

KUMA 2.1

Kaspersky Unified Monitoring
and Analysis Platform

kaspersky

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



Корпоративная
безопасность

Кибербезопасность
на стыке IT / OT-систем



Kaspersky
Unified Monitoring
and Analysis
Platform



Промышленная
безопасность

XDR



Kaspersky
Symphony

XDR



Kaspersky
Industrial
CyberSecurity

Архитектура KUMA

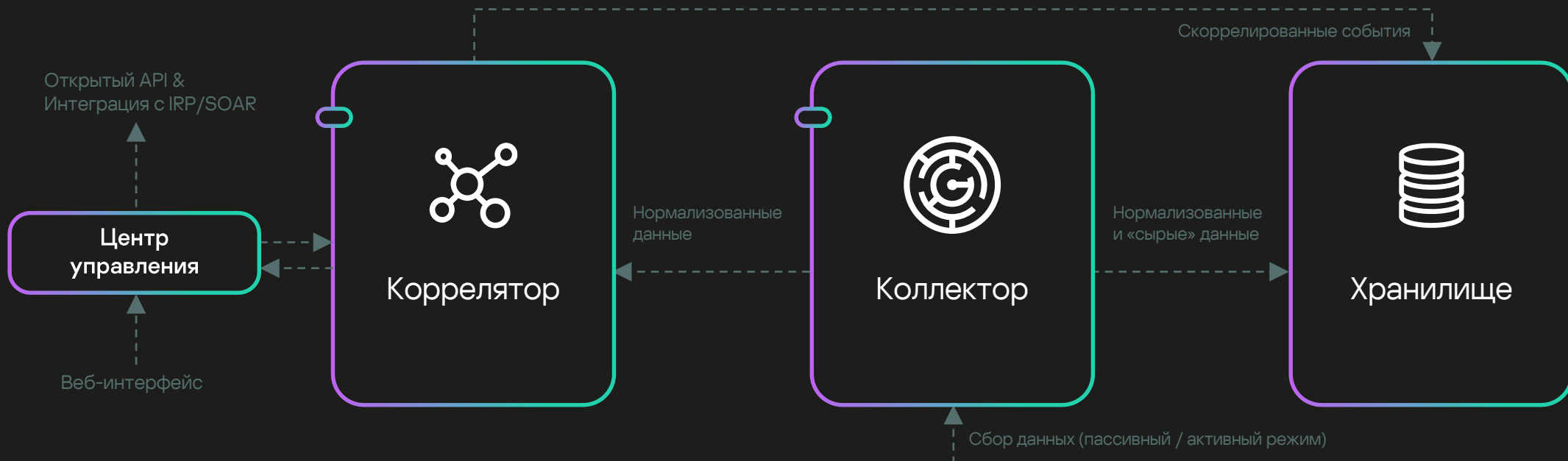
Архитектура KUMA

○ Взаимодействие

Оповещения и реагирование

Инвентаризация

Обогащение



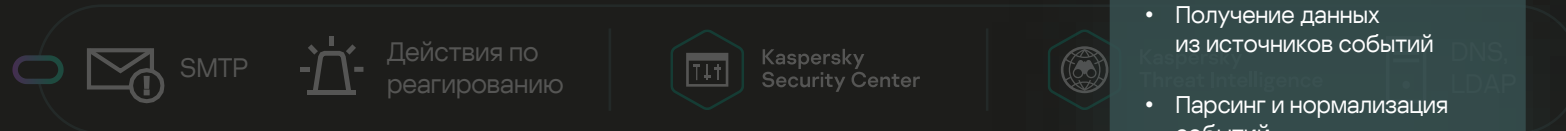
Архитектура KUMA

○ Взаимодействие

Оповещения и реагирование

Инвентаризация

Обогащение

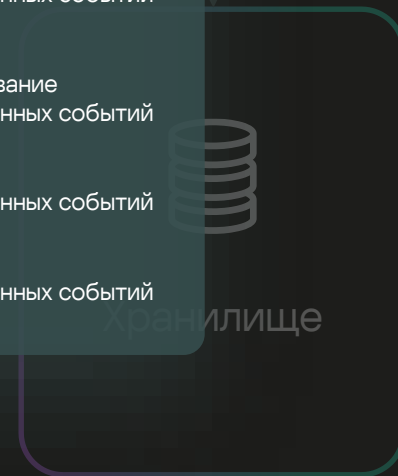
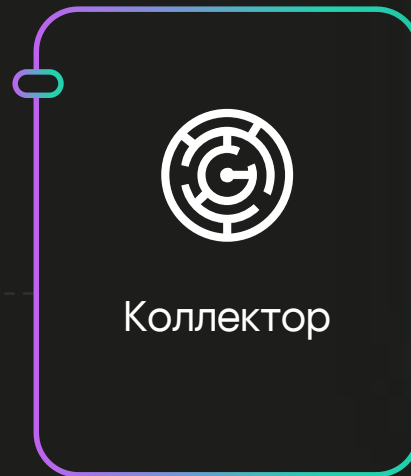
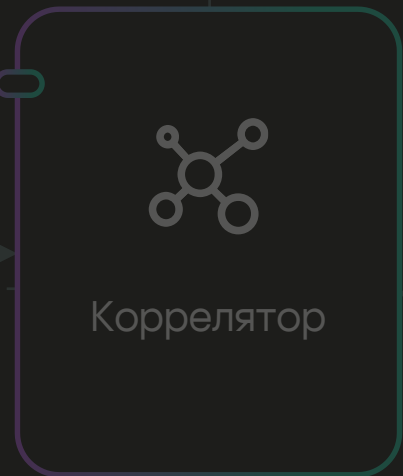


- Получение данных из источников событий
- Парсинг и нормализация событий
- Фильтрация нормализованных событий
- Обогащение и преобразование нормализованных событий
- Агрегация нормализованных событий
- Передача нормализованных событий

Открытый API & Интеграция с IRP/SOAR

Центр управления

Веб-интерфейс



Нормализованные данные

Сбор данных (пассивный / активный режим)

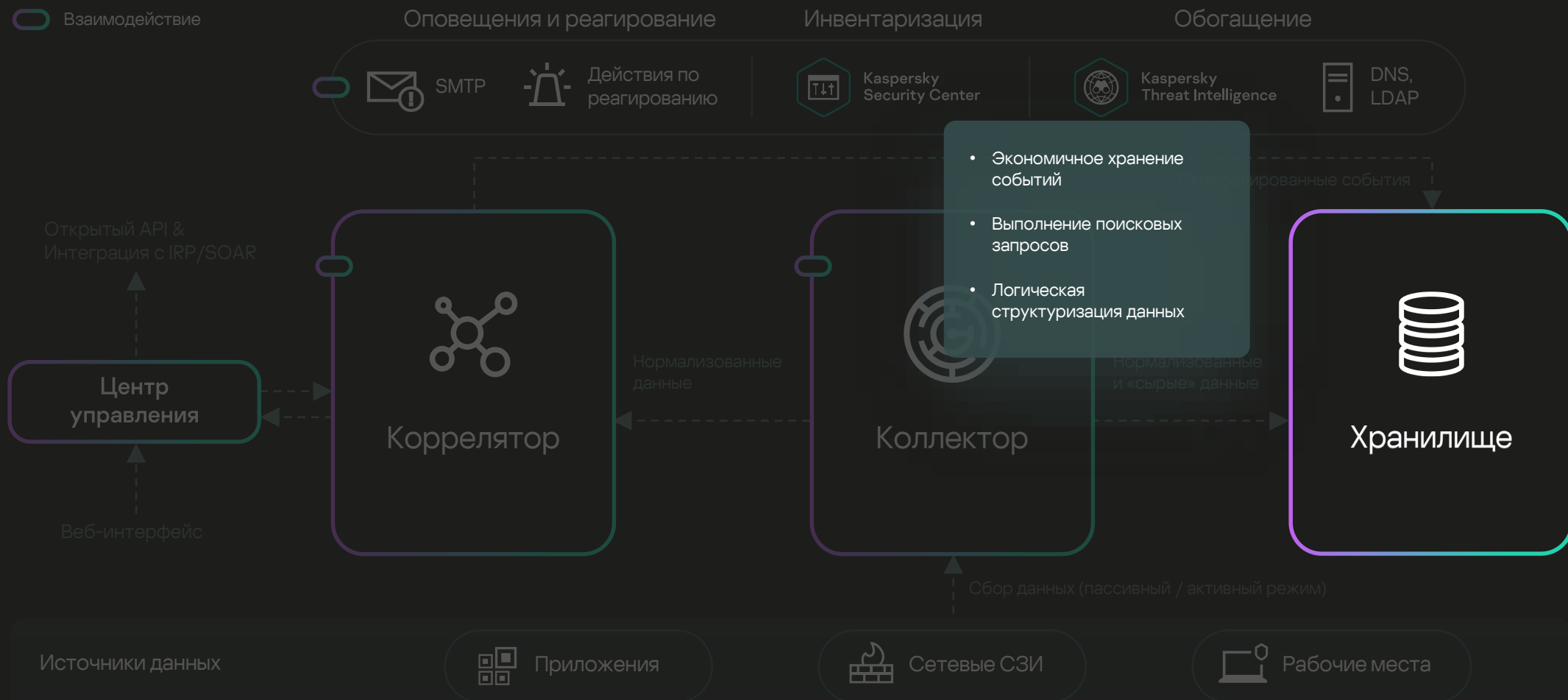
Источники данных

Приложения

Сетевые СЗИ

Рабочие места

Архитектура KUMA



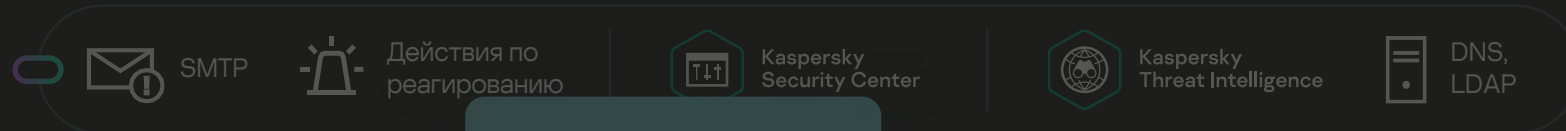
Архитектура KUMA

Взаимодействие

Оповещения и реагирование

Инвентаризация

Обогащение



- Корреляция событий
- Обогащение
- Взаимодействие с внешними системами для реагирования
- Маршрутизация корреляционных событий

Открытый API & Интеграция с IRP/SOAR

Центр управления

Коррелятор

Коллектор

Хранилище

Веб-интерфейс

Источники данных

Приложения

Сетевые СЗИ

Рабочие места

Сбор данных (пассивный / активный режим)

Нормализованные и «сырые» данные

Скоррелированные события

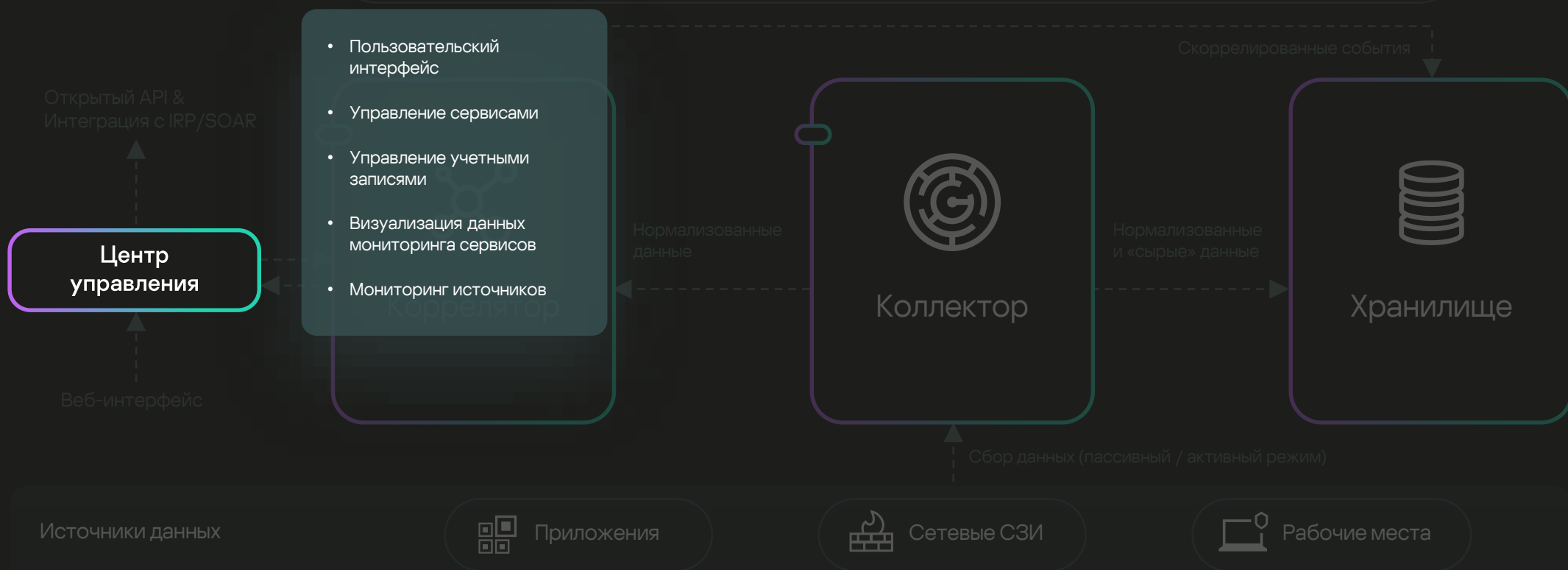
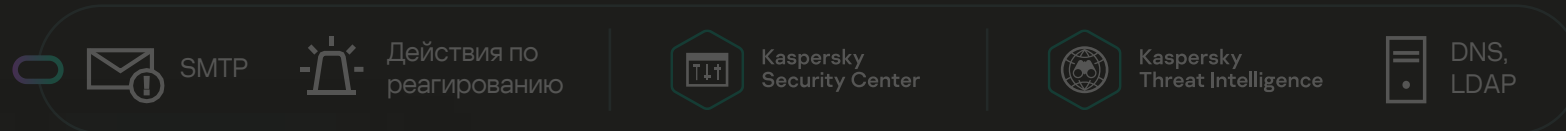
Архитектура KUMA

○ Взаимодействие

Оповещения и реагирование

Инвентаризация

Обогащение



Программное обеспечение с ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

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

Поддерживаемые способы сбора и получения СОБЫТИЙ

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

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.

Операционные системы

Windows, Linux, FreeBSD

Интеграция IRP / SOAR

Security Vision, R-Vision

Коннекторы

TCP listener

NATS

File

SNMP

UDP listener

Kafka

SQL

WMI

Netflow v9/10

HTTP

sFlow

Netflow Ipfix

Нормалайзеры

JSON

CSV/TSV

Regexp
(регулярные выражения)

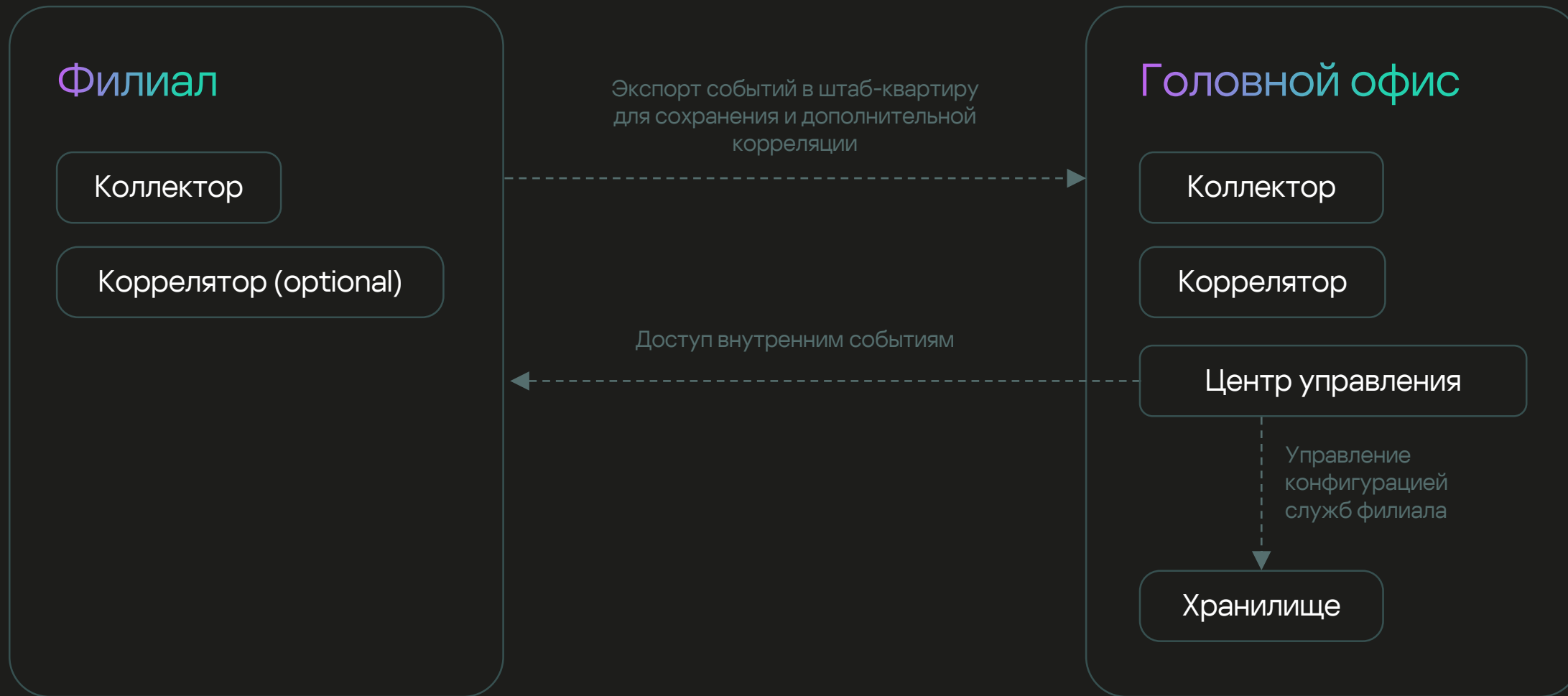
XML

CEF

Key/Value
ключ-значение

Syslog (RFC3164 & RFC5424)

Windows Event Log



Поддержка Multitenancy

Разделение данных,
конфигурации и прав доступа

Возможность ограничения EPS
для каждого тенанта отдельно

Целевой сценарий для MSSP
и центров ГосСОПКА

Тенанты

Показать отключенных

<input type="checkbox"/>	Название	Ограничение EPS	Описание	Выключено	Создан
<input type="checkbox"/>	test	0			1 сент. 2021 г. 13:07:25
<input type="checkbox"/>	Main	0			27 авг. 2021 г. 15:45:41

Добавить тенанта

Название

Ограничение EPS

Описание

Лицензирование

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

		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 ТАМом 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 по:

FQDN

IP

CVE

ОС

Версия билда ОС

Логические операторы AND, OR, NOT и группировки

Возможность проверки условий

Изменить категорию [X]

*Название
Windows

*Родительская категория
Main/Categorized assets/OS

*Тенант
Main

*Способ категоризации
Активно

*Уровень важности
Низкий

Описание
Описание

Автоматическая категоризация выключена

*Регулярность категоризации
1ч

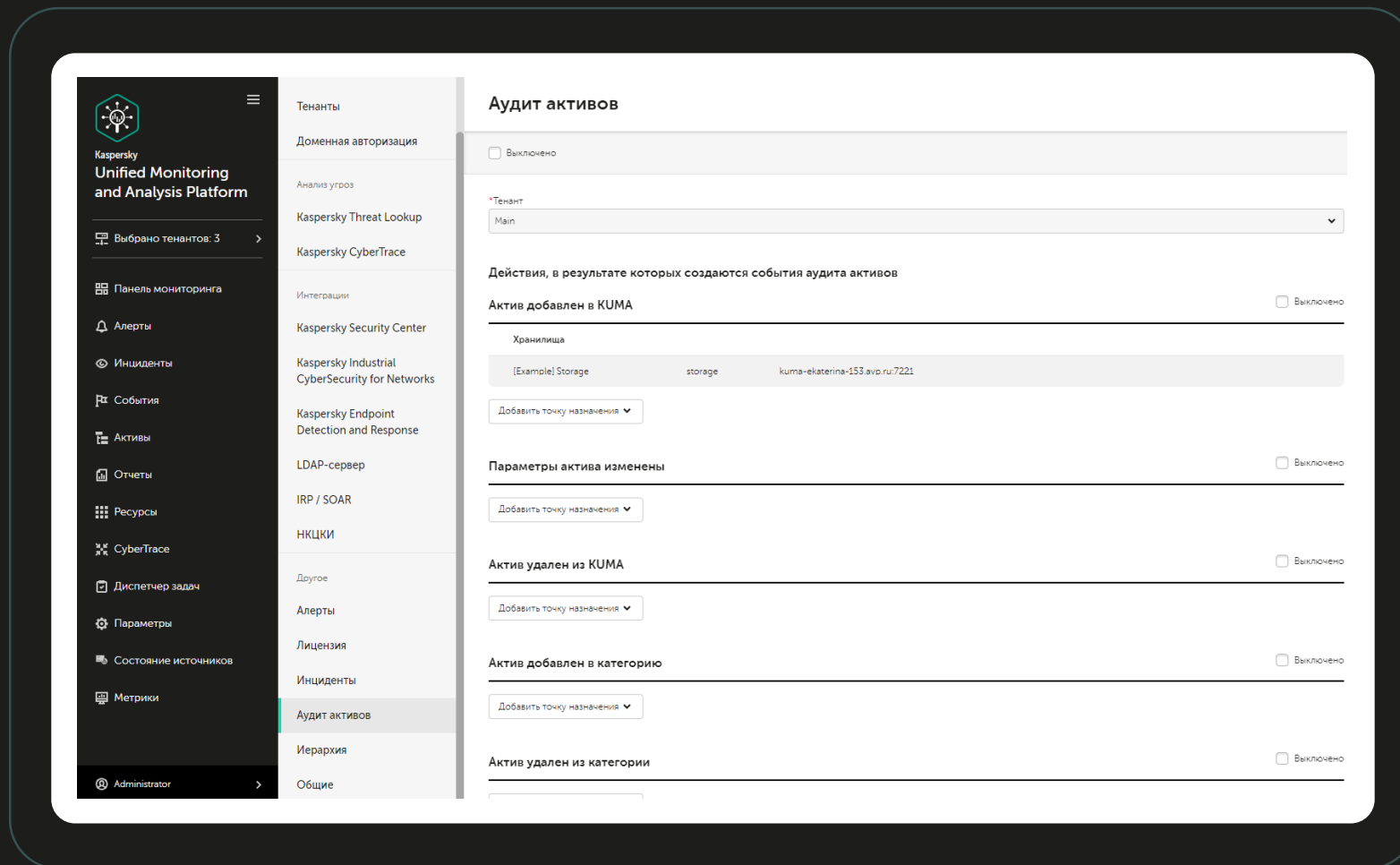
*Условия
И + Добавить условие + Добавить группу
Если ОС like Windows

Проверить условия

События аудита
для каждого тенанта

Можно направить
в коррелятор
и создавать алерты
на появление
уязвимостей

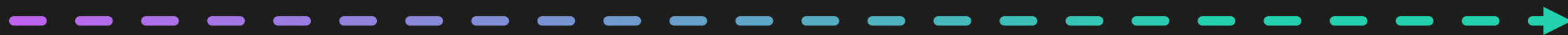
Можно строить
графики анализа
состояния активов



Пример 2. Сбор и анализ расширенной телеметрии



Пример 3. Потокное «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

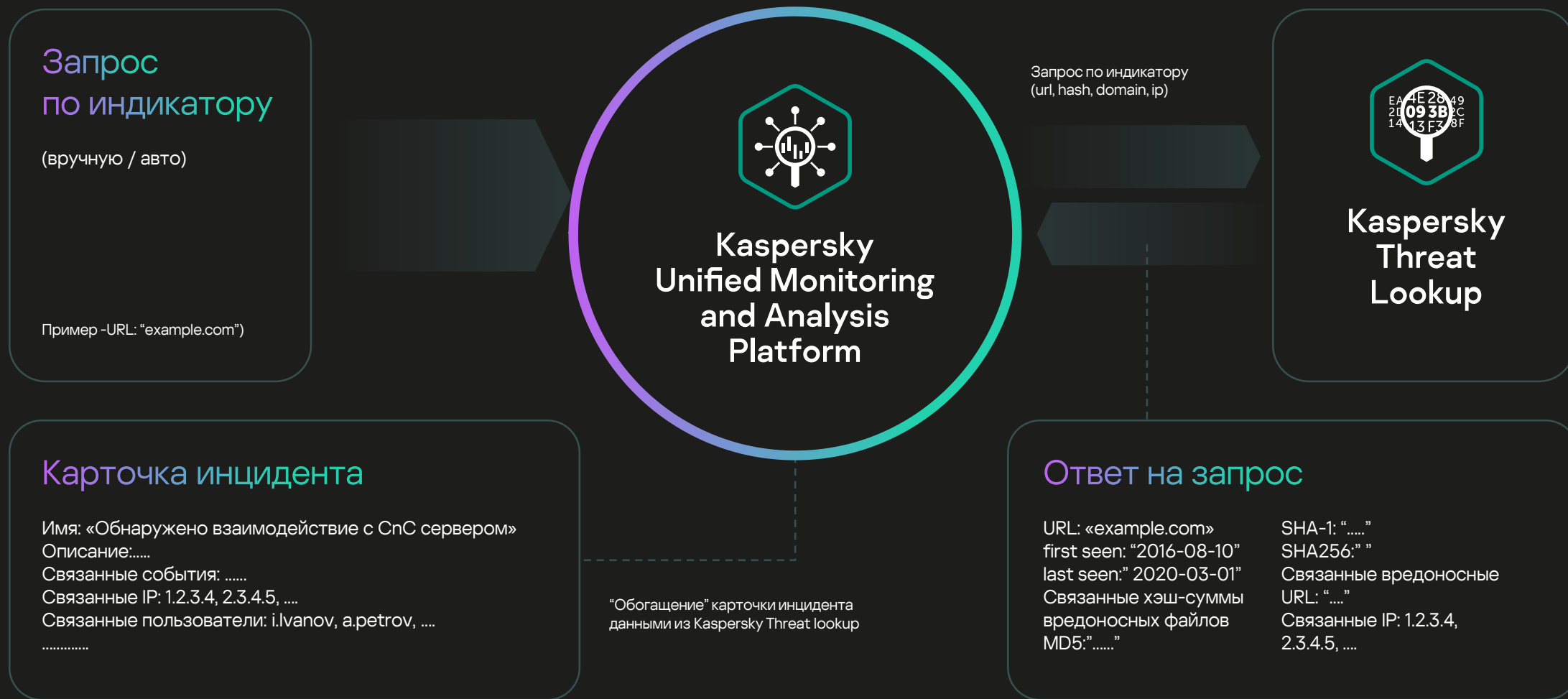
Correlator



Kaspersky Unified Monitoring and Analysis Platform

«Обогащенные» события

Пример 4. «Обогащение» событий по запросу



Реагирование из карточки

Перемещение в группу
администрирования
(влияет на политику
антивируса)

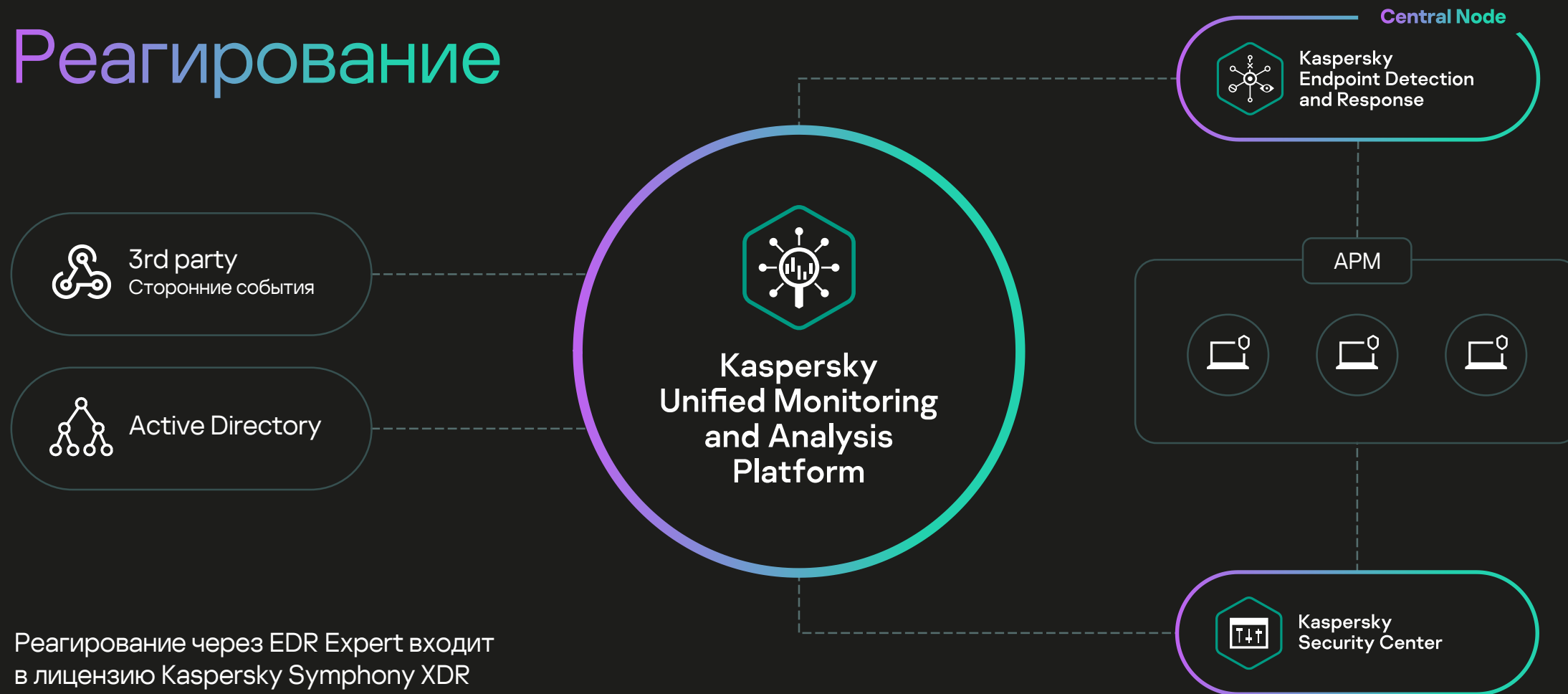
Установка патчей
для уязвимостей

The image shows a sequence of three overlapping screenshots from the Kaspersky Security Center (KSC) interface, illustrating the process of reacting to vulnerabilities from a card.

- Top Screenshot: "Информация об активе"** (Asset Information). It shows details for an asset named "KSC13-WIN2016-2" with a tenant named "Main". Buttons for "Удалить", "Изменить", and "Переместить" are visible.
- Middle Screenshot: "Выберите группу"** (Select group). It shows a list of groups under "Уязвимости Kaspersky Security Center". Two groups are selected: "KLA12206 в Mozilla Firefox 83.0 (x64 en-US)" and "KLA12448 в Mozilla Firefox 83.0 (x64 en-US)".
- Bottom Screenshot: "Сведения об обновлениях"** (Update details). It shows a table of updates to be installed. A blue banner states: "Выбранные обновления будут установлены на все активы с уязвимостями, принадлежащими серверу KSC, где было обнаружено актив с уязвимостью, а также всем его дочерним серверам KSC." The table lists updates for Mozilla Firefox 100.0 on server "ksc13-win2016-2.avp.ru".

<input type="checkbox"/>	Идентификаторы уязвим...	Название	Лицензионное соглашен...	Статус обновления	Сервер KSC	Название пр...
<input type="checkbox"/>	KLA12029, KLA12033, KLA12050...	Mozilla Firefox 100.0	Да	Нет решения	ksc13-win2016-2.avp.ru	Mozilla Firefox
<input type="checkbox"/>	KLA12029, KLA12033, KLA12050...	Mozilla Firefox 100.0	Да	Нет решения	ksc13-win2016-2.avp.ru	Mozilla Firefox
<input type="checkbox"/>	KLA12029, KLA12033, KLA12050...	Mozilla Firefox 100.0	Да	Нет решения	ksc13-win2016-2.avp.ru	Mozilla Firefox
<input type="checkbox"/>	KLA12029, KLA12033, KLA12050...	Mozilla Firefox 100.0	Да	Нет решения	ksc13-win2016-2.avp.ru	Mozilla Firefox

Реагирование



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

The screenshot displays the Kaspersky Unified Monitoring and Analysis Platform interface. The main window shows a list of assets under the 'Активы' (Assets) section. A modal window titled 'Информация об активе' (Asset Information) is open, showing details for a specific asset.

Название	Создан	Последнее обновление
*	24.05.2022 15:35:20	07.06.2022
* (1)	24.05.2022 15:35:20	07.06.2022
* (2)	24.05.2022 15:35:20	07.06.2022
* (3)	24.05.2022 15:35:20	07.06.2022
* (4)	24.05.2022 15:35:20	07.06.2022
* (5)	24.05.2022 15:35:20	07.06.2022
* (6)	24.05.2022 15:35:20	07.06.2022
* (9) - тест	24.05.2022 15:35:20	07.06.2022
0	24.05.2022 15:35:20	07.06.2022
0 A K S (1)	24.05.2022 15:35:20	07.06.2022
0 A K S_edited	24.05.2022 15:35:20	07.06.2022
0 K N S	24.05.2022 15:35:20	07.06.2022
0 K N S (1)	24.05.2022 15:35:20	07.06.2022
1	13.04.2022 11:42:50	13.04.2022
1	07.06.2022 10:57:10	07.06.2022

Информация об активе

Статус: KICS for Networks
Разрешенное

Идентификатор: 173de63b-105c-4e64-896f-b3b0c4665524

Создано: 24.05.2022 15:35:20

Последнее обновление: 07.06.2022 22:22:28

IP-адрес сервера KICS for Networks: 10.70.75.65

Идентификатор компонента KICS for Networks: 2

IP-адрес: 160.40.55.236

MAC-адрес: 3c:95:09:20:95:02

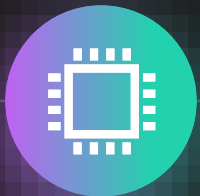
Операционная система: Windows 8

Уязвимости KICS for Networks

- Разрешенное устройство неактивно
- Категория: Небезопасная архитектура сети, CVSS: 6.5, Идентификатор: 745
- Описание: Устройство * (1), которому присвоен статус Разрешенное, не проявляет активность длительное время.

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

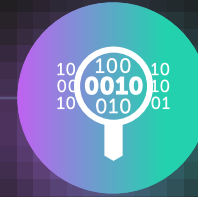
Запуск скрипта



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.

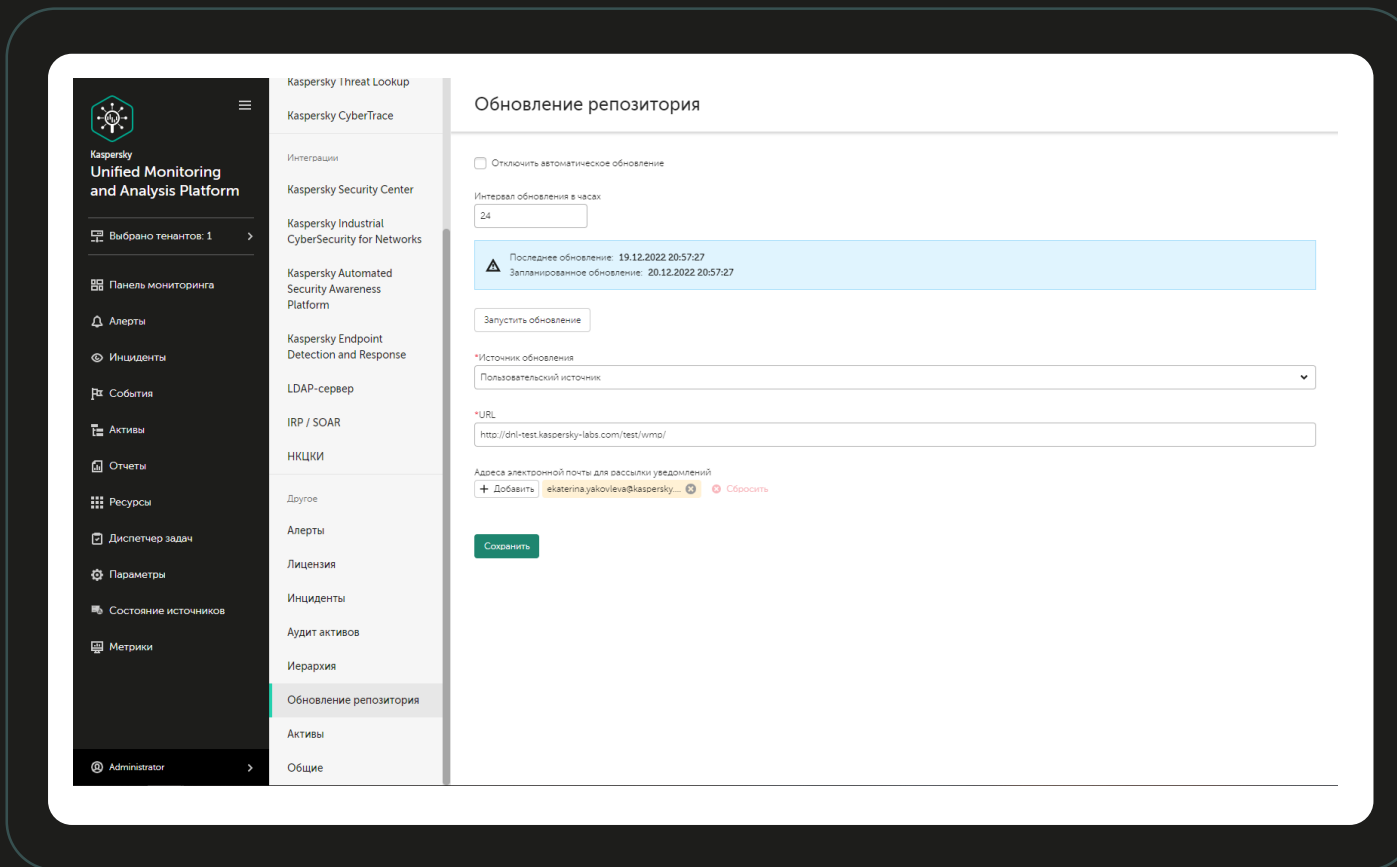
Выдан: 28 сентября 2021 г.
Действителен до: 28 сентября 2026 г.

Переоформлен: 7 ноября 2022 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 техническим условиям 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 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».

The screenshot displays the Kaspersky Unified Monitoring and Analysis Platform interface. The main window is titled 'Ресурсы и сервисы' (Resources and Services) and is divided into several sections:

- Сервисы (Services):** Includes 'Активные сервисы' (Active Services) and 'Подключить источник' (Connect Source).
- Ресурсы (Resources):** Includes 'Импортировать ресурсы' (Import Resources), 'Правила корреляции' (Correlation Rules), 'Точки назначения' (Destinations), and 'Словари' (Dictionaries).
- Импорт ресурсов > Репозиторий (Import Resources > Repository):** This section is currently active and shows a table of available packages for import. The table has columns for 'Название' (Name), 'Дата выпуска' (Release Date), 'Версия' (Version), and 'Установленная версия' (Installed Version). The packages listed are: 'Все ресурсы' (All Resources), 'Словари с новой тулзы' (Dictionaries with new tools), 'Package пакет с ресу...' (Package with resources), and 'OOTB package'.
- Импорт ресурсов > Репозиторий (Modal Window):** This modal window provides detailed information about a selected package. It includes fields for 'Тенант' (Tenant), 'Источники импорта' (Import Sources), and 'Репозиторий' (Repository). It also displays the 'Пакеты репозитория' (Repository Packages) table and a 'Журнал изменений' (Change Log) section.

The 'Package Information' modal window shows the following details:

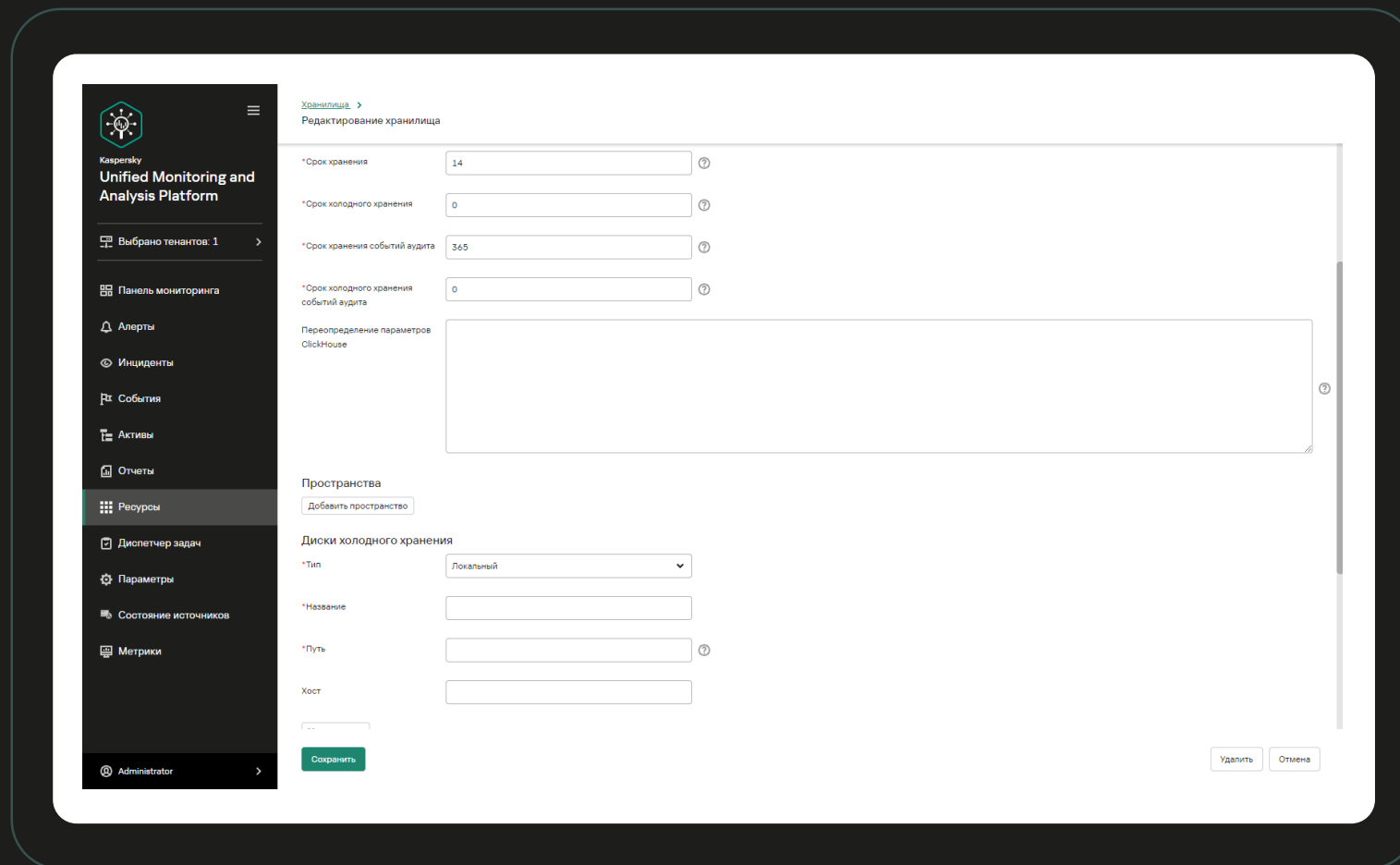
- Описание (Description):** Package with out of the box resources.
- Дата выпуска (Release Date):** 19.12.2022 20:57:26
- Версия (Version):** 1
- Установленная версия (Installed Version):** Не установлен (Not installed)
- Количество ресурсов (Number of Resources):** 108
- Журнал изменений (Change Log):** Будут импортированы следующие ресурсы: (The following resources will be imported:)
- Все ресурсы (All Resources):** Коннектовы, Нормализаторы, [OoTB] Fortimail, [OoTB] Syslog, [OoTB] IPFIX, [OoTB] NetFlow v9, [OoTB] aSense Syslog, [OoTB] regexl Continet IPS/IDS 6-TLS, [OoTB] Juniper - JUNOS, [OoTB] MS DHCP file, [OoTB] CEF, [OoTB] Windows Extended v0.3, [OoTB] Apache Access file/Common or Combined Log Format, [OoTB] NetFlow v5.

Дополнительный этап хранения событий

Оптимизация стоимости оборудования за счет **разделения хранения** этапов.

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:

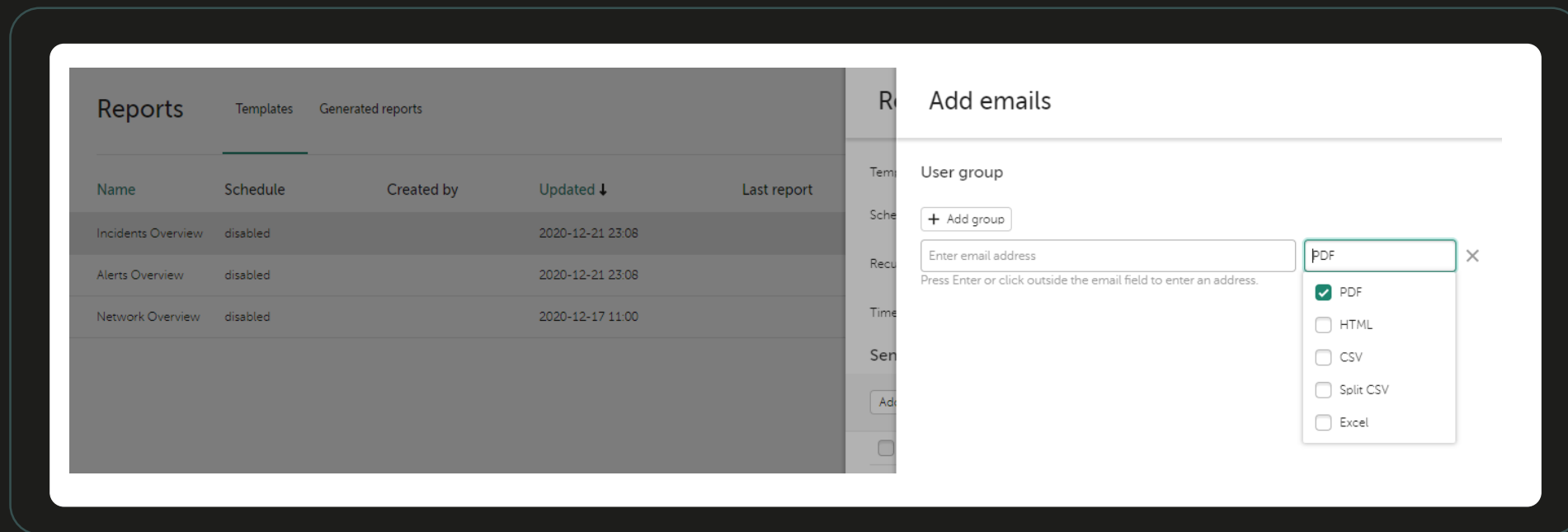
HTML

PDF

CSV

раздельный CSV

Excel



Синхронизация статусов инцидентов

Категоризация активов в соответствии с КИИ-категориями

Возможность приложить файл к инциденту

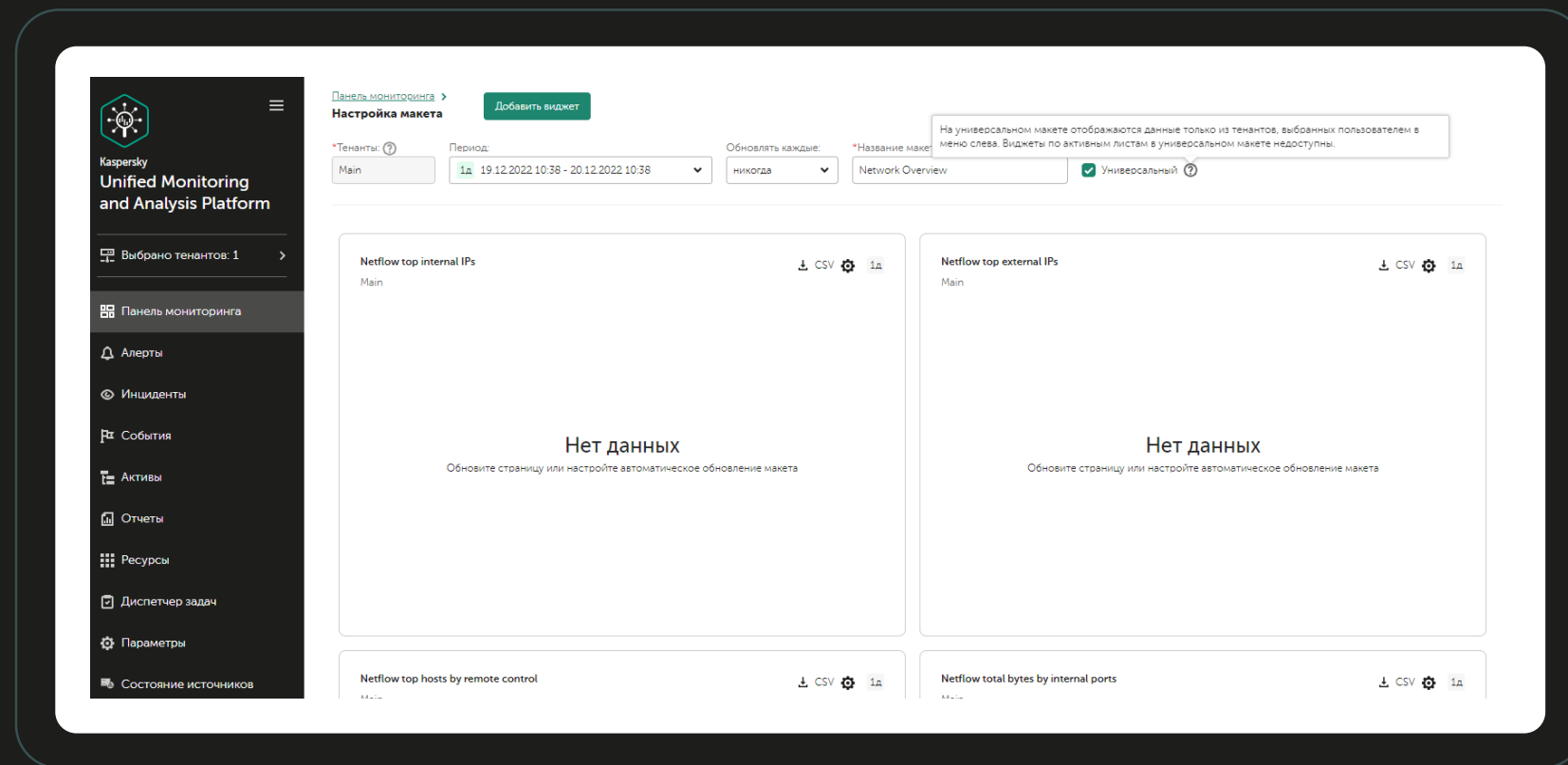
Интерактивный чат со специалистами НКЦКИ

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

Единые для
всех тенантов
(общие)
шаблоны
дашбордов

Скачивание
данных в CSV



Новые интеграции для реагирования*

KASAP:

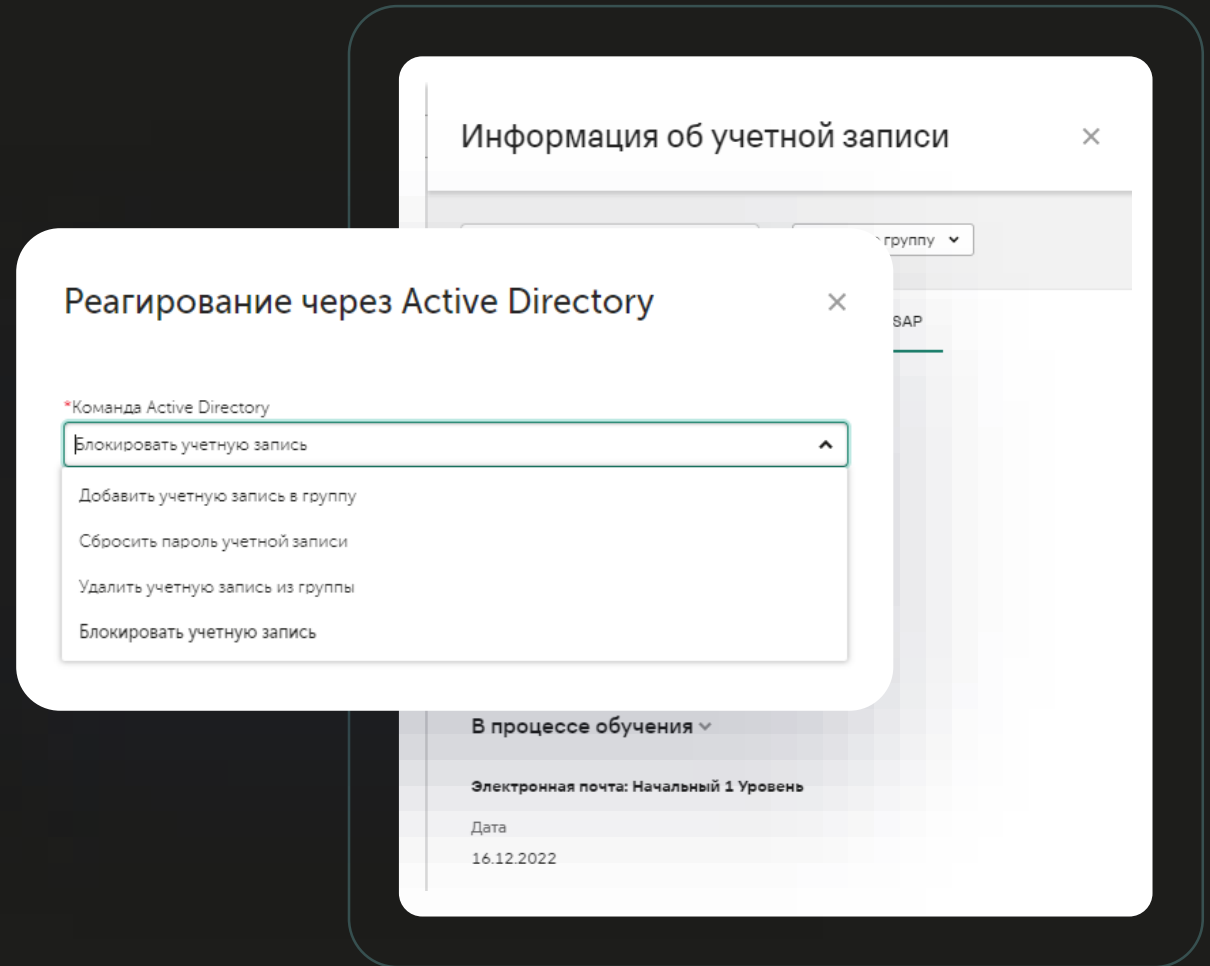
Информация по результатам обучения

Записать пользователя на курс

Active Directory:

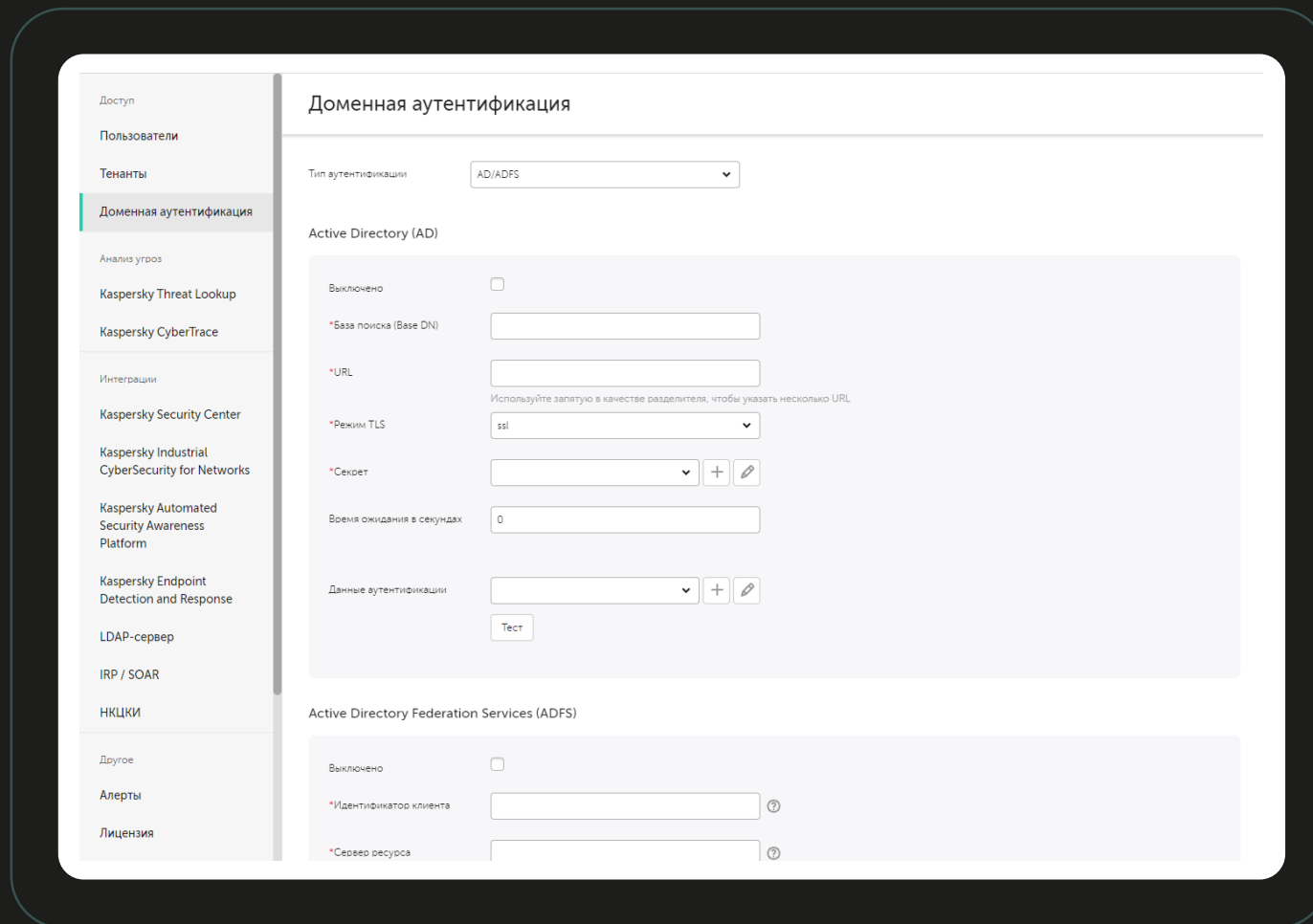
Управление группами (добавить-удалить)

Сброс пароля
Блокировка УЗ

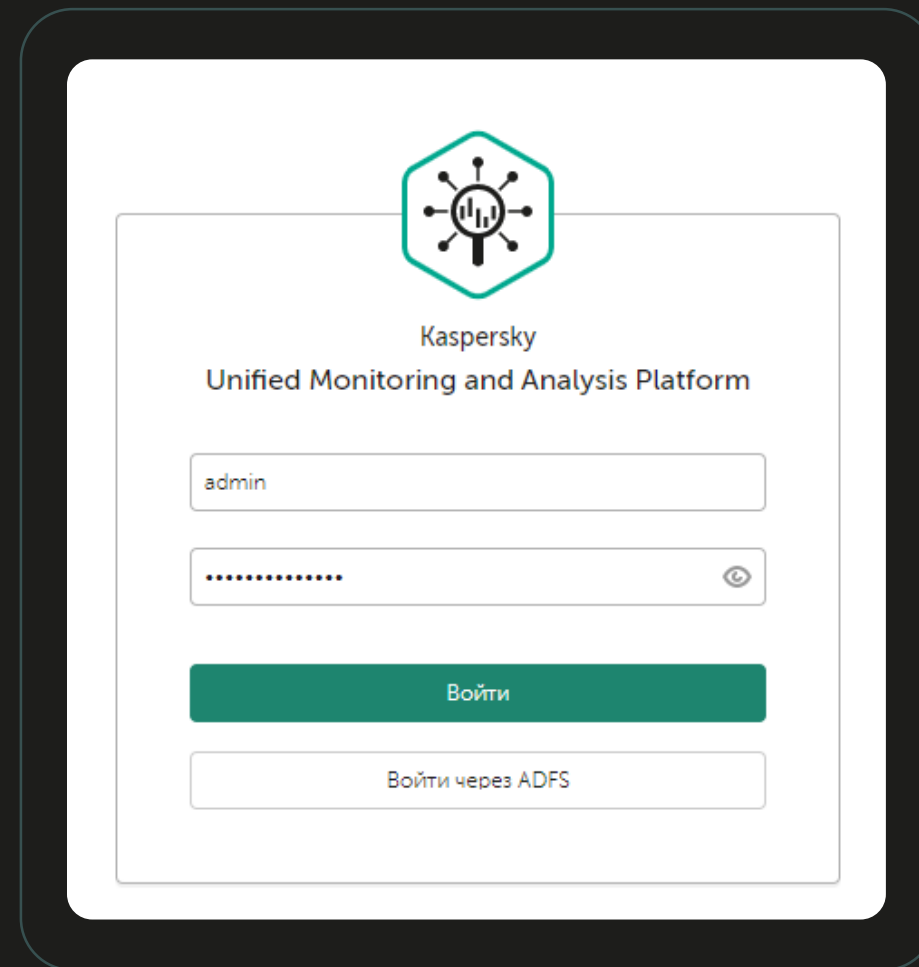


* Доступно только в лицензии Kaspersky Symphony XDR

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

The image displays a user interface for managing assets. The main window is titled 'Активы' and contains a section for 'Настраиваемые поля' (Custom Fields) with a table and a 'Добавить поле' (Add Field) button. A modal window titled 'Изменить актив' (Edit Asset) is overlaid on top, showing various fields for asset configuration. The modal includes a dropdown for 'Тенант' (Tenant), text inputs for 'IP-адрес' (IP Address), 'Полное доменное имя' (Full Domain Name), 'MAC-адрес' (MAC Address), 'Владелец' (Owner), 'Категория' (Category), 'Категория КИИ' (Category of Critical Information Infrastructure), 'Название ОС' (OS Name), and 'Версия ОС' (OS Version). There are also sections for 'Настраиваемые поля' and 'Программное обеспечение' (Software) with a 'kaspersky_custom_field' entry. A 'Сохранить' (Save) button is visible at the bottom of the modal.

Активы

Подробнее о пользовательских полях активов с

При удалении настраиваемых полей также уд

Настраиваемые поля

Название	Маска
⋮ kaspersky_custom_field	RE2)

Добавить поле

Сохранить

Изменить актив

*Тенант: Main

IP-адрес: 10.68.70.210
Можно задать несколько IP-адресов, указав их через запятую

Полное доменное имя: kes-win-new.avp.ru

MAC-адрес: 5e:4d:00:01:7d:c8
Можно задать несколько MAC-адресов, указав их через запятую

Владелец:

Категории: [Icon]

Категория КИИ: Информационный ресурс не является объектом КИИ

Настраиваемые поля

kaspersky_custom_field: value

Программное обеспечение

Название ОС: Microsoft Windows 10

Версия ОС: 19045.000000

Сохранить Отмена

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

The screenshot displays the 'Активы' (Assets) management interface. The main area shows a list of assets with search filters applied: 'ОС' (OS) and 'Windows' (using the 'like' operator), and 'Последнее обновление' (Last updated) on or before '2022-12-20 11:36:50'. A calendar overlay is visible, showing the date '2022-12-20' selected. The interface includes a left sidebar for tenant selection, a top navigation bar with 'Добавить актив' (Add asset) and 'Импортировать активы KSC' (Import KSC assets) buttons, and a bottom bar with 'Добавить категорию' (Add category), 'Переместить в группу KSC' (Move to KSC group), 'Экспортировать CSV' (Export CSV), and 'Привязать к категории' (Link to category) buttons.

дек. 2022							11:36:50		
пнд	втр	срд	чтв	птн	сбт	вск	11	36	50
28	29	30	1	2	3	4	12	37	51
5	6	7	8	9	10	11	13	38	52
12	13	14	15	16	17	18	14	39	53
15	16	17	18	19	20	21	15	40	54
19	20	21	22	23	24	25	16	41	55
26	27	28	29	30	31	1	17	42	56
2	3	4	5	6	7	8	18	43	57

Обновленные правила агрегации алертов

46

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

Правила сегментации >
Редактирование правила сегментации

*Название: by DestinationAddress

*Тенант: Общий

*Тип: По группирующим полям

*Группирующие поля правила корреляции: + Добавить поле DestinationAddress ×
× Сбросить

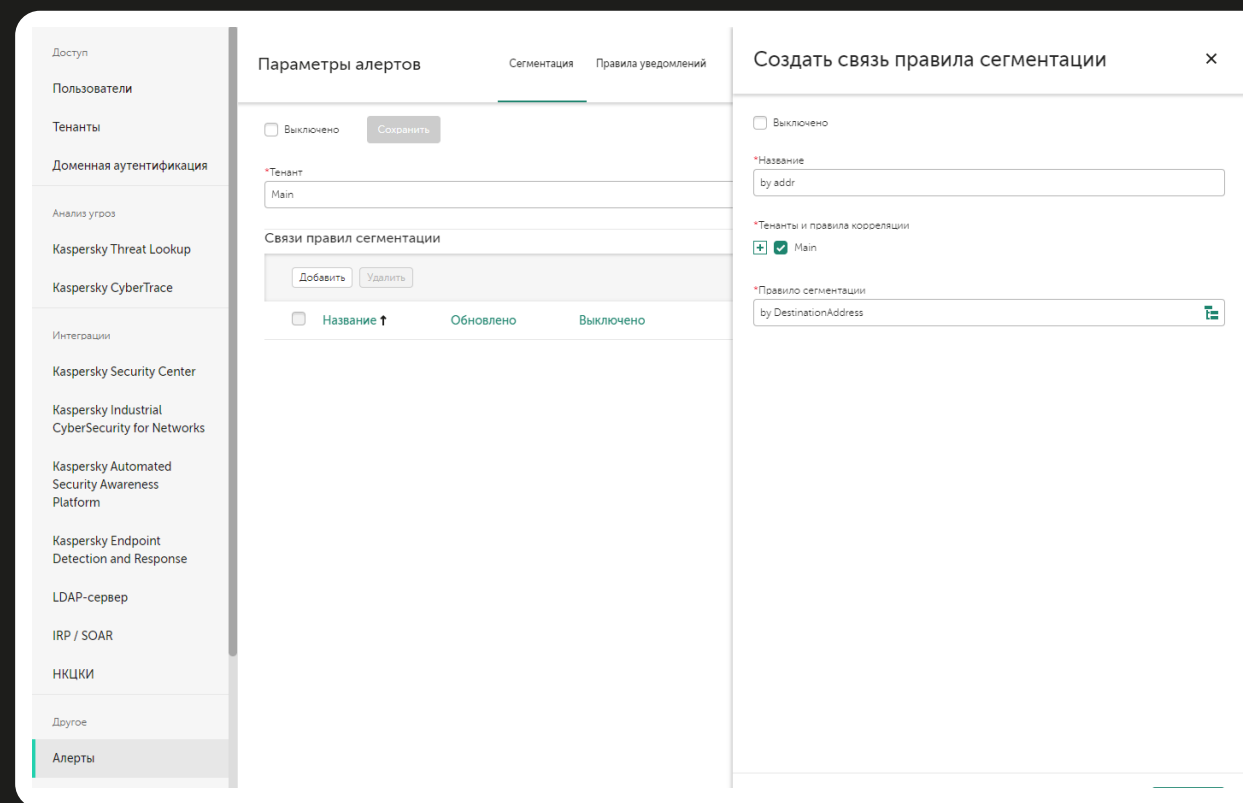
*Шаблон именования алертов: {{.DestinationAddress}} - {{.Timestamp}}

Описание:

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

The image shows a screenshot of a security management interface. On the left, a panel titled "Информация об активе" (Active Information) displays various security status indicators for a device. On the right, a modal window titled "Информация о событии" (Event Information) provides detailed data for a specific event, with several fields highlighted by red boxes.

Информация об активе

Удалить | Изменить | Переместить в группу KSC | За...

Расширенный статус KSC
Антивирусные базы обновлялись слишком давно

Идентификатор расширенного статуса KSC
OK

Статус постоянной защиты
Выполняется (если антивирусное приложение не поддерживает категорию...
Выполняется)

Статус шифрования
На хосте нет правил шифрования

Статус защиты от спама
Неизвестно

Статус антивирусной защиты почтовых серверов
Неизвестно

Статус защиты данных от утечек
Неизвестно

Статус Endpoint Sensor
Выполняется

Последнее обновление антивирусных баз
10.12.2022 11:08:00

Последнее обновление информации
20.12.2022 08:47:39

Последнее обновление защиты
20.12.2022 08:09:50

Информация о событии

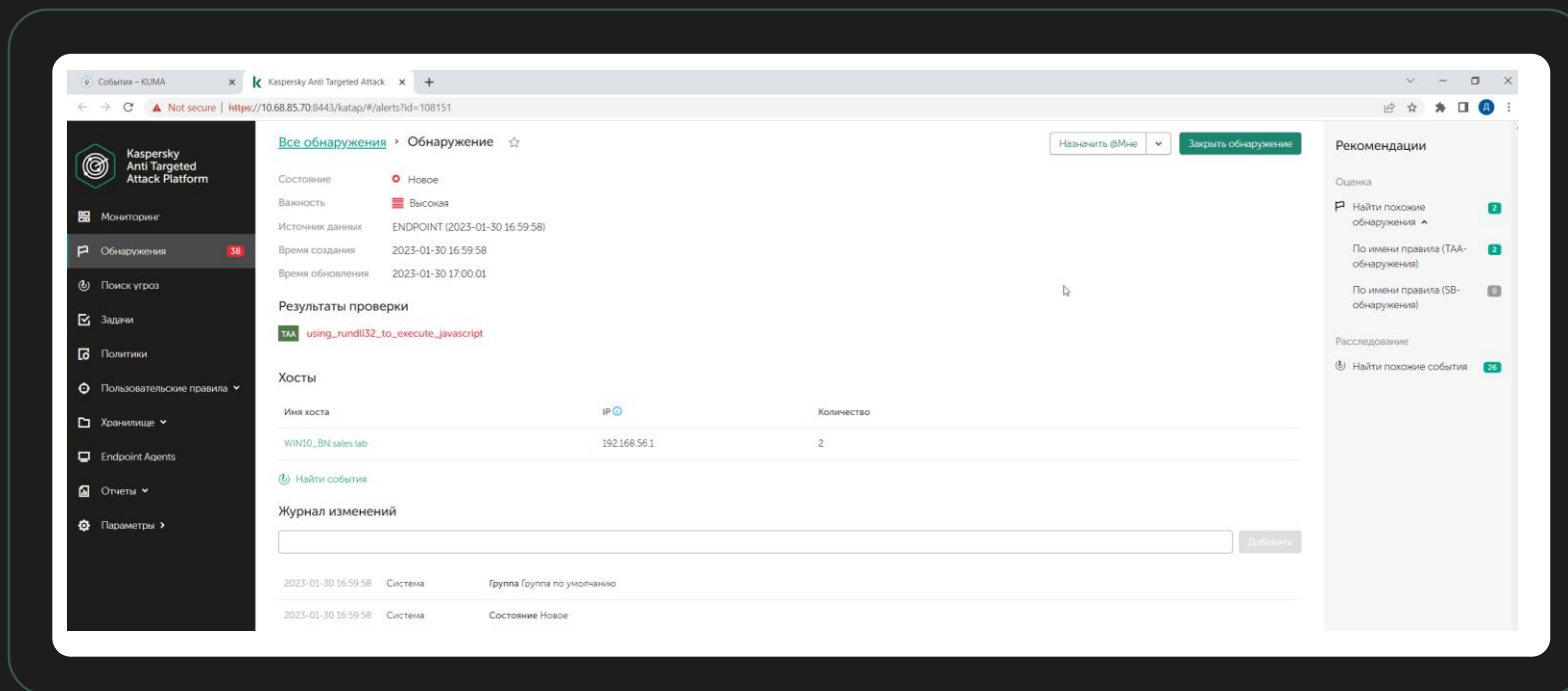
TenantName	Main
Timestamp	30.01.2023 16:59:58.405
Name	TAA has tripped on events database
EndTime	30.01.2023 16:59:58.405
DeviceAddress	10.68.85.70
DeviceAssetID	KATA_4.1
DeviceEventClassID	taaScanning
DeviceExternalID	https://10.68.85.70:8443/odata/#/Alerts?Id=108151
DeviceProduct	KATA
DeviceReceiptTime	30.01.2023 13:59:58.405
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
DeviceVersion	4.1.0-3484.4.1.0-3484
SourceAssetID	WIN10_BN
SourceHostName	WIN10_BN.sales.lab
DeviceCustomString1	using_rundll32_to_execute_javascript
DeviceCustomString6Label	SHA256
Service	KATA(TCP/5145)
EventOutcome	108151
Severity	High
Type	Base
Extra	version: CEF:0

Исходное событие

```
CEF:0|40 Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|4.1.0-3484|taaScanning|TAA has tripped on events database|High|dvc=10.68.85.70|deviceExternalId=KATA_4.1|eventId=108151|rt=Jan 30 2023 13:59:58|host=WIN10_BN.sales.lab|cs1=using_rundll32_to_execute_javascript
```


Расширенная интеграция KES/KEDR/КАТА

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



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



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



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!