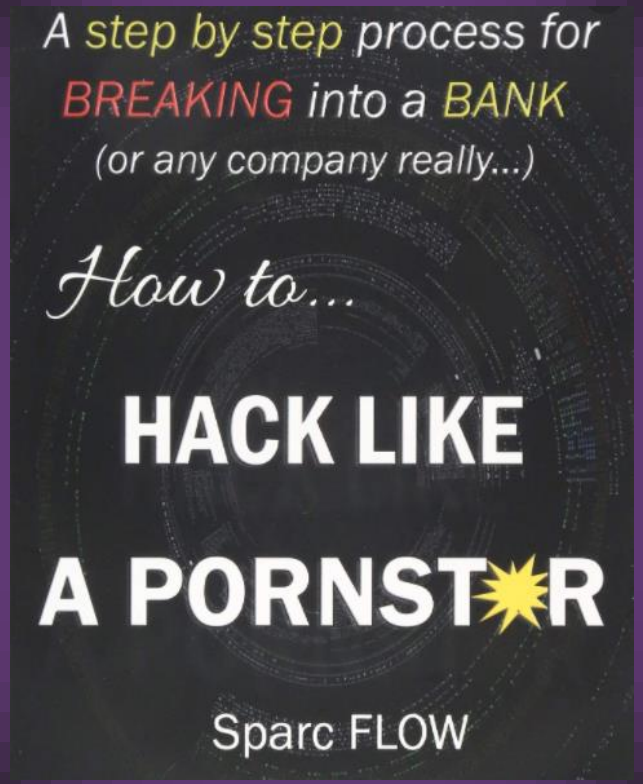
Центральный элемент единой платформы безопасности

kaspersky

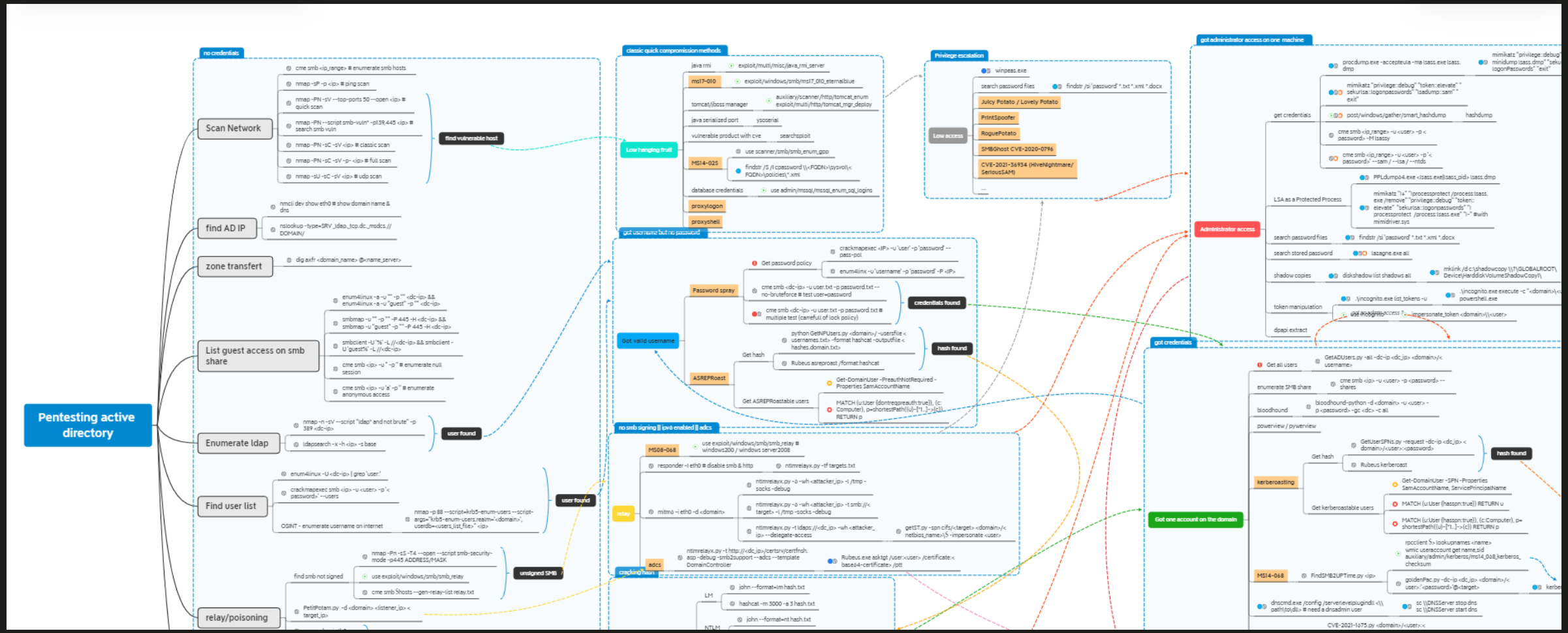
Борис Осепов, инженер предпродажной поддержки

Есть два вида компаний:
те, что были взломаны, и те,
что пока еще не знают, что были взломаны.

Спарк Флоу
(Sparc Flow)
How to
Investigate
Like a Rockstar

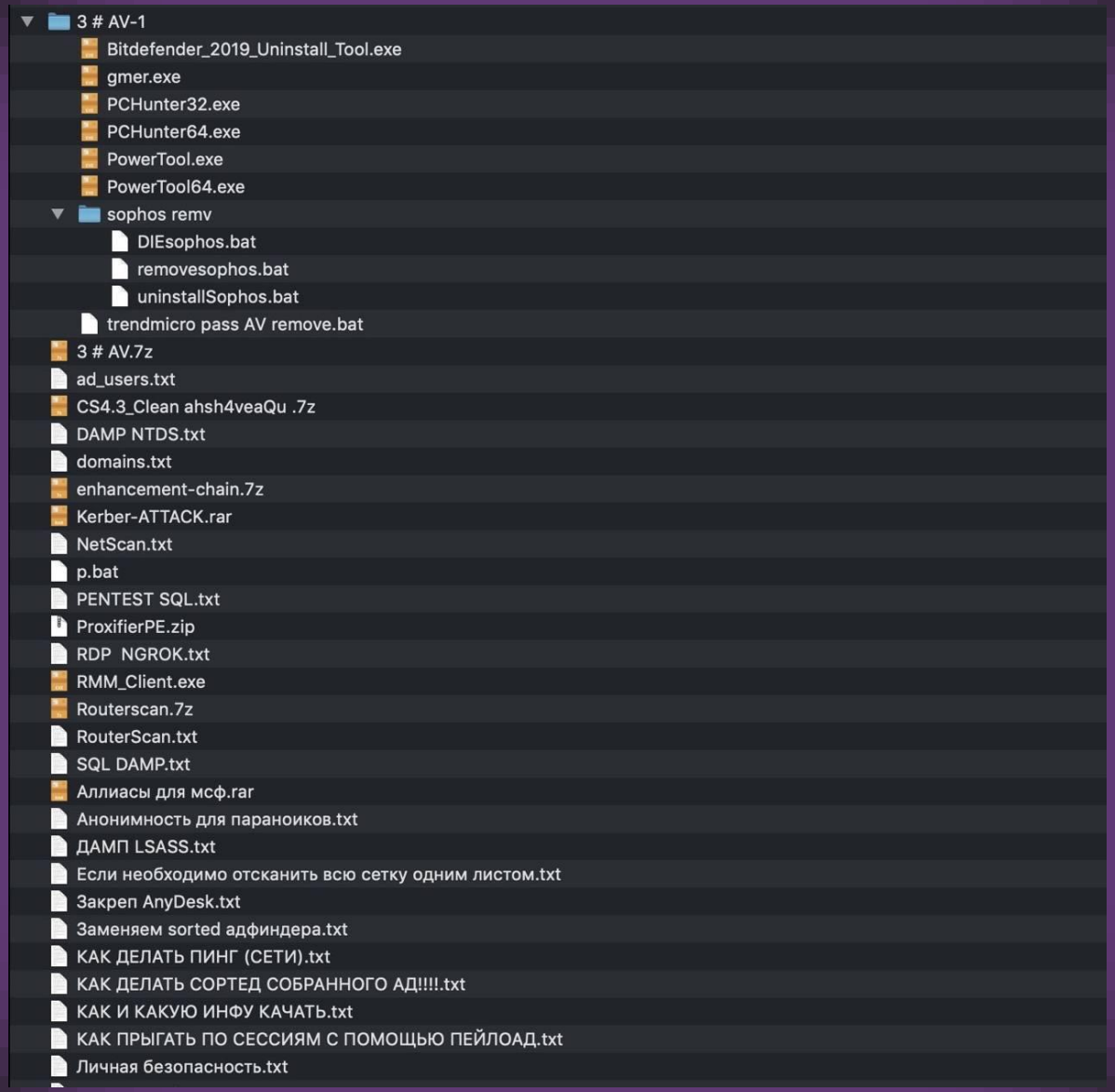


Подготовка злоумышленников



https://www.xmind.net/m/5dypm8/#

Подготовка злоумышленников бывает и такая ☺



А насколько подготовлены вы?

- Процедура управления инцидентами?
- Выстроенный процесс реагировании на инциденты?
- Регламент резервного копирования?
- А может RDP наружу? ☺

Масштаб угроз

1994

1

новый вирус каждый час

2006

1

новый вирус каждую минуту

2011

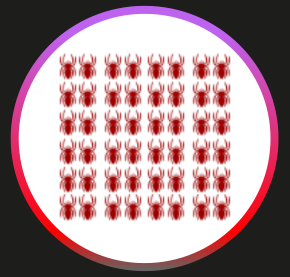
1

новый вирус каждую секунду

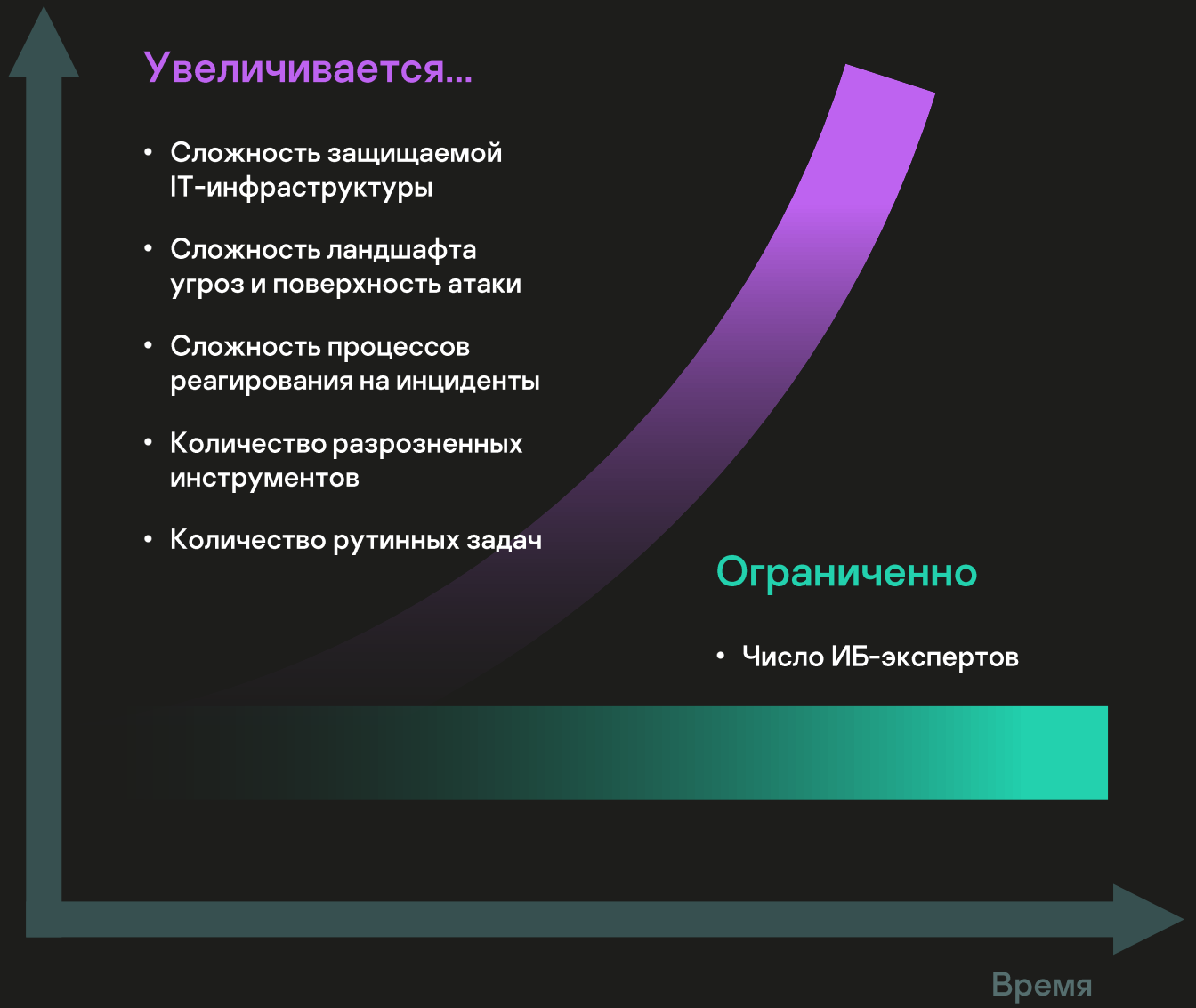
2021

370 000

новых вредоносных образцов в день



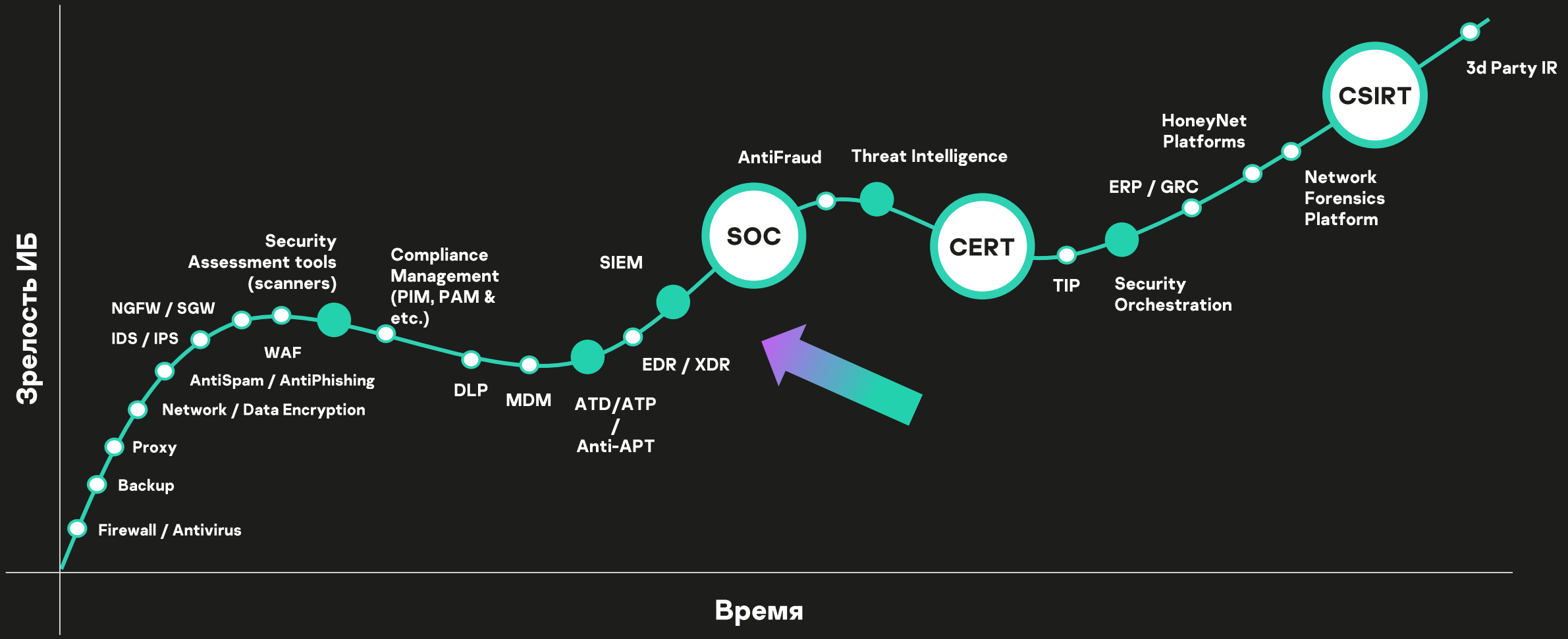
IT-безопасность: современные реалии



Общий дефицит ИБ-экспертов на рынке труда

- Неоптимальное использование времени и таланта экспертов
- Недостаточная поддержка ИБ-сотрудников
- Отсутствие программ подготовки собственных специалистов

Зрелость систем защиты компании



Инцидент - до и после

Известные угрозы

- Блокировка или автоматическое обнаружение угроз

Продукты, оповещения

КОМПРОМЕТАЦИЯ

Неизвестные угрозы

- Выявление сложных
- угроз
- Расследование

Поиск киберугроз

Сдерживание угроз

- Реагирование и пошаговые рекомендации

Реагирование на инциденты

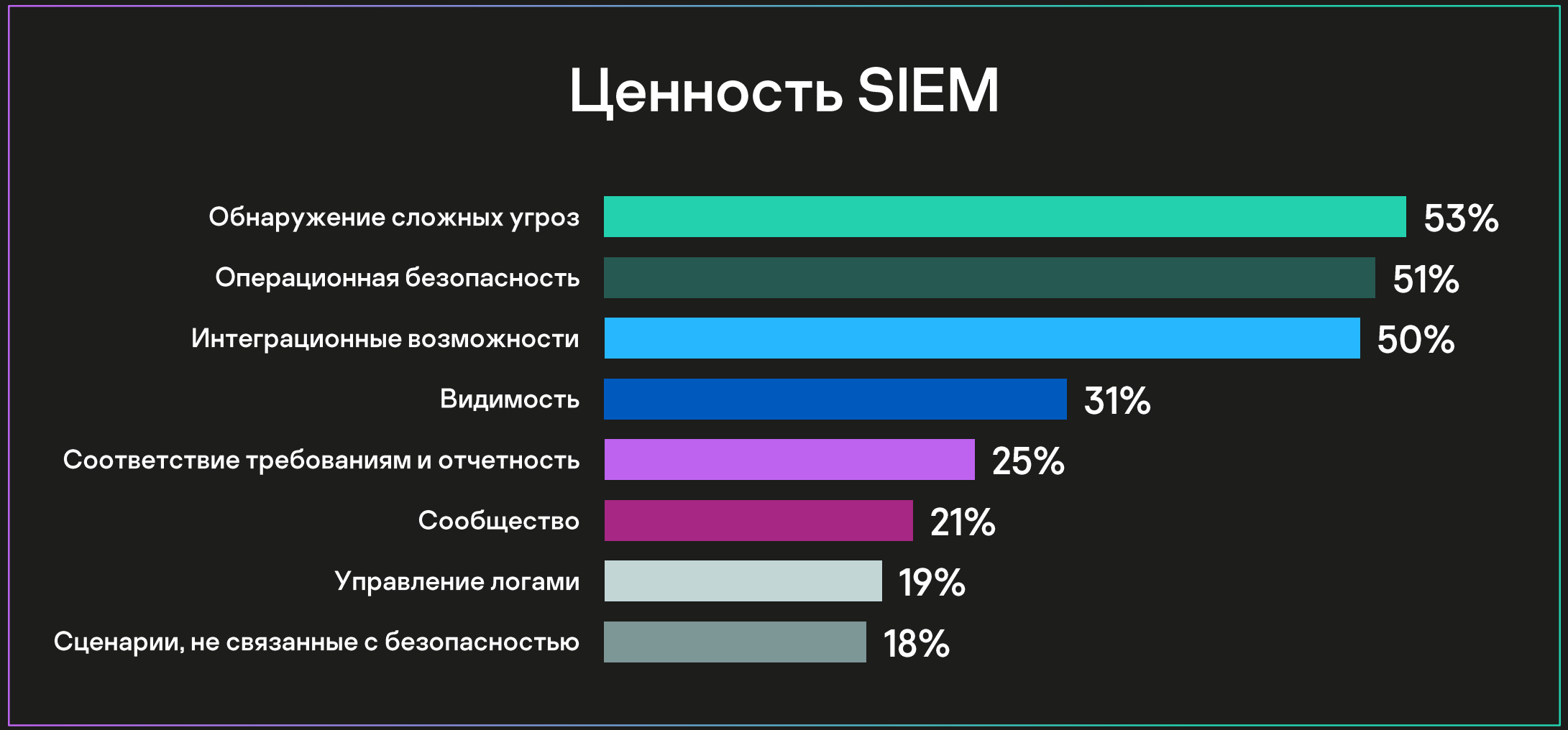
До компрометации

После компрометации

Время

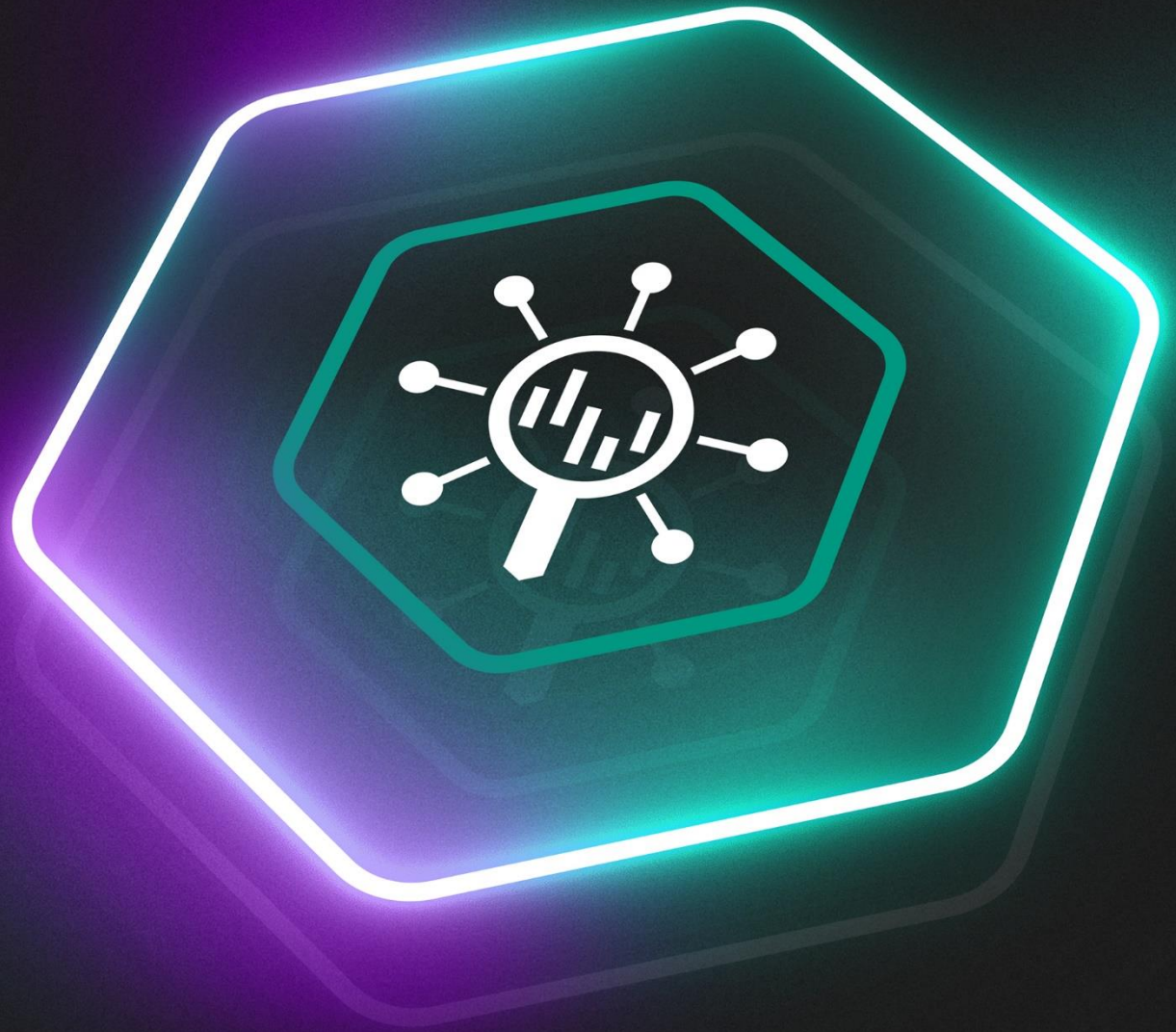
Современный эталон реагирования

SIEM — основная платформа SOC сегодня

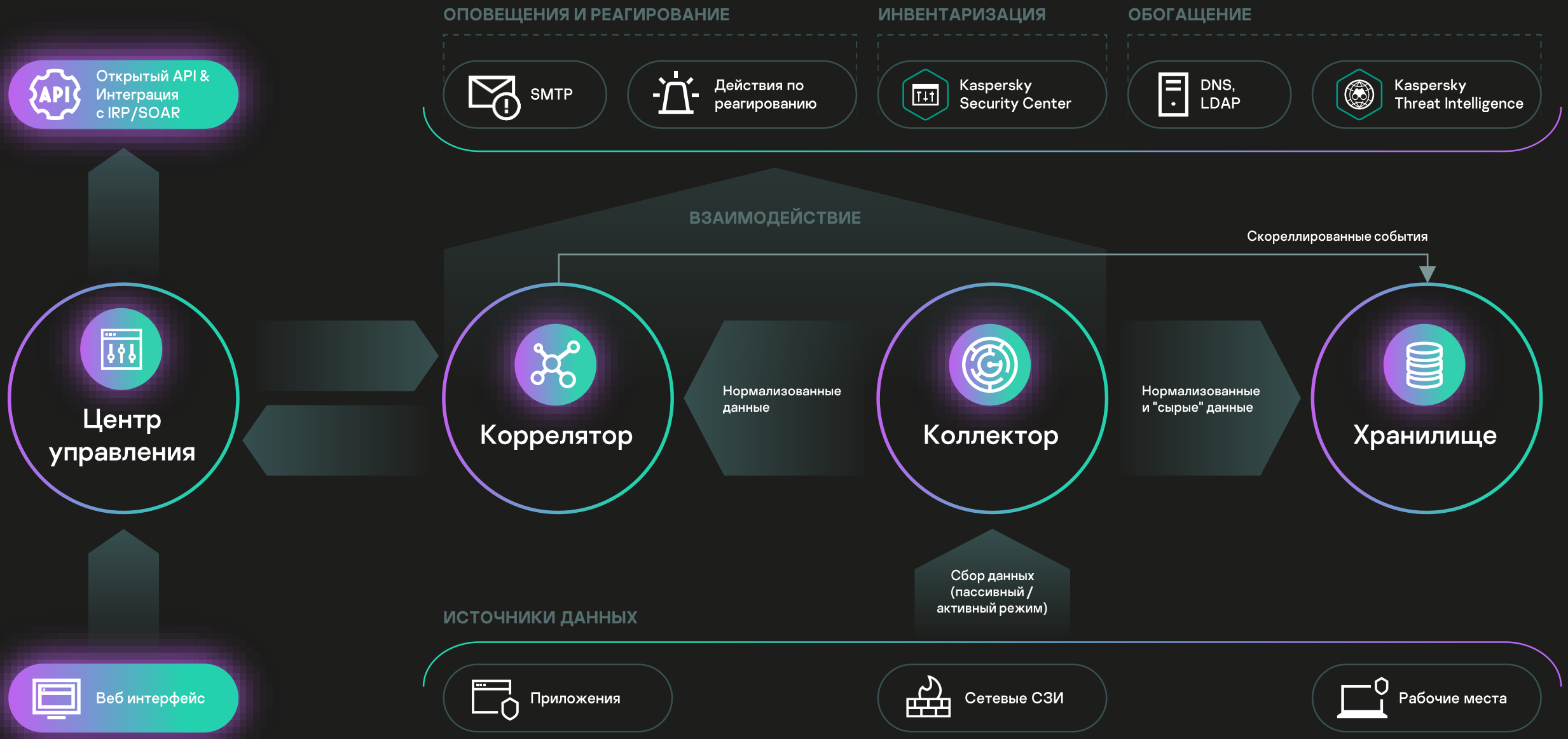


Источник: 2020 by The Enterprise Strategy Group, Inc

Kaspersky Unified Monitoring and Analysis Platform



Архитектура KUMA



Лицензирование

Модули

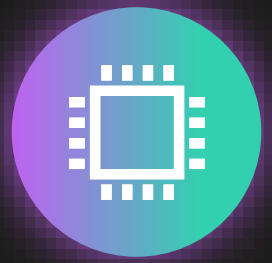
- Учет по количеству «чистых» EPS (шаг по 100 EPS)
- min лицензия от 500 EPS
- По используемым модулям:
  - ГосСОПКА
  - Netflow
  - High Availability
- Срок действия 1 и 2 года

Техническая поддержка

	Стандартная поддержка Premium	Расширенная поддержка Premium+
Режим работы, SLA	1 приоритет - 2 часа, 24*7 2 - 6 часов, 5*8 3 - 8 часов, 5*8 4 - 10 часов, 5*8	1 приоритет – 30 мин, 24*7 2 – 4 часа, 24*7 3 - 6 часов, 5*8 4 - 8 часов, 5*8
Консультации по настройке	Да	Да
Исправления ошибок (в том числе private fix)	Да	Да
Количество пользовательских коннекторов	10 *по мере развития продукта цифра будет уменьшена	20
Выделенный аккаунт менеджер, мониторинг качества	Нет	Да
Включено часов Professional services *для разработки дополнительных коннекторов, ревью архитектуры и схемы развёртывания итд	0	16 часов *не менее 2 часов одна сессия

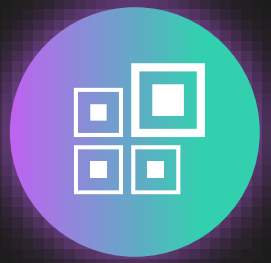
Конкурентные преимущества

Ключевые преимущества



Высокая производительность

300k+ EPS на один узел



Масштабируемость

Гибкая микросервисная архитектура

Низкие системные требования

Интеграция «из коробки»

С продуктами сторонних поставщиков и решениями «Лаборатории Касперского»

Kaspersky Unified Monitoring and Analysis Platform (SIEM)

Единая консоль мониторинга и анализа инцидентов ИБ

Kaspersky Unified Monitoring and Analysis Platform

- Kaspersky Security для бизнеса
- Kaspersky Endpoint Detection and Response
- Kaspersky Anti Targeted Attack
- Kaspersky Security для интернет-шлюзов
- Kaspersky Security для почтовых серверов

- Решения сторонних поставщиков

- Kaspersky Security Center
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace
- Kaspersky Threat Lookup
- Kaspersky Industrial CyberSecurity

Преимущества Сертификат ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4455

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
28 сентября 2021 г.

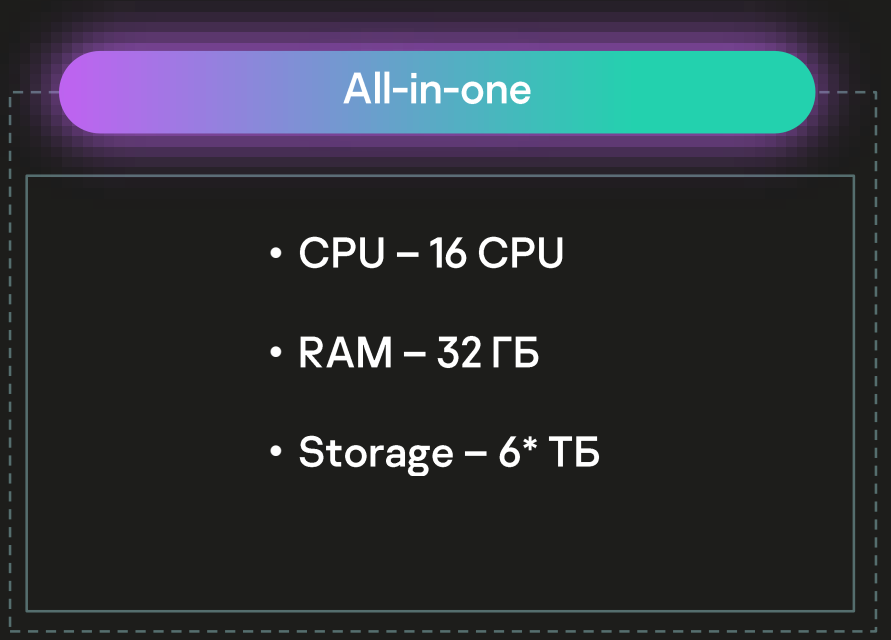
Выдан: 28 сентября 2021 г. Переоформлен: 26 октября 2021 г.
Действителен до: 28 сентября 2026 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Unified Monitoring and Analysis Platform (версия 1.5)»**, разработанное и производимое АО «Лаборатория Касперского», является системой управления событиями информационной безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и технических условиях ТУ 643.46856491.00116-02 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00116-02 30 01.

Технические детали

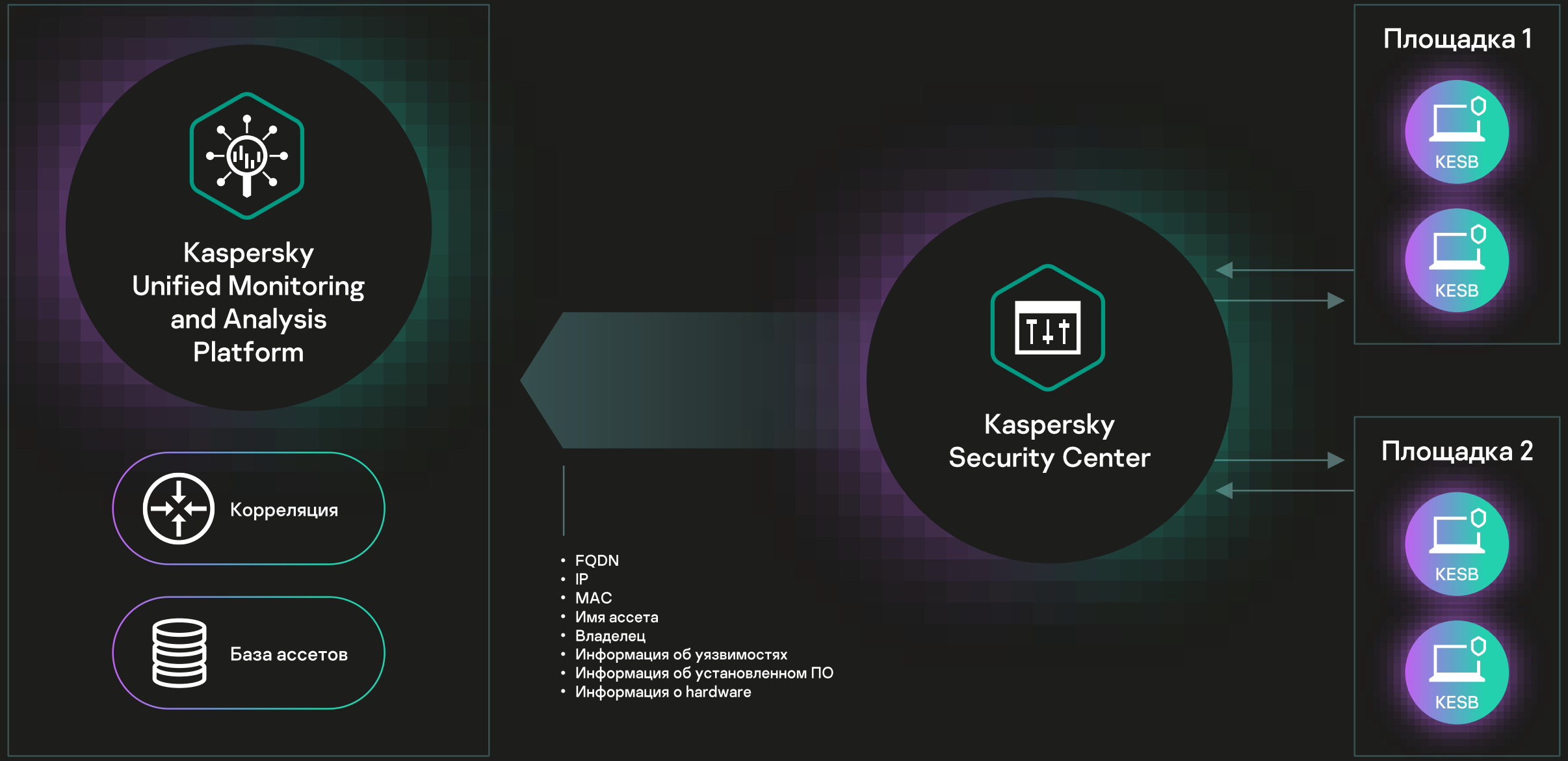
Примерный сайзинг

< 5k EPS, 90 дней хранения

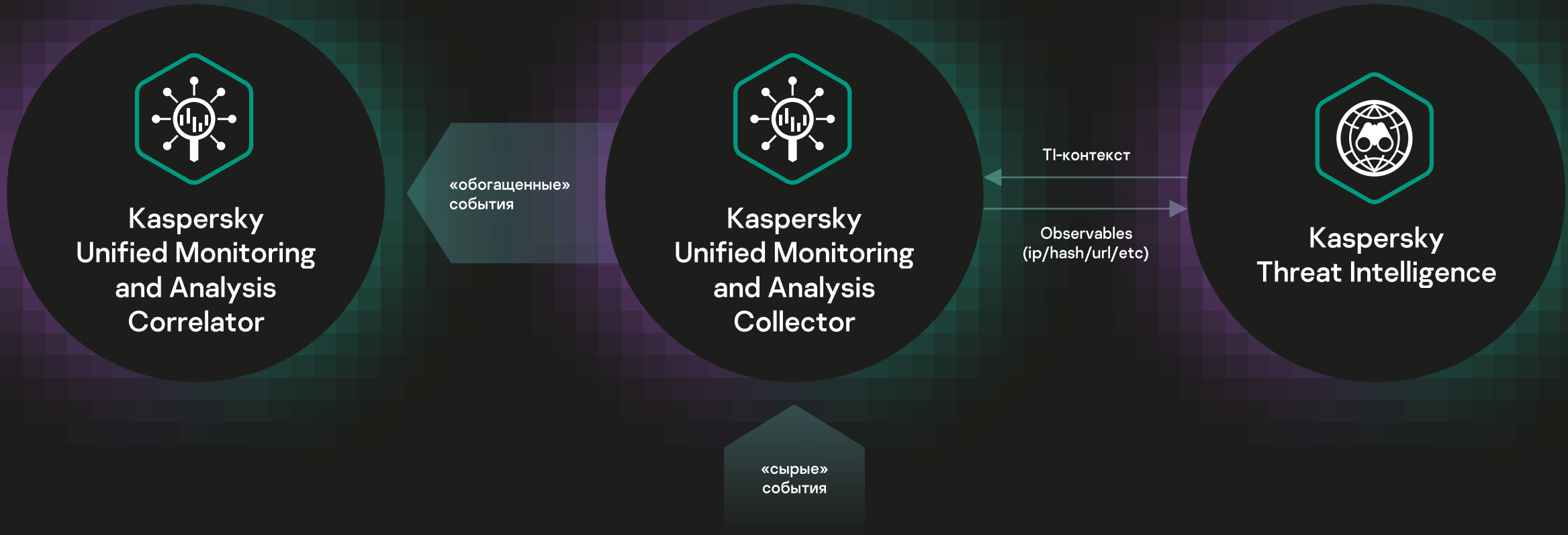


*Объем хранилища зависит от длительности хранения событий

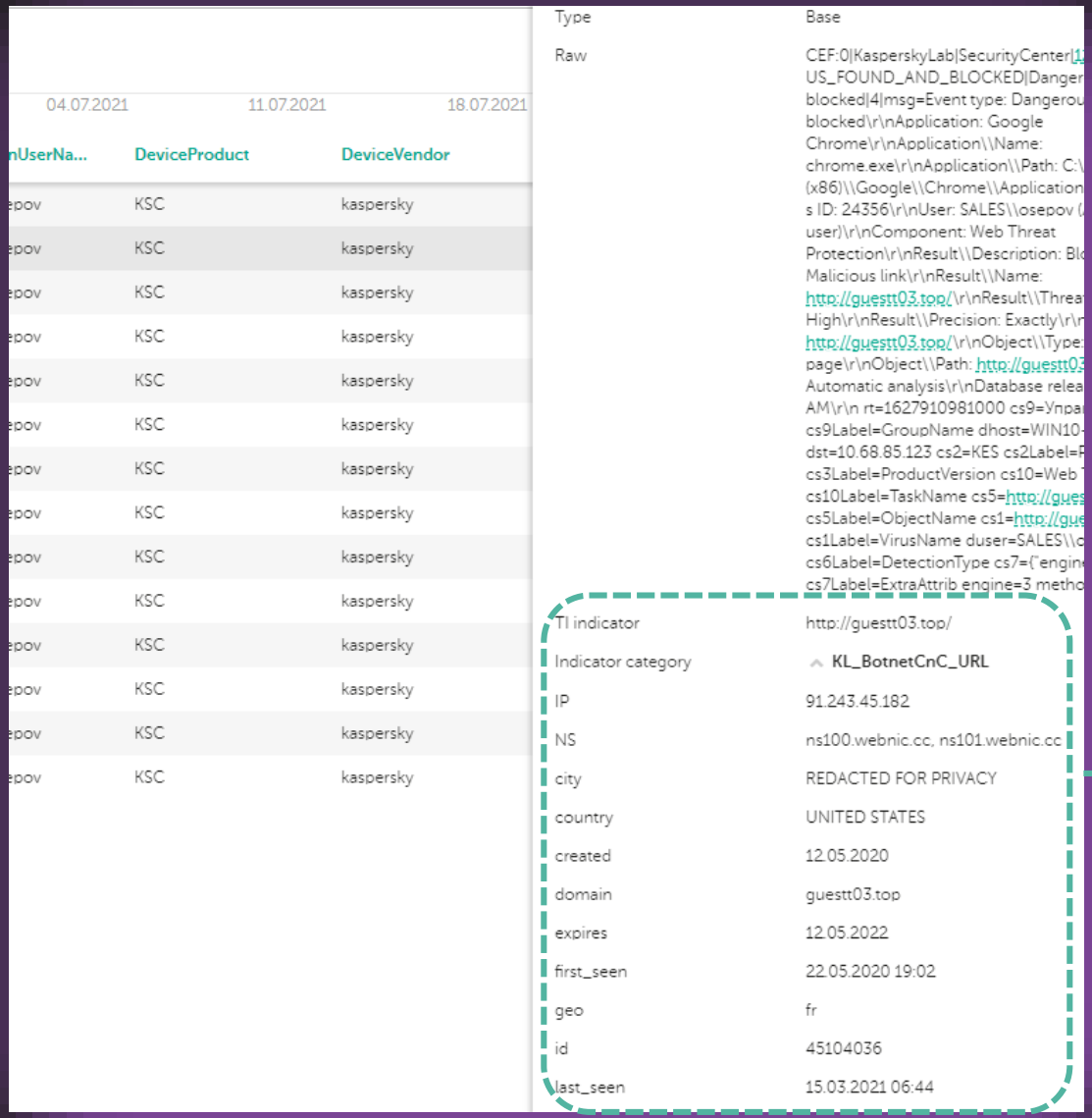
Инвентаризация информационных активов



Потоковое «обогащение» событий

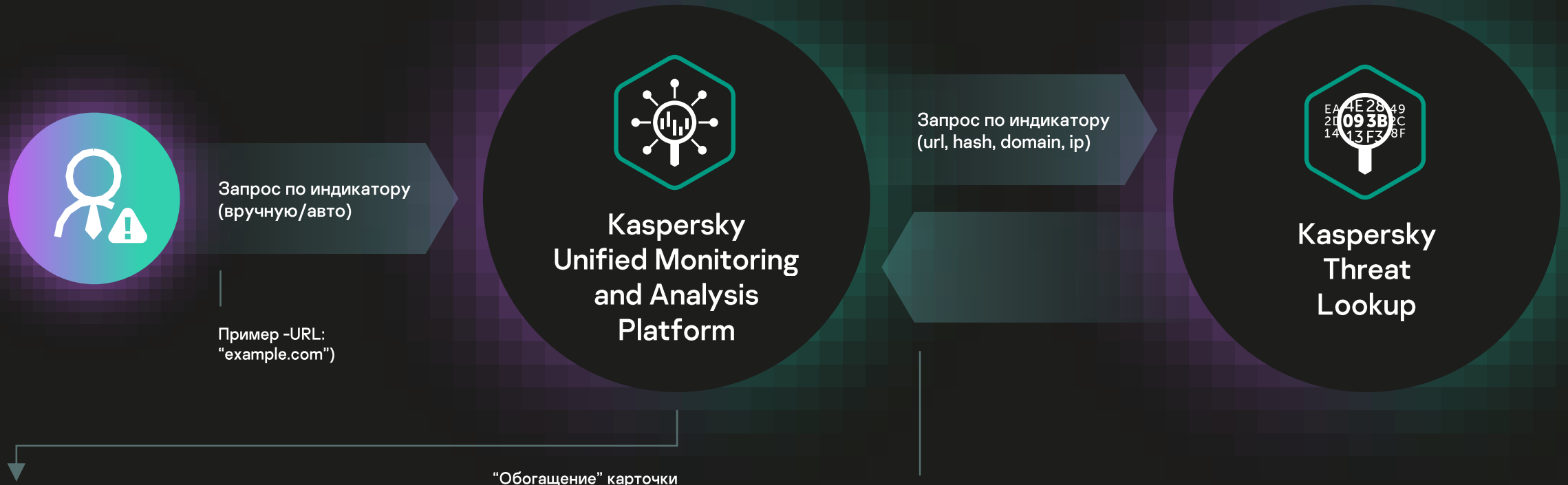


Обогащение с помощью CyberTrace



Обогащенные данные

«Обогащение» событий по запросу



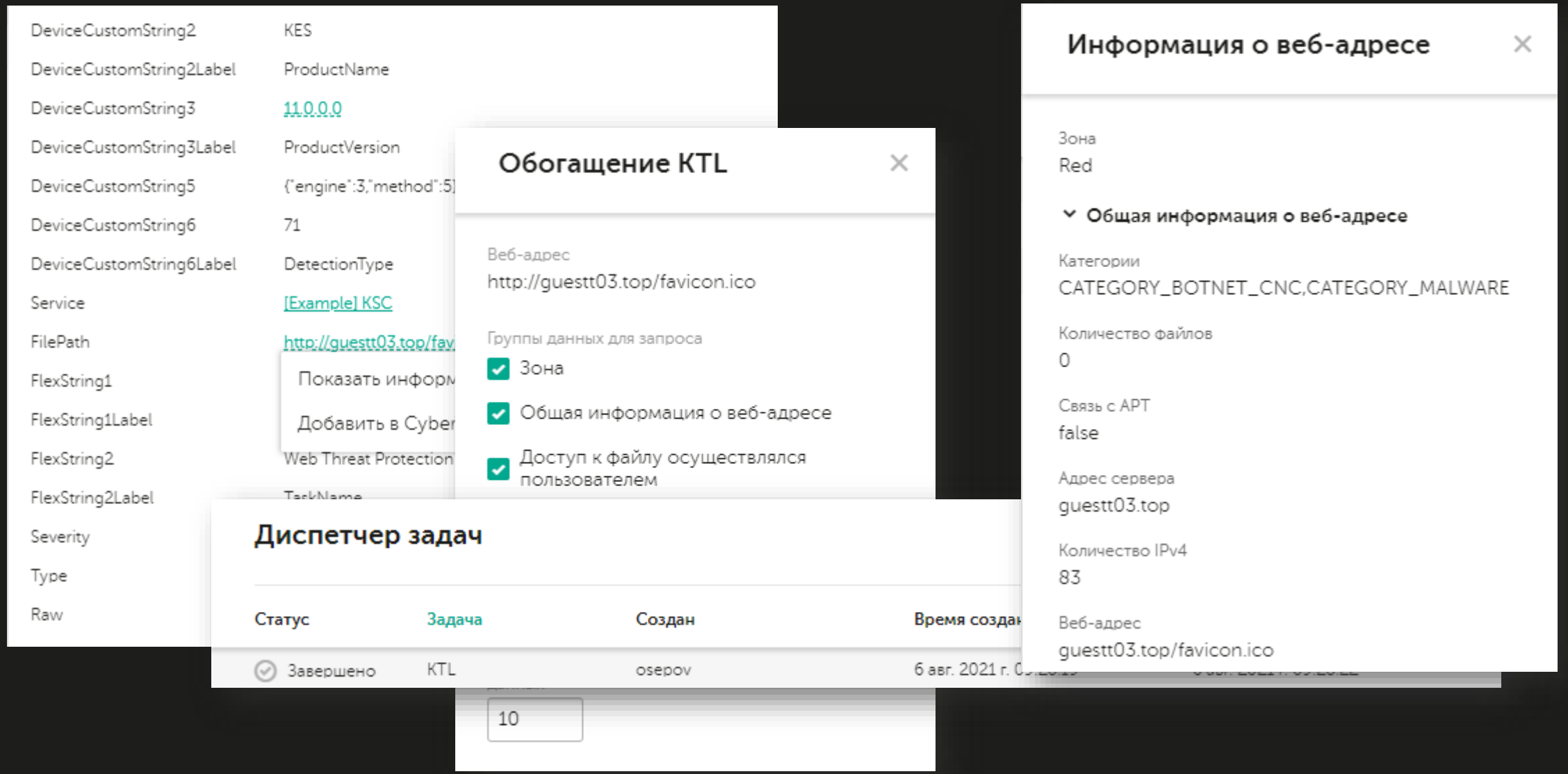
Карточка инцидента

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, ...
.....

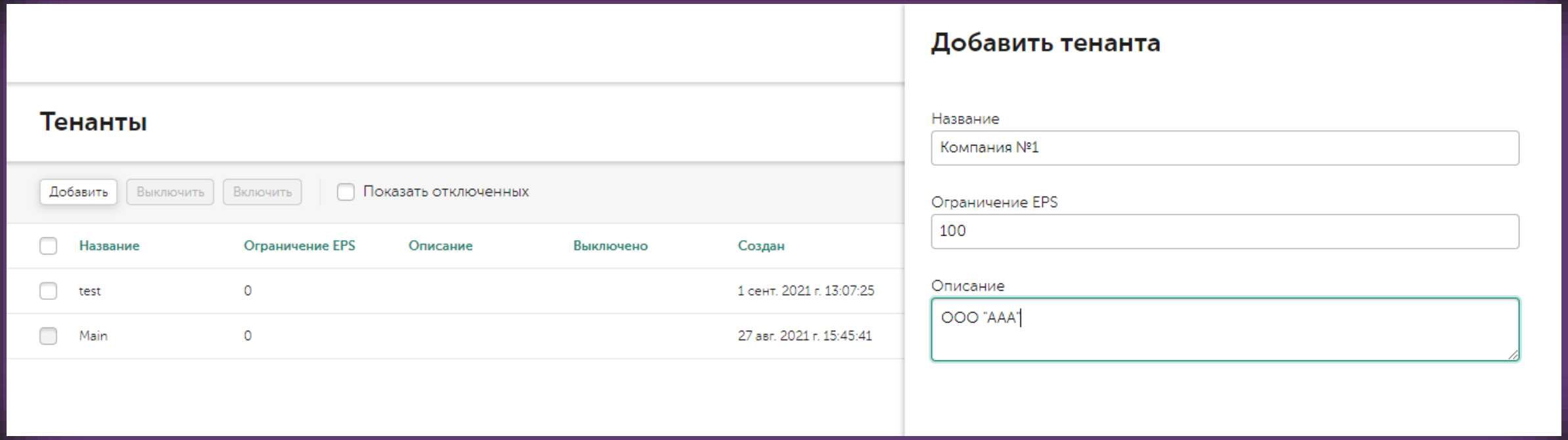
Ответ на запрос

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, ...

Обогащение с помощью KTL

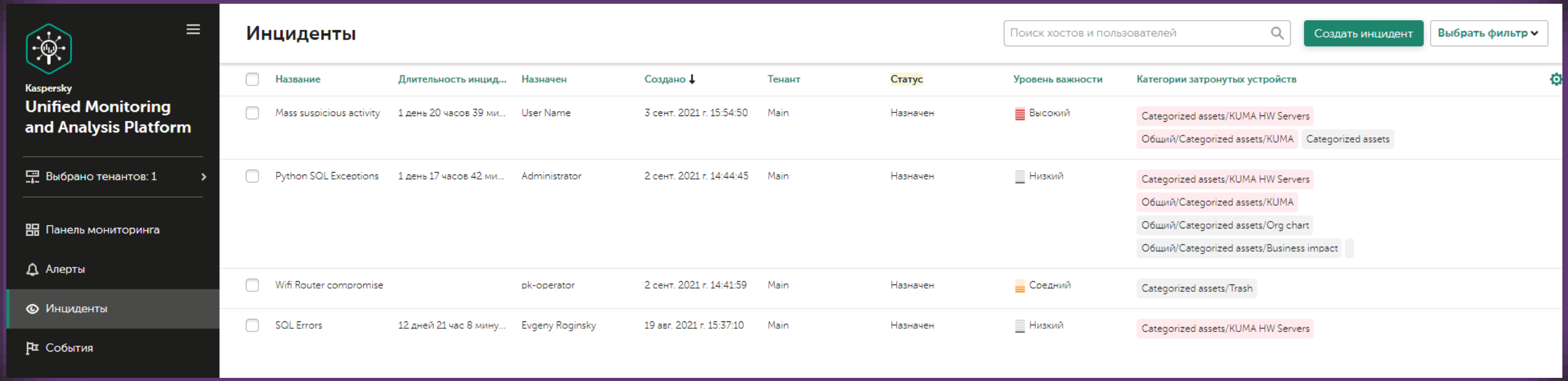


Поддержка Multitenancy



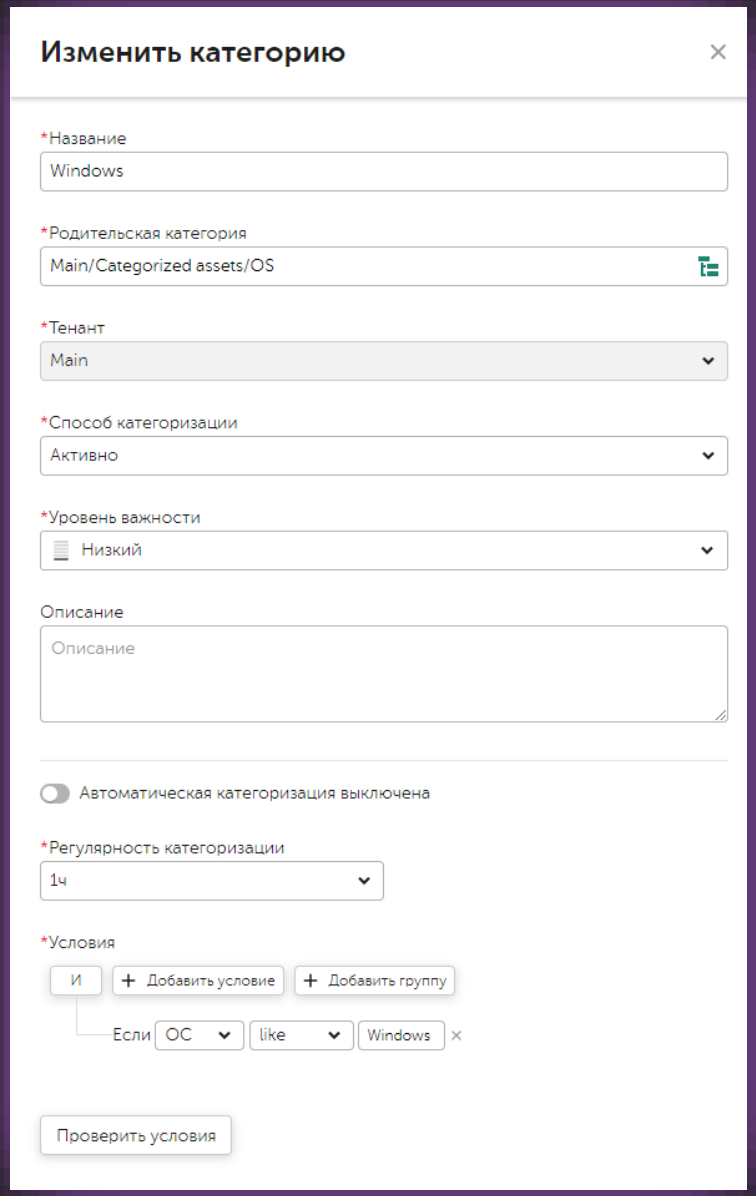
- **Разделение данных, конфигурации и прав доступа**
- **Возможность ограничения EPS для каждого тенанта отдельно**
- **Целевой сценарий для MSSP и центров Госсопка**

Новые функции по управлению инцидентами



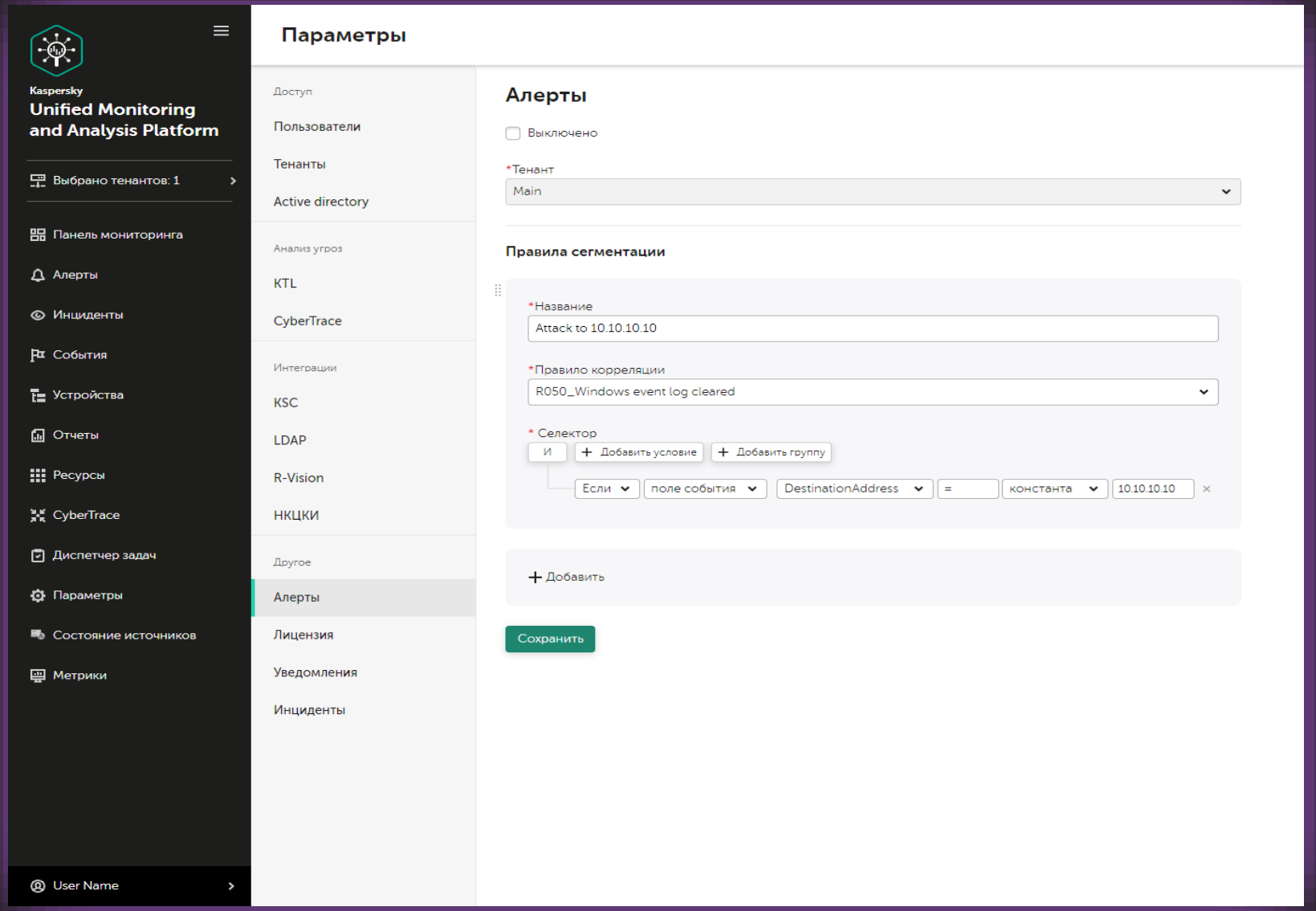
- Экспорт в НКЦКИ
- Создание инцидентов автоматически или вручную
- Управление инцидентами - назначение ответственного, изменение приоритета, эскалация, ведение истории, т. д.

Динамическая категоризация активов

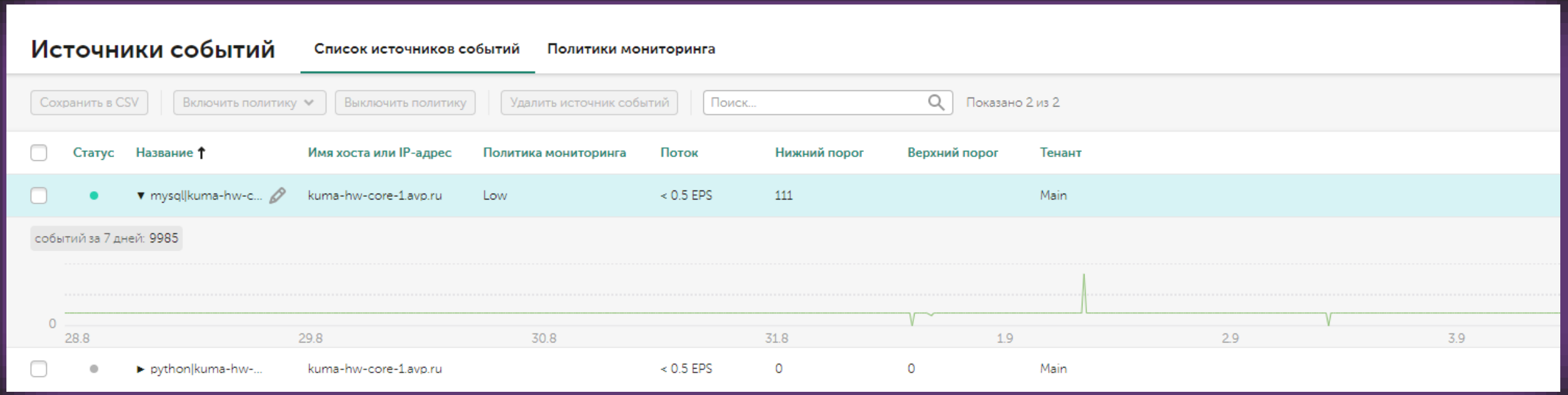


- **Динамическая категоризация по:**
  - **FQDN**
  - **IP**
  - **CVE**
  - **ОС**
  - **Версия билда ОС**
- **Логические операторы AND, OR, NOT и группировки**
- **Возможность проверки условий**

Группировка алертов

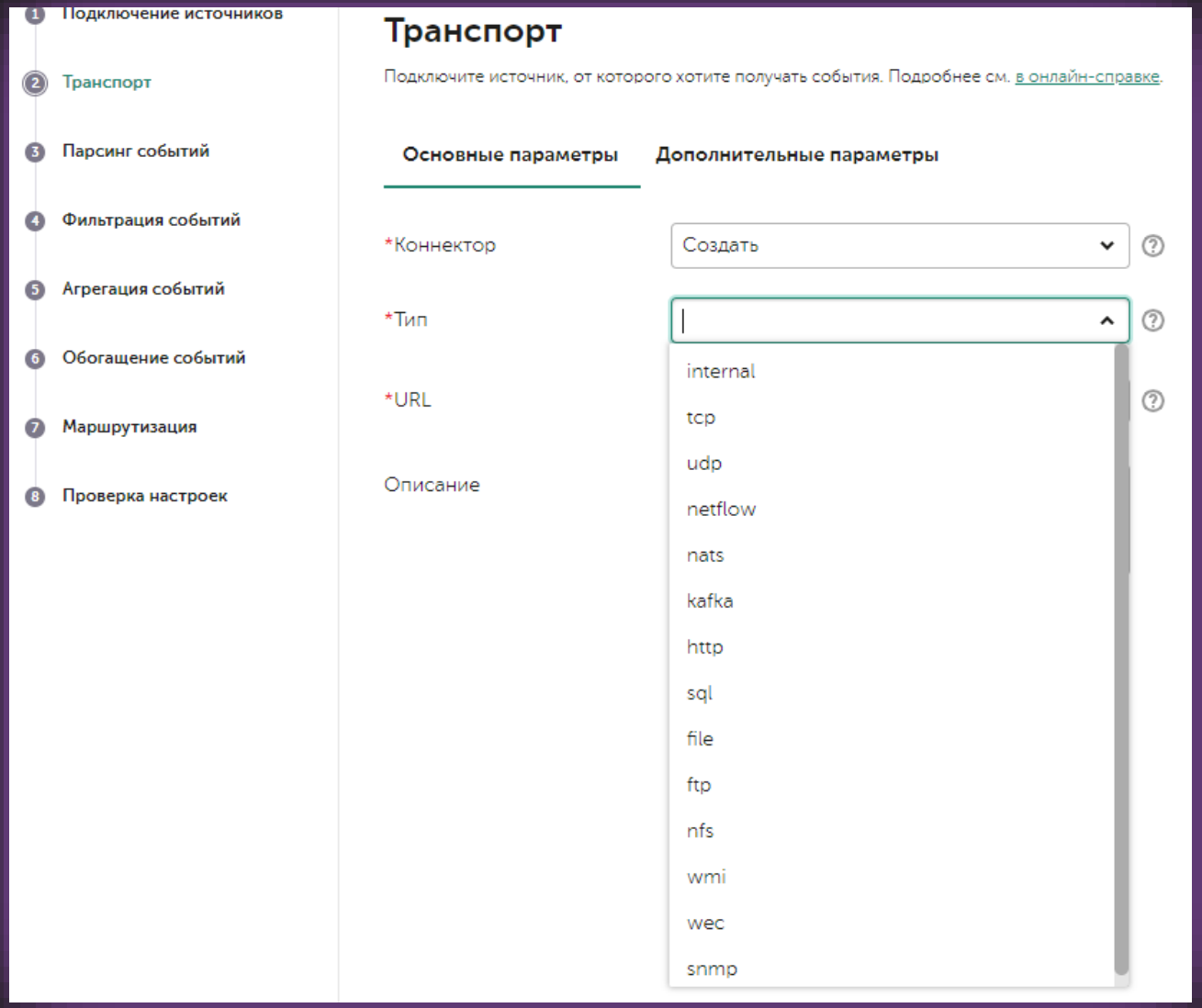


Мониторинг доступности источников



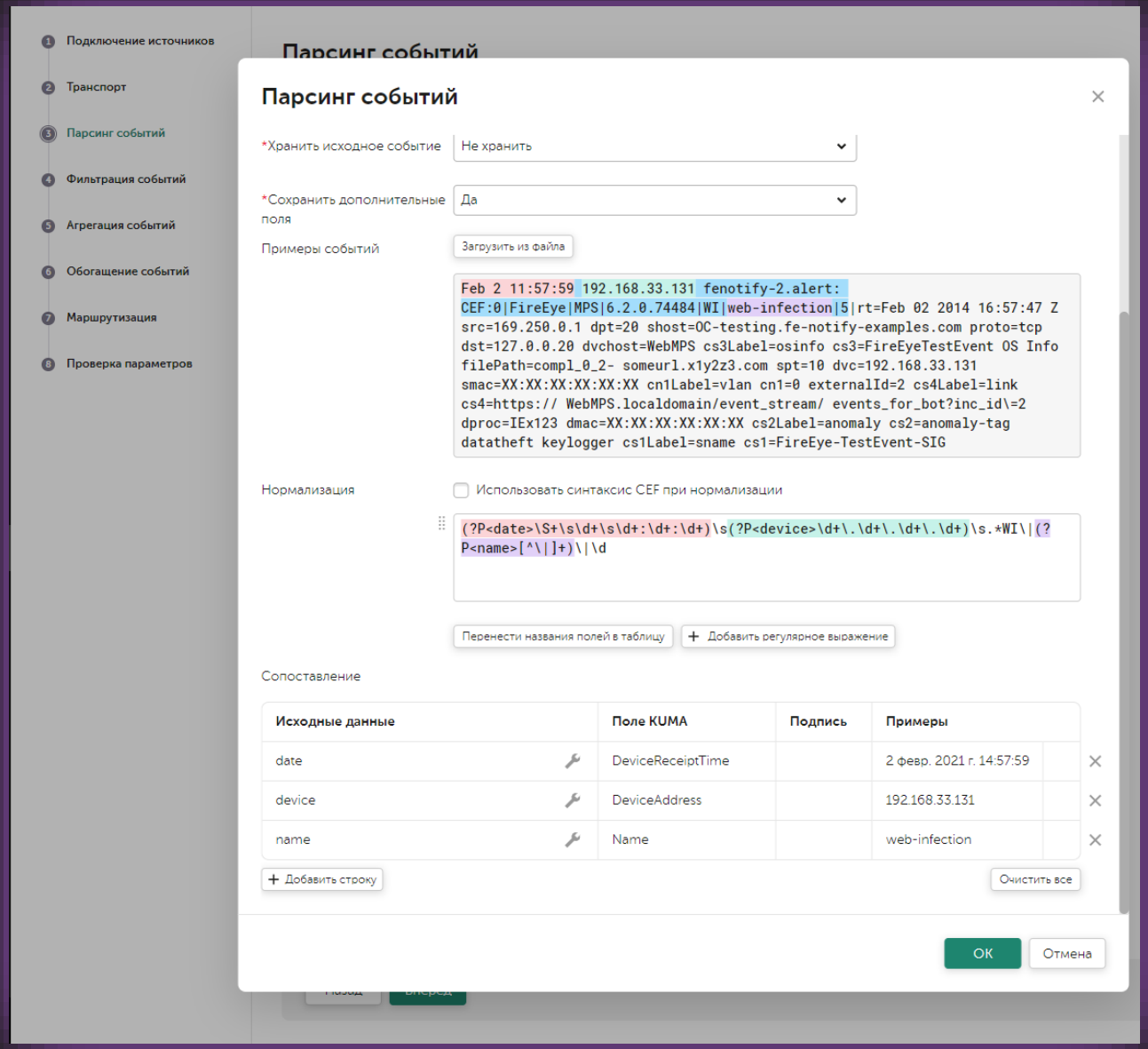
- **Мониторинг источников по минимальному кол-ву событий в период времени**
- **Уведомление по почте в случае недоступности**
- **Возможность задать разные политики**

Поддержка новых видов транспорта



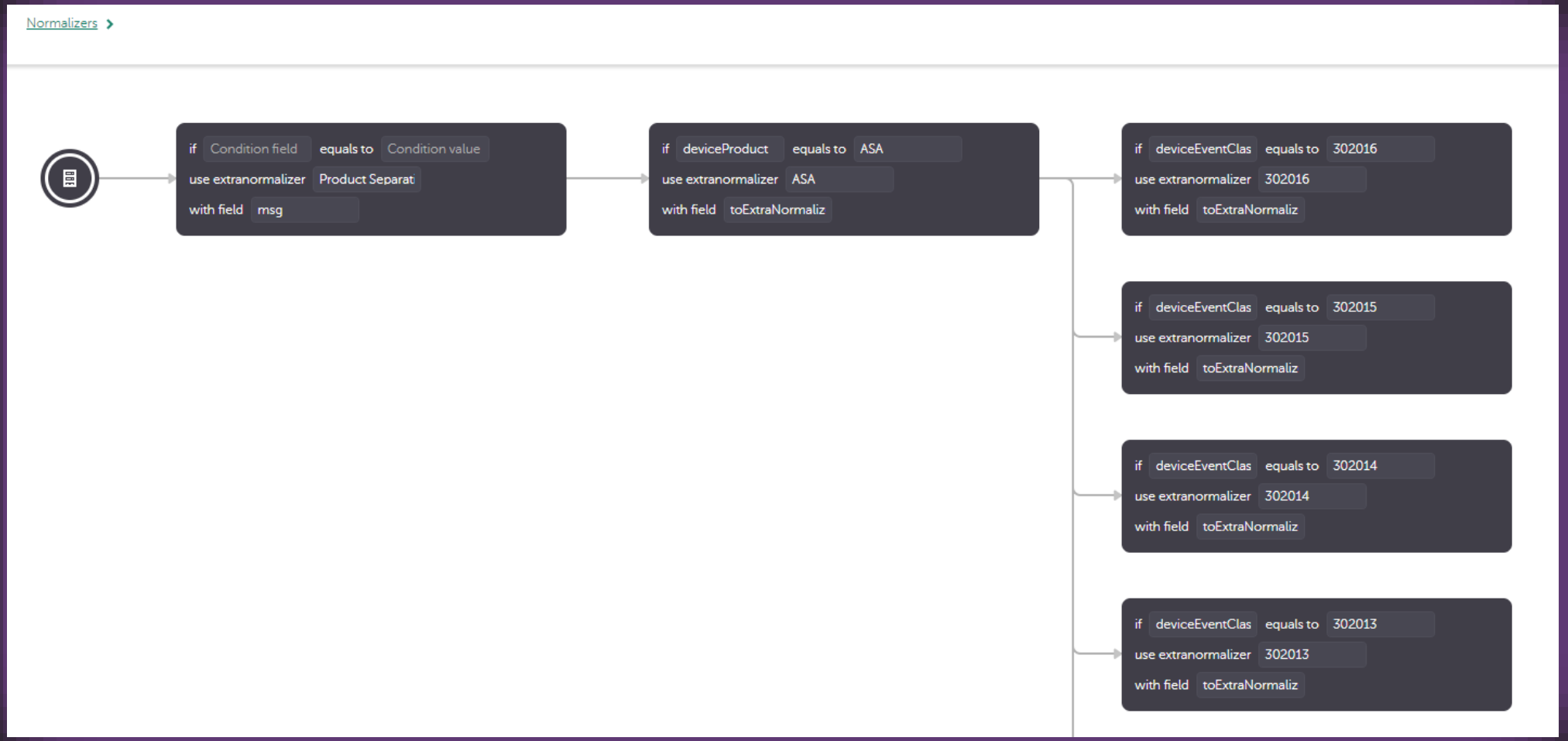
- **Поддержка сбора событий через механизм Windows Management Instrumentation (WMI)**
- **FTP**
- **NFS**
- **SNMP v1/v2/v3**

Мастер добавления нового источника



- **Пошаговый мастер для добавления нового источника**
- **Проверка правил нормализации на примерах событий**
- **Подсвечивание синтаксиса**

Мастер добавления нового источника



Другие новые функции

- Переход на Oracle Linux 8
- Новый пакет правил корреляции (>50шт)
- Поддержка новых источников данных «из коробки»
- Поддержка сбора логов из SQL базы KSC
- Улучшения UI/UX
- Возможность бэкапа и восстановления полной конфигурации
- Авторизация пользователей через AD
- Настраиваемая агрегация алертов
- Расширение списка поддерживаемых источников данных
- Замена инсталлятора на Ansible (поддерживает и распределенную установку)
- RESTful API
  - Возможность работы с ассетами и активными списками
  - Поддержка multitenancy
  - Возможность работы с событиями, алертами
- и др.

KUMA Релиз 1.6 (12.2021)

- Поддержка сценариев иерархического развёртывание
- Поддержка Astra Linux («Смоленск»)
- Утилита для конвертации sigma-правил в ресурсы KUMA
- Расширение списка поддержанных источников логов
- Расширение набора правил корреляции.

Демонстрация

Спасибо