Kaspersky Unified Monitoring and Analysis Platform, зачем мы создали еще одну SIEM?

Бударин Евгений

kaspersky

Кто использует SIEM?

Зачем нужен SIEM?

Обнаружение сложных угроз ИБ

Расследование инцидентов

Соответствие требованиям

О SIEM

SIEM – Security Information & Event Management

- Сбор, агрегация, нормализация данных
- Централизованное хранилище данных
- Корреляция событий
- Оповещение
- Отчеты

Активный сбор журналов регистрации

xFlows

Журналы регистрации

Журналы регистрации

Источники данных

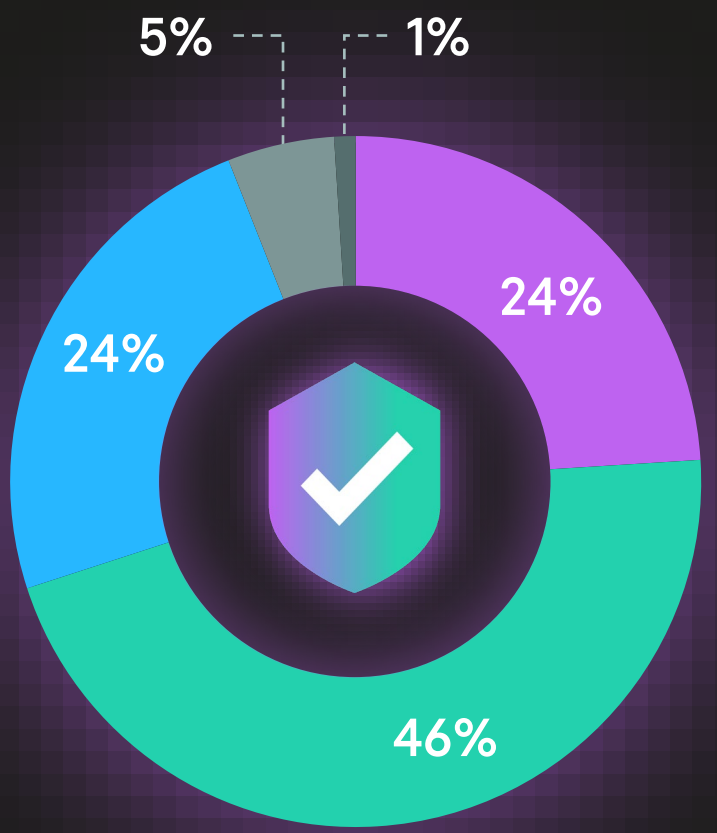
Приложения

Сетевые СЗИ

АРМ

Эффективность SIEM по обнаружению угроз и реагированию на них

70% респондентов считают, что технология SIEM остается по-прежнему **одной из эффективных** и действенных при обнаружении угроз и реагировании на них



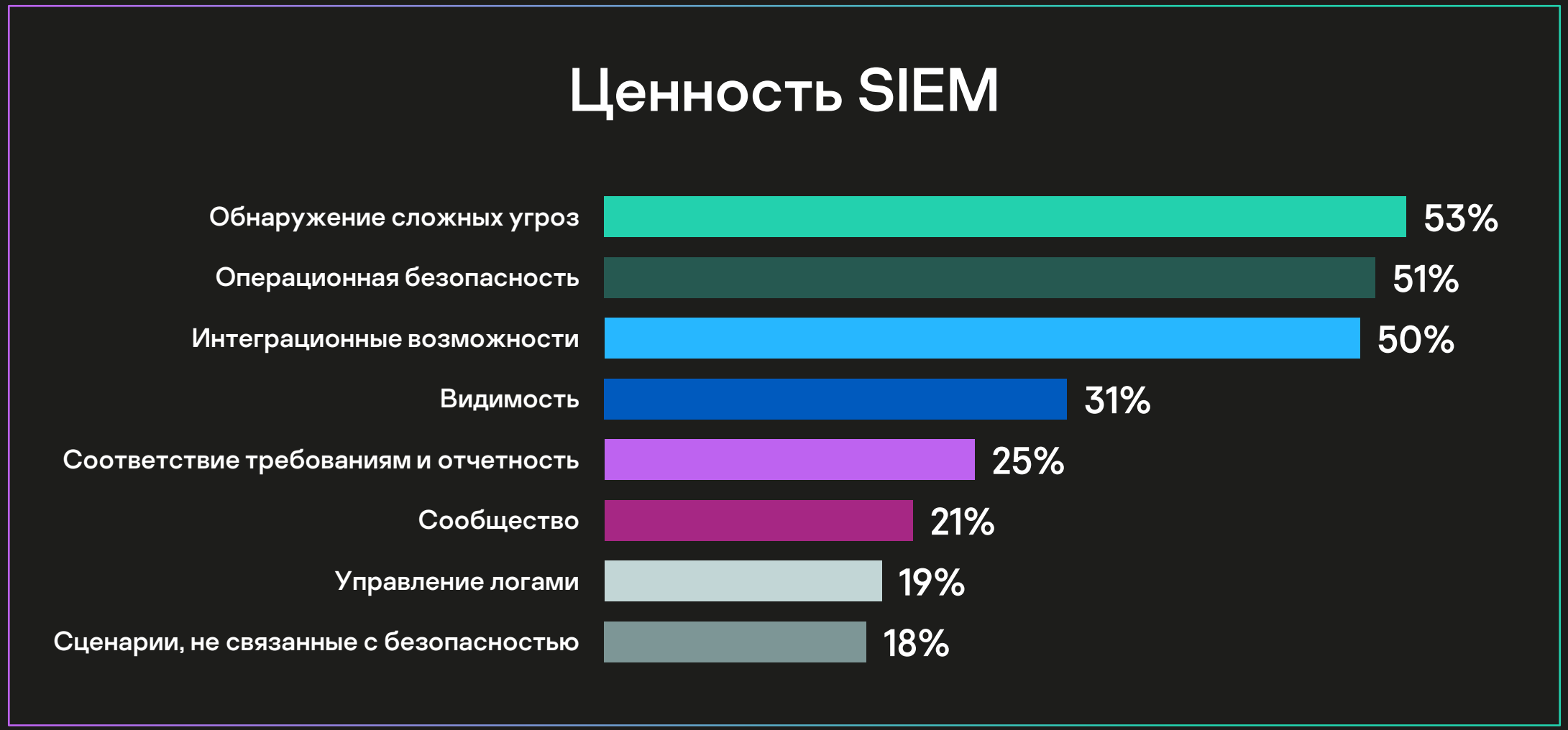
Эффективность SIEM

по обнаружению угроз и реагированию на них:

- Очень эффективна
- Эффективна
- Частично эффективна
- Не сильно эффективна
- Не эффективна

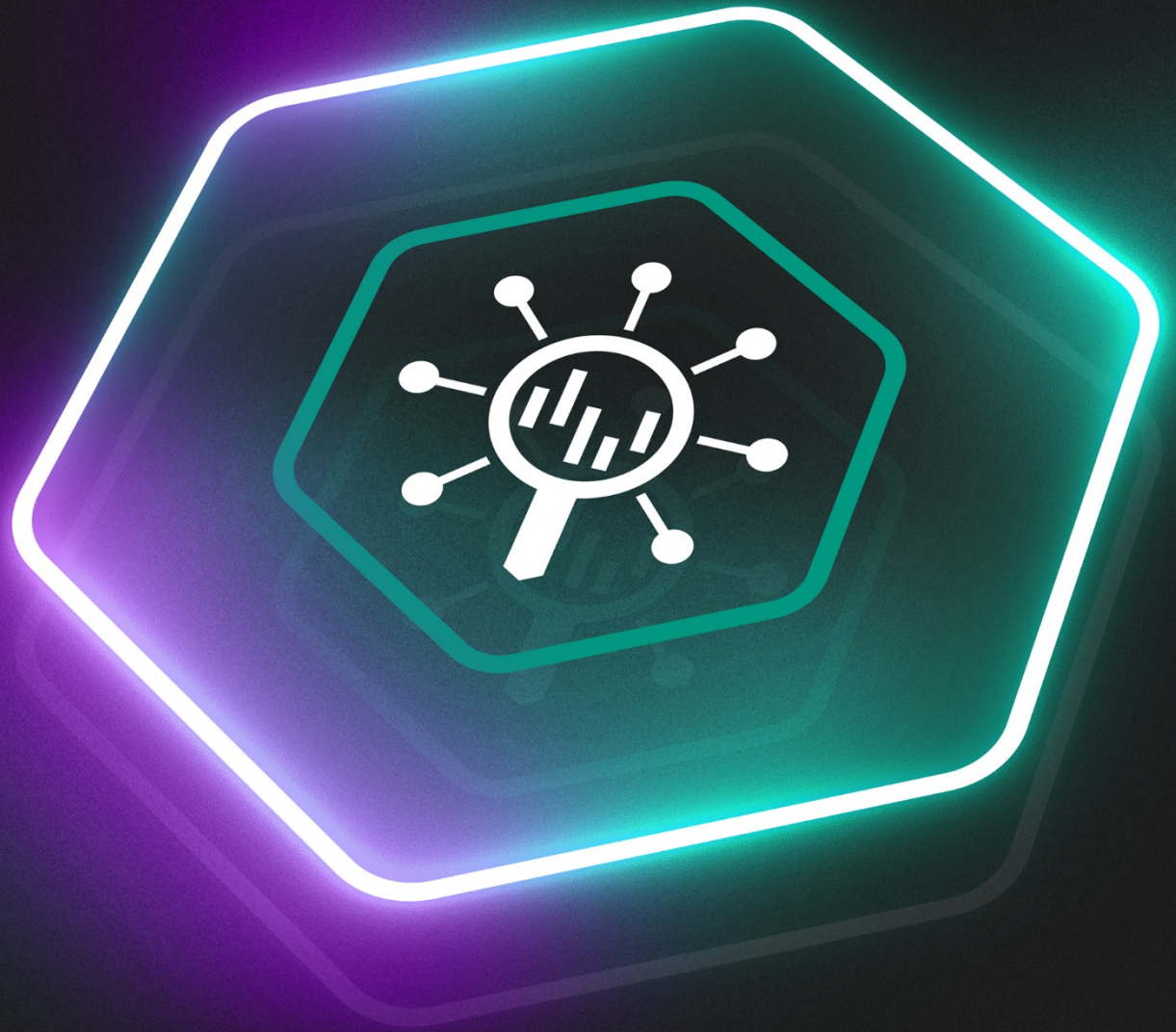
Источник: 2020 by The Enterprise Strategy Group, Inc

SIEM — основная платформа SOC сегодня



Источник: 2020 by The Enterprise Strategy Group, Inc

Kaspersky Unified Monitoring and Analysis Platform

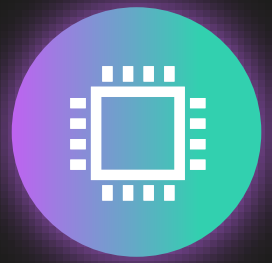


Обеспечение единой концепции кибербезопасности

Решение Kaspersky Unified Monitoring and Analysis Platform (KUMA) — ключевой компонент на пути к реализации единой концепции кибербезопасности

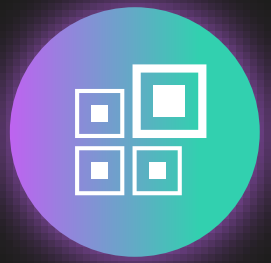
KUMA обеспечивает гибкий комплексный подход к противодействию сложным угрозам и целевым атакам и учитывает специфику различных отраслей, существующую ИБ системуи помогает обеспечить соответствие требованиям внешних регулирующих органов.

Ключевые преимущества



Высокая производительность

300k+ EPS на один узел



Масштабируемость

Гибкая микросервисная архитектура

Низкие системные требования

Интеграция «из коробки»

С продуктами сторонних поставщиков и решениями «Лаборатории Касперского»

Мониторинг и расследование инцидентов

Kaspersky Security для бизнеса

Kaspersky Endpoint Detection and Response

Kaspersky Anti Targeted Attack

Kaspersky Security для интернет-шлюзов

Kaspersky Secure для почтовых серверов

Единая консоль мониторинга и анализа инцидентов ИБ

Kaspersky Unified Monitoring and Analysis Platform

Решения сторонних поставщиков

Kaspersky Security Center

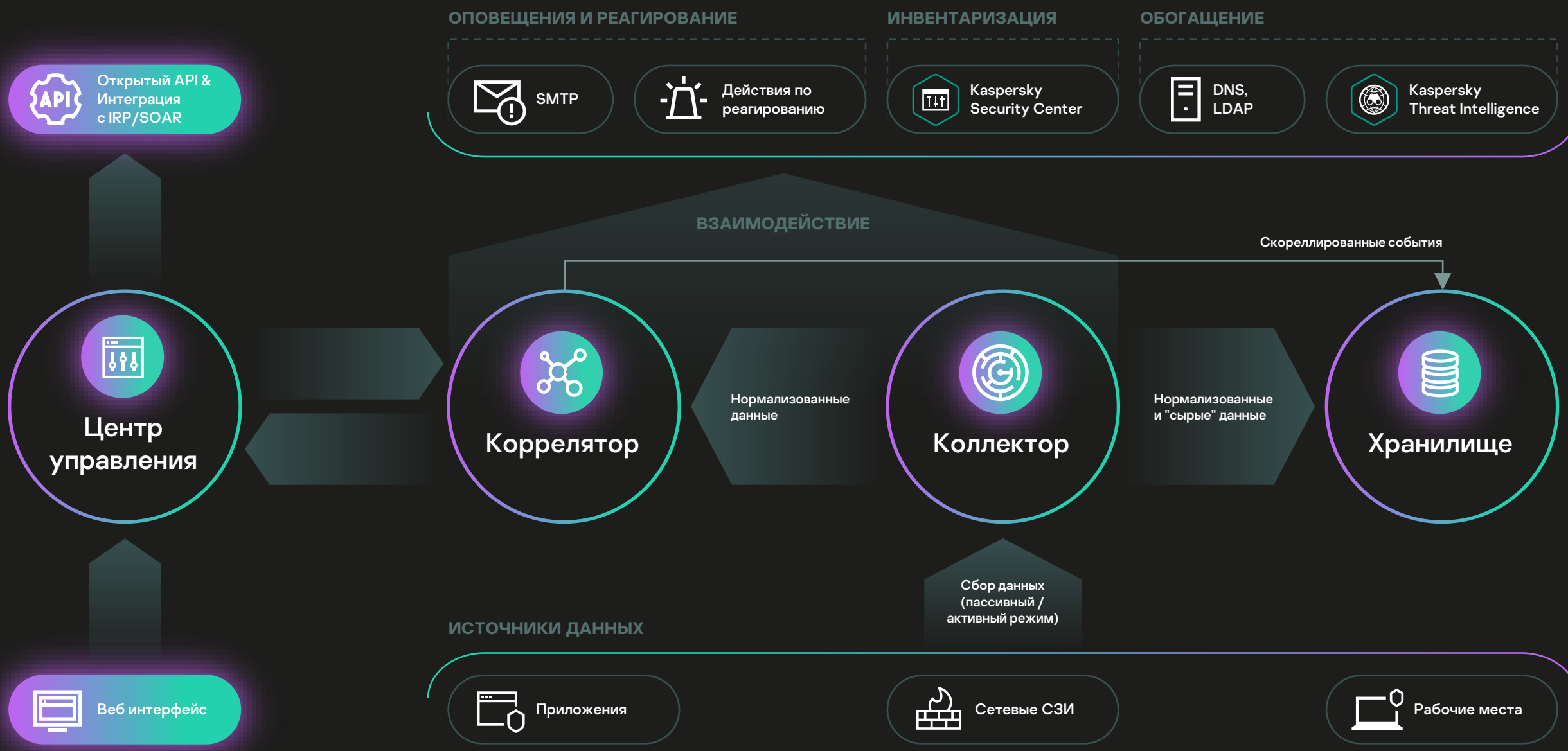
Kaspersky Threat Data Feeds

Kaspersky CyberTrace

Kaspersky Threat Lookup

Kaspersky Industrial CyberSecurity

Архитектура KUMA



Поддерживаемые источники данных «из коробки»

Kaspersky

- Kaspersky Security для бизнеса
- Kaspersky Security Center
- Kaspersky EDR
- Kaspersky EDR для бизнеса Оптимальный
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace
- Kaspersky Threat Lookup
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Network

Стороннее взаимодействие

- Программное обеспечение с открытым исходным кодом (Unbound, Dovecot, Nginx, Apache, DNS BIND, pfSense (с OpenVPN), Exim, Squid, Postfix и др.)
- Операционные системы (Windows, Linux, FreeBSD)
- Ключевые продукты от различных поставщиков (Microsoft, Palo Alto Networks, Cisco, VMWare, Код безопасности, CheckPoint, R-Vision, Fortinet, Positive Technologies, Infotecs, InfoWatch, Бастион, Huawei, Oracle, MikroTik, Бифит, TrendMicro и др.)
- Другое (Netflow, Kafka, NATS, SQL, TCP, UDP, HTTP, Files, SNMP, WMI)

Коннекторы и нормалайзеры (парсеры)

Коннекторы

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

Нормалайзеры

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

Распределенная инфраструктура

Примерный сайзинг

~ 40k EPS

Коллектор + Коррелятор + Ядро

Коллектор

- CPU – 8 vCPU
- RAM – 4 ГБ;
- Storage – 100 ГБ

Коррелятор

- CPU – 8vCPU;
- RAM – 16 ГБ;
- Storage – 100 ГБ

Центр анализа

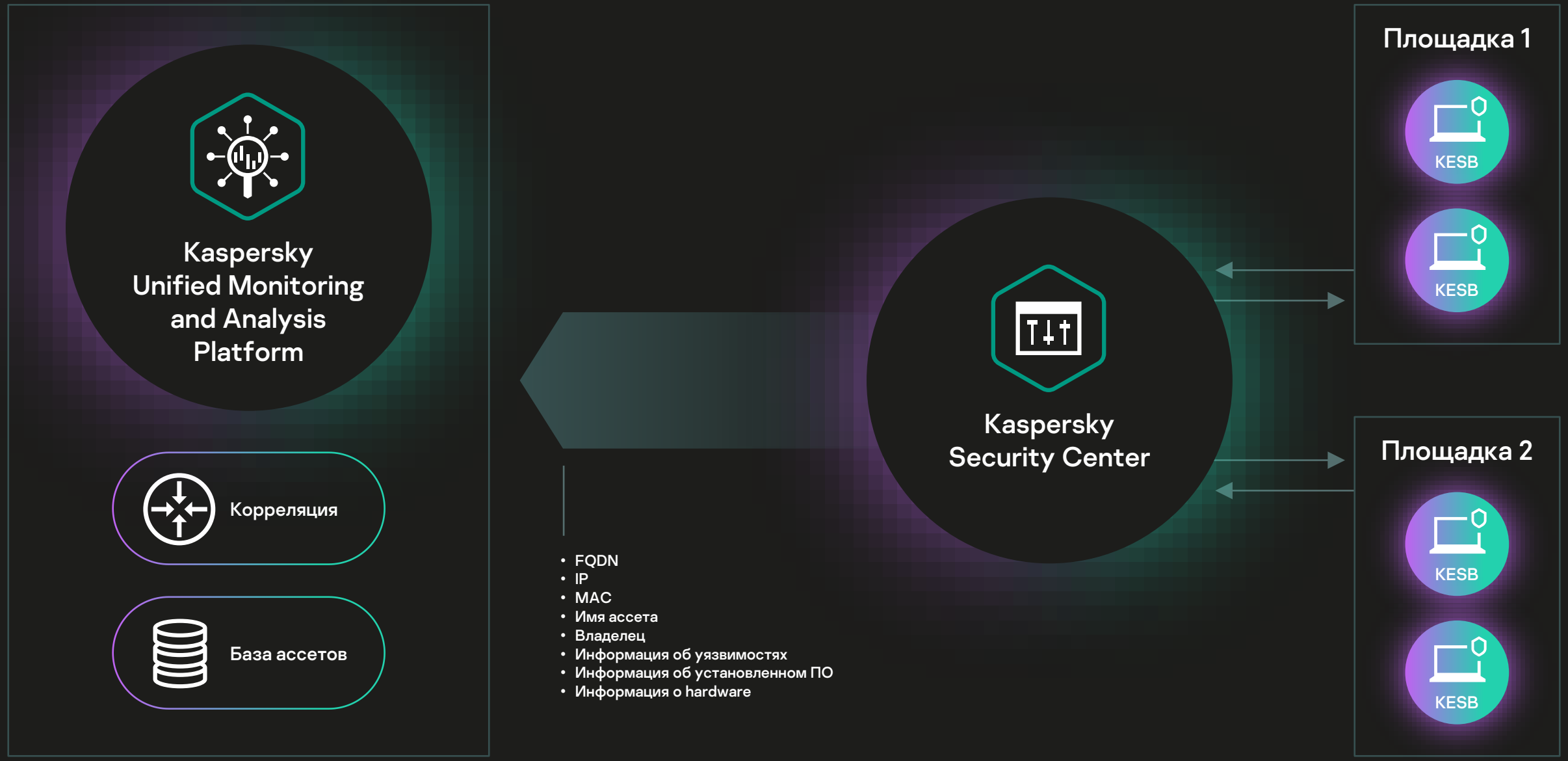
- CPU – 4 vCPU
- RAM – 8 ГБ;
- Storage – 100 ГБ

Хранилище событий

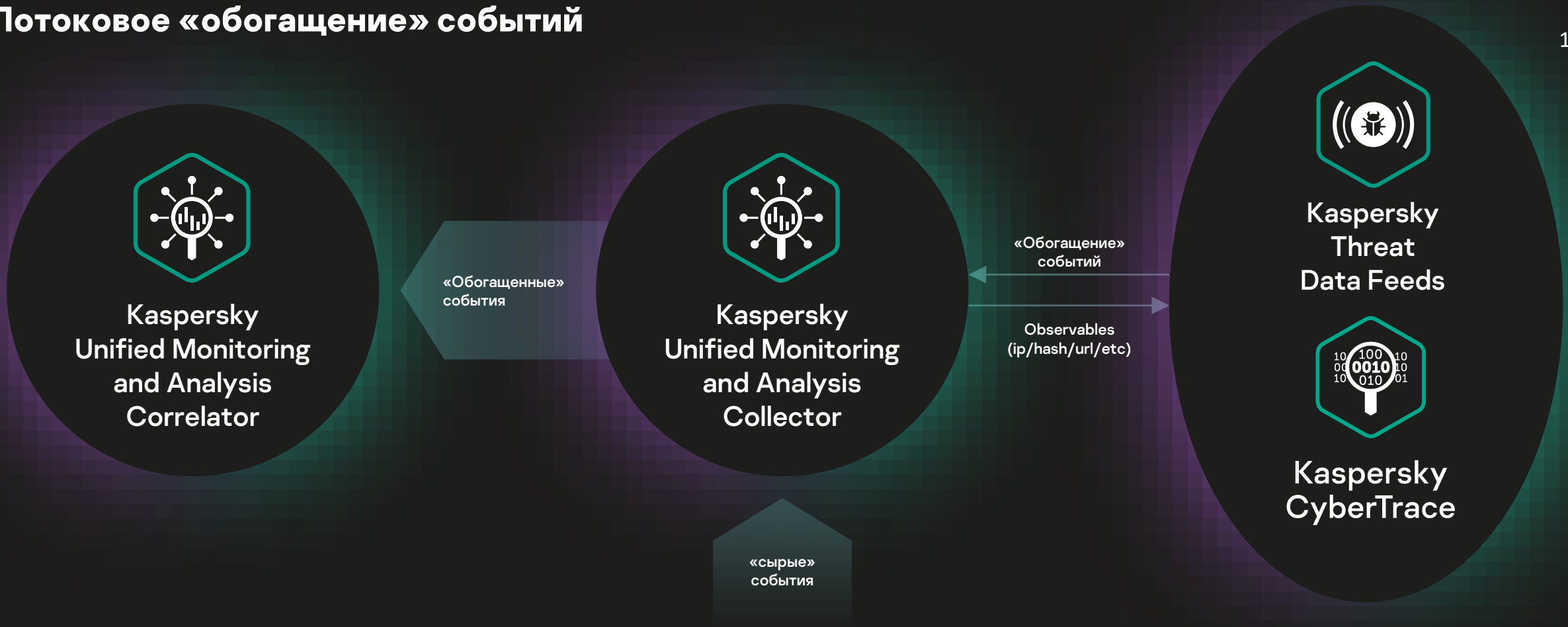
- CPU– 24 vCPU
- RAM – 48 ГБ;
- Storage– 500* ГБ

*Объем хранилища зависит от длительности хранения событий

Инвентаризация информационных активов



Потоковое «обогащение» событий

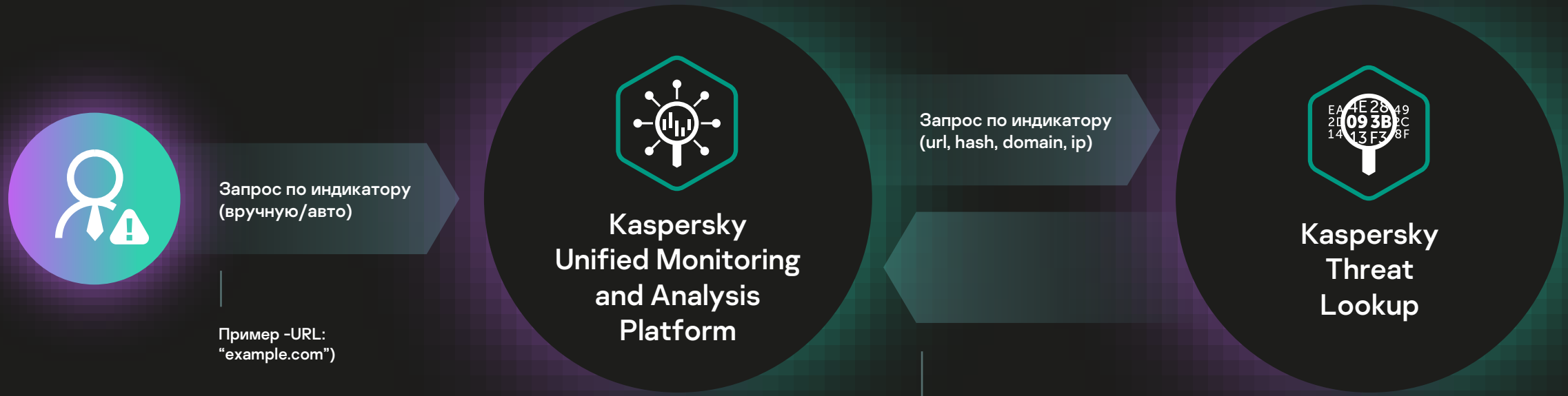


Потоки данных об угрозах

- IP REPUTATION FEED
- HASH FEED (WIN / *nix / MacOS / AndroidOS / iOS)
- URL FEEDS (Malicious, Phishing and C&C)
- RANSOMWARE URL FEED
- APT IOC FEEDS
- VULNERABILITY FEED
- PASSIVE DNS (pDNS) FEED
- IoT URL FEED
- WHITELISTING FEED
- ICS HASH FEED
- И ДРУГОЕ

Kaspersky Threat Data Feeds

«Обогащение» событий по запросу



“Обогащение” карточки инцидента данными из Kaspersky Threat lookup

Карточка инцидента

Имя: «Обнаружено взаимодействие с CnC сервером»
Описание:.....
Связанные события: .....
Связанные IP: 1.2.3.4, 2.3.4.5, ...
Связанные пользователи: i.Ivanov, a.petrov, ...
.....

Ответ на запрос

URL: «example.com»
first seen: “2016-08-10”
last seen:” 2020-03-01”
Связанные хэш-суммы вредоносных файлов
MD5:”.....”
SHA-1: “.....”
SHA256:” ”
Связанные вредоносные URL: “....”
Связанные IP: 1.2.3.4, 2.3.4.5, ...

Базовая метрика – EPS

Минимальная лицензия от 500 EPS

Срок действия:

- 1 год
- 2 года

Дополнительные функциональные модули:

- Netflow
- Отказоустойчивость

Техподдержка включена в стоимость, 2 опции:

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

Без ограничений:

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

Спасибо!

kaspersky