K2 кибер безопасность

kaspersky

Единый мониторинг промышленного и корпоративного сегментов: проще, эффективнее, экономнее

Егор Куликов

Руководитель направления безопасности КИИ и АСУ ТП, К2 Кибербезопасность

Андрей Бондюгин

Руководитель направления предпродажной поддержки решений для бизнеса, «Лаборатория Касперского»

Одно порождает другое: почему инциденты в одном сегменте создают угрозы для другого

01

КСПД

Основное

Много смежных систем, между некоторыми сегментами изоляция условная

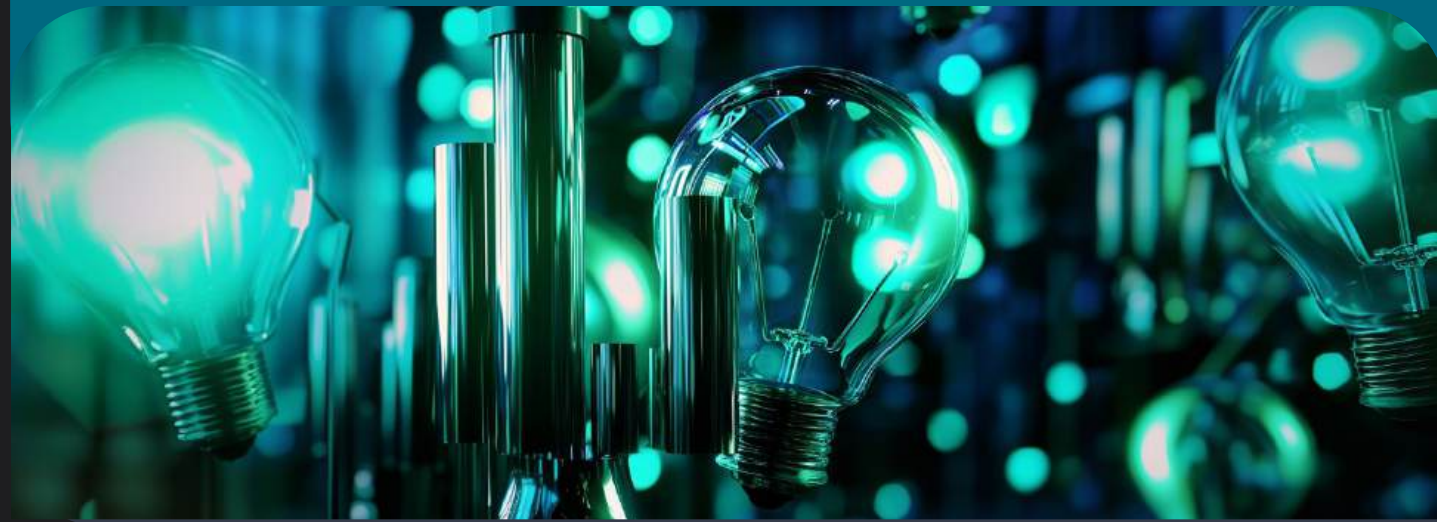
Удаленный доступ с КСПД в АСУ ТП

Уязвимая архитектура управления СЗИ

MES обычно располагается в менее доверенном для АСУ ТП корпоративном сегменте:

- Корпоративные ИС с выходом в Интернет
- Множество персонала разной квалификации
- Большой парк АРМ, серверов и инфраструктурных сервисов
- Проще получить физический доступ к оборудованию

Разный уровень защищенности сегментов, сегменты MES защищены как правило хуже — они не всегда подпадают под законодательство о защите КИИ



АСУ ТП

Правило работает и в обратную сторону

01

В АСУ ТП устаревшая инфраструктура, которая не позволяет закрыть известные уязвимости

02

Зачастую есть связь через Интернет — подрядчики, системы обновления

03

Есть также связь с MES-системами

Проще значит лучше, или как единый мониторинг КСПД и ТСПД помогает эффективнее контролировать уровень защищенности

02

Отдельная инфраструктура SIEM для АСУ ТП и КСПД

- SIEM для корпоративного сегмента
- SIEM для технологического сегмента
- Отдельные команды по мониторингу
- Двойные затраты на лицензии и вычислительные ресурсы
- Разрозненный подход к анализу событий
- Более изолированная инфраструктура без связи с КСПД

K2 кибер безопасность

kaspersky

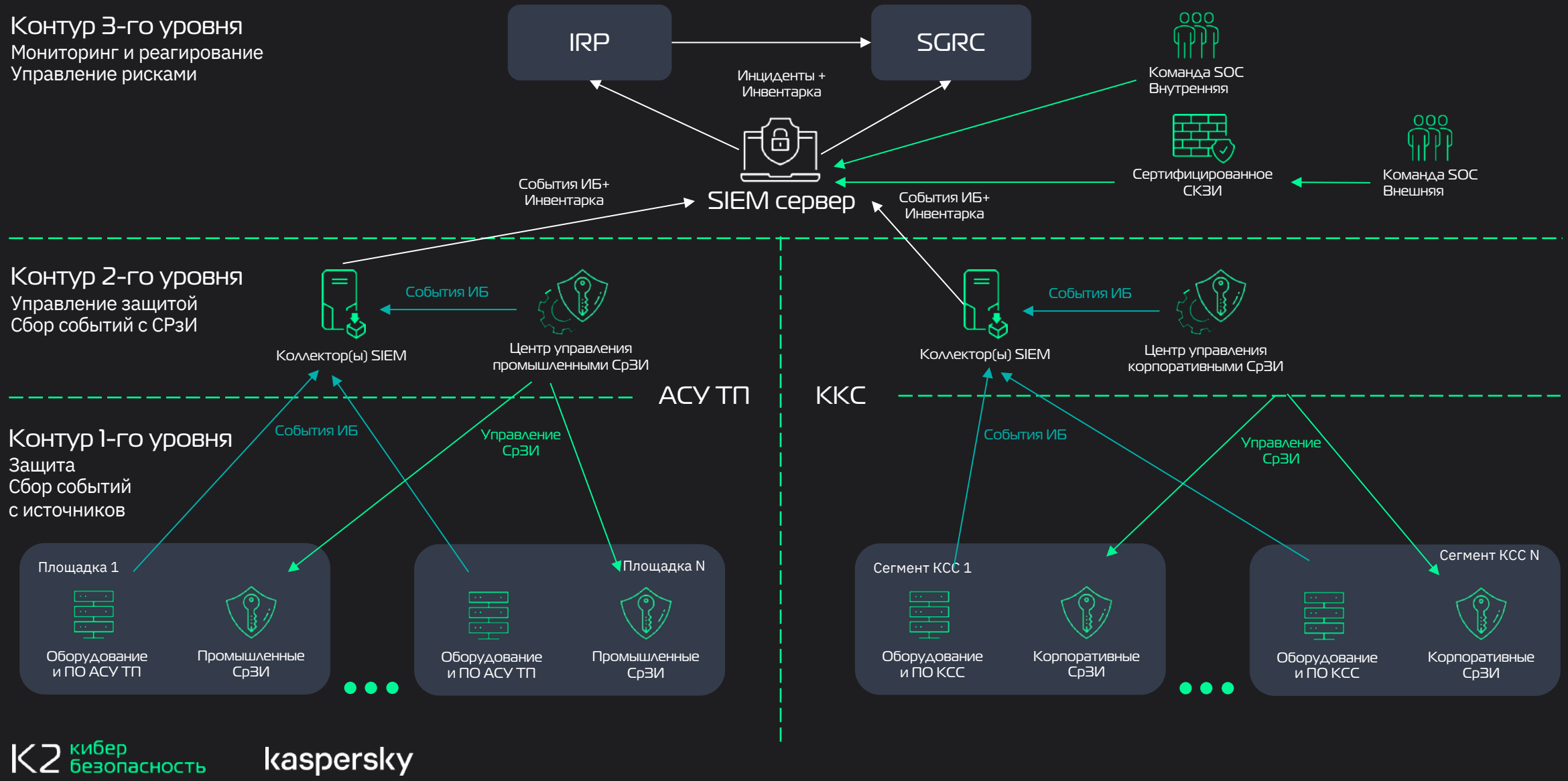
Единая инфраструктура SIEM для АСУ ТП и КСПД

- Единый SIEM
- Команда видит сразу всю картину по инфраструктуре
- Экономия на лицензиях, вычислительных ресурсах и обслуживании
- Требуется более тщательное проектирование архитектуры безопасности

K2 кибер безопасность

kaspersky

Схема единого SIEM



K2 кибер безопасность

kaspersky

Особенности

Команда с экспертизой и в КСПД, и в АСУ ТП

Множество источников усложняет мониторинг событий ИБ

Производство работает 24x7

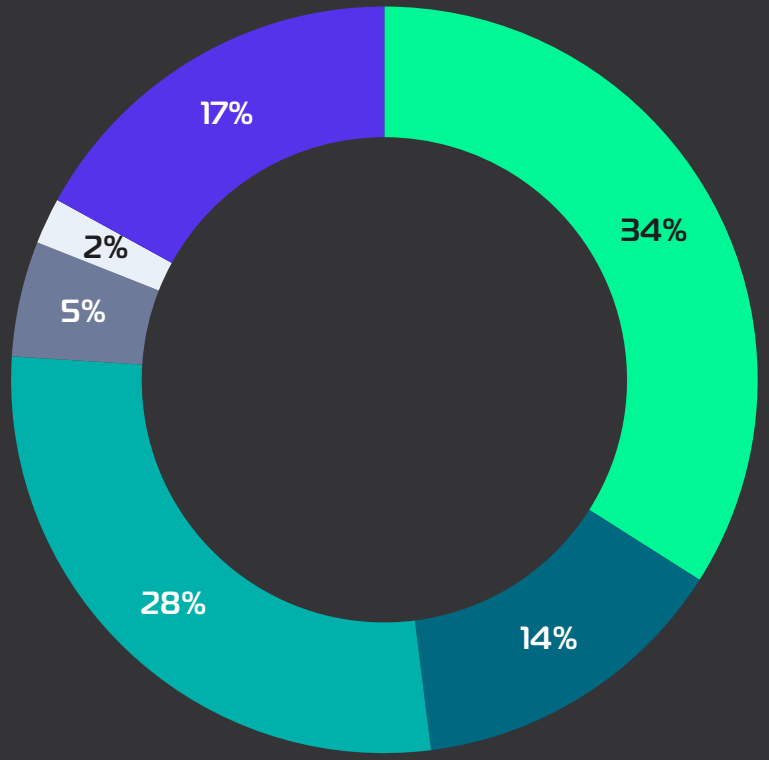
Команда ИБ зачастую работает 8x5

Для мониторинга 24x7 нужно больше специалистов

Выбрать один из трех: зачем промышленному предприятию SOC и на какой модели остановиться

03

Почему бизнес интересуется SOC*

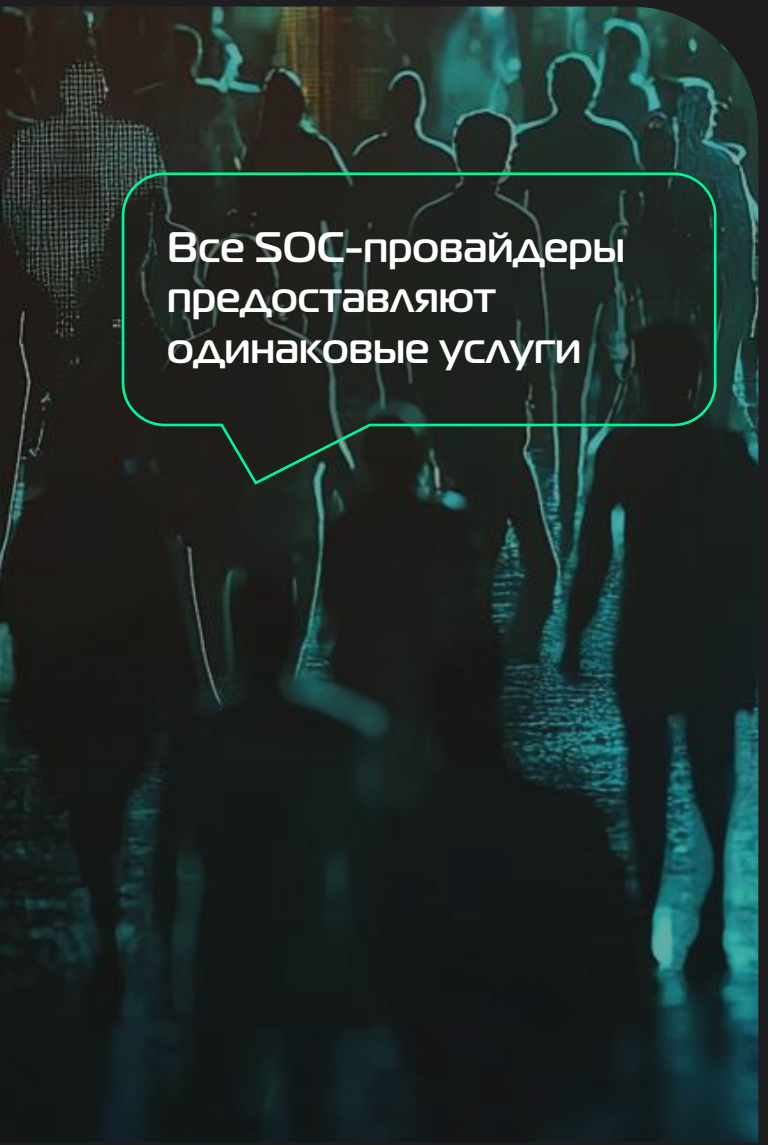


- Дефицит кадров
- Рост кибератак на компанию
- Отсутствие собственной экспертизы
- Ужесточение законодательства
- Требования корпоративных политик ИБ
- Другое

*Anti-Malware, 2024

Все ли SOC одинаковые

K2 кибер безопасность kaspersky



Основные услуги

- Мониторинг
- Анализ инцидентов
- Предоставление рекомендаций по реагированию

Расширенные функции

- Выявление и анализ уязвимостей (VM)
- Обогащение данных об актуальных киберугрозах (TI)
- Расследование инцидентов
- Проактивный поиск угроз (TH)

Реагирование

- Средства автоматизации (SOAR, EDR, XDR, MDR, NDR)
- Сервис по поддержке функционирования и администрированию СЗИ

Дополнительные функции

- Тесты на проникновение
- Консалтинг ИБ — моделирование угроз, формирование регламентов
- Предоставление облачных мощностей
- Предоставление сервисов ИБ (по MSSP-модели: WAF, Anti-DDoS, NGFW, Anti-Bot)

Действительно ли свой SOC лучше и дешевле внешнего

Собственный SOC

Работы	Длительность
Выбор вендора	от 2 месяцев
Закупка лицензий*	от 1 месяца
Закупка серверных мощностей/СХД	от 2 месяцев
Проектирование системы	от 1 месяца
Внедрение и настройка системы	от 2 месяцев
Подключение источников	от 2 месяцев
Формирование/обучение команды SOC	от 3 месяцев
Выстраивание/поддержка процессов	от 6 месяцев
Разработка контента/конфигурациями	Непрерывный процесс

Действительно ли свой SOC лучше и дешевле внешнего

SOC как услуга

Работы	Длительность
Выбор провайдера услуги	от 1 месяца
Определение области мониторинга	от 1 месяца
Подготовка инфраструктуры	от 2 недель
Подключение источников	от 2 месяцев
Контроль уровня SLA, анализ отчетности	на период использования услуги (1 год)
Участие в анализе инцидентов, принятии мер по реагированию	
Участие в принятии мер по устранению уязвимостей	
Анализ области мониторинга	

Действительно ли свой SOC лучше и дешевле внешнего

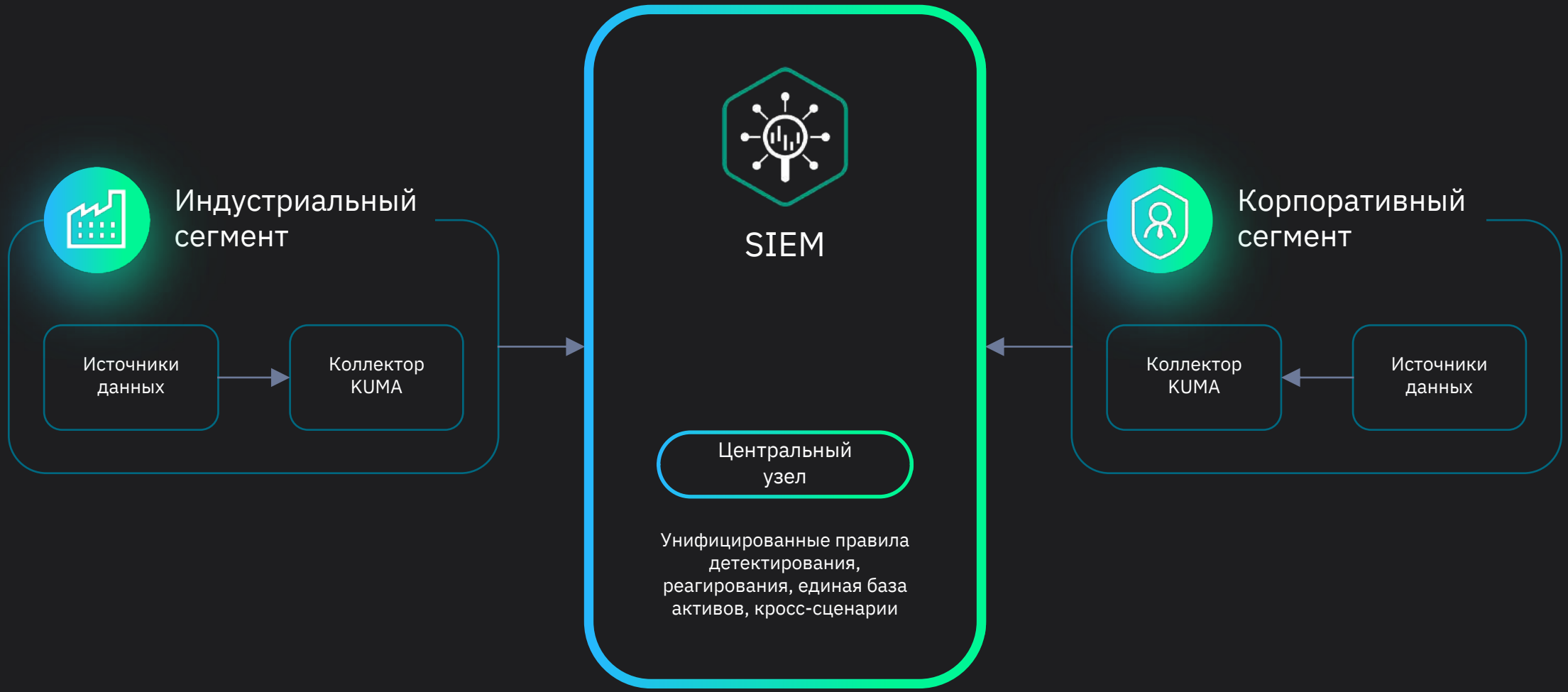
Гибридный SOC

Работы	Длительность
Выбор вендора	от 1 месяца
Проектирование системы	от 1 месяца
Закупка лицензий	от 1 месяца
Закупка серверных мощностей/СХД	от 2 месяцев
Внедрение и настройка системы	от 2 месяцев
Подключение источников, анализ области мониторинга	от 1 месяцев
Выбор провайдера услуги	от 1 месяца
Контроль уровня SLA, анализ отчетности	на период использования услуги (1 год)
Выбор вендора	
Участие в анализе инцидентов, принятии мер по реагированию	
Участие в принятии мер по устранению уязвимостей	

Под «капотом» SOC

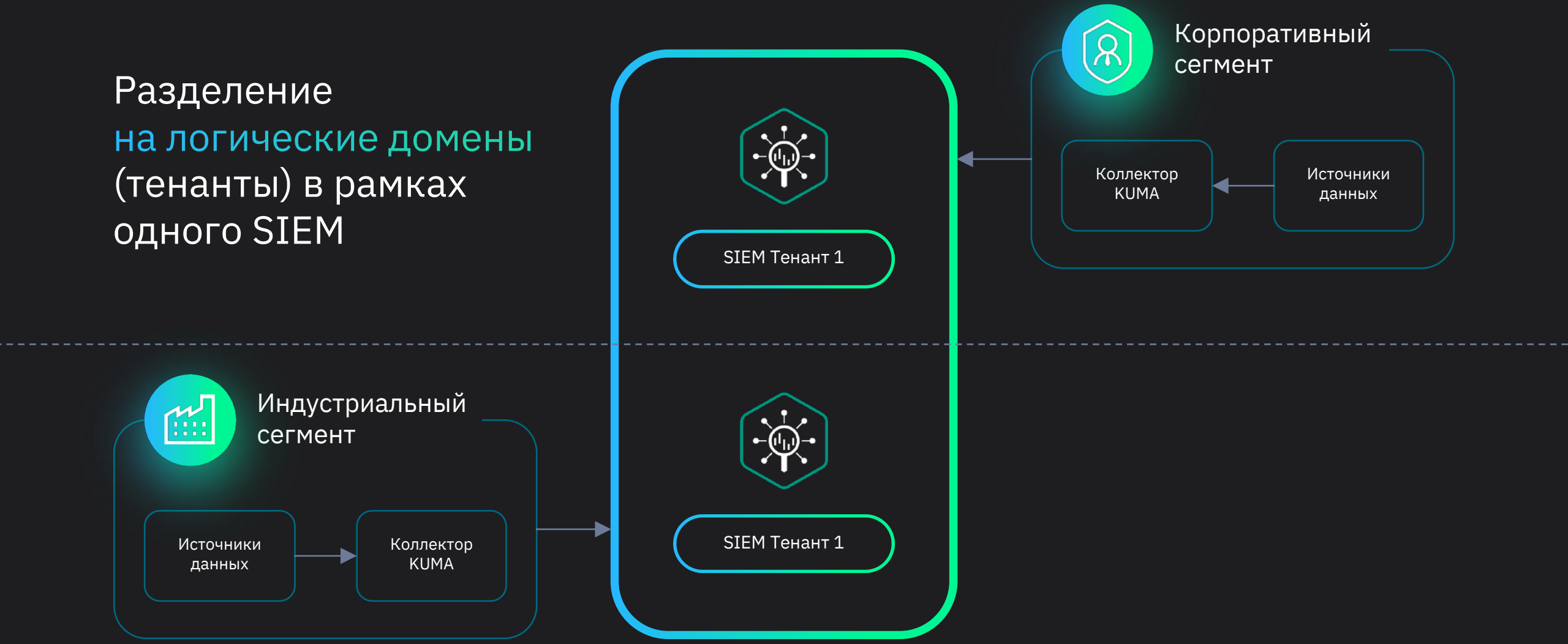
04

Разные сегменты, один SIEM



Разные сегменты, один SIEM

Разделение
на логические домены
(тенанты) в рамках
одного SIEM



Цельное предложение для мониторинга OT и IT сред

Особенности SOC для технологического сегмента

Вопрос не только в SIEM

Необходимо покрыть

распределенную
и неоднородную
инфраструктуру
с ограничением сетевого
доступа

Необходимо исключить

влияние на технологические
процессы

Активное реагирование

требует участия специалистов
по АСУ ТП
и не может быть
автоматическим

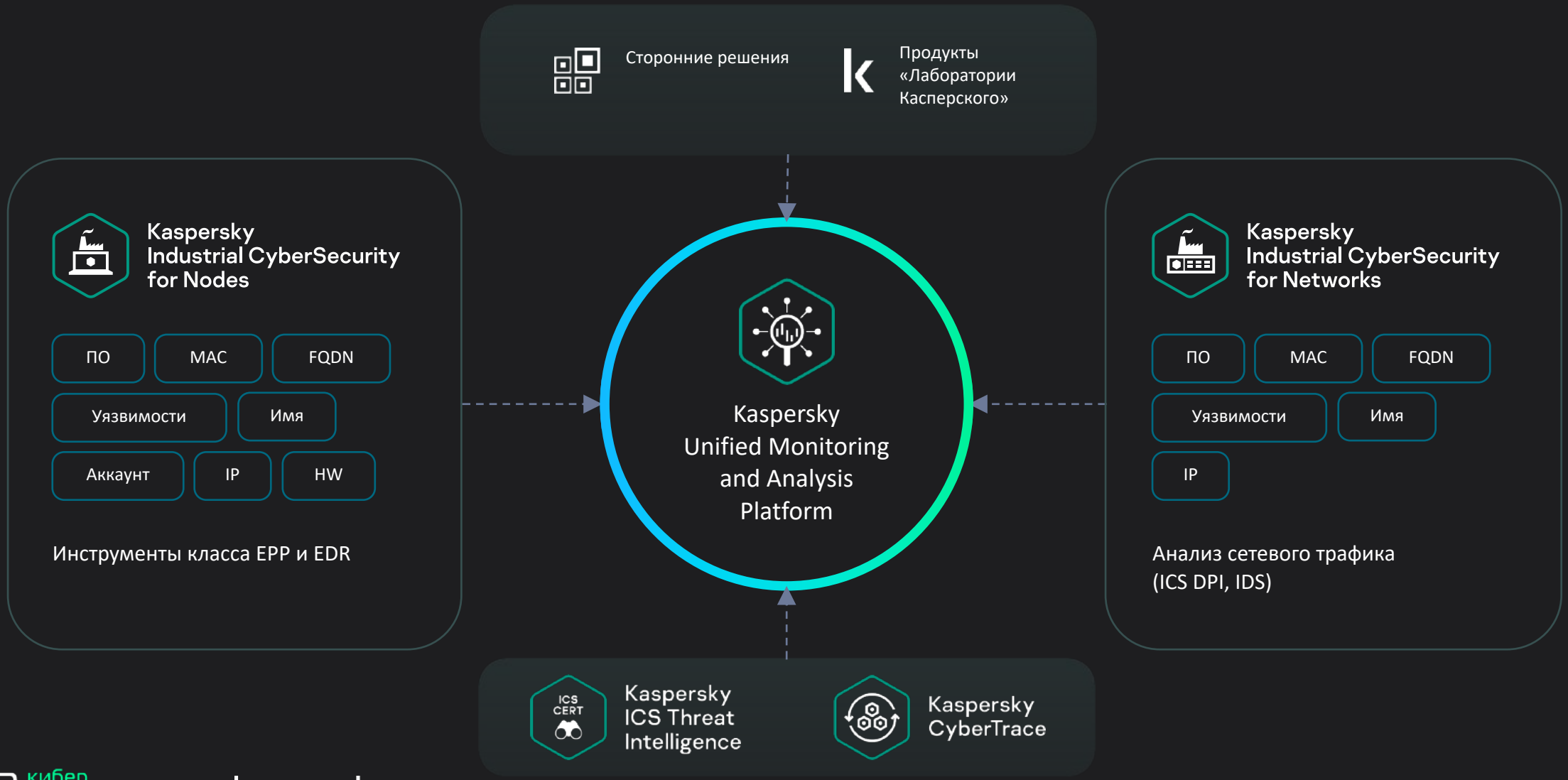
Средства обнаружения и реагирования

должны иметь сертификаты
совместимости
с оборудованием АСУ ТП

Специализированные компетенции

необходимы для специалистов SOC,
как и специализированный контент
для SIEM

Состав открытой OT XDR-платформы



K2 кибер безопасность

kaspersky

Архитектура платформы и основные функции

Kaspersky Industrial CyberSecurity

Управление активами и рисками

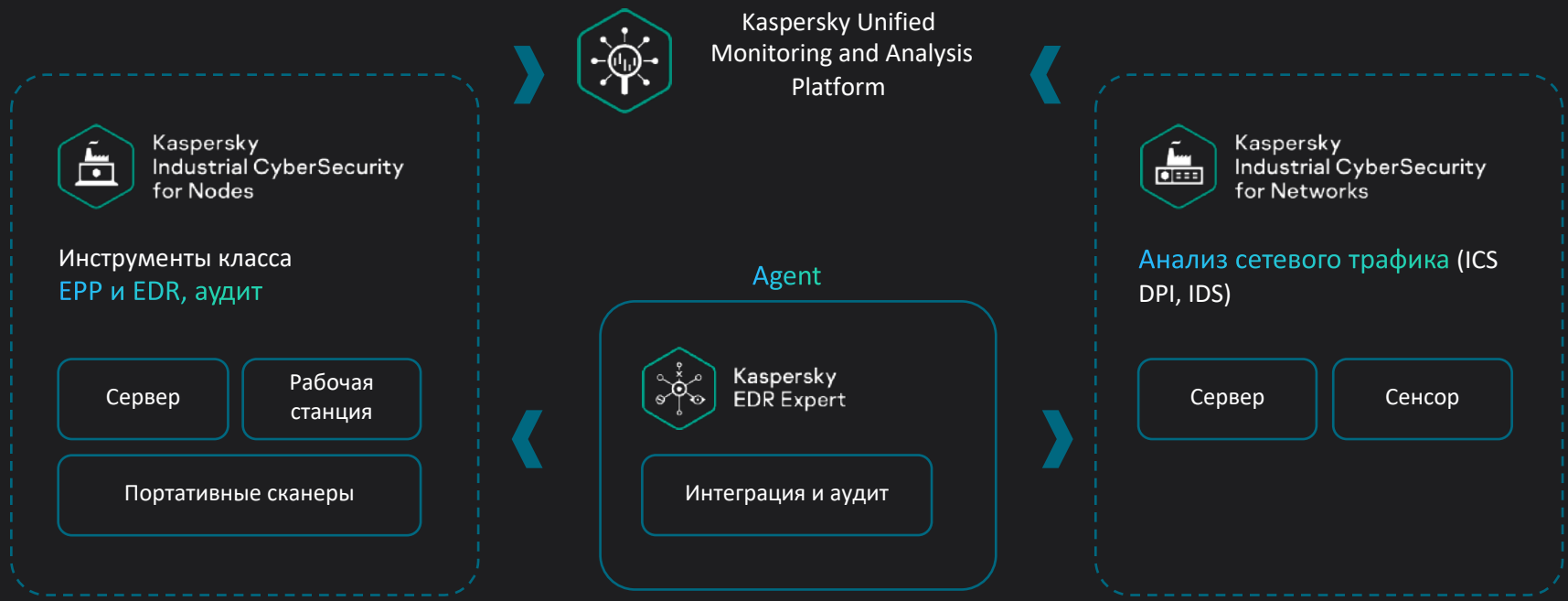
Пассивное обнаружение компонентов OT и уязвимостей. Опциональный активный опрос, ориентированный на риски, ситуационная осведомленность и отчетность

Детектирование и реагирование на уровне сети

Анализ сетевого трафика для обнаружения вторжений на самом низком уровне (протоколы ICS, DPI и сигнатуры IDS)

Детектирование и реагирование на уровне конечных узлов

Защита от вредоносных программ, контроль доверенных устройств и ПО. ICS EDR позволяет анализировать первопричины инцидентов в OT



K2 кибер безопасность

kaspersky

Kaspersky Investigation and Response Assistant

KIRA

Искусственный интеллект от «Лаборатории Касперского», который помогает аналитику в реальном времени

Умеет:

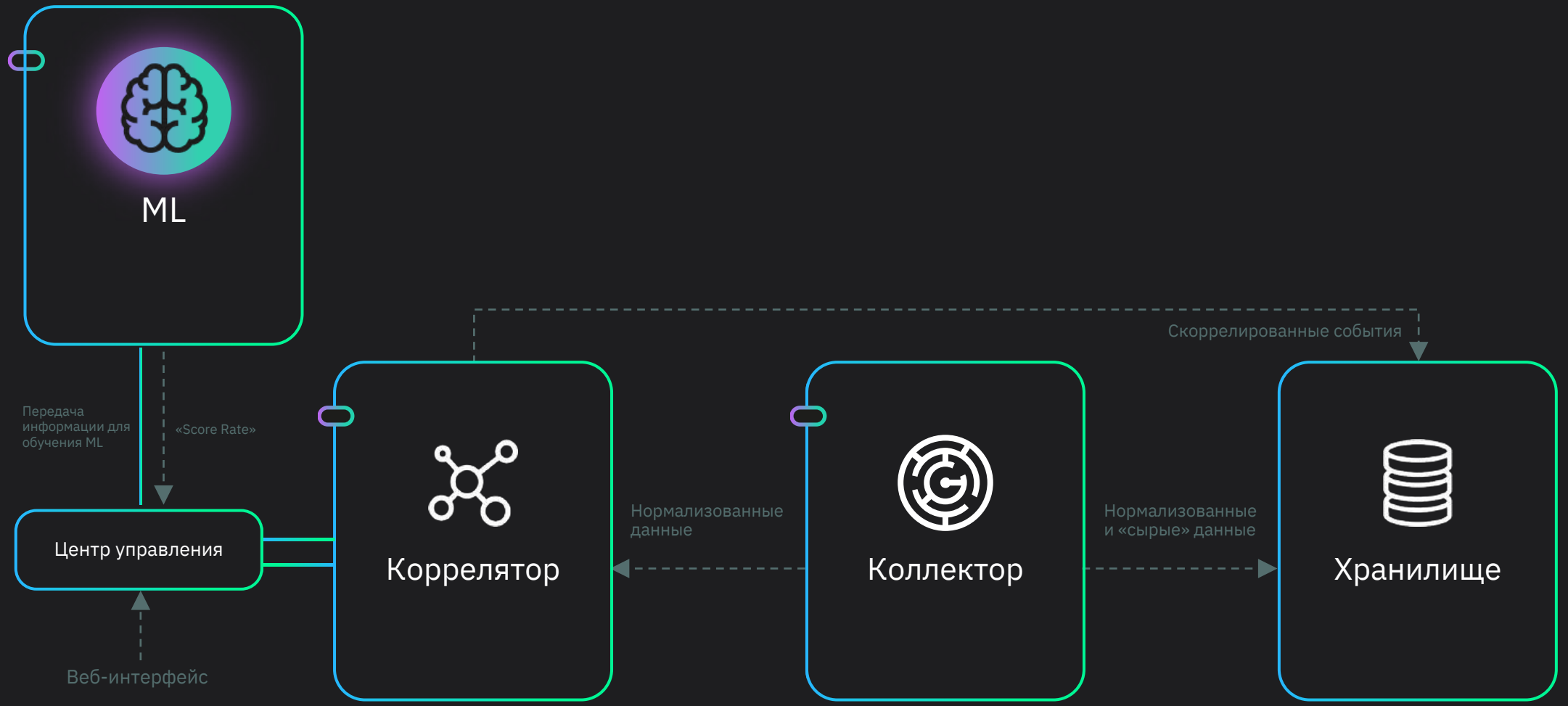
- Приоритезация алертов
- Предоставление подробного анализа с кратким содержанием для принятия быстрых решений

и продолжает учиться

K2 кибер безопасность

kaspersky

Архитектура KUMA с ИИ-модулем



Ждем вас на нашем стенде № 6.2

Егор Куликов

Руководитель направления безопасности КИИ и АСУ ТП

E-Mail: EKulikov@k2int.ru

Telegram: @egork79

K2 кибер безопасность

Андрей Бондюгин

Руководитель направления предпродажной поддержки решений для бизнеса

E-Mail: Andrey.Bondyugin@kaspersky.com
Telegram: @Andrey_bondyugin

kaspersky