KUMA 2.1

Kaspersky Unified Monitoring and Analysis Platform

kaspersky

Актуальные ИБ-вызовы, в т.ч. связанные с SIEM

Разрозненные средства защиты, которые усложняют работу специалистов ИБ, отнимают много ресурсов и повышают стоимость владения

Необходимость получения контекстной информации о событиях безопасности для упрощения процесса реагирования

Высокие требования к производительности SIEM-систем как ключевое требование

Поиск альтернативных SIEM-систем в условиях политики импортозамещения

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky
Unified Monitoring
and Analysis Platform

Kaspersky
Total Security
для бизнеса

Kaspersky
Security для
интернет-шлюзов

Kaspersky
Threat Data
Feeds

Kaspersky
EDR Expert

Kaspersky
Anti Targeted
Attack

Kaspersky
Security для
почтовых серверов

Kaspersky
CyberTrace

Kaspersky
Threat Lookup

Kaspersky
Industrial
CyberSecurity

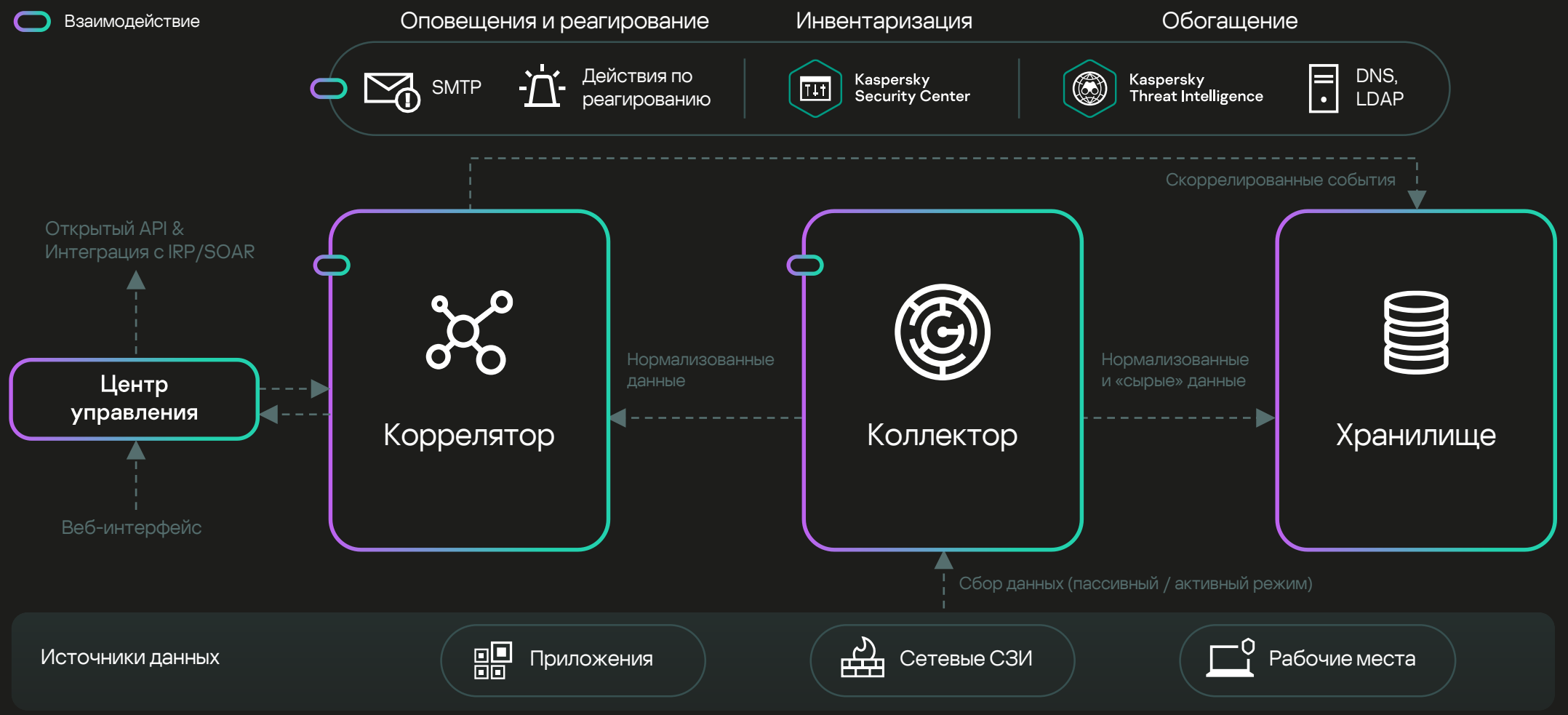
Kaspersky
Security Center

Решения сторонних
поставщиков

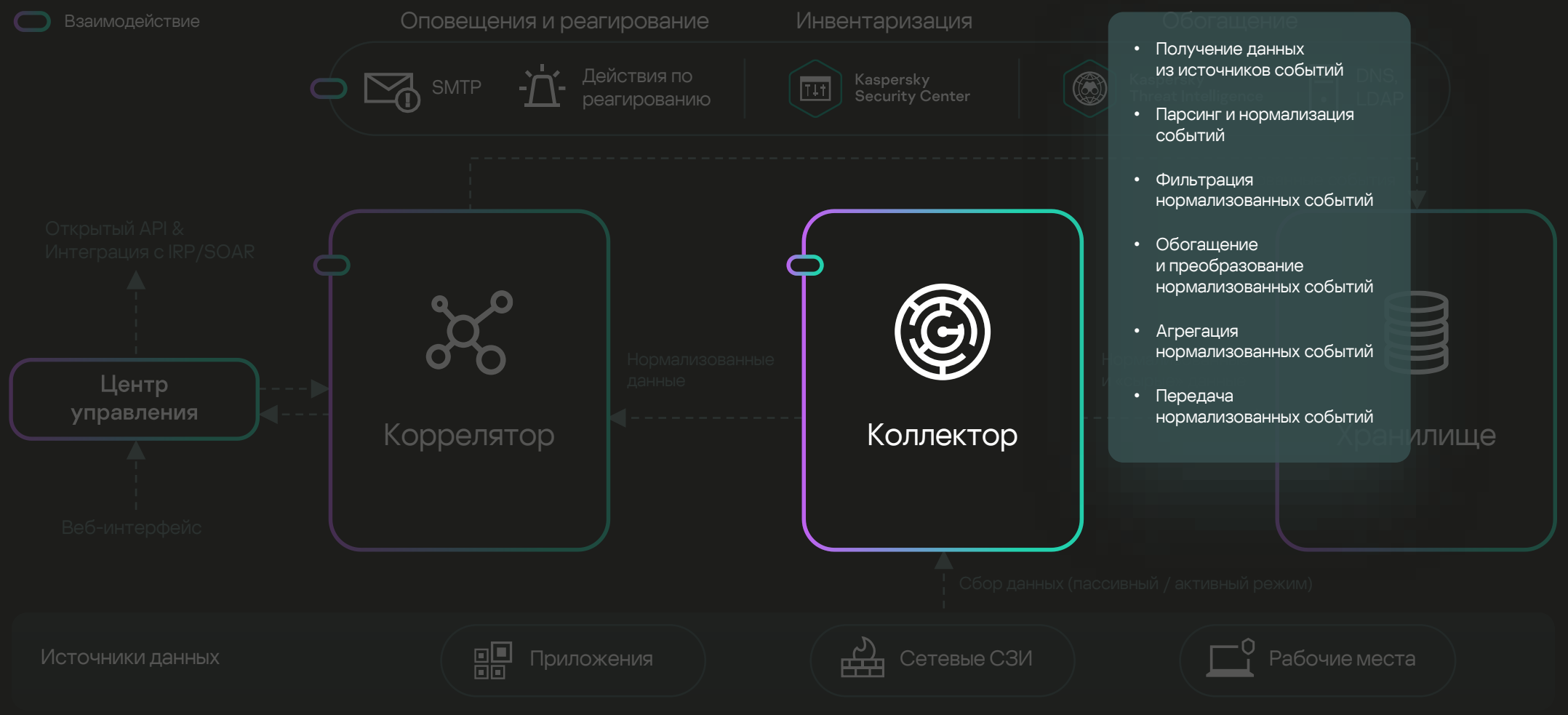
Kaspersky Unified Monitoring and Analysis Platform

Архитектура KUMA

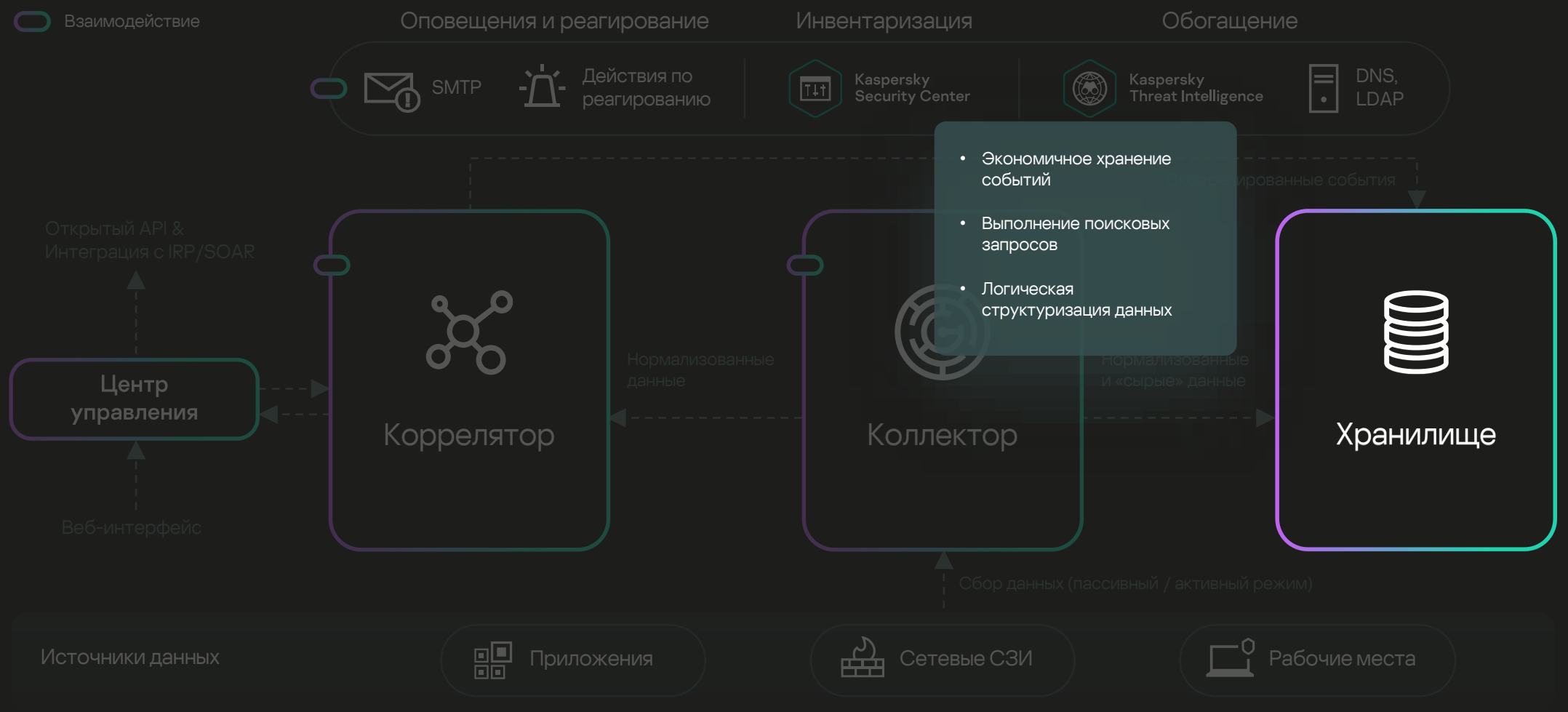
Архитектура KUMA



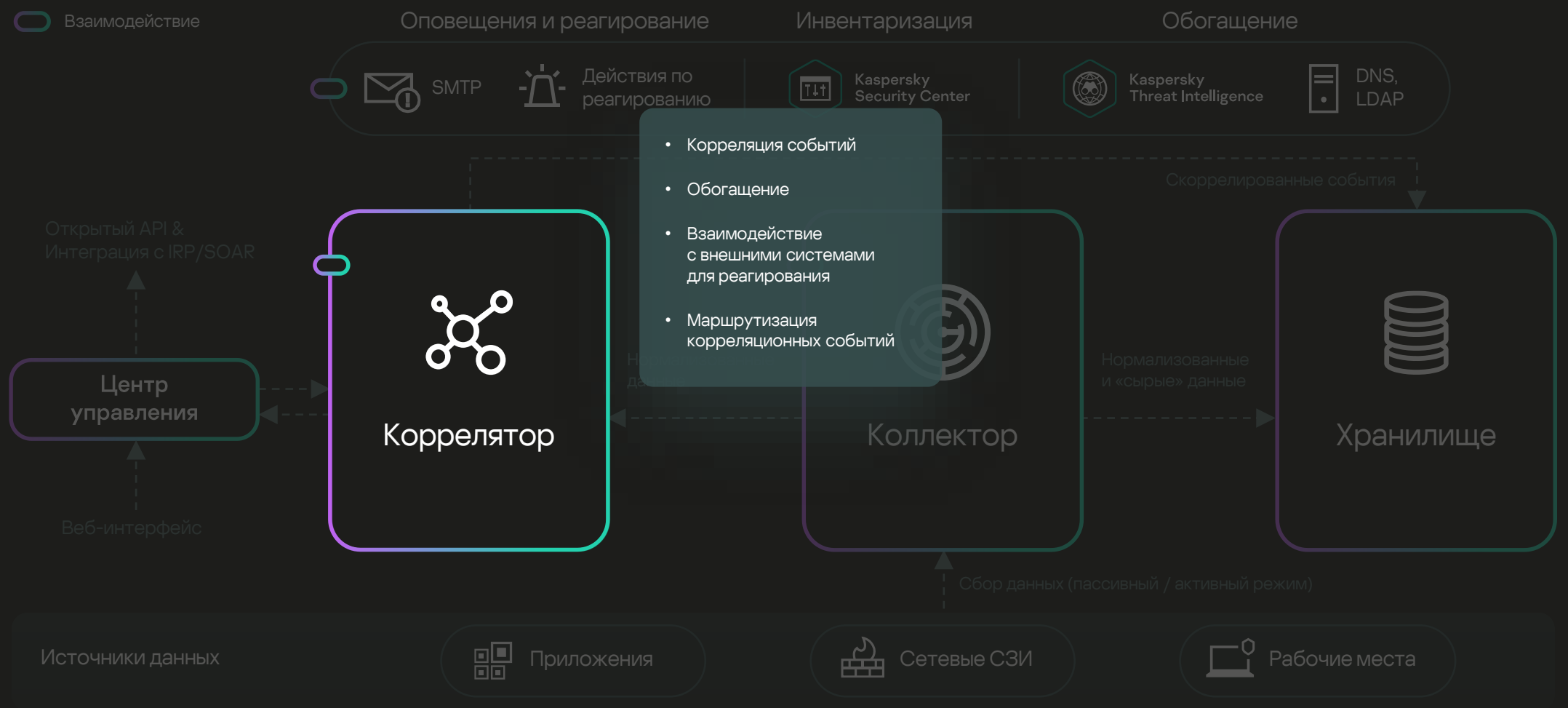
Архитектура KUMA



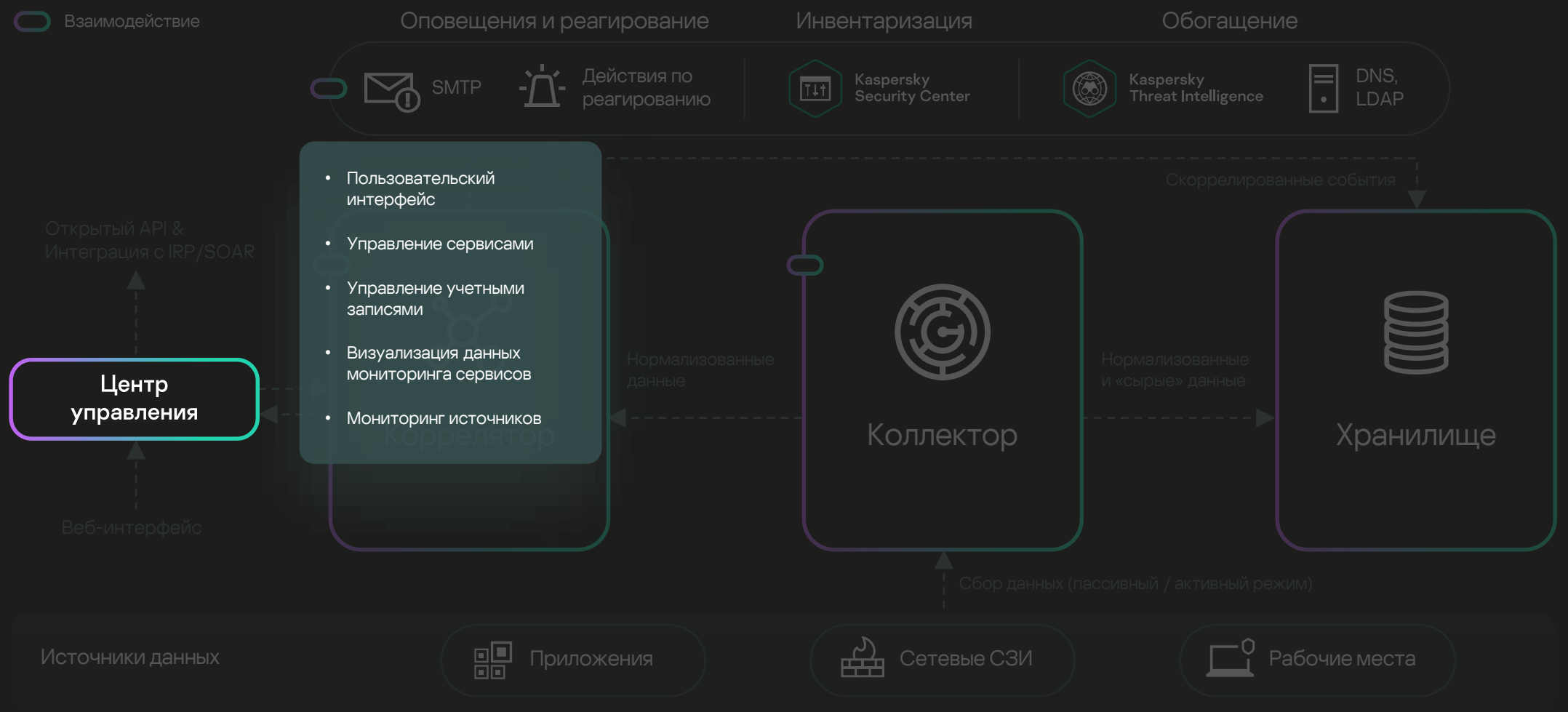
Архитектура KUMA



Архитектура KUMA



Архитектура KUMA



Поддерживаемые источники данных «из коробки» и другие интеграции

Программное обеспечение с открытым исходным кодом

Unbound, Dovecot, Nginx, Apache, DNS BIND, pfSense (с OpenVPN), Exim, Squid, Postfix и др.

Ключевые продукты от различных поставщиков

Microsoft, Palo Alto Networks, Cisco, Juniper, TrendMicro, VMWare, Код безопасности, CheckPoint, Fortinet, Positive Technologies, Infotecs, InfoWatch, Бастион, Huawei, Oracle, MikroTik, Бифит, 1С, С-Терра и др.

Поддерживаемые способы сбора и получения событий

Netflow, Kafka, NATS, SQL, TCP, UDP, HTTP, Files, SNMP, WMI

Операционные системы

Windows, Linux, FreeBSD

Интеграция IRP / SOAR

Security Vision, R-Vision

Коннекторы и нормалайзеры (парсеры)

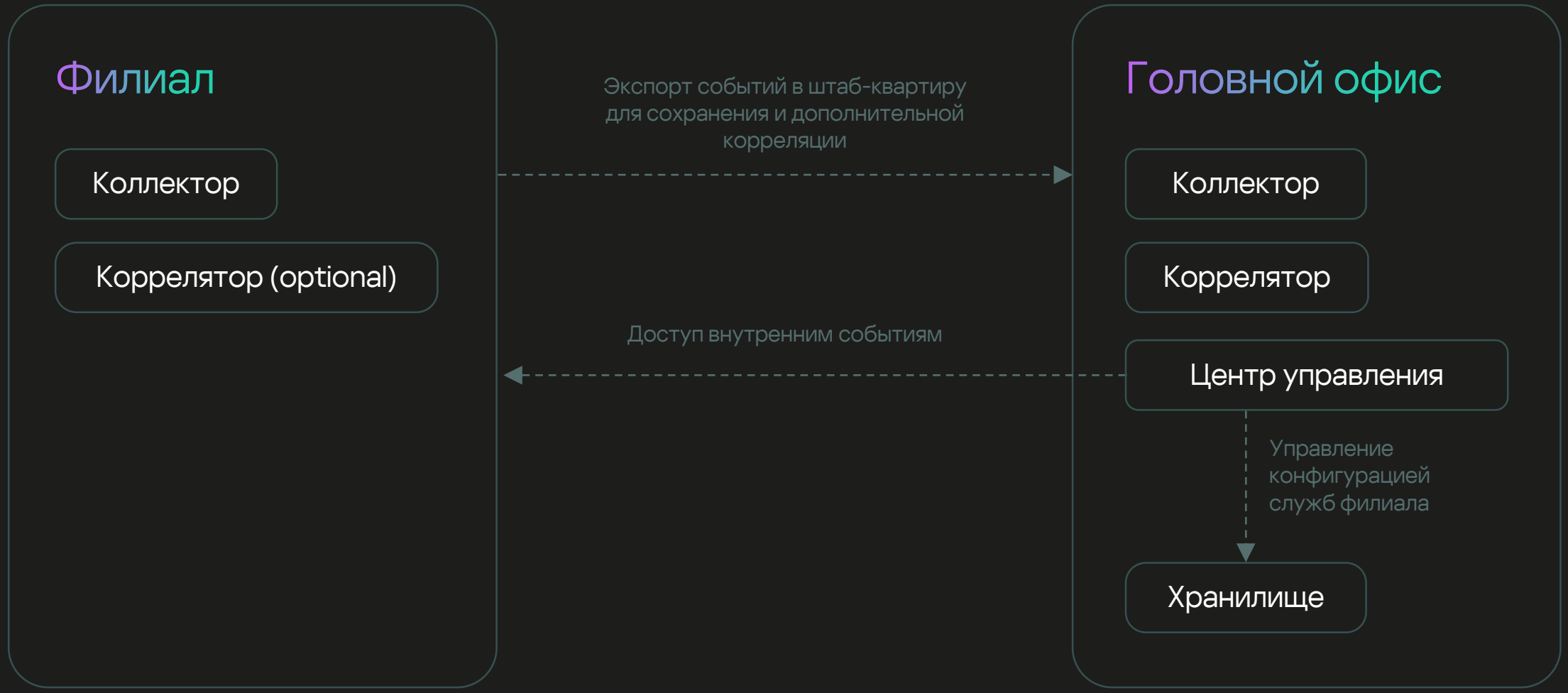
Коннекторы

- TCP listener
- UDP listener
- Netflow v9/10
- NATS
- Kafka
- HTTP
- File
- SQL
- sFlow
- SNMP
- WMI
- Netflow Ipfix

Нормалайзеры

- JSON
- CEF
- CSV/TSV
- Key/Value
  ключ-значение
- Regexp
  (регулярные выражения)
- Syslog (RFC3164 & RFC5424)
- XML
- Windows Event Log

Распределенная инфраструктура

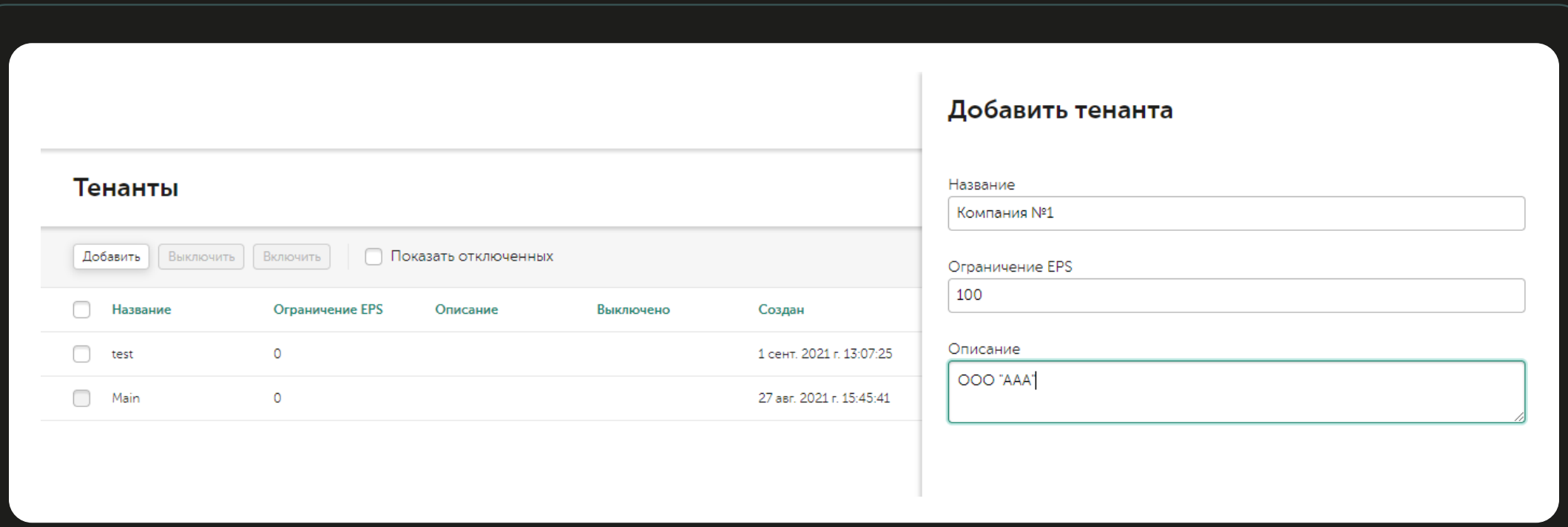


Поддержка Multitenancy

Разделение данных,
конфигурации и прав доступа

Возможность ограничения EPS
для каждого тенанта отдельно

Целевой сценарий для MSSP
и центров ГосСОПКА



Лицензирование

Модули

Шаг по

100 EPS

Учет по количеству «чистых» EPS

Минимальная лицензия от

500 EPS

Дополнительные модули

- ГосСОПКА
- Netflow
- High Availability

Срок действия

- 1 год
- 2 года
- 3 года

Техническая поддержка

		Premium	Premium Plus
Каналы связи	Company account (веб-портал, уведомления через почту)	•	•
	Телефон	•	•
Время реакции в зависимости от уровня критичности	Критический (24/7)	2 часа	0,5 часа
	Высокий (в рабочие часы)	6 часов	4 часа
	Средний (в рабочие часы)	8 часов	6 часов
	Низкий (в рабочие часы)	10 часов	8 часов
Доступные услуги	Программные исправления	•	•
	Удаленное подключение для диагностики проблем	•	•
	Постпроектная поддержка	•	•
	Частные исправления	•	•
	Рекомендации по оптимизации	•	•
	Мониторинг качества оказания ТП и отчеты по выполнению SLA		•
	Персональный технический менеджер		•
	Регулярные статус-встречи с TAMом для ретроспективного анализа зарегистрированных инцидентов, связанных с ТП		Ежеквартальный отчет
	Парсеры логов под заказ	10	20
	Количество включенных часов Professional Services (не менее 2 часов на 1 сессию)	0	16 часов (2 дня)

Примеры кросс-продуктового функционала

Пример 1. Инвентаризация информационных активов

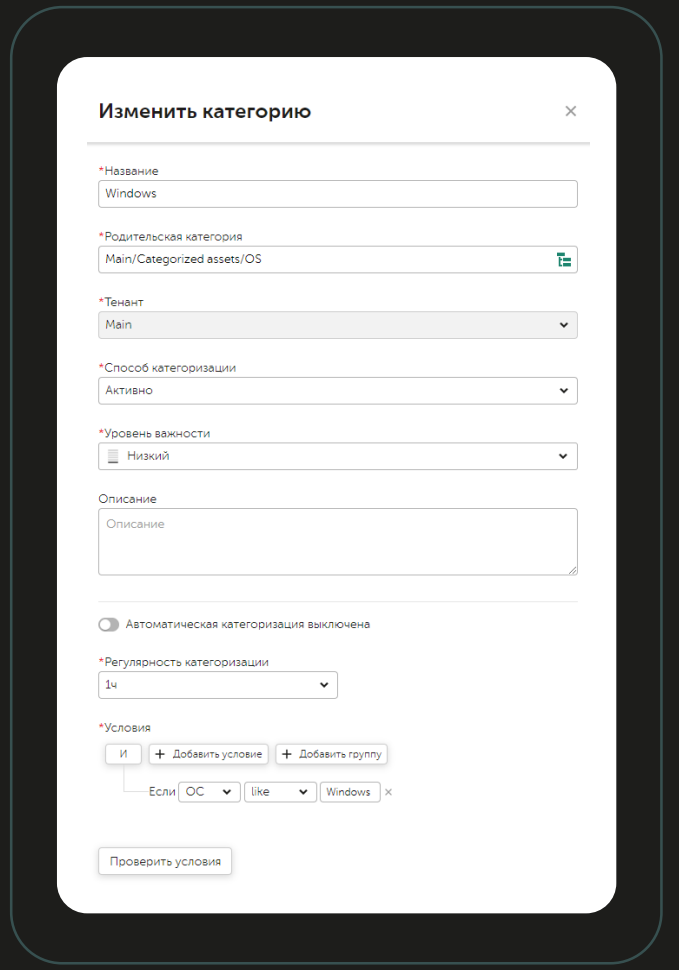
Динамическая категоризация активов

Динамическая категоризация по:

FQDN | IP | CVE | ОС | Версия билда ОС

Логические операторы AND, OR, NOT и группировки

Возможность проверки условий

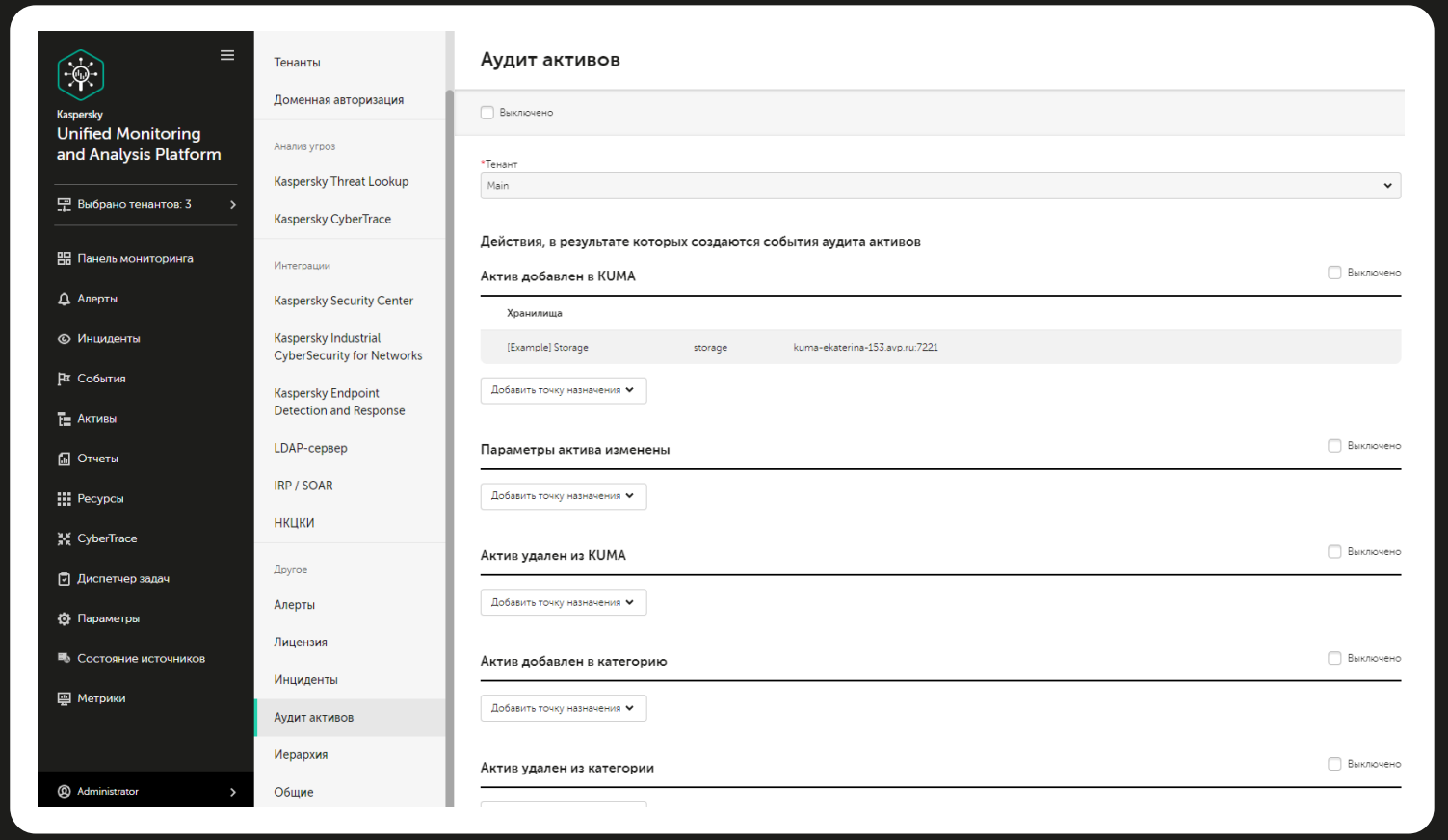


Аудит активов

События аудита
для каждого тенанта

Можно направить
в коррелятор
и создавать алерты
на появление
уязвимостей

Можно строить
графики анализа
состояния активов



Пример 2. Сбор и анализ расширенной телеметрии

Единый агент EPP+EDR

Драйвер сети

Драйвер перехвата OS API

Драйвер мониторинга файловой системы

Драйвер мониторинга процессов и сервисов

Обогащение и фильтрация

~15k EPD

Создание, модификация файлов и т .д.

Запуск, инъекция процессов и т.д.

Сетевые соединения, DNS-запросы, скачивание файла, e-mail и т.д.

Изменение реестра, Event logs, WMI, автозапуск и т.д.

Инциденты AV, DeviceControl и т.д.

GERT
Группа реагирования

SOC Team

GREAT Центр глобальных исследований и анализа угроз

EDR Central Node

Обогащение

Визуализация

Корреляция

+ Инциденты EDR

Threat Intelligence

3rd party
Сторонние события

KUMA

Обогащение

Визуализация

Корреляция

Пример 3. 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

Пример 4. «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

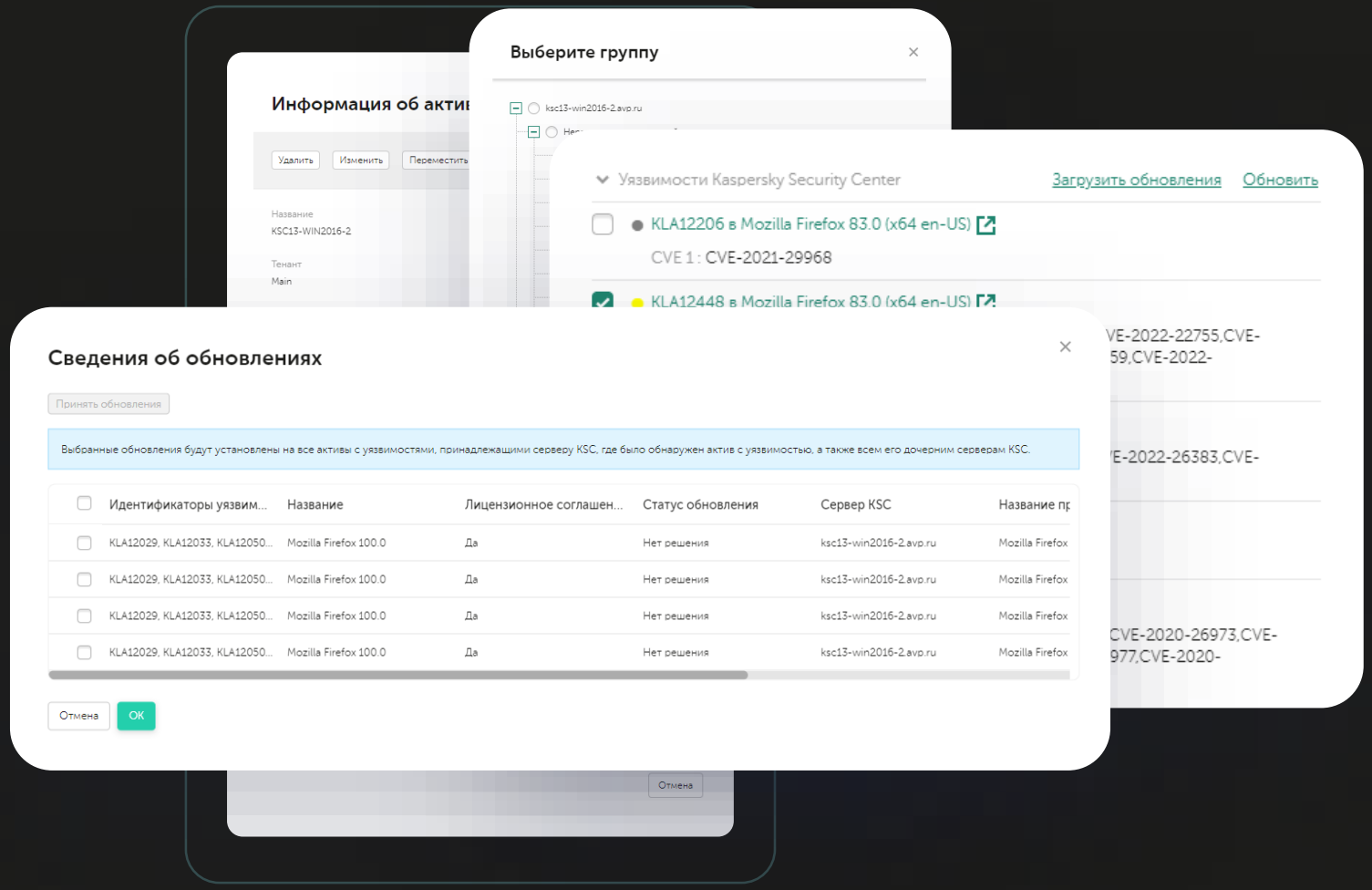
URL: «example.com»
first seen: “2016-08-10”
last seen:” 2020-03-01”
Связанные хэш-суммы вредоносных файлов MD5:”.....”

SHA-1: “.....”
SHA256:” ”
Связанные вредоносные URL: “....”
Связанные IP: 1.2.3.4, 2.3.4.5, ...

Реагирование из карточки

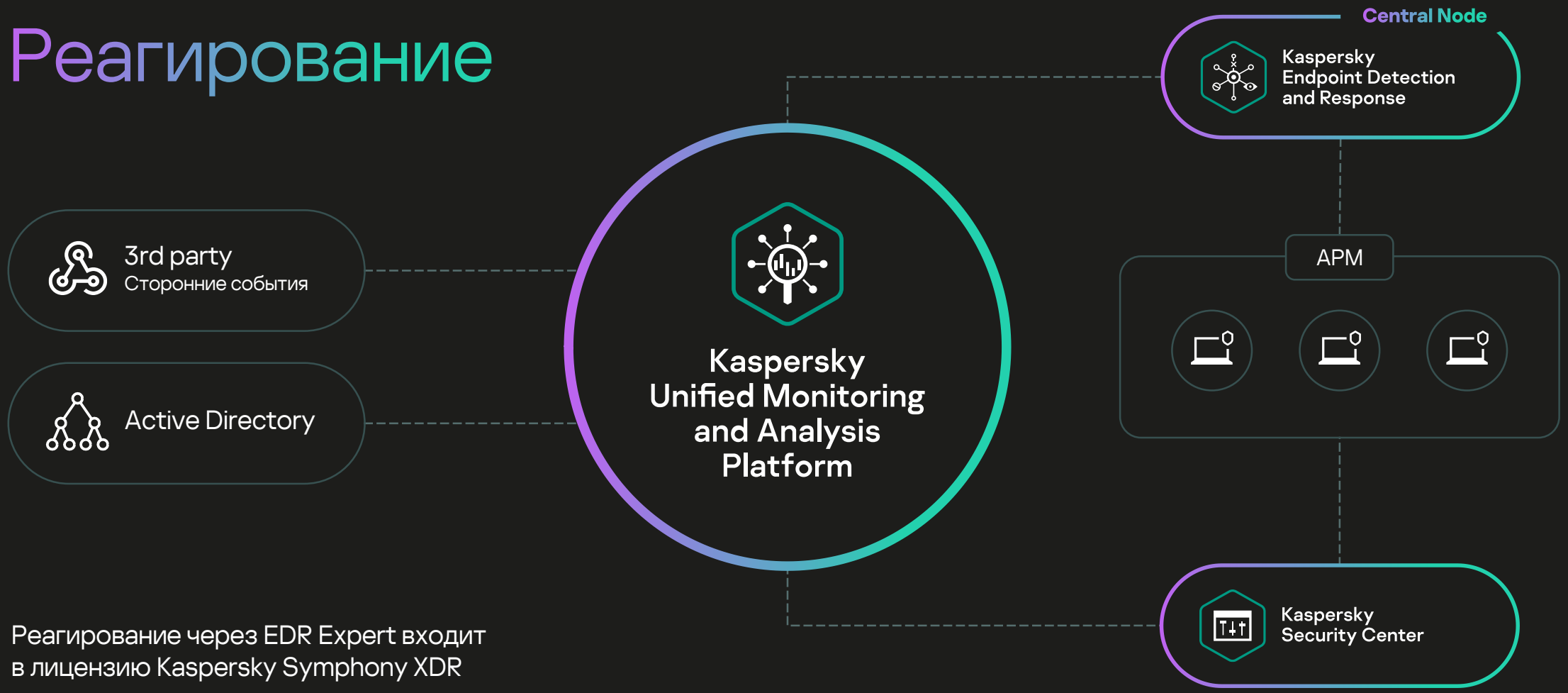
Перемещение в группу администрирования (влияет на политику антивируса)

Установка патчей для уязвимостей



Пример 6. Автоматизированное реагирование на инциденты KES/KEDR

Реагирование



Реагирование через EDR Expert входит в лицензию Kaspersky Symphony XDR

Пример 7. Скрипты для автоматического реагирования

KEDR Response (script)

- Изоляция хоста и снятие с изоляции
- Блокировка хеша по md5 и sha256 на хосте
- Запуск исполняемого файла на хосте по полному пути
- Логирование реагирования в системном журнале

Telegram Response

Оповещения об алерте в телеграм канале

AD Response

- Блокировка УЗ и разблокировка
- Выход пользователя из активных сессий
- Добавление УЗ в группу и исключение из группы

UserGate Response

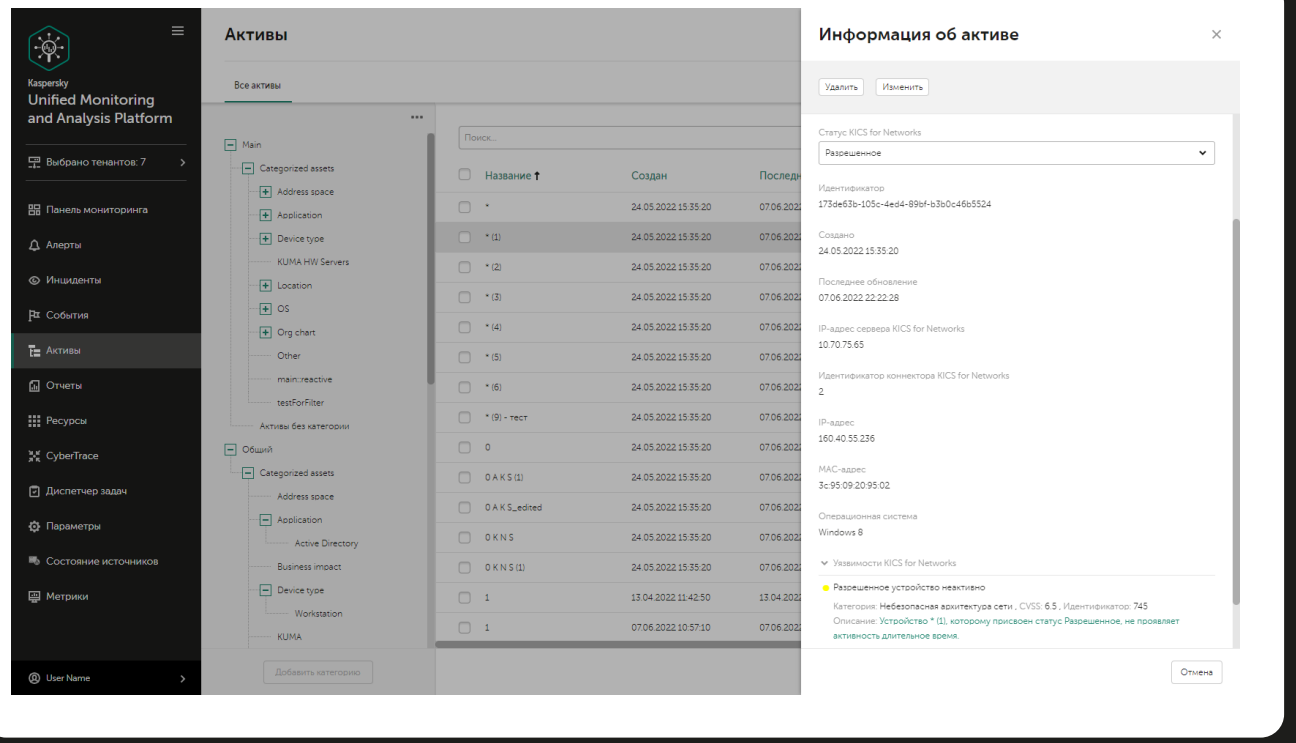
- Блокировка по IP
- Блокировка по URL
- Блокировка по Домену

Пример 8. Интеграция с Kaspersky Industrial CyberSecurity

Kaspersky
Industrial CyberSecurity
for Networks

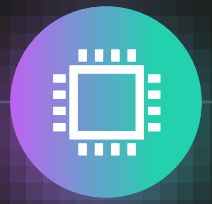
Импорт активов вместе
с уязвимостями

Реагирование вручную
из карточки



Ключевые преимущества

Ключевые преимущества



Высокая производительность

300k+ EPS на один узел

Низкие системные требования

Современный язык

Эффективное хранилище

Масштабируемость

Гибкая микросервисная архитектура

Единый интерфейс веб-консоли

Все настройки в одном окне

Интеграция «из коробки»

С продуктами сторонних поставщиков и решениями «Лаборатории Касперского»

Низкий порог входа

Не требует знания специальных языков запросов или написания правил

Автоматические и ручные реагирования

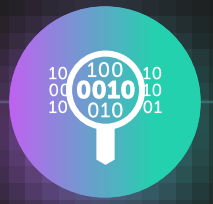
Интеграция с KES, KEDR, KICS

Запуск скрипта

Интеграция с ГосСОПКА

Отправка инцидентов в НКЦКИ

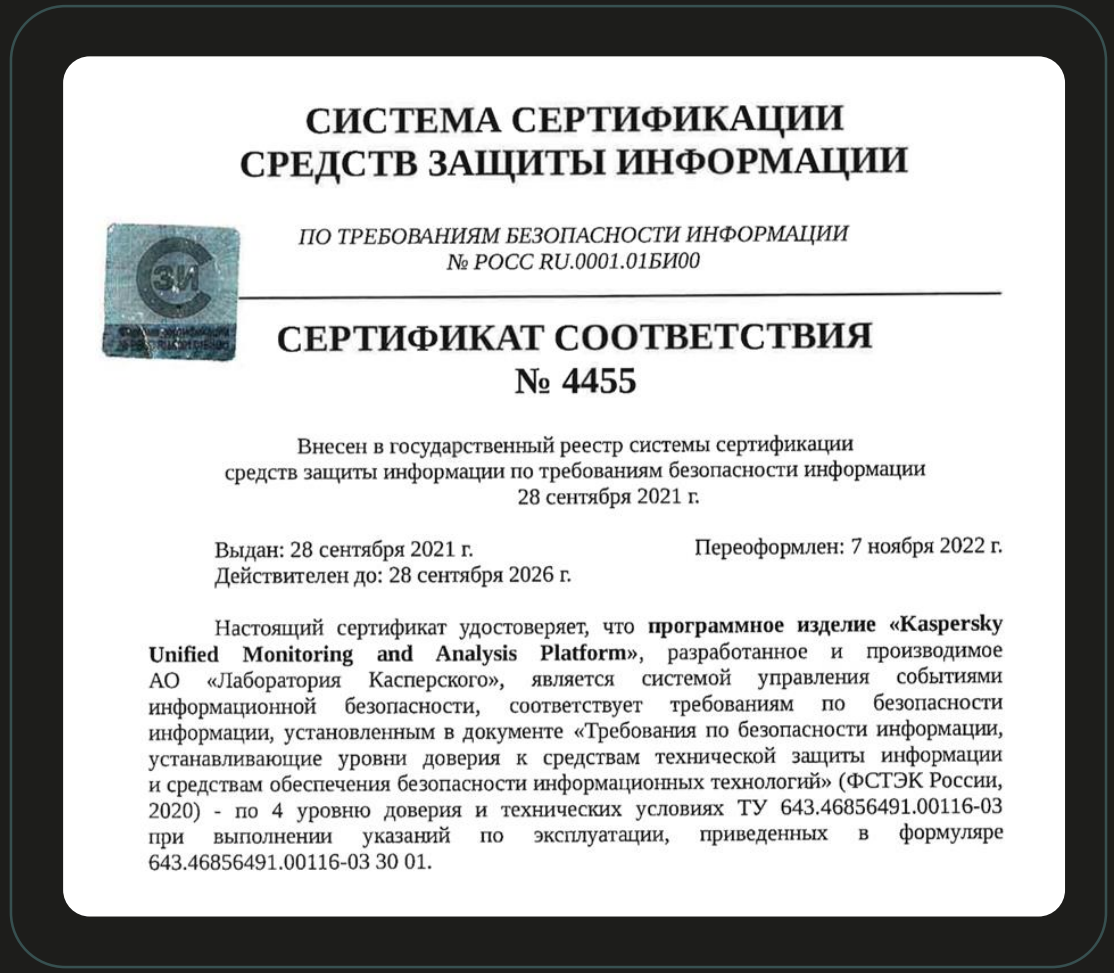
Получение обратной связи и фидов



Интеграция с CyberTrace

Обогащение событий данными фидов

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.

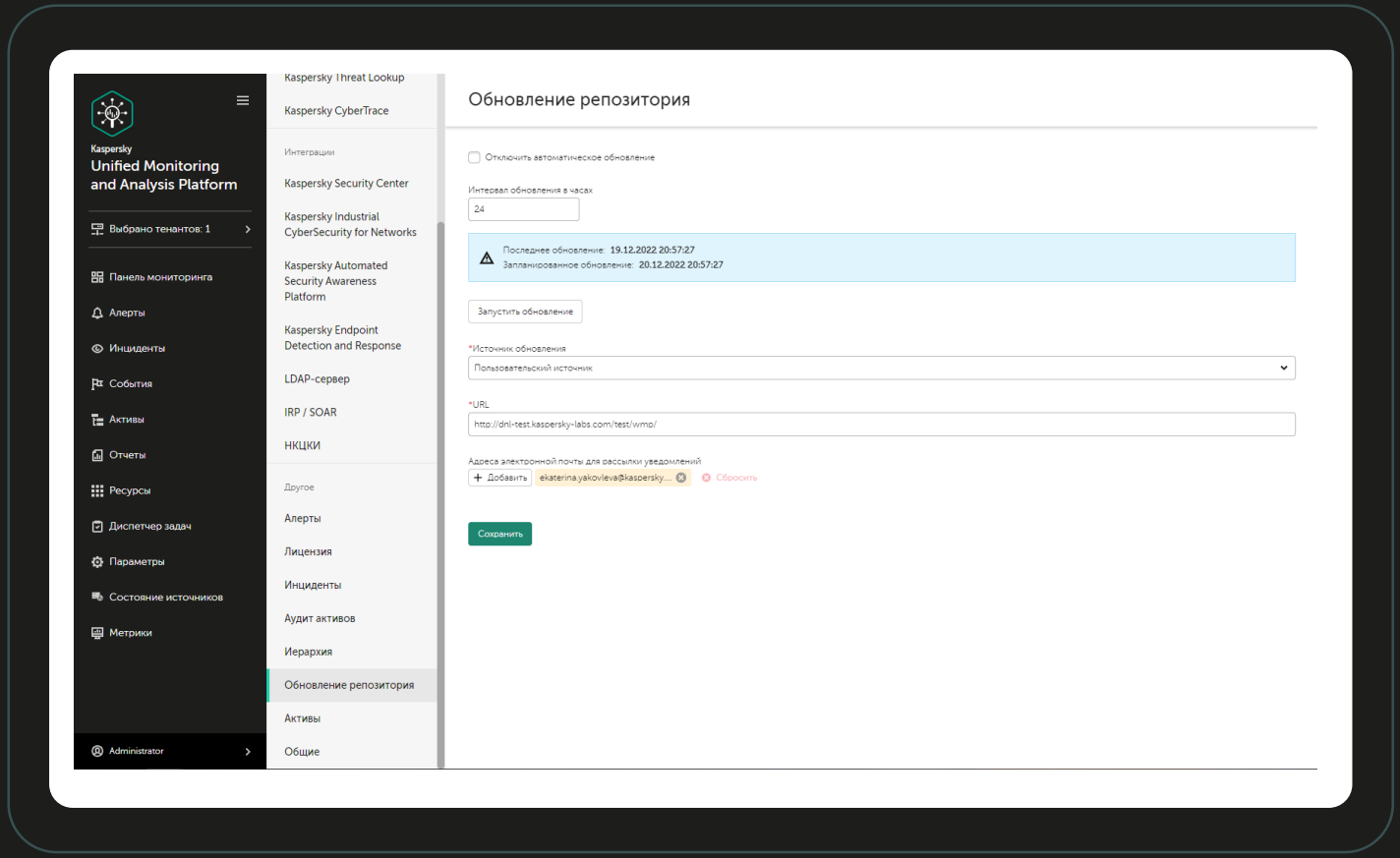
Выдан: 28 сентября 2021 г. Переоформлен: 7 ноября 2022 г.
Действителен до: 28 сентября 2026 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Unified Monitoring and Analysis Platform»**, 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 643.46856491.00116-03 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00116-03 30 01.

Новые функции версии 2.1

Подсистема автоматического обновления нормалайзеров и правил корреляции

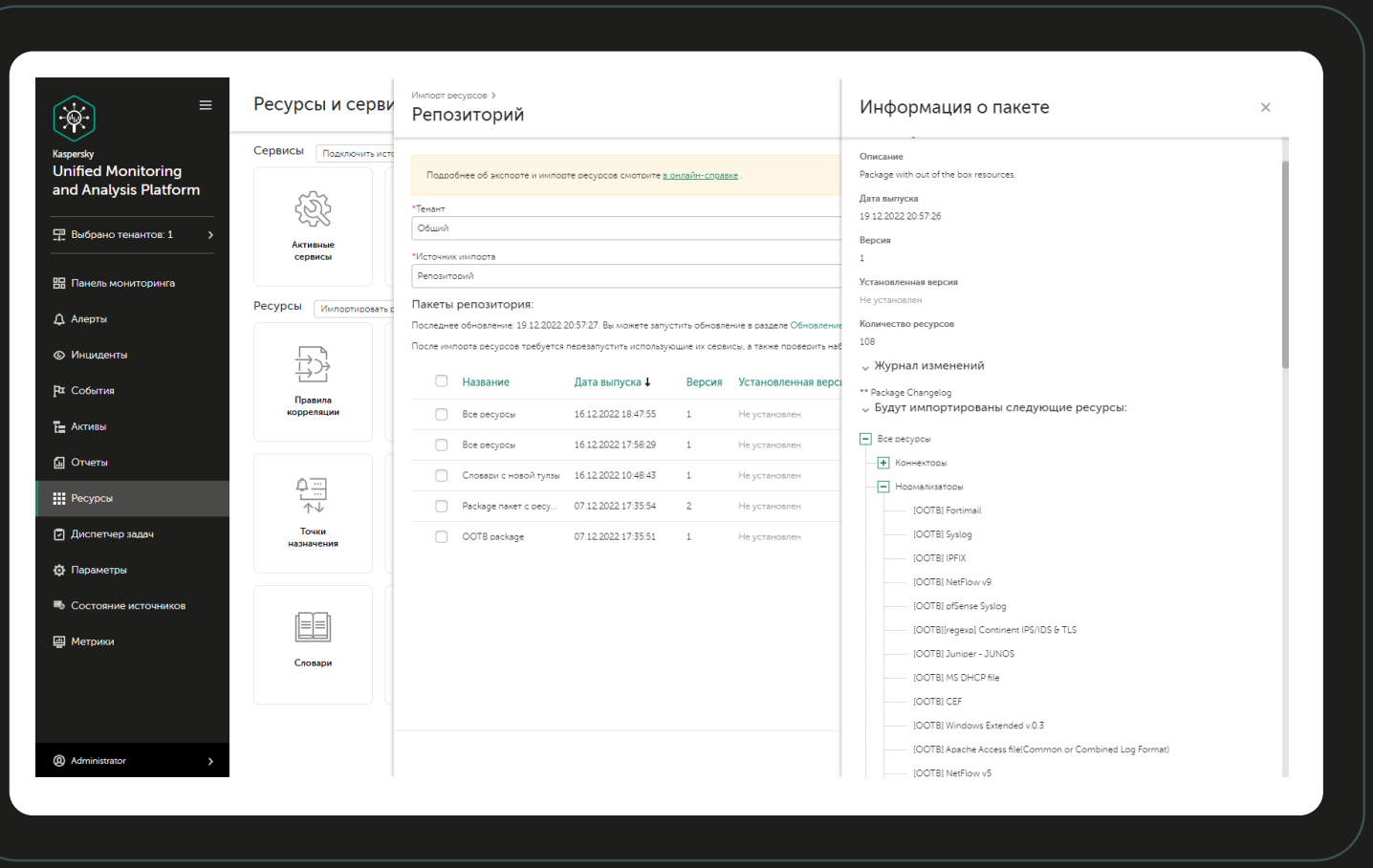
Подсистема обновления оперативно получает информацию о доступных обновлениях контента, анализирует содержимое каждого обновления и принимает решение о внедрении новых ресурсов в эксплуатируемую инфраструктуру.



Подсистема автоматического обновления нормалайзеров и правил корреляции

Все изменения применяются по решению оператора – подсистема обновлений информирует о новых доступных ресурсах.

Система поддерживает обновление в том числе без прямого доступа к интернету с использованием механизма «зеркала обновления».

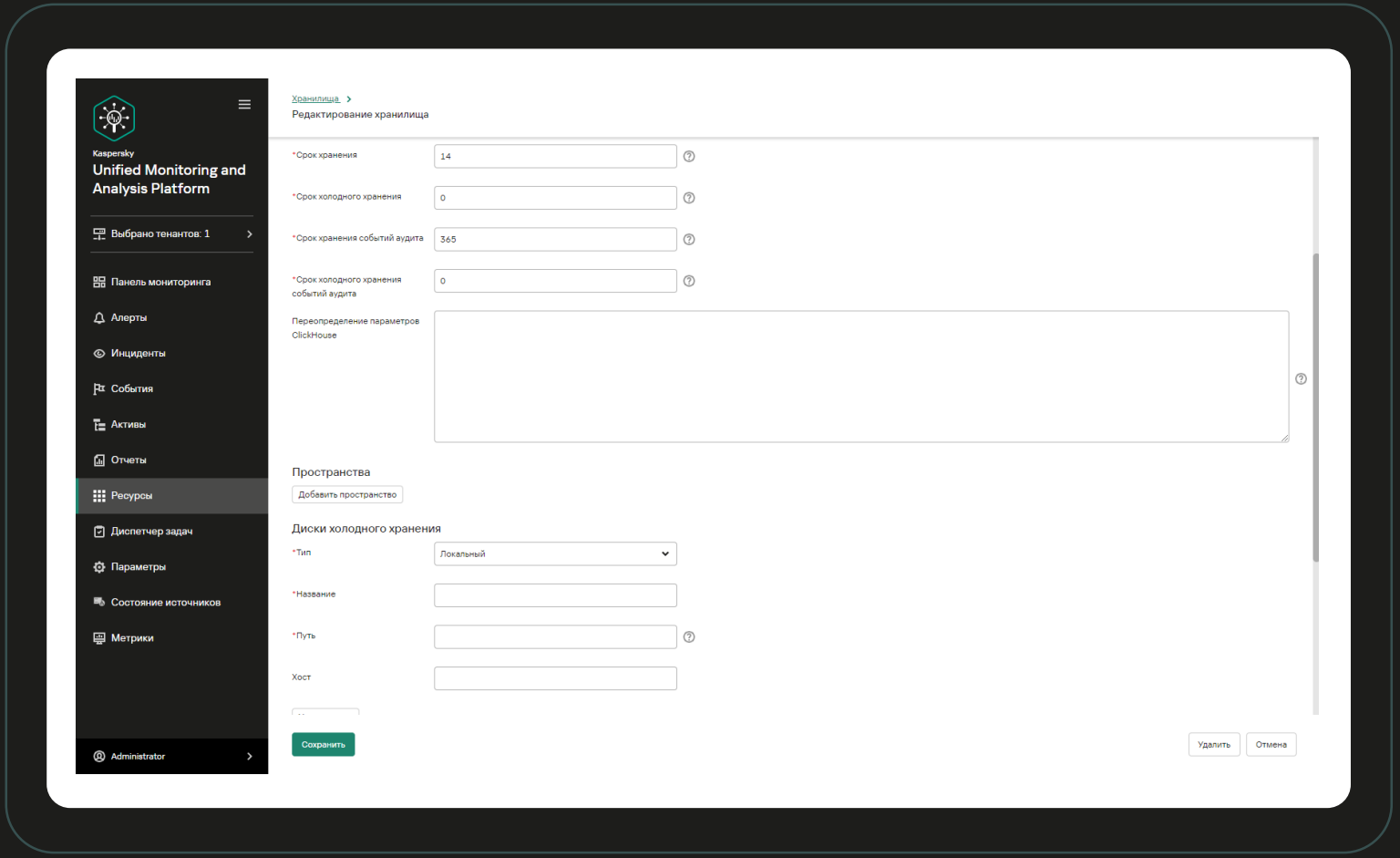


Дополнительный этап хранения событий

Оптимизация стоимости оборудования за счет разделения хранения этапы.

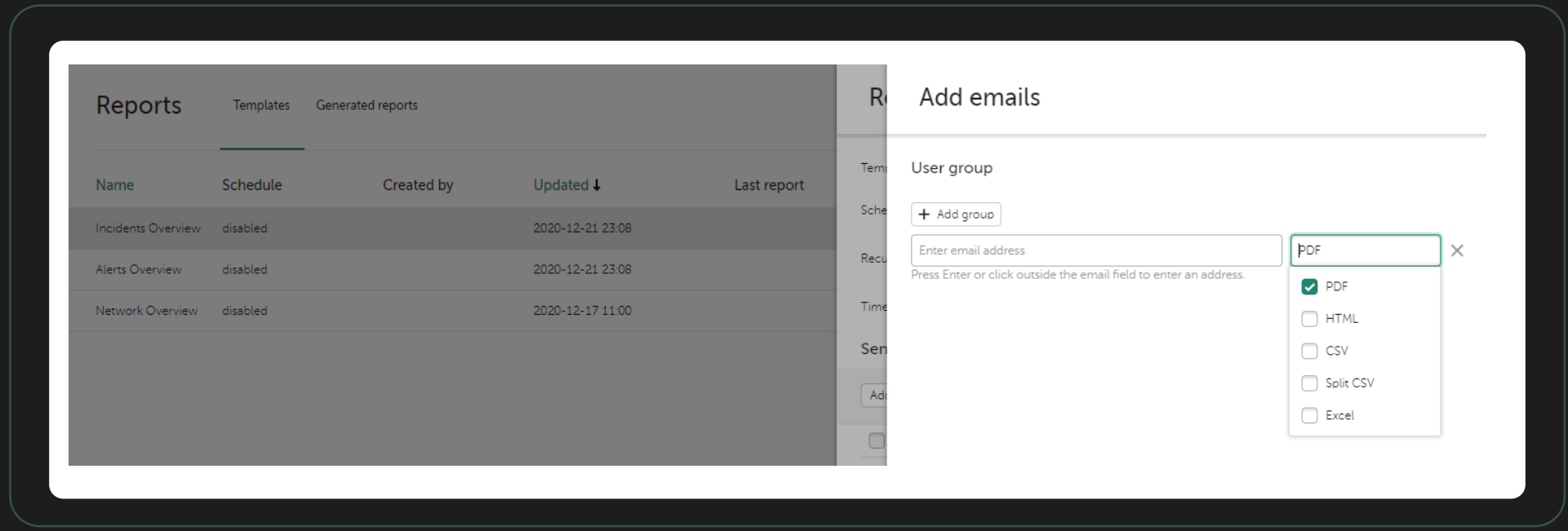
Передача «исторических» данных на менее производительное оборудование через заданный интервал.

Единый поиск со всеми поддерживаемыми возможностями SQL по всем данным независимо от того, на каком хранилище события находятся.



Доступны следующие форматы:

HTML | PDF | CSV | раздельный CSV | Excel



Расширена интеграция с ГосСОПКА

Синхронизация статусов инцидентов

Категоризация активов в соответствии с КИИ-категориями

Возможность приложить файл к инциденту

Интерактивный чат со специалистами НКЦКИ

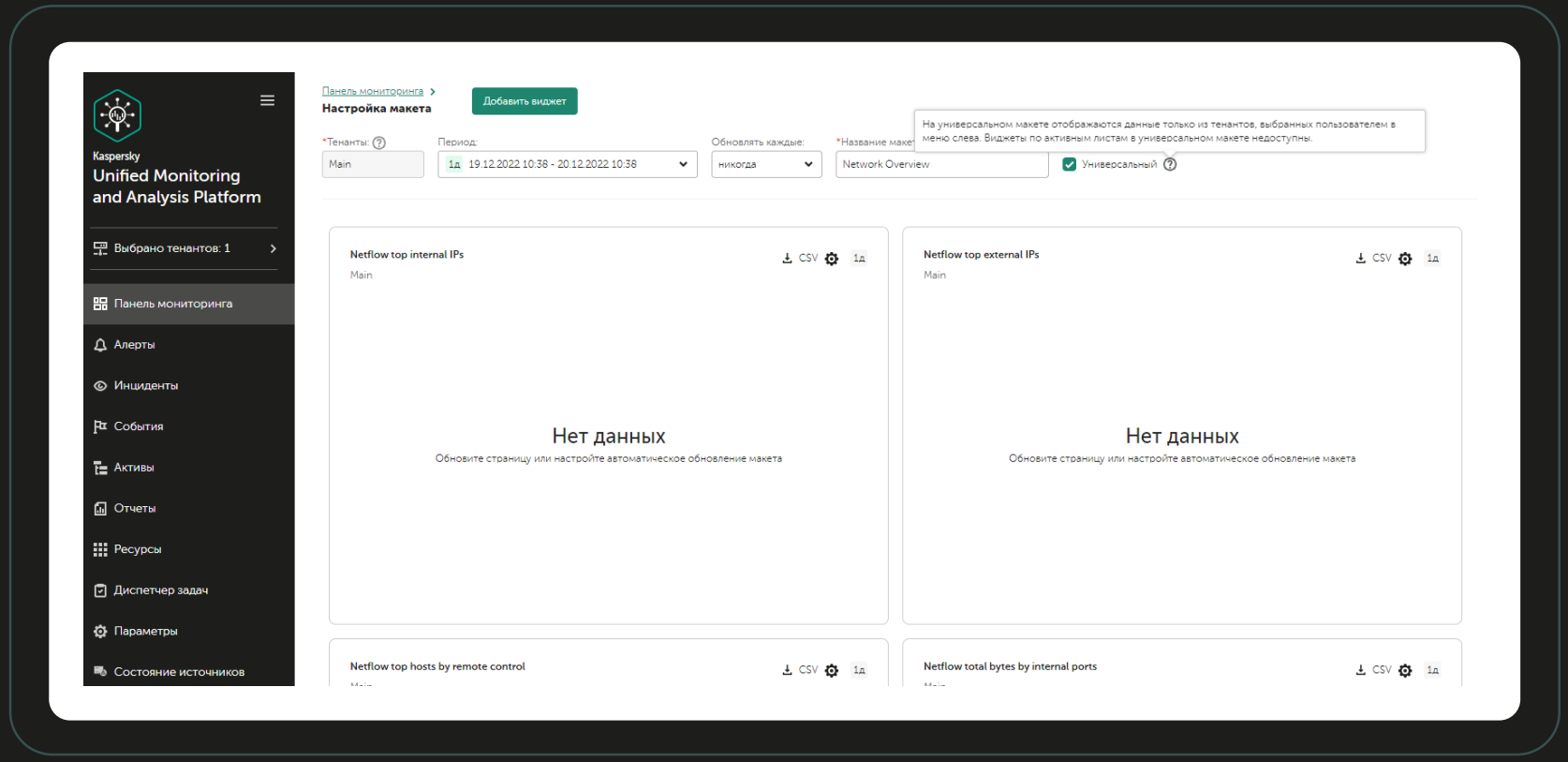
Сравнение актуальных значений параметров инцидентов в KUMA со значениями, переданными в ГосСОПКА

Поддержана передача инцидентов в режиме иерархии инсталляций KUMA – родительские узлы KUMA смогут информировать НКЦКИ об инцидентах, выявленных на подчинённых системах

Обновления в дашбордах

Единые для всех тенантов (общие) шаблоны дашбордов

Скачивание данных в CSV



Новые интеграции для реагирования*

KASAP:

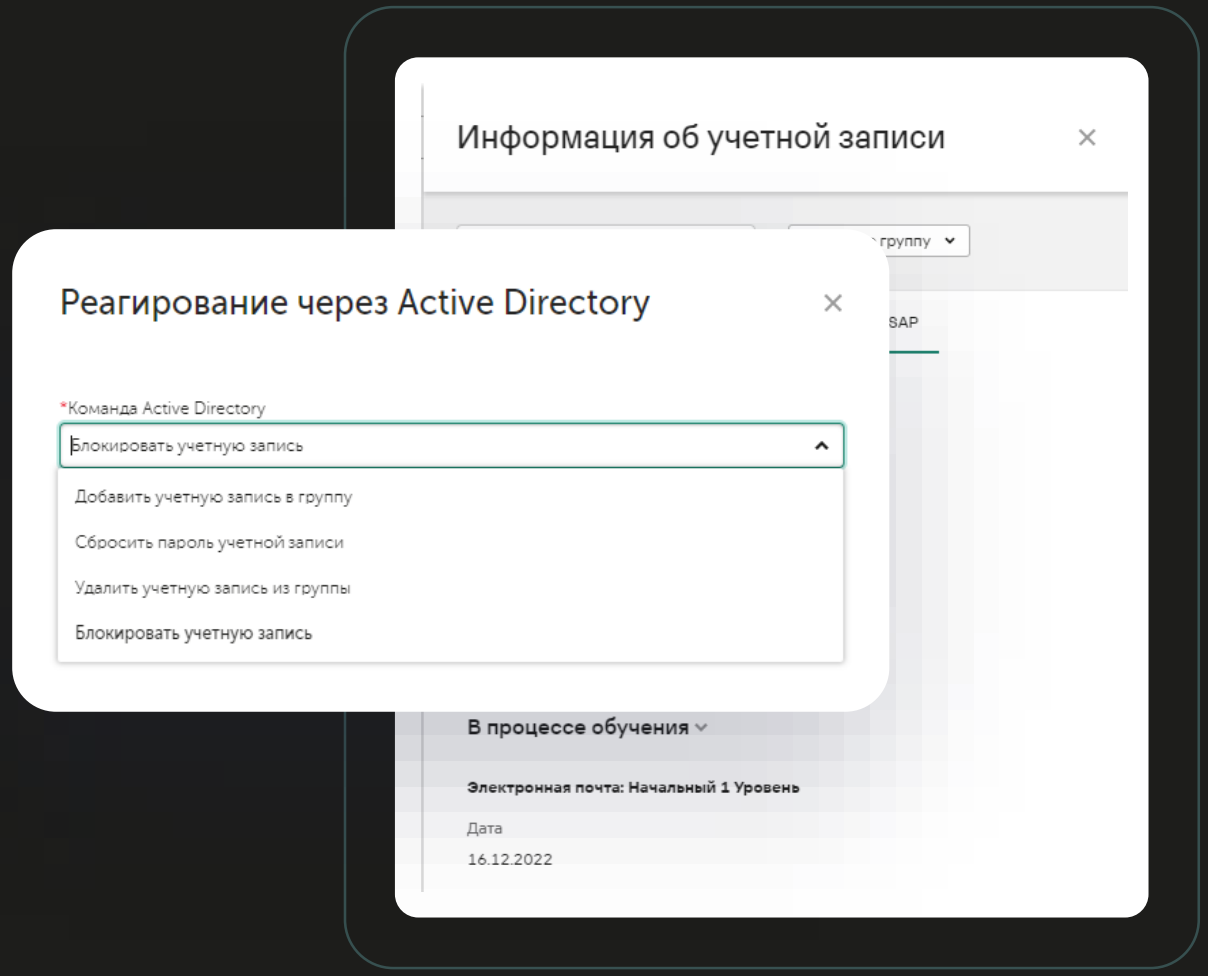
Информация по результатам обучения

Записать пользователя на курс

Active Directory:

Управление группами (добавить-удалить)

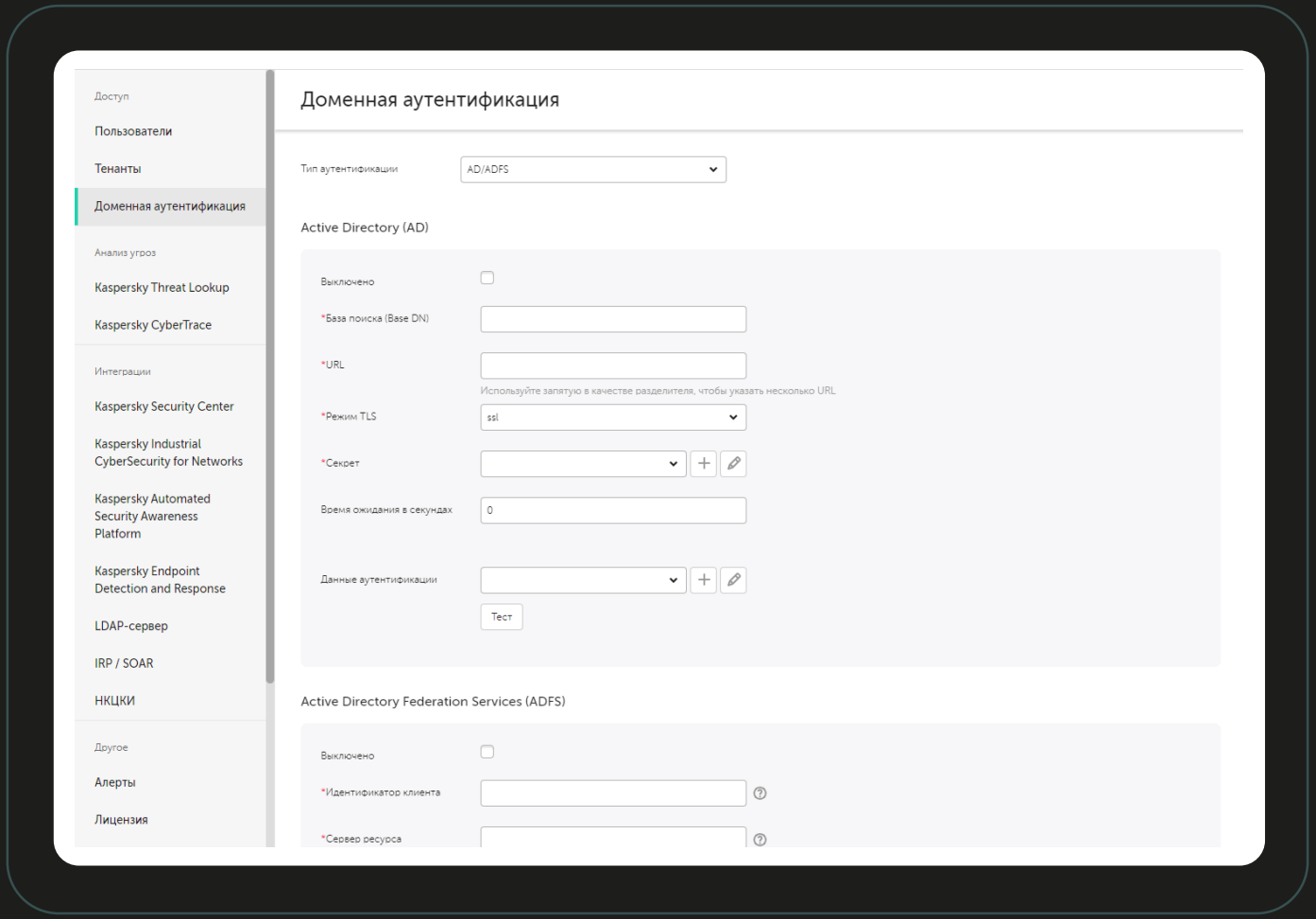
Сброс пароля
Блокировка УЗ



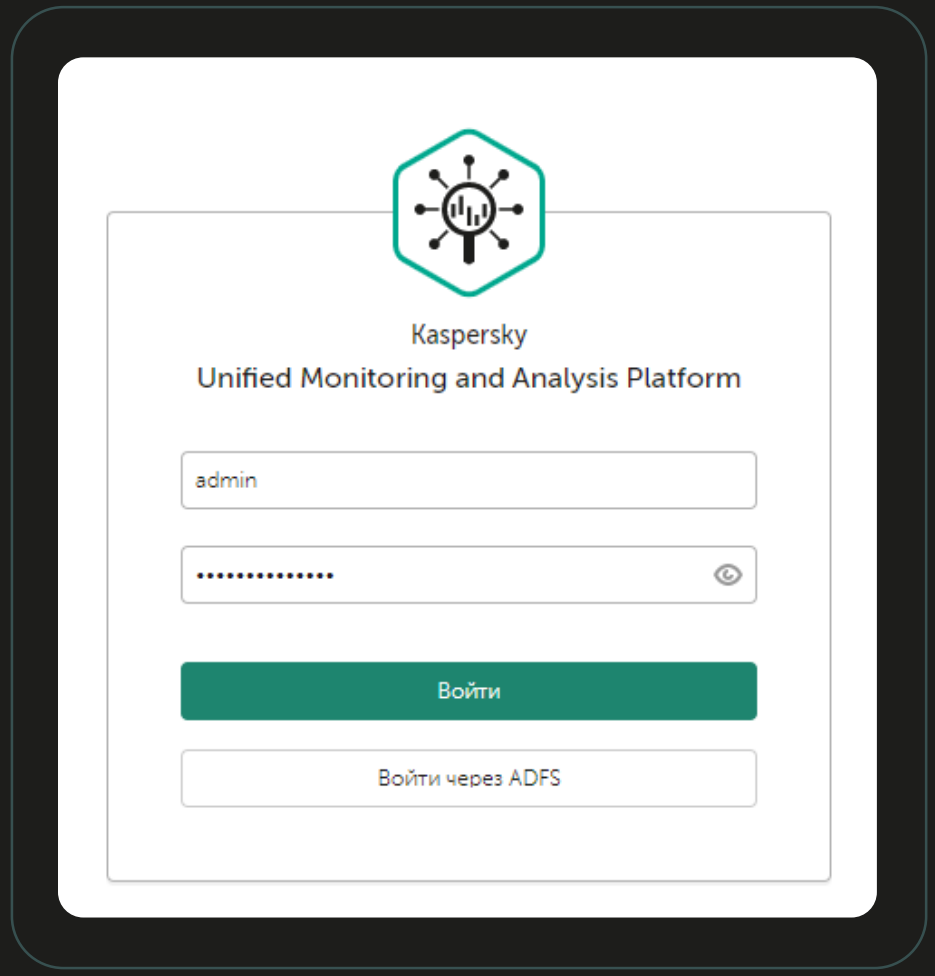
* Доступно только в лицензии Kaspersky Symphony XDR

Новые возможности входа в систему

Добавлена интеграция с Active Directory Federation Server для входа в систему без ввода логина и пароля (сценарий Single Sign On — SSO)

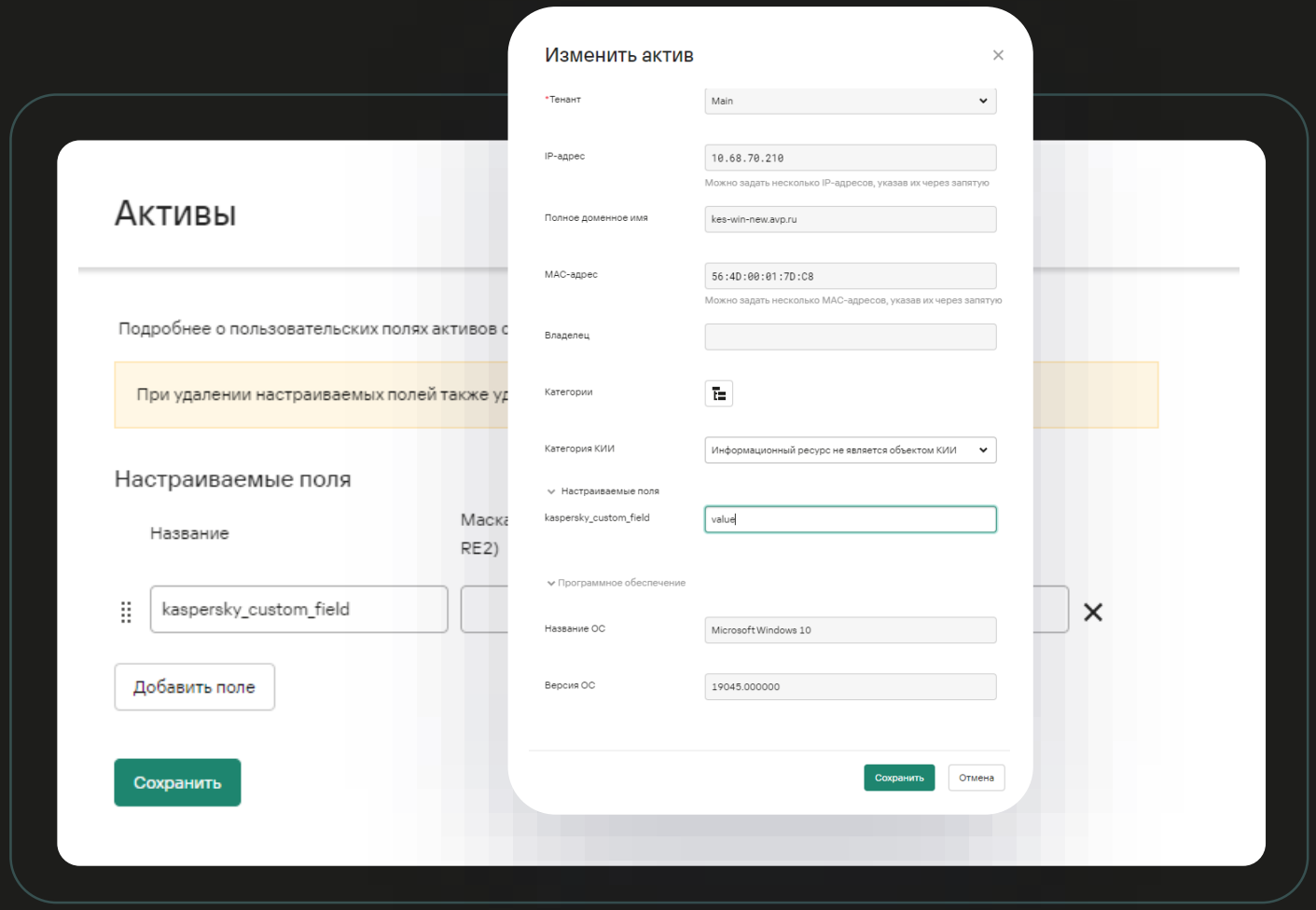


Добавлена поддержка домена FreeIPA для входа в систему



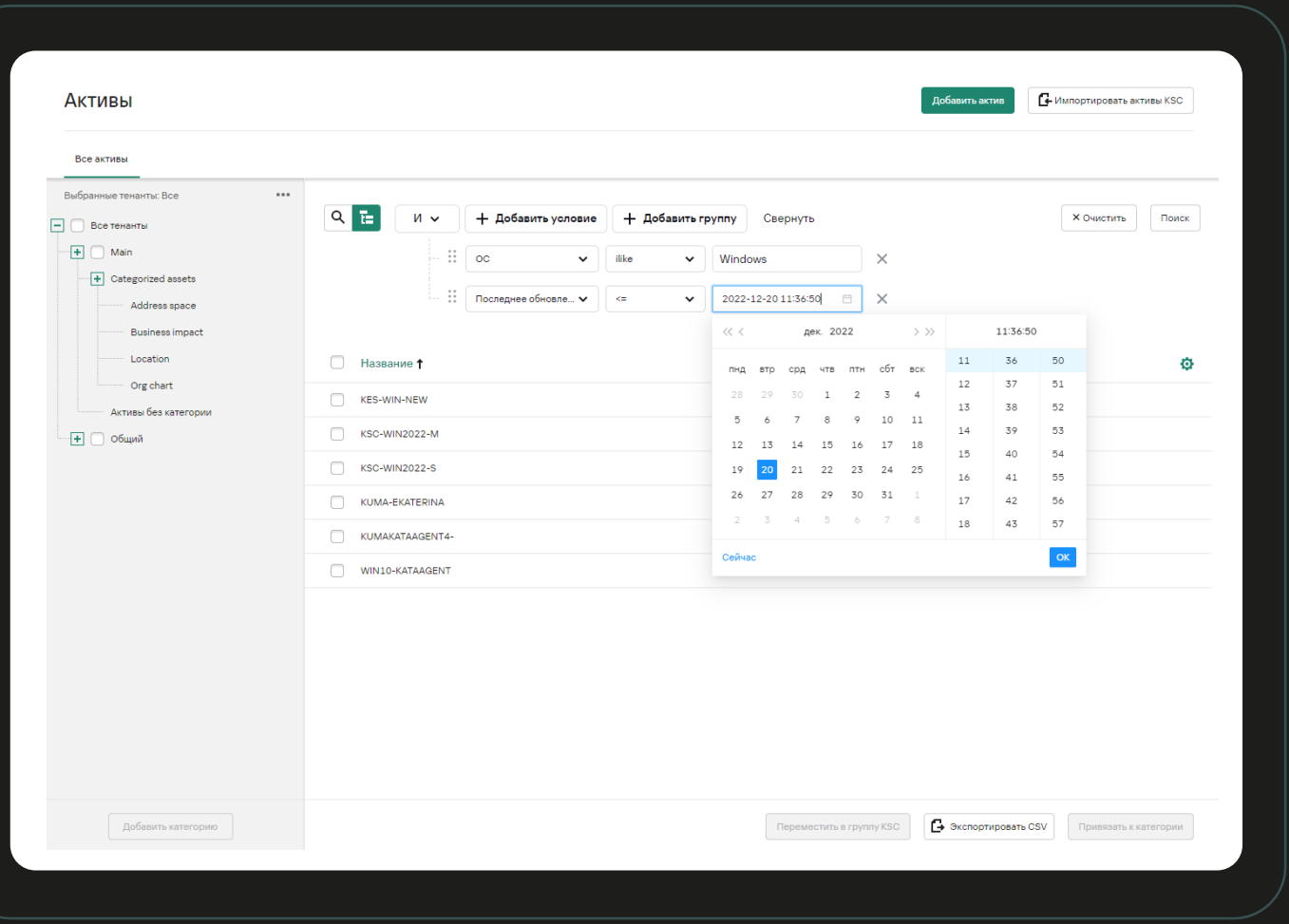
Новые возможности работы с активами

Добавлена возможность настройки модели карточки активов. Добавленные поля могут заполняться вручную через WebUI или через RestAPI



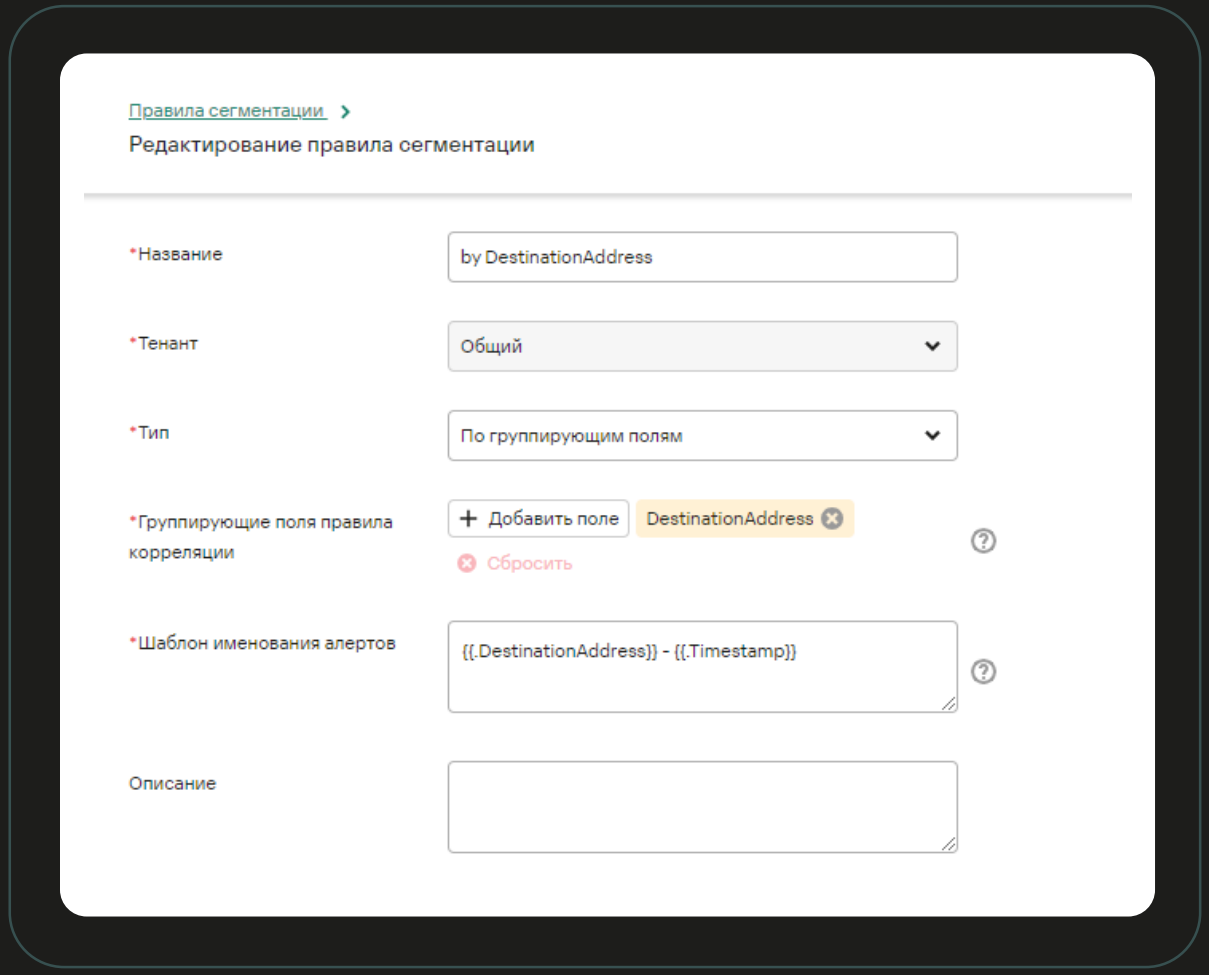
Новые возможности работы с активами

Добавлена возможность поиска по активам с учётом названий полей, а также возможность экспорта результатов поиска в файл



Обновленные правила агрегации алертов

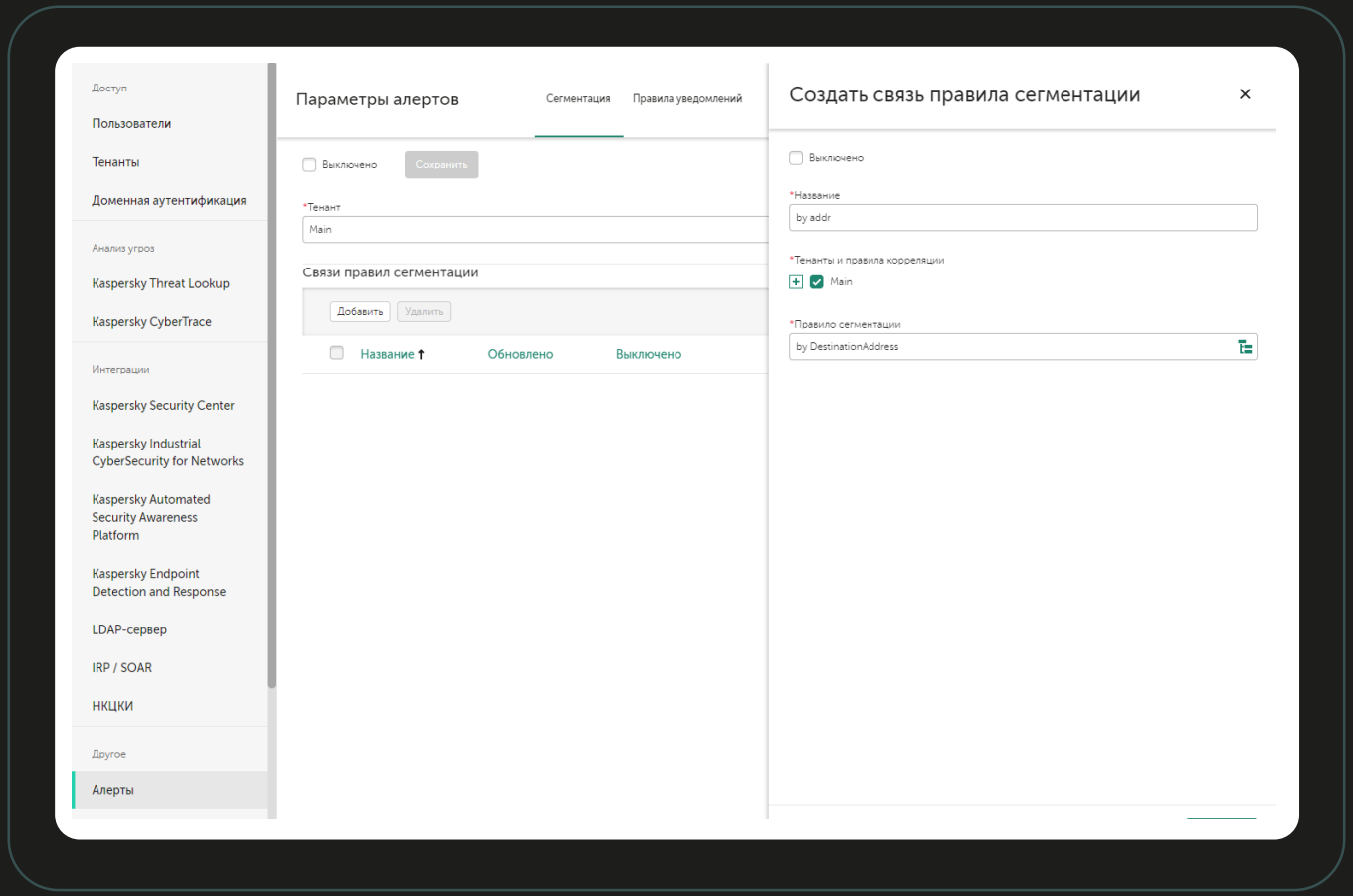
Добавлена возможность выделить ключевые поля алертов для группировки срабатываний по ним, что позволит выделить создавать группы алертов, объединённых по атакуемому ресурсу или источнику атаки



Обновленные правила агрегации алертов

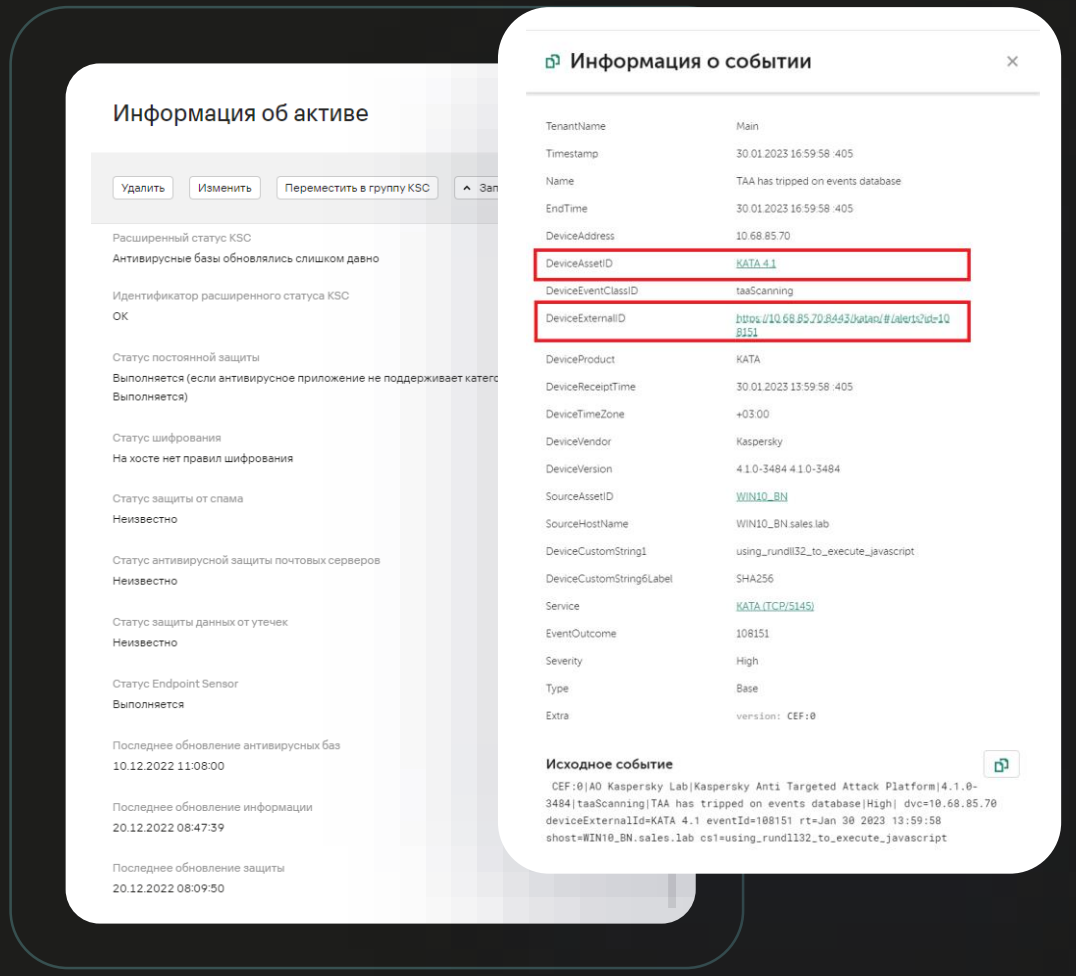
Добавлена возможность задать максимальное количество срабатываний в одном алерте, что востребовано в интеграциях, при которых алерт рассматривается как задача для администратора.

Новые срабатывания к алертам, взятым в работу (т.е. статус которых изменён) не будут добавляться.



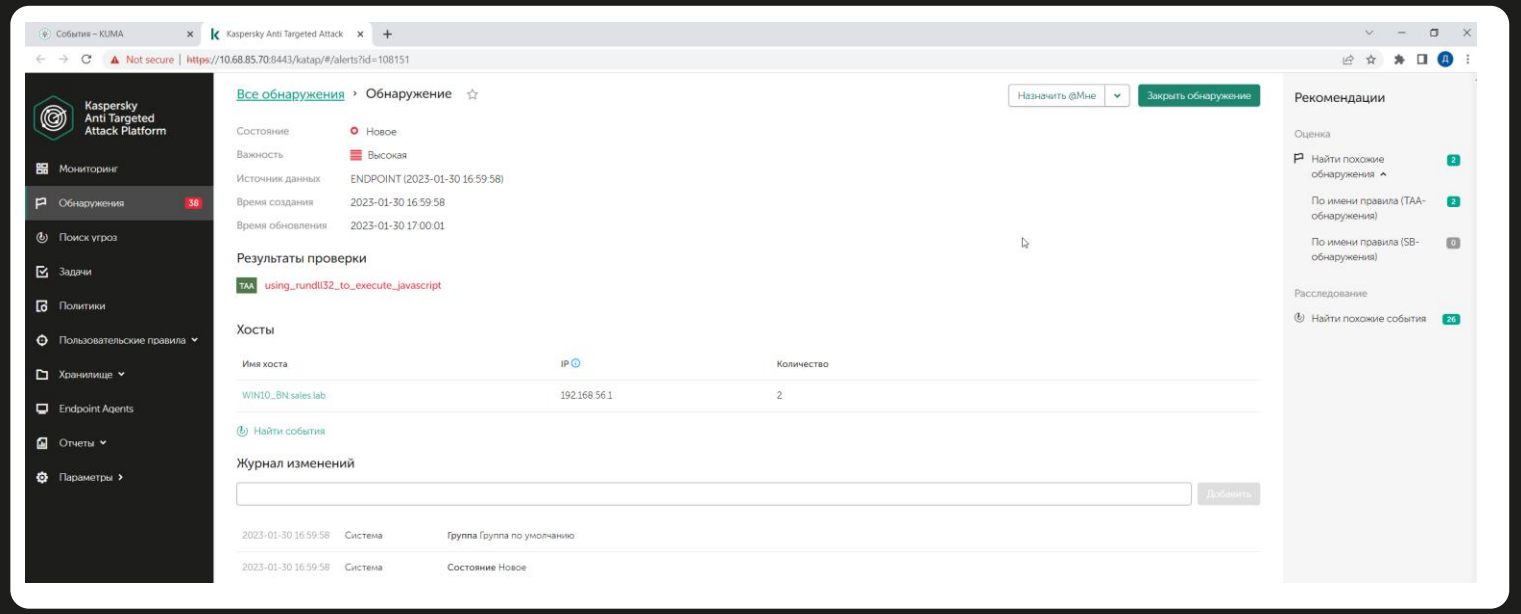
Расширена интеграция с KES / KSC

Отображение сведений о состоянии защиты



Расширенная интеграция KES/KEDR/KATA

Для событий
о срабатываниях
KATA/EDR
добавлена ссылка,
позволяющая
перейти на
карточку алерта
в KATA/EDR



Другие улучшения

Преобразование hex, base64, base64url
Для обработки событий auditd и др.

Расширена отказоустойчивость системы

В компонент KUMA Core добавлена поддержка режима отказоустойчивости

Добавлены пресеты полей событий, позволяющие быстро настраивать колонки таблицы поиска в зависимости от анализируемых логов

Добавлены новые коннекторы:

SNMP-Traps | 1C

Добавлены нормализаторы

- Oracle Audit Trail
- Windows XP/2003
- KEDR telemetry
- Ahnlab UTM – (Firewall, IPS, и т.д.)
- Broadcom Symantec Endpoint Protection
- Citrix NetScaler
- Eltex MES Switches
- Huawei Eudemon
- Kerio Control
- Minerva EDR
- PTsecurity ISIM
- PTsecurity Sandbox
- Radware DefensePro AntiDDoS
- Sophos XG
- PTC Winchill Fracas
- Конфидент Dallas Lock
- Bifit Mitigator
- Zecurion SW

KUMA — дальнейшее развитие

III кв. 2023

3.0

Редактор контента в виде кода (Web UI и API)

Автоматическое распознавание источника событий

Коннектор для API источников

Интеграция с MaxPatrol VM

Предустановленные дашборды для продуктов ЛК

Доработка интерфейса — возможность отправить правила на корреляторы

Расширение модели ассета (поддержка нескольких fqdn адресов для хостов)

Доработки коррелятора — мультимаппинг

Пересылка событий в сторонние системы в формате CEF

Исключение телеметрии продуктов ЛК из счетчика EPS

Развитие API

[возможны изменения] Доработки интерфейса — актуальный статус сервисов, список AL, сохранение истории поиска

[возможны изменения] Поддержка списков в полях

KUMA — дальнейшее развитие

I кв. 2024

3.1

Поддержка подписочных лицензий и онлайн-активация для MSSP

Поддержка многострочных событий и событий с повторяющимися полями

Интеграция с RedCheck VM для импорта активов и уязвимостей

Контент (правила корреляции, отчеты, дашборды) для соответствия требованиям КИИ и банковского сектора

Доработки интерфейса – организация сохраненных поисковых запросов в виде папок

Сертификация ФСТЭК, РБ

[возможны изменения] Федеративный поиск по нескольким хранилищам

[возможны изменения] Гибкая ролевая модель

[возможны изменения] Трассировка использования ресурсов

Спасибо!