kaspersky

Kaspersky Unified Monitoring and Analysis Platform

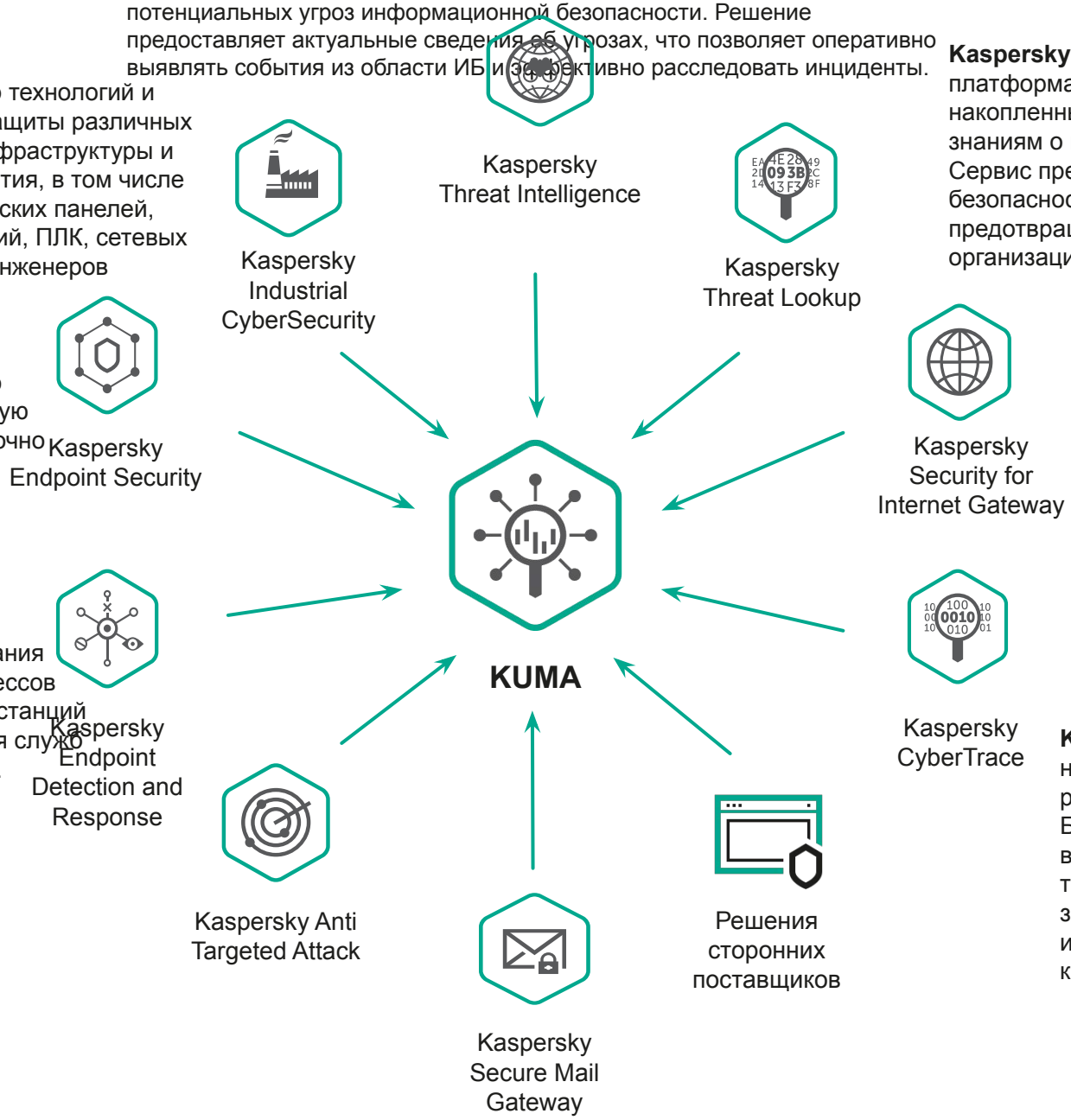
Pavel Taratynov
SOC Program Architect

Мониторинг и расследование инцидентов**Kaspersky Threat Intelligence** Portal (TIP) — сервис «Лаборатории **Касперского**», предназначенный для анализа потенциальных угроз информационной безопасности. Решение предоставляет актуальные сведения об угрозах, что позволяет оперативно выявлять события из области ИБ и эффективно расследовать инциденты.

Kaspersky Industrial CyberSecurity — **это** набор технологий и сервисов, созданных для защиты различных уровней промышленной инфраструктуры и других элементов предприятия, в том числе серверов SCADA, операторских панелей, инженерных рабочих станций, ПЛК, сетевых соединений и даже самих инженеров

Kaspersky Endpoint Security – **это** пакет программ для многоуровневой защиты любого предприятия. Вы можете подобрать подходящую версию, как для небольшого, так и для достаточно крупного предприятия.

Kaspersky Endpoint Detection and Response – **это** агентское решение для централизованного расследования и реагирования предлагающее автоматизацию ключевых процессов ИБ, глубинный мониторинг состояния рабочих станций в сети и средств цифровой криминалистики для служб ИБ и команд SOC (**Security** Operational Center).



Kaspersky Threat Lookup – **это** мощная единая платформа, открывающая доступ ко всем накопленным «Лабораторией **Касперского**» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет вашим специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред.

Kaspersky Security для **интернет**-шлюзов обеспечивает защиту корпоративной сети от всех видов **интернет**-угроз, включая загрузку вредоносного ПО, атаки с использованием эксплойтов через сайты-«рассадники» и кражу ученых данных через фишинговые сайты.

Единая консоль мониторинга и анализа инцидентов ИБ

Kaspersky CyberTrace предоставляет набор инструментов для эффективной работы с потоками данных об угрозах: База данных со всеми индикаторами с возможностью полнотекстового поиска, а также поддержкой сложных поисковых запросов для поиска по всем полям индикатора, включая поля, содержащие контекст.

Ключевые преимущества

Производительность

До 300k+ EPS на один узел

Количество событий в секунду - **EPS** (events per second)
Примерно такое количество событий в секунду поставляет каждый соответствующий компонент в ИТ-инфраструктуре заказчика.

Масштабируемость

- *Вертикальная и горизонтальная*
- **Вертикальное** — это когда добавляют больше оперативки, дисков и т. д. на уже существующий сервер, а **горизонтальное** — это когда ставят больше серверов в дата-центры, и сервера там уже как-то взаимодействуют.

Низкие системные требования

Ключевые преимущества (продолжение)

Тесная интеграция с Threat Intelligence

Интеграция из «коробки» с TI платформой CyberTrace и Kaspersky Threat Lookup

RESTful API

*Для работы с событиями, алертами, и активами**

REST API — это способ взаимодействия сайтов и веб-приложений с сервером.

Автоматическая инвентаризация сети

С помощью агентов KES **Агент администрирования** осуществляет взаимодействие между Сервером **администрирования** и программами «Лаборатории Касперского», установленными на рабочих станциях и серверах.

*Интеграция с сканнерами защищенности, CMDB**

CMDB помогает консолидировать, структурировать и наглядно представлять данные о средствах автоматизации, необходимые для управления ИТ-ресурсами и услугами

Автоматизированное реагирование

Через KSC, пользовательские скрипты
*Интеграция с KEDR**

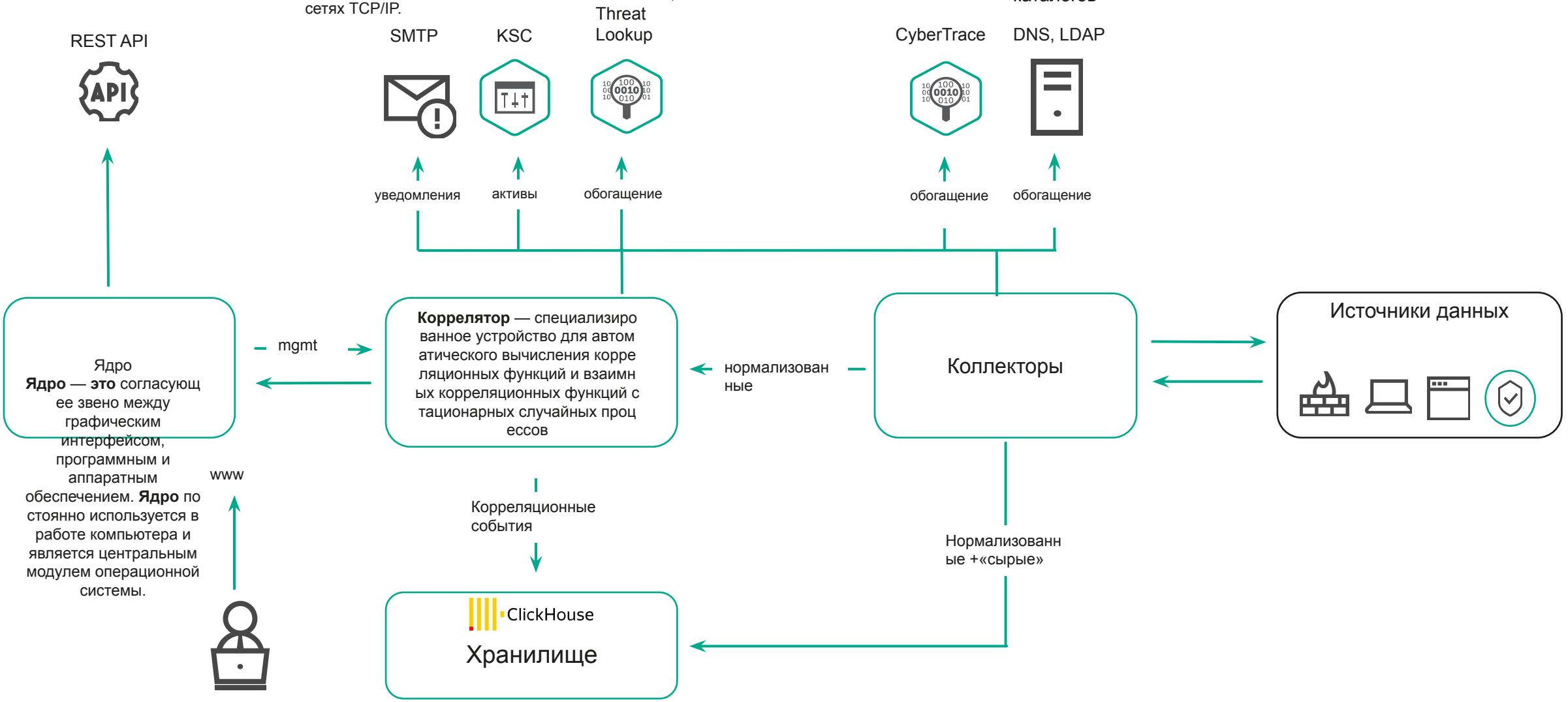
* Запланировано в рамках релизов Q3-Q4 2021

Архитектура KUMA

SMTP — это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP.

Kaspersky Security Center — это инструмент для централизованного управления комплексной системой защиты, который предоставляет администратору доступ к детальной информации об уровне безопасности корпоративной сети и позволяет гибко настраивать все компоненты системы защиты.

LDAP — протокол прикладного уровня для доступа к службе каталогов



Варианты развертывания

Инсталляция «Все-в-одном»

Подходит для инсталляций не требовательных к производительности и PoC.

- Виртуальная среда или физическая среда
- Все компоненты устанавливаются на один сервер
- Развертывание в течение 15 мин
- До 5-10 тыс. EPS

Распределенная инсталляция

Подходит для большинства типовых ИТ-инфраструктур

- Виртуальные машины или физические серверы
- Возможность установить локальный коррелятор и коллектор на удаленную площадку
- Возможность реализовать схемы отказоустойчивости и балансировки
- Централизованное управление через единую web-консоль

Иерархическая инсталляция*

Подходит для MSSP, организаций с дочерними обществами и/или смешанной организационной структурой.

- Виртуальные машины или физические серверы
- Несколько центральных и подчиненных площадок с сложно-подчиненной иерархией
- Поддержка мульти-тенантности
- Возможность гибкой настройки прав доступа к контенту и данным SIEM
- Локальные инсталляции SIEM на удаленных площадках

Примерный сайзинг (подбор оптимальной конфигурации аппаратного обеспечения для какой-либо информационной системы)

до 2k EPS, 30 дней хранения

All-in-one
- CPU – 12vCPU
- RAM – 32 ГБ;
- Storage – 4 ТБ

до 5k EPS, 180 дней

Коллектор+Коррелятор +Ядро:
- CPU – 16 vCPU
- RAM – 32 ГБ;
- Storage – 1,5 ТБ

Хранилище :
- CPU – 16 vCPU
- RAM – 32 ГБ;
- Storage – 20 ТБ

20k EPS, 365 дней

Ядро
- CPU: 8 vCPU
- RAM: 12 GB
- Disk: 500 GB

Коррелятор
- CPU: 8 vCPU
- RAM: 32 GB
- Disk: 500 GB

Zookeeper-3
- 4vcpu
- 6 RAM
- 50GB

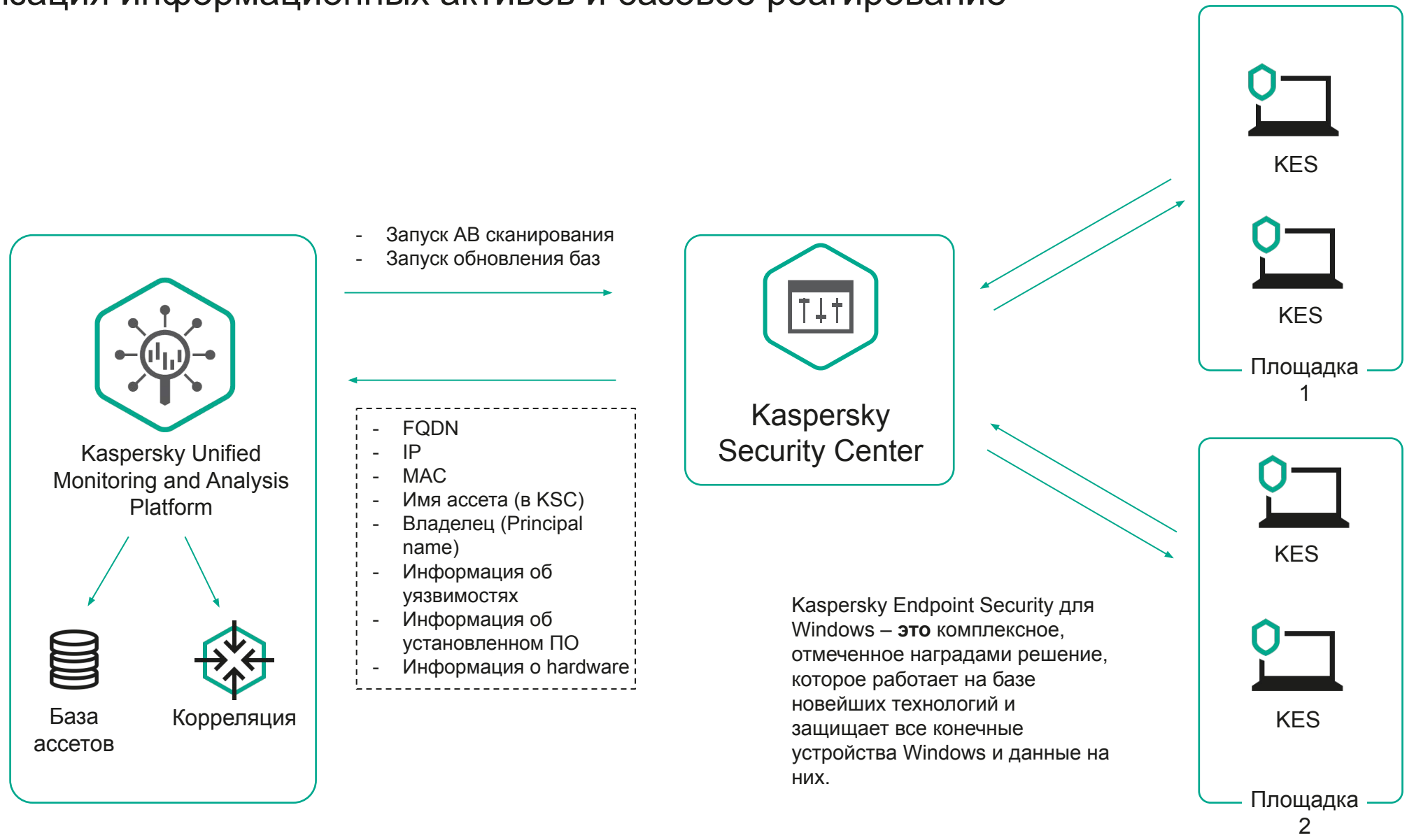
ZooKeeper - **это** централизованная служба для поддержки информации о конфигурации, именования, обеспечения распределенной синхронизации и предоставления групповых служб

Коллектор
- CPU: 8 vCPU

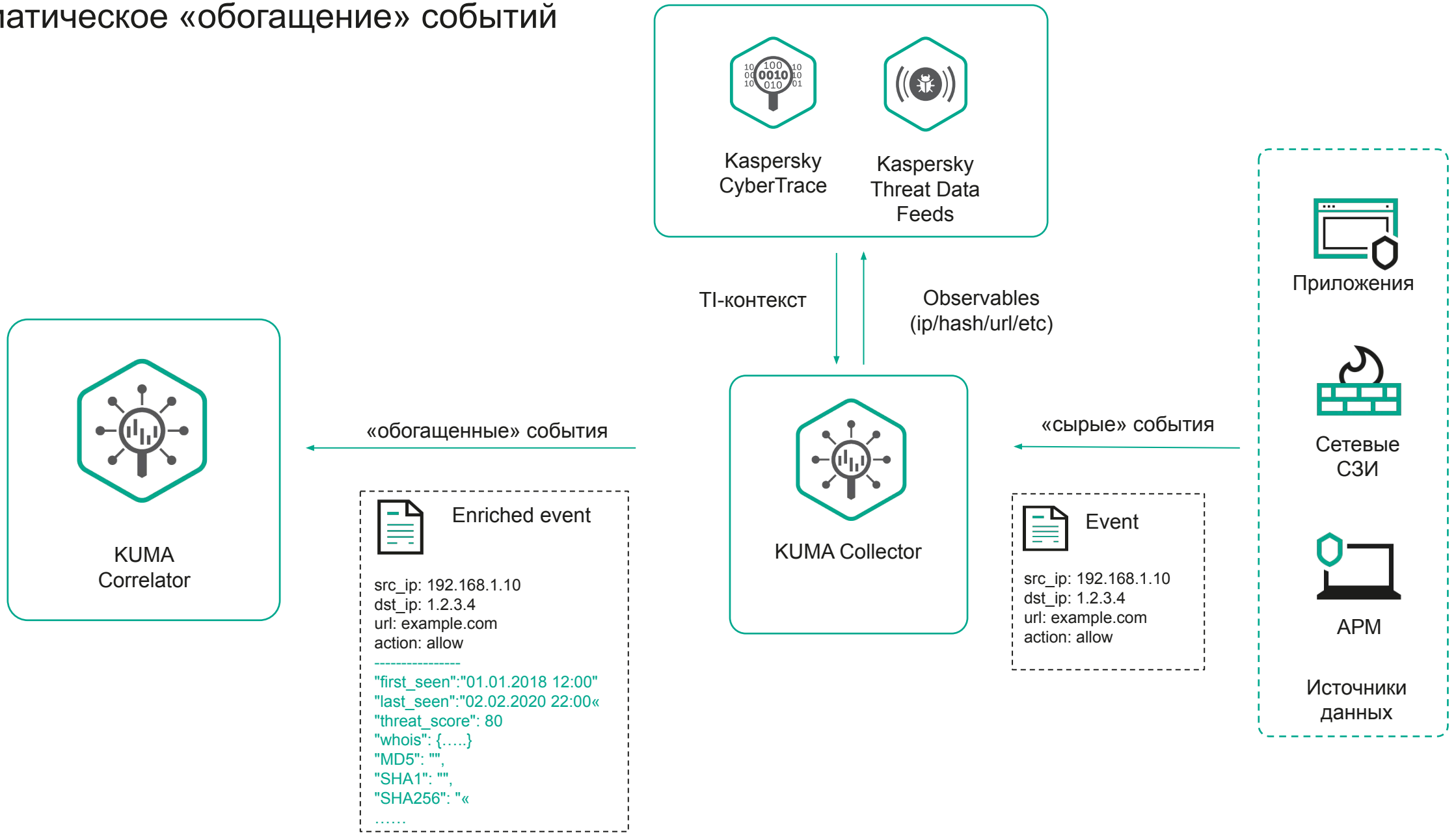
*объем хранилища зависит от длительности хранения событий

Интеграции «из коробки»

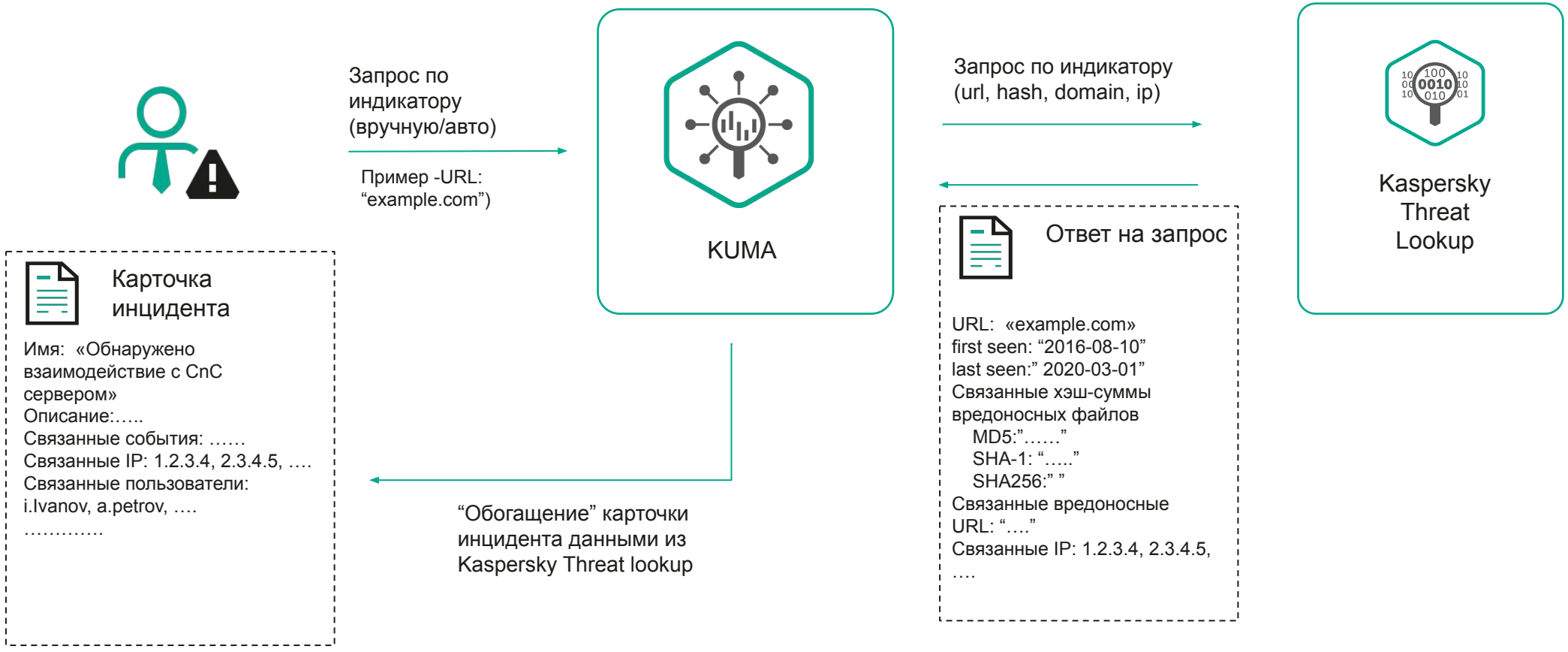
Инвентаризация информационных активов и базовое реагирование



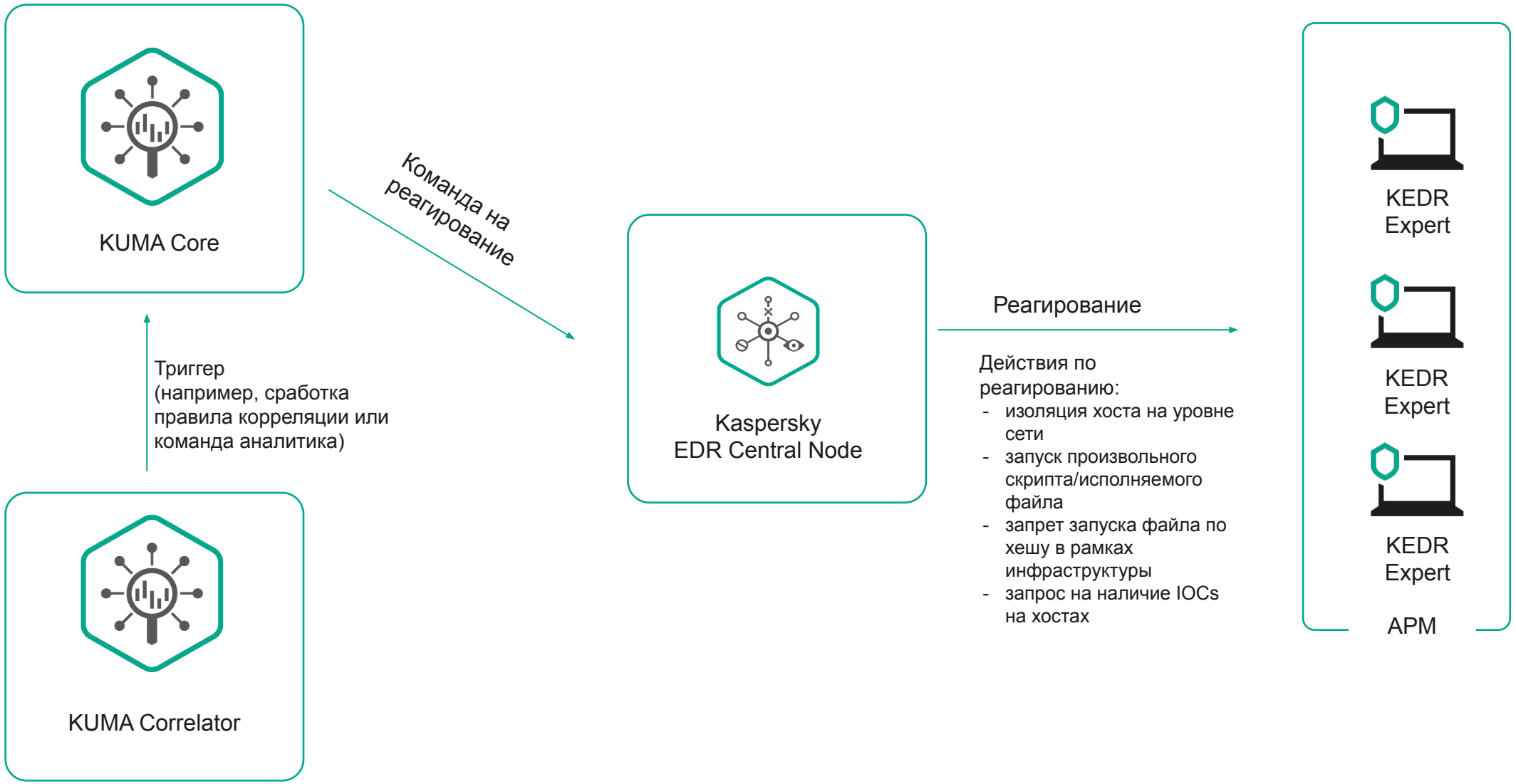
Автоматическое «обогащение» событий



«Обогащение» событий по запросу

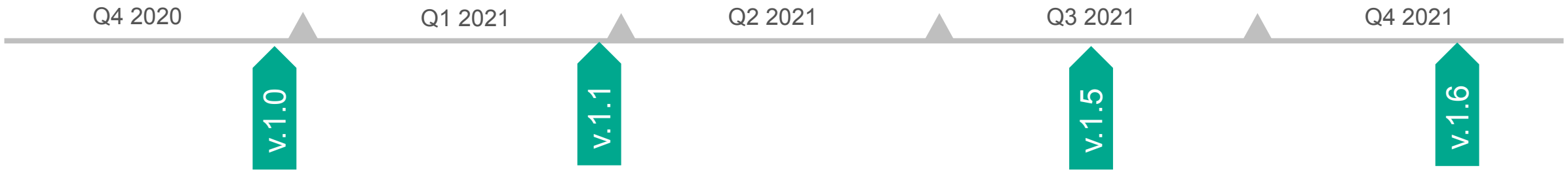


Интеграция с Kaspersky EDR*



Планы по развитию на 2021-2022 г.

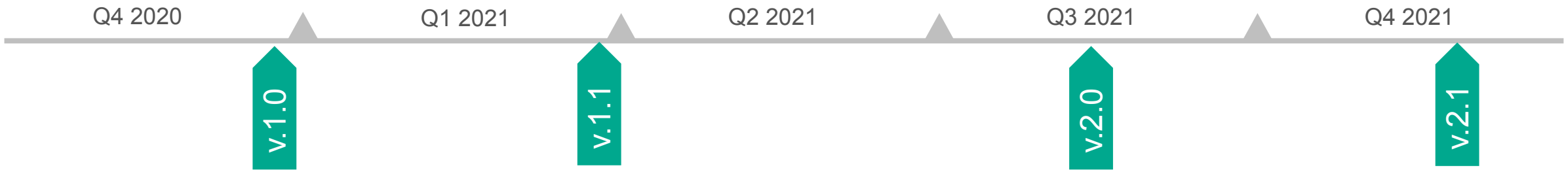
2021 RoadMap for KUMA (SIEM from Kaspersky)



1.0 – первый публичный релиз (12.2020):

1. Единая модель данных
2. Web GUI
3. Поддержка кастомизации парсеров
4. Поддержка 3rd party источников «из коробки»
5. Поддержка сохранение «сырых» событий
6. Поддержка Active List
7. Ретроспективный анализ (ретроскан)
8. Поддержка режимов отказоустойчивости и балансировки
9. Настраиваемые дашборды и отчеты
10. Обогащение событий ИБ информацией из LDAP, DNS, Kaspersky CyberTrace, Kaspersky ThreatLookup
11. Автоматическое реагирование через пользовательские скрипты
12. Автоматическая инвентаризация активов с Kaspersky Endpoint Security
13. Open API
14. Role-based Access Control

2021 RoadMap for KUMA

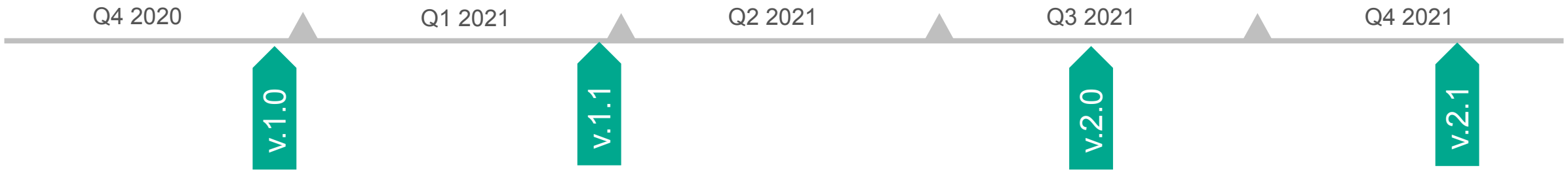


Релиз 2.0 (09.2021):

1. Основные функции:
    - Авторизация пользователей KUMA через AD
    - Ведение списка и мониторинг состояния источников событий
    - Multitenancy
    - Расширение списка поддерживаемых протоколов получения данных логов (WMI, FTP(s), NFS Share, SNMP)
    - Улучшения UI/UX по разделу настройки (разработка «мастеров» для самых критичных настроек – подключение источников логов, разработка правил корреляции)
    - Расширение списка поддерживаемых источников логов
    - Возможность сохранения резервной копии всех настроек (в том числе дашборды, отчёты, база пользователей, интеграции итд) и восстановления из резервной копии

2. Управление активами:
    - Извлечение активов из событий ИБ
    - API для управления assets, поддержка CMDB

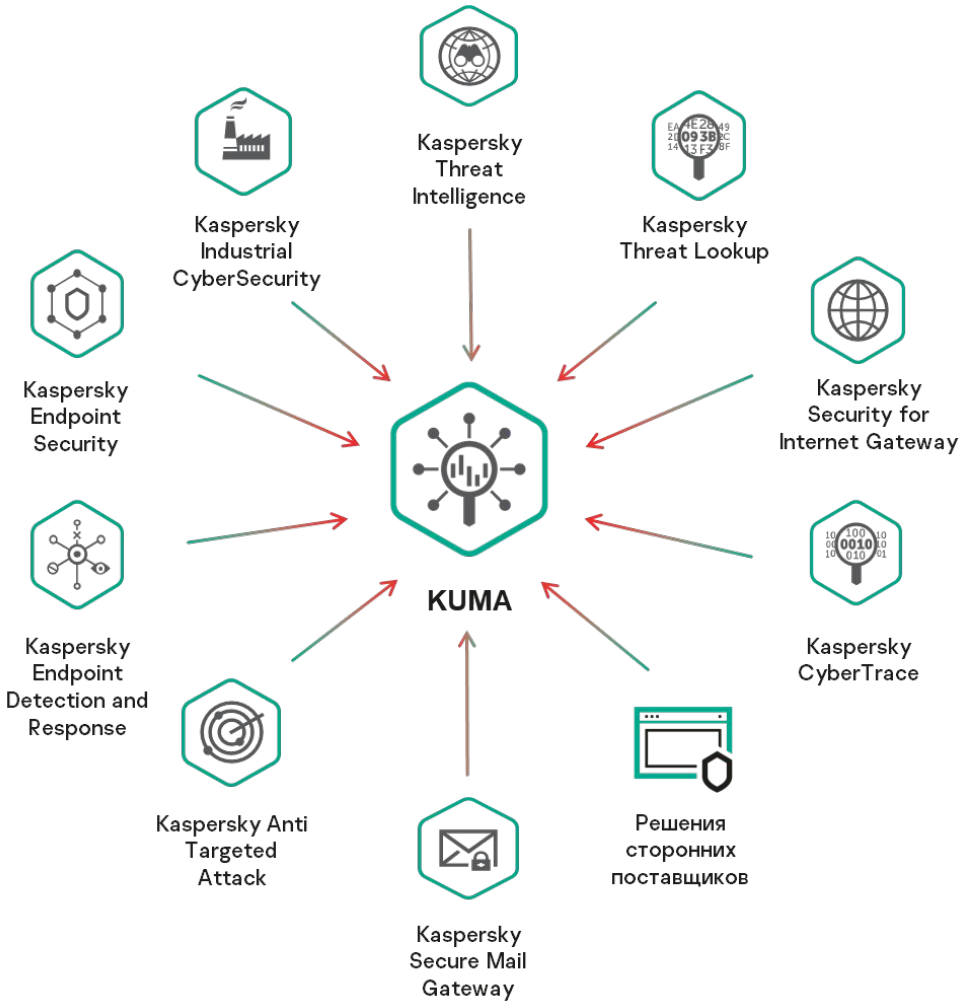
2021 RoadMap for KUMA



Релиз 2.1 (12.2021):

- Поддержка сценариев иерархического развёртывание
- Поддержка Astra Linux
- Поддержка сценария дашборда на больших экранах
- Утилита для конвертации sigma-правил в ресурсы KUMA
- Расширение списка поддержанных источников логов
- Расширение набора правил корреляции

Дальнейшее развитие решения*



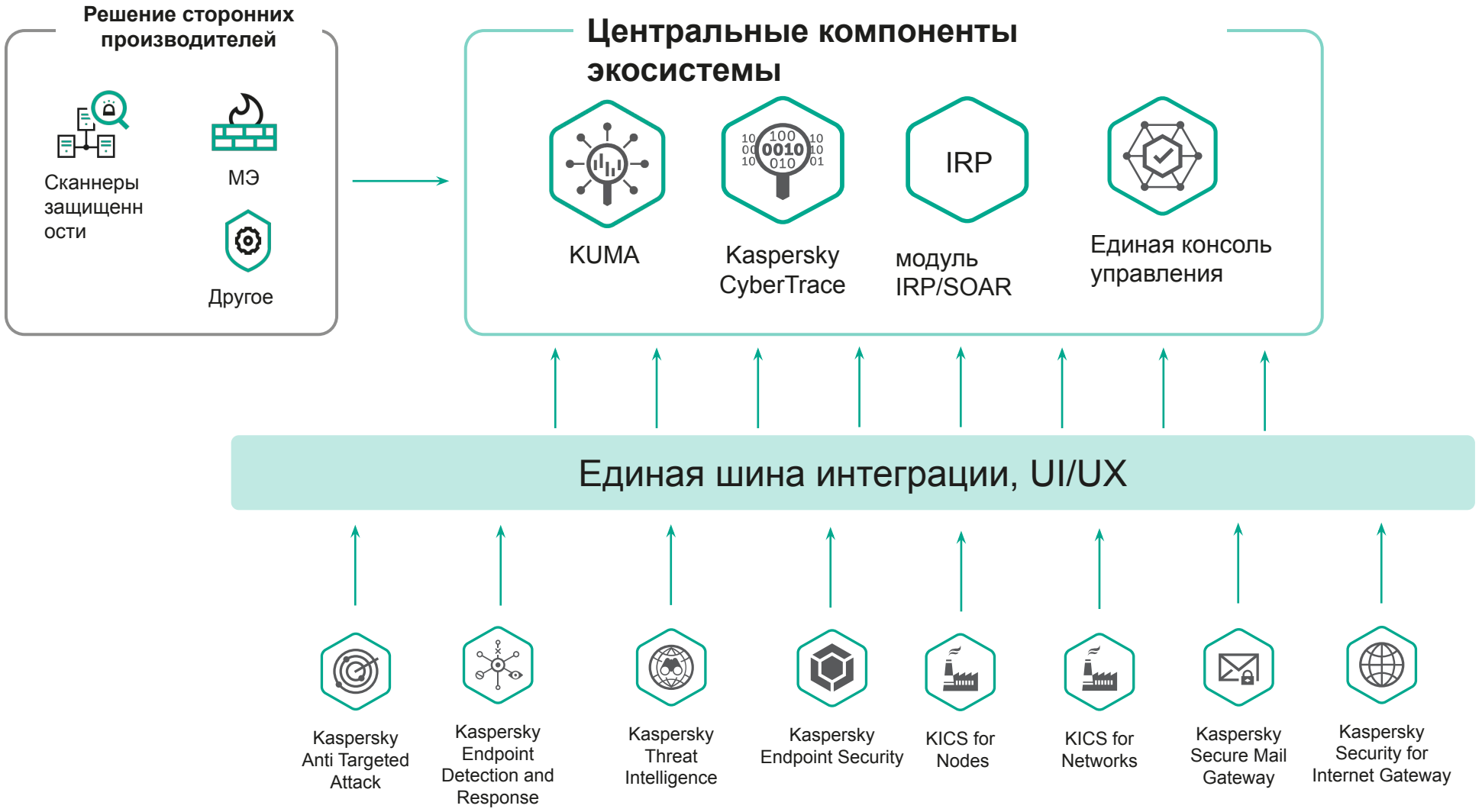
Машинное обучение – для обнаружения и анализа событий ИБ

Модули оркестрации и автоматизации

Поддержка облачных сценариев

** Возможные направления дальнейшего развития*

Экосистема Kaspersky



Базовая метрика – EPS

Минимальная лицензия от 500 EPS

Срок действия:

- 1 год
- 2 года

Дополнительные функциональные модули:

- Netflow
- Отказоустойчивость
- Взаимодействие с ГосСОПКА

Без ограничений:

- Кол-во компонентов системы (коллекторы, корреляторы)
- Поток Netflow

Техподдержка включена в стоимость, 2 опции:

- Стандартная (уровень MSA for Business)
- Расширенная (MSA Enterprise)

kaspersky

Спасибо за внимание!

kaspersky.com

В ближайшем релизе (Q3 2021)

…. Подробности в Roadmap 2021

ГОССОПКА
Обнаружение. Предупреждение. Ликвидация.

Модуль интеграции с ГосСОПКА

ATT&CK®

Правила корреляции на базе MITRE TTP

Мульти-тенантность

Сценарии интеграции с KICS*

- **Получение событий**

- **Автоматическое обнаружение активов***

- **Информация об уязвимостях***

* В процессе анализа и планирования

Поддерживаемые источники данных

Kaspersky

- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Detection and Response
- Kaspersky Security Center
- Kaspersky Secure Mail Gateway
- Kaspersky Web Traffic Security
- Kaspersky CyberTrace
- Kaspersky Threat Lookup
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Network

Сторонних поставщиков

- Palo Alto NGFW & Panorama
- FortiGate UTM
- FortiAnalyzer
- Windows OS (Windows Event Log)
- CheckPoint
- Netflow v5/v9/IPFIX
- Cisco ASA
- Cisco IOS (R&S)
- Cisco WSA
- ViPNet Coordinator 4.x
- Exim
- Unbound
- Dovecot
- Nginx
- BIFIT Mitigator
- Apache
- MS DNS
- Bind 9.x
- MS DHCP
- pfSense (OpenVPN)
- Linux (auth,rights, owner,FW)

Коннекторы и парсеры

Коннекторы

- TCP listener
- UDP listener
- Netflow v9
- NATS
- Kafka
- HTTP
- File
- SQL

Нормалайзеры

- JSON
- CEF
- CSV/TSV (with configurable delimiter)
- Key/Value (with configurable delimiter)
- Regexp
- Syslog (RFC3164 & RFC5424)
- XML
- Windows Event Log

KUMA V1.0

- Единая модель данных
- Поддержка кастомизации парсеров
- Поддержка 3rd party источников «из коробки»
- Поддержка сохранение «сырых» событий
- Поддержка Active List
- Ретроспективный анализ (ретроскан)
- Поддержка режимов отказоустойчивости и балансировки
- Настраиваемые дашборды и отчеты
- Анализ и визуализация событий с гибким поисковыми запросами к БД
- RESTful API (события, алерты)
- Role-based Access Control
- Обогащение событий ИБ из LDAP, DNS, Kaspersky CyberTrace, Kaspersky ThreatLookup
- Автоматическое реагирование через пользовательские скрипты
- Автоматическая инвентаризация активов с Kaspersky Endpoint Security