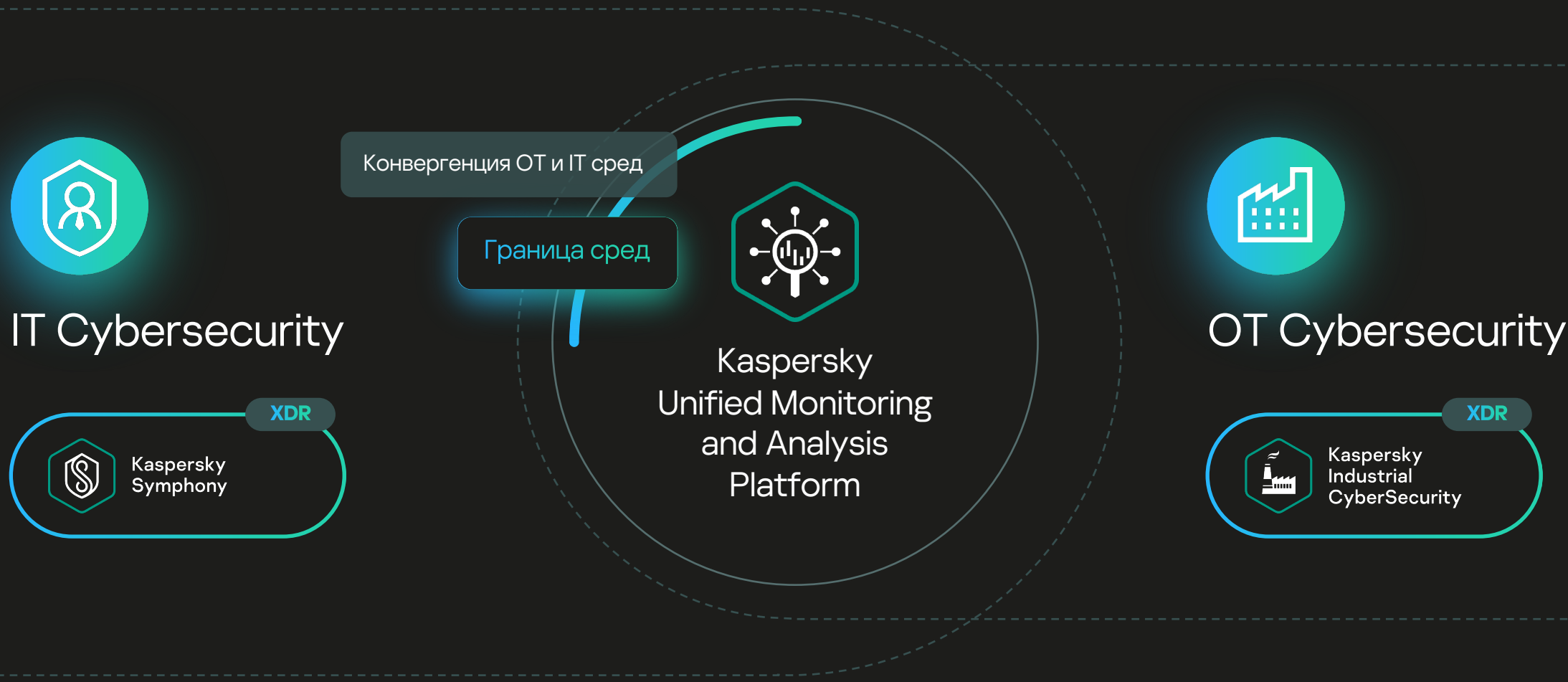
KICS for Networks
и KICS for Nodes
смогут определять
уязвимости
в промышленном ПО
и оборудовании

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



Kaspersky Unified Monitoring and Analysis Platform

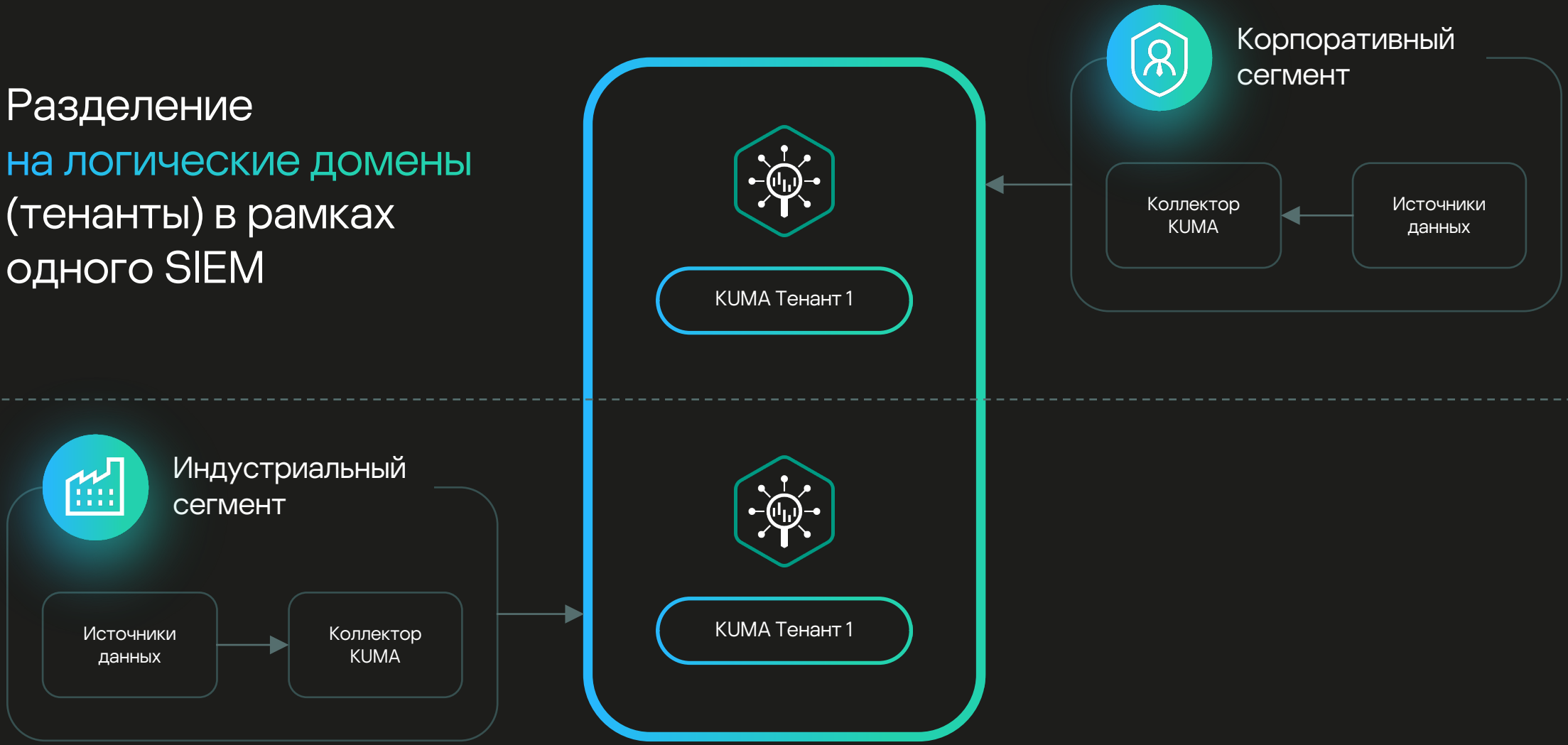
Цельное предложение для защиты OT и IT сред



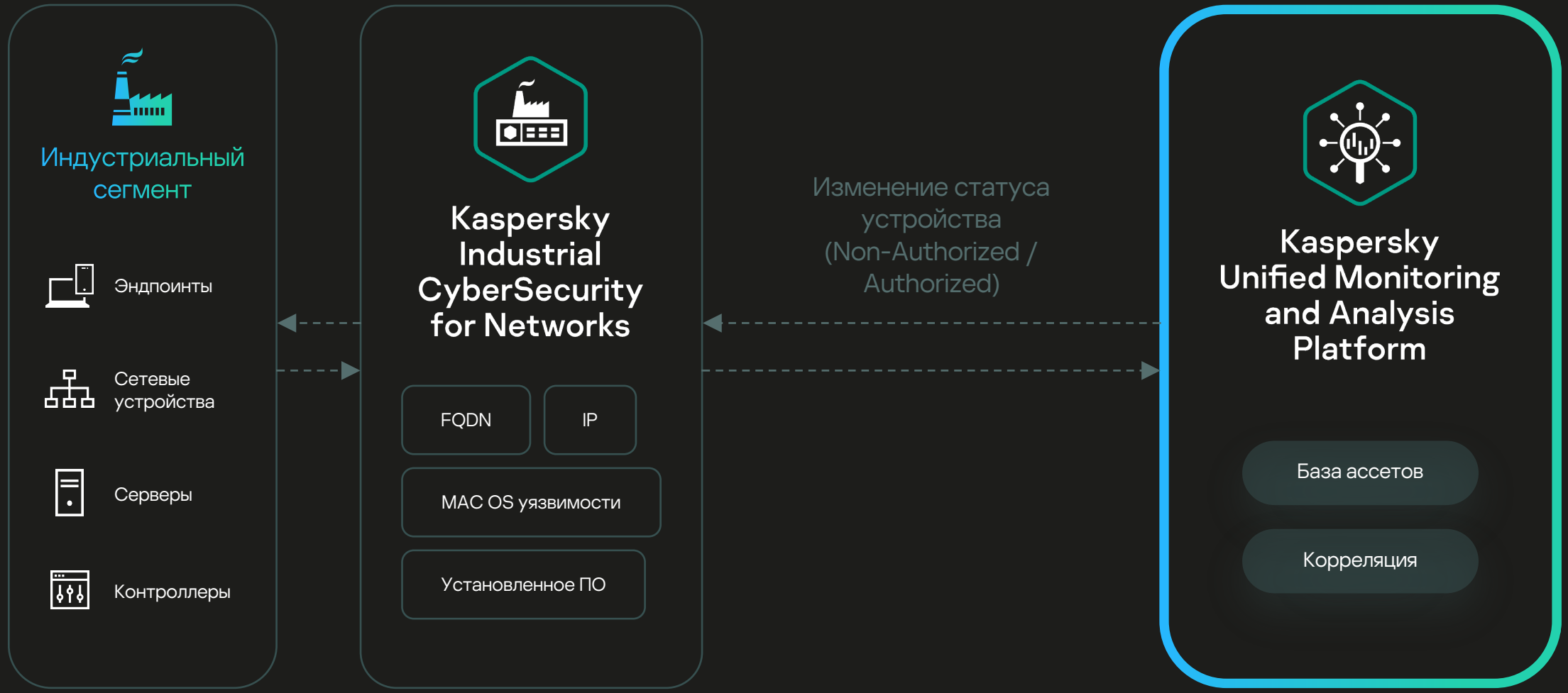
Разные сегменты, один SIEM

Разные сегменты, один SIEM

Разделение
на логические домены
(тенанты) в рамках
одного SIEM



Интеграция с KICS for Network



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

Подробнее

Kaspersky ICS CERT

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

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

Статус CVE Numbering Authority (CNA)

Членство в международных организациях:

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

Threat Intelligence — источники


Почему
Kaspersky?

Почему Kaspersky?

Глобальное присутствие, опыт и знания мирового уровня

Высокий статус в индустрии безопасности IT/OT-систем

Более 80 сертификатов о совместимости с решениями вендоров АСУ ТП

ICS CERT

Собственное международное подразделение ICS CERT

Доказанная эффективность технологий и соответствие стандартам

Наши преимущества

Мировая известность

Бренд, известный во всем мире. Одна из крупнейших частных компаний в сфере кибербезопасности

Надежная защита

Более 10 лет «Лаборатория Касперского» разрабатывает и предлагает решения для защиты промышленных предприятий

Многогранность

«Лаборатория Касперского» обладает проектным опытом внедрения в разных отраслях: добыча полезных ископаемых, электроэнергетика, промышленность, транспорт и пр.

Экспертность

Компания имеет в своем составе специализированные экспертные подразделения (ICS CERT, GREAT), в составе которых работают эксперты международного уровня

Высочайшее качество

Качество решений и сервисов подтверждено международными аналитическими агентствами

Применение экосистемы KICS (совместно с орг. мерами) позволяет реализовать:

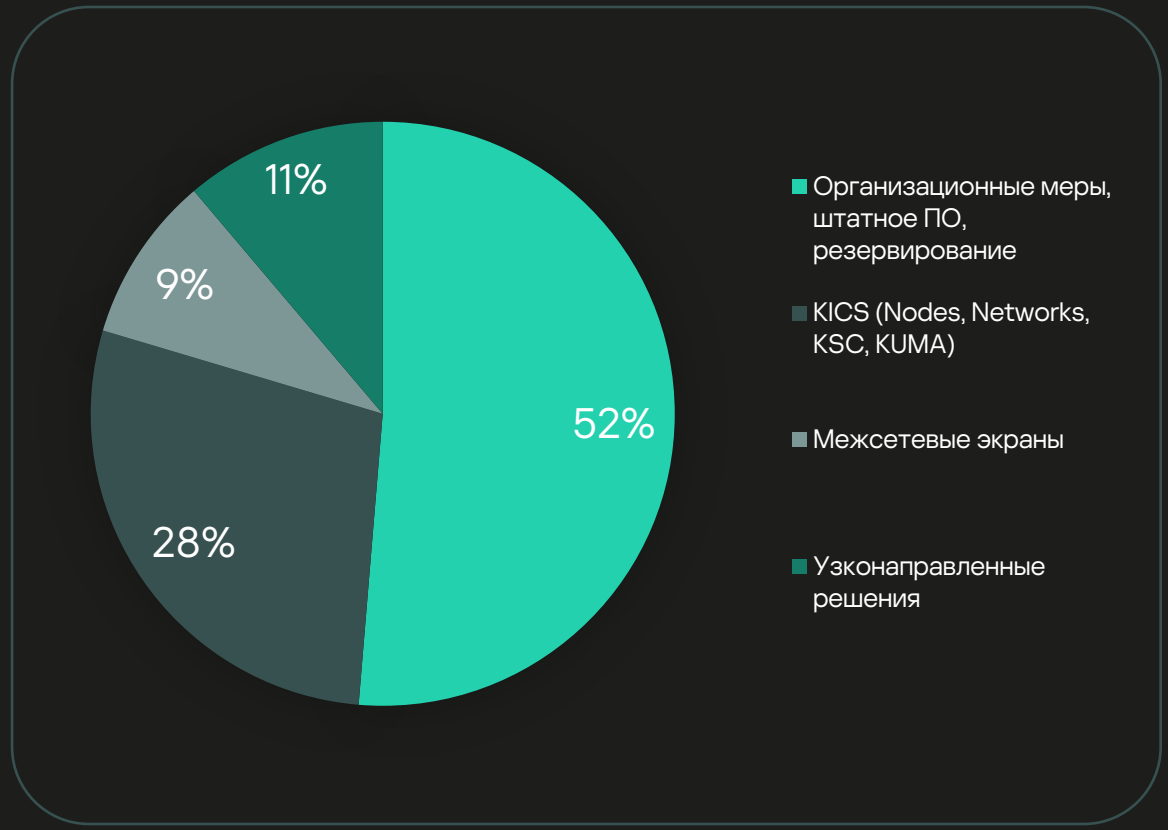
80%

всех мер приказа ФСТЭК №239

84%

базового набора мер для объектов КИИ 3-й категории

% закрытия



~20%

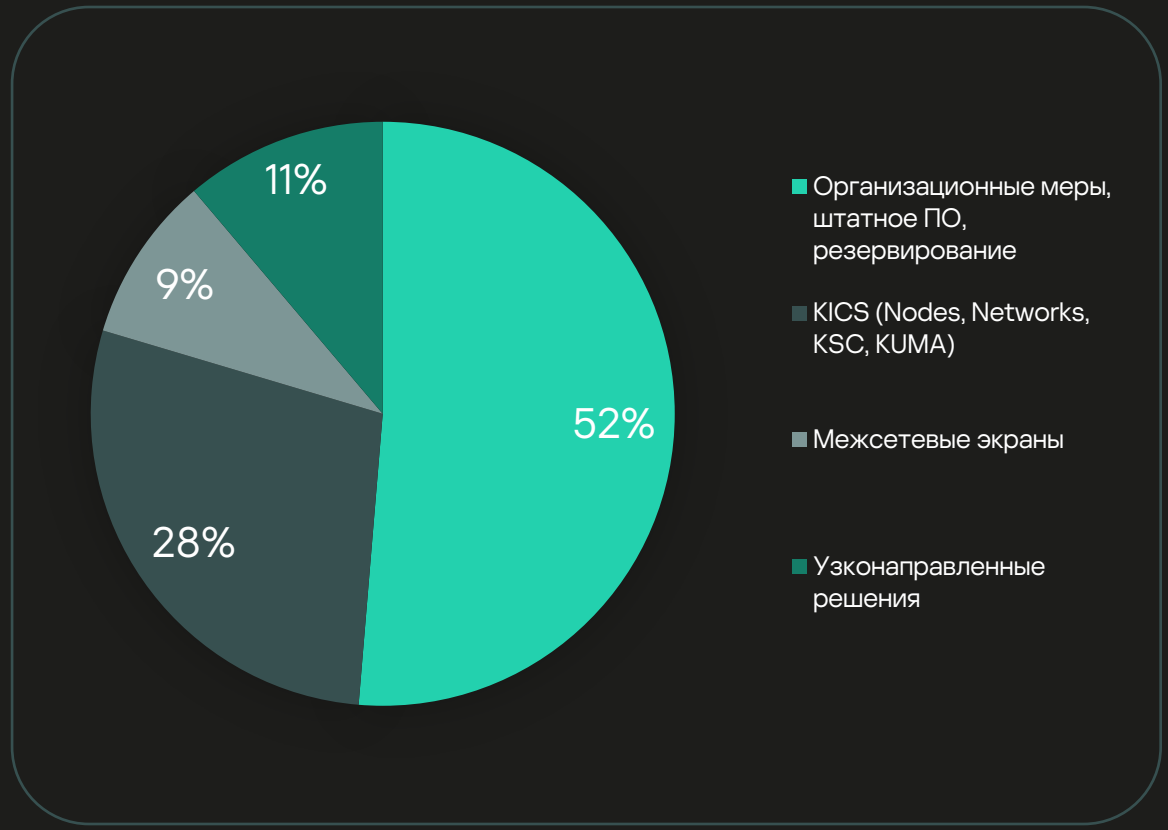
Направления, которые не закрываем

Межсетевые экраны (NGFW) – 9%!

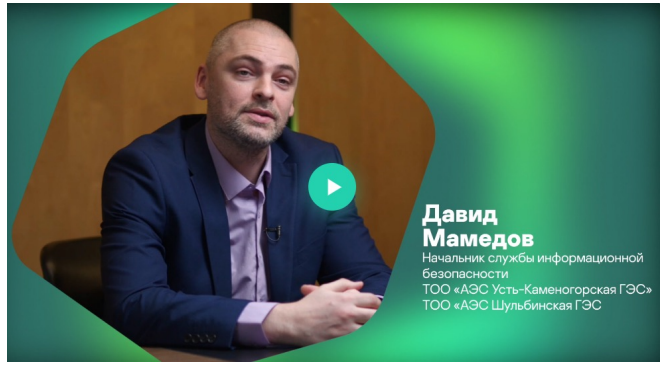
Резервное копирование

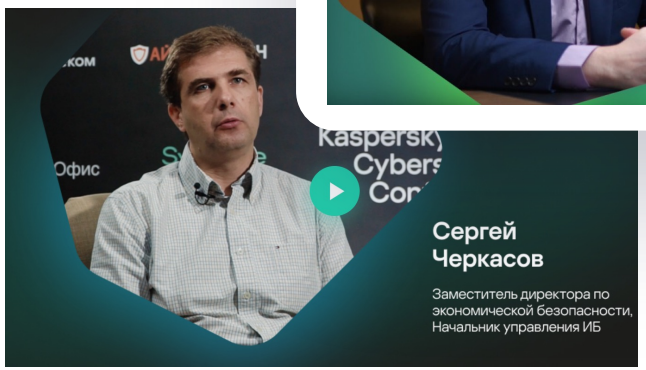
Аутентификация пользователей и управление учетными записями (IdM)

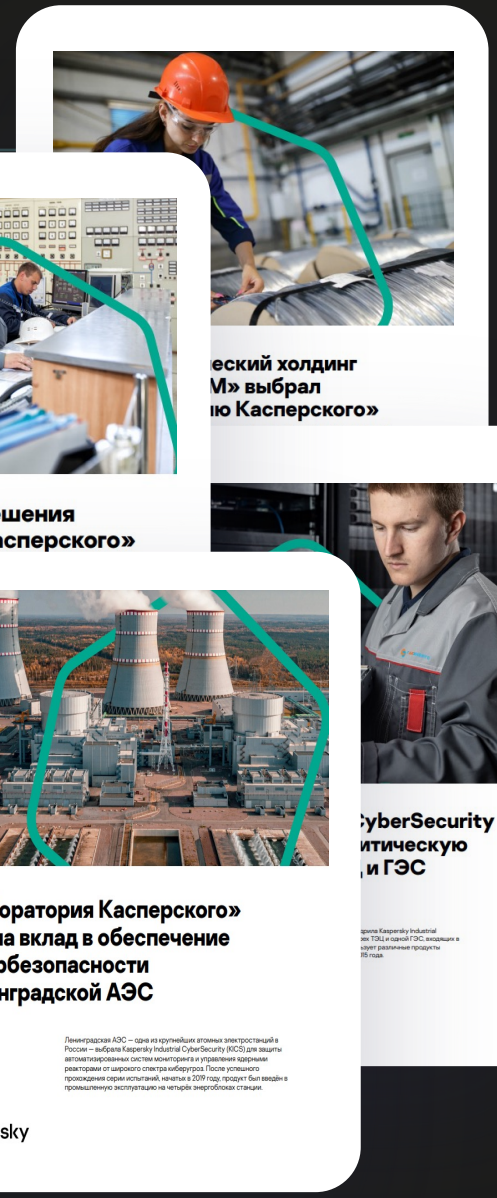
Криптографическая защиты и контроль удаленного доступа (криптошлюзы, PAM)



Истории успеха







Спасибо!