kaspersky

Kaspersky Industrial Cybersecurity Conference 2020

# Павел Таратынов

Архитектор центров информационной безопасности, АО «Лаборатория Касперского»

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

kaspersky

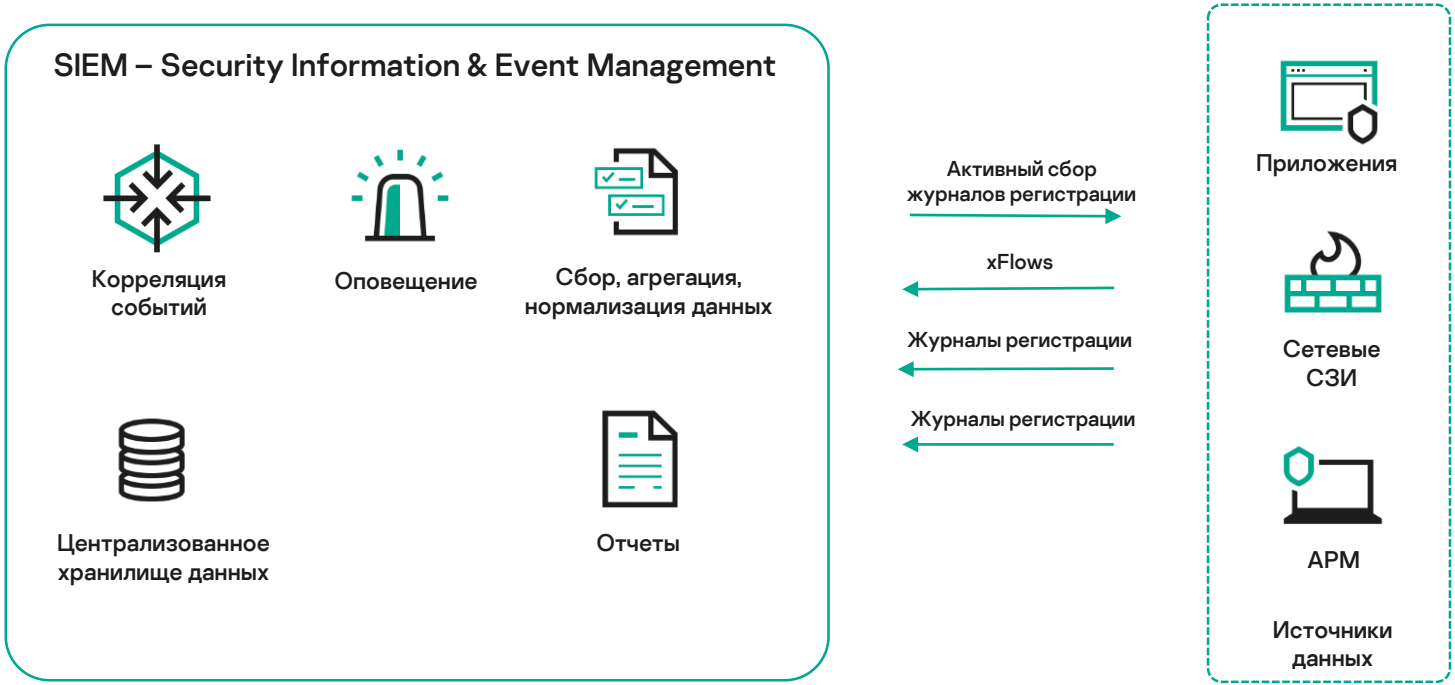
# Единая платформа Kaspersky для мониторинга и анализа инцидентов ИБ

Павел Таратынов,
«Лаборатория Касперского»

Kaspersky Industrial Cybersecurity Conference 2020

# Что такое SIEM





# Зачем нужен SIEM?



**Обнаружение сложных угроз ИБ**

**Расследование инцидентов**

**Соответствие требованиям**

# Проблематика классических SIEM

**Производительность**
Не справляются с текущими объемами данных

**Сложность внедрения, эксплуатации, масштабирования**

**Стоимость владения**

# Эволюция SIEM

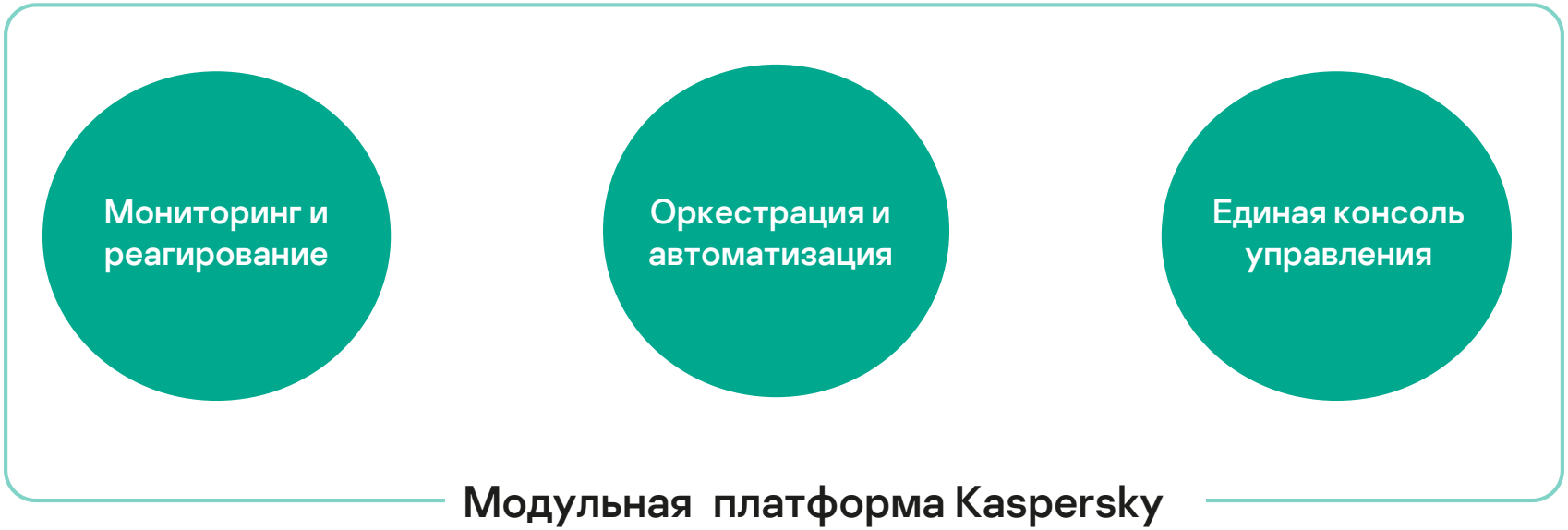


**Классический SIEM**

- Log management
- Корреляция
- Отчеты

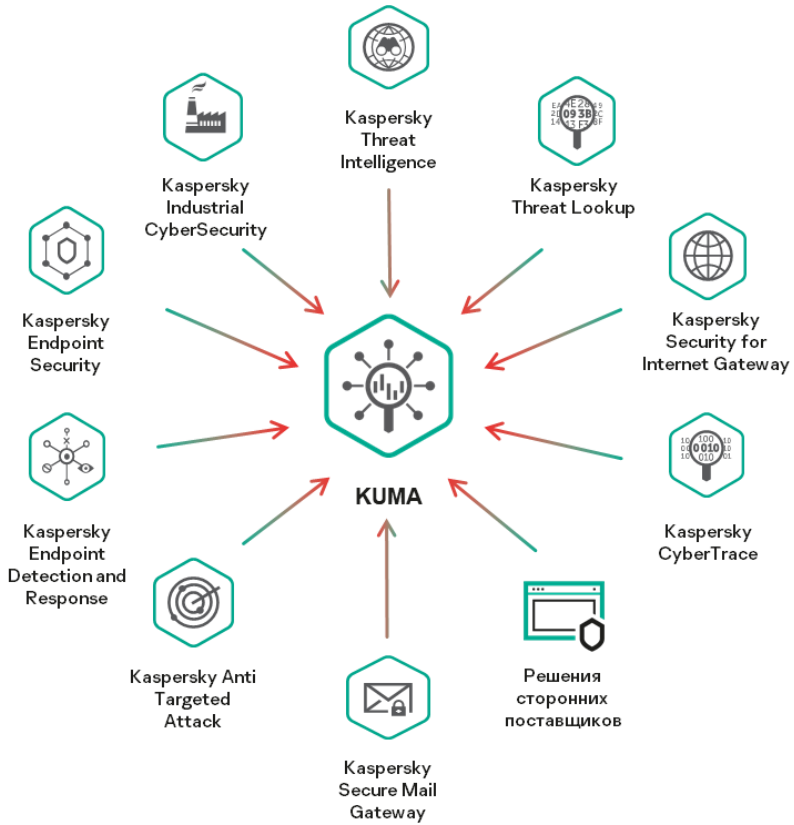
**NG-SIEM**

- Log management
- Корреляция
- Отчеты
- Работа с контекстом (asset mgmt, Threat Intelligence)
- Автоматизация и оркестрация
- Механизмы обнаружения и анализа на базе ML/AI
- Расширенный анализ и визуализация данных


Мониторинг и реагирование
Оркестрация и автоматизация
Единая консоль управления
Модульная платформа Kaspersky

# Kaspersky Unified Monitoring & Analysis Platform (KUMA)






Единая консоль **мониторинга** и **анализа** инциденты ИБ

# Ключевые преимущества



**Производительность**

*300k+ EPS на одну ноду коррелятора*

**Гибкая архитектура**

*Современная микросервисная архитектура*

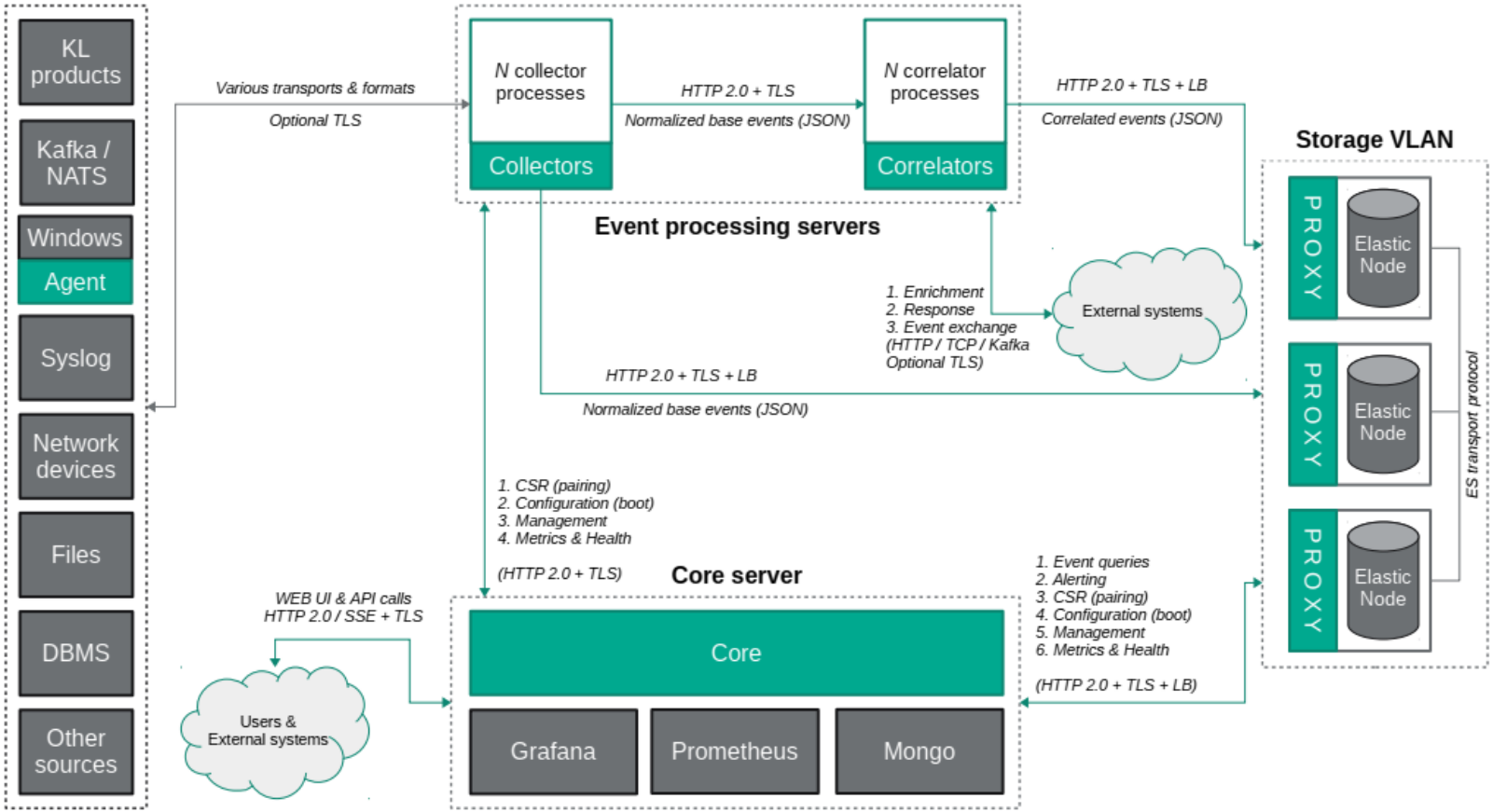
**Низкие системные требования**

**Интеграции «из коробки»**

*С решениями «Лаборатории Касперского» и сторонних поставщиков*

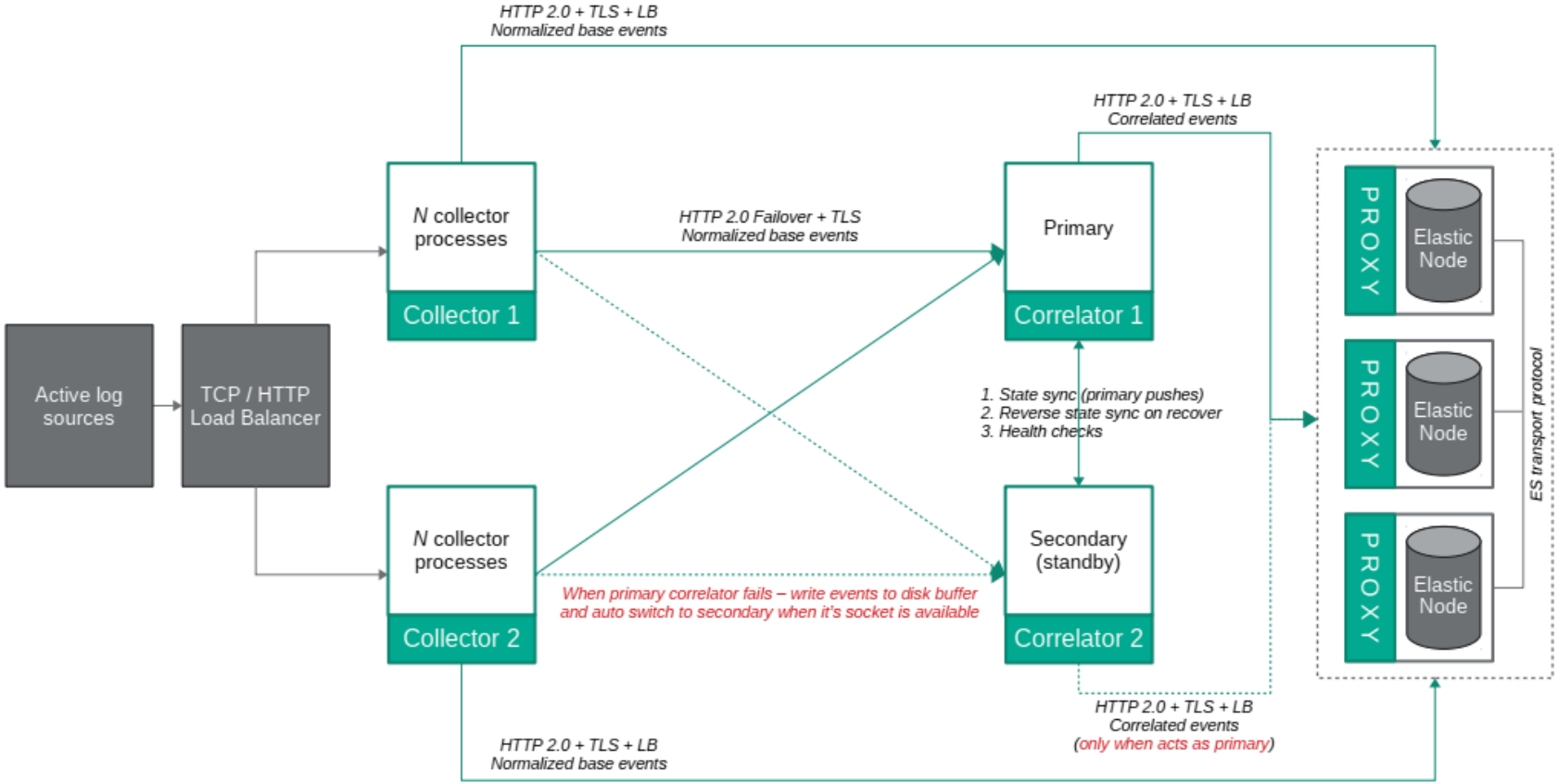
# Архитектура KUMA





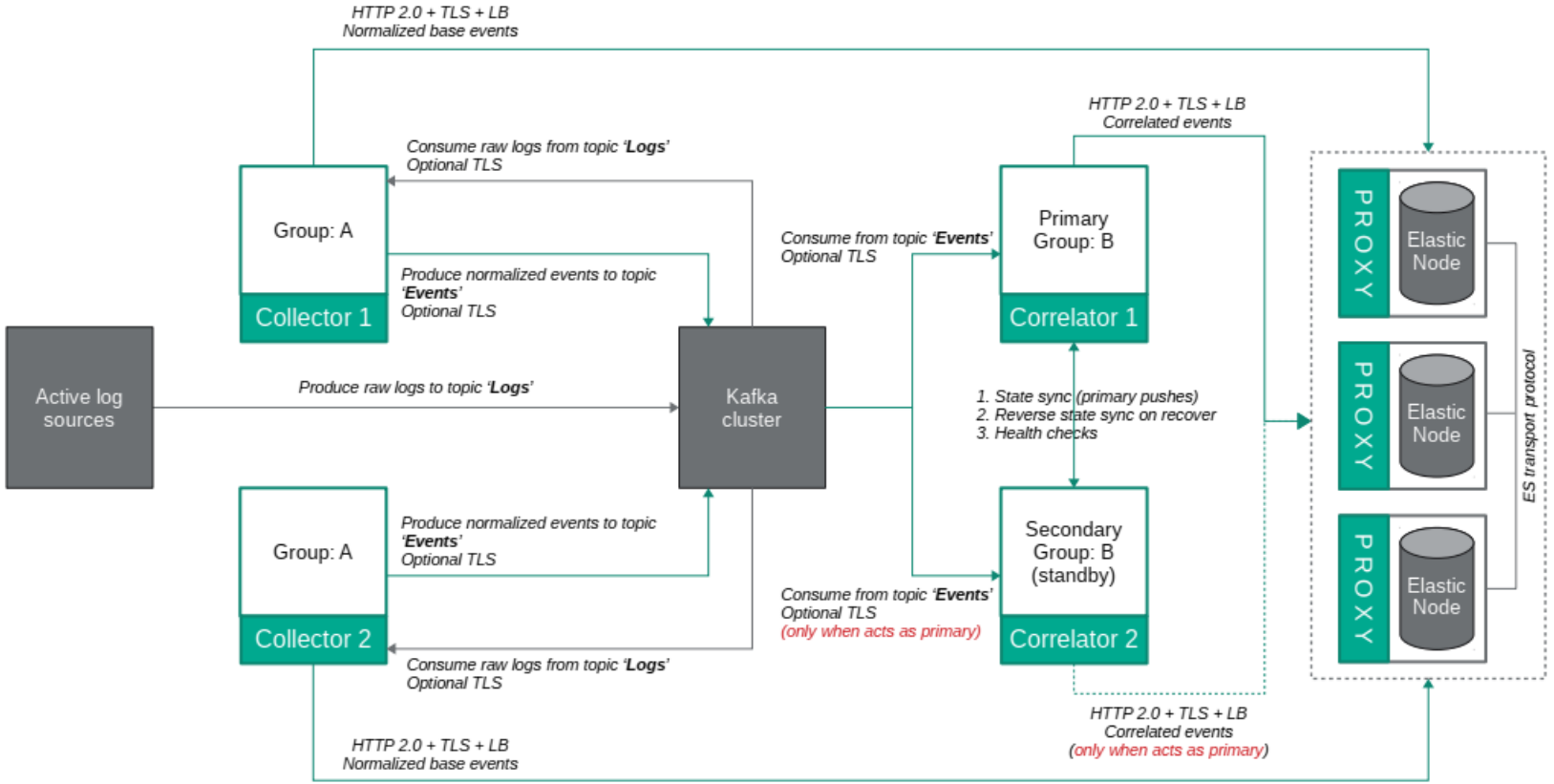
# Отказоустойчивость и балансировка нагрузки





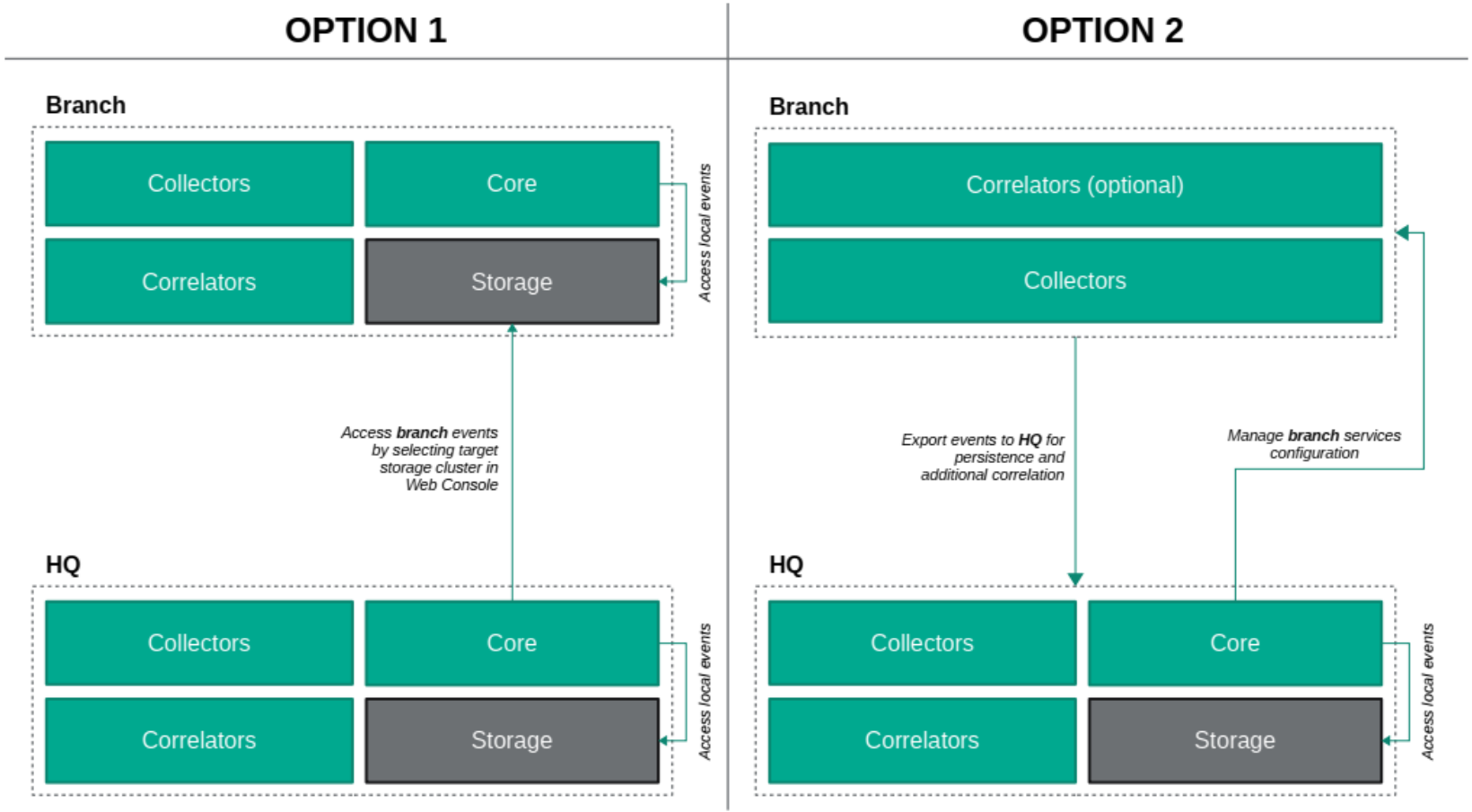
# Опция внедрения с брокером сообщений





# Распределенная инфраструктура





# Поддерживаемые источники данных (Q4 2020)



## 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 Networks

## Сторонние поставщики

- Palo Alto NGFW & Panorama
- FortiGate UTM
- FortiAnalyzer
- Windows OS (Windows Event Log)
- Netflow v5/v9
- Cisco ASA
- Cisco IOS (R&S)
- Cisco WSA
- ViPNetCoordinator
- Exim
- Unbound
- Dovecot
- Nginx
- Apache
- Bind
- Linux (auth,rights, owner,FW)
- FreeBSD (auth,rights, owner,FW)
- VMWare

# 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

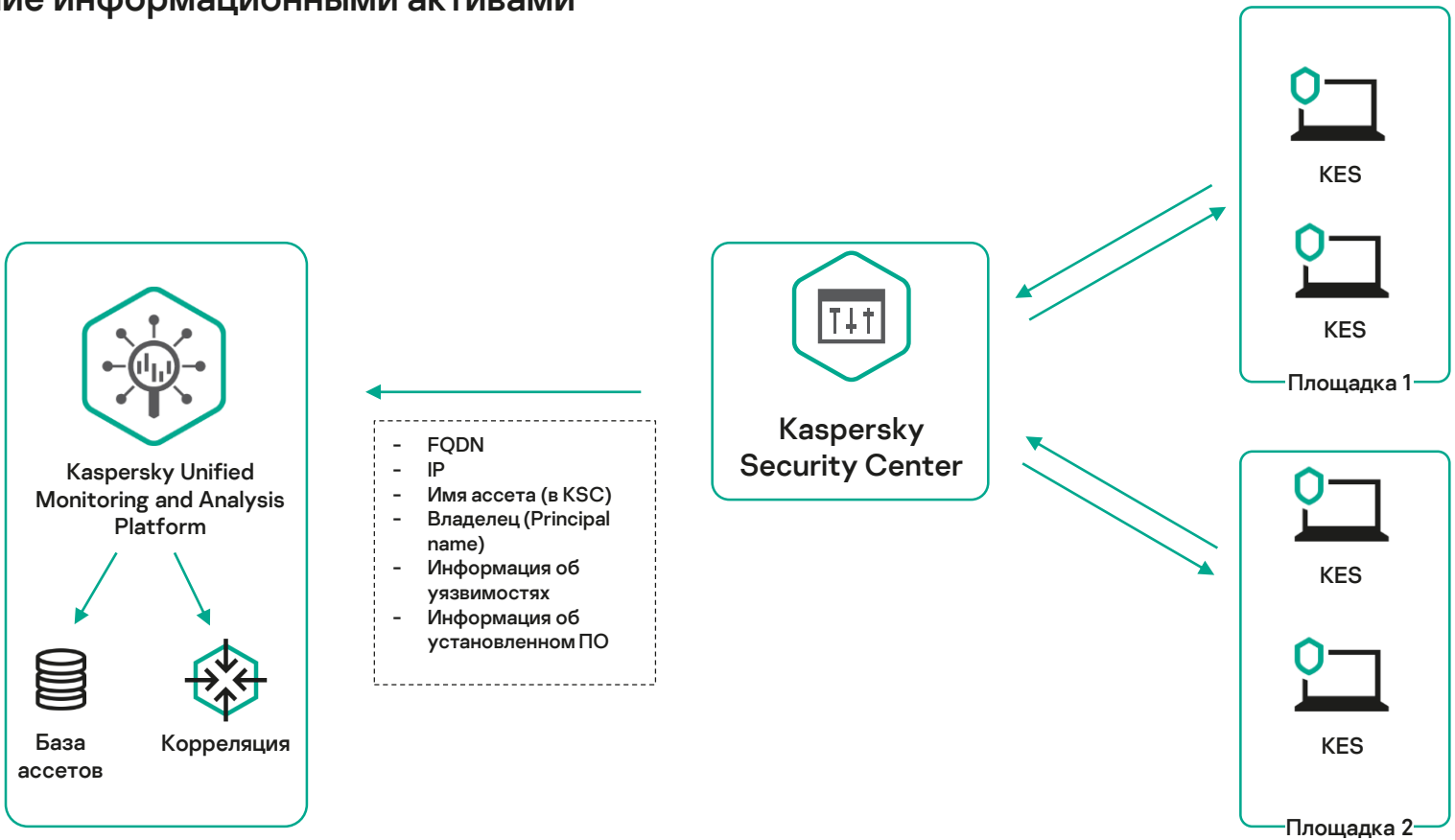
# KUMA Scope 2020



- Единая модель данных
- GUI
- 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
- RESTful API
- Role-based Access Control
- Обогащение событий ИБ через LDAP, DNS, Kaspersky CyberTrace, Kaspersky ThreatLookup
- Автоматическая инвентаризация активов с Kaspersky Endpoint Security

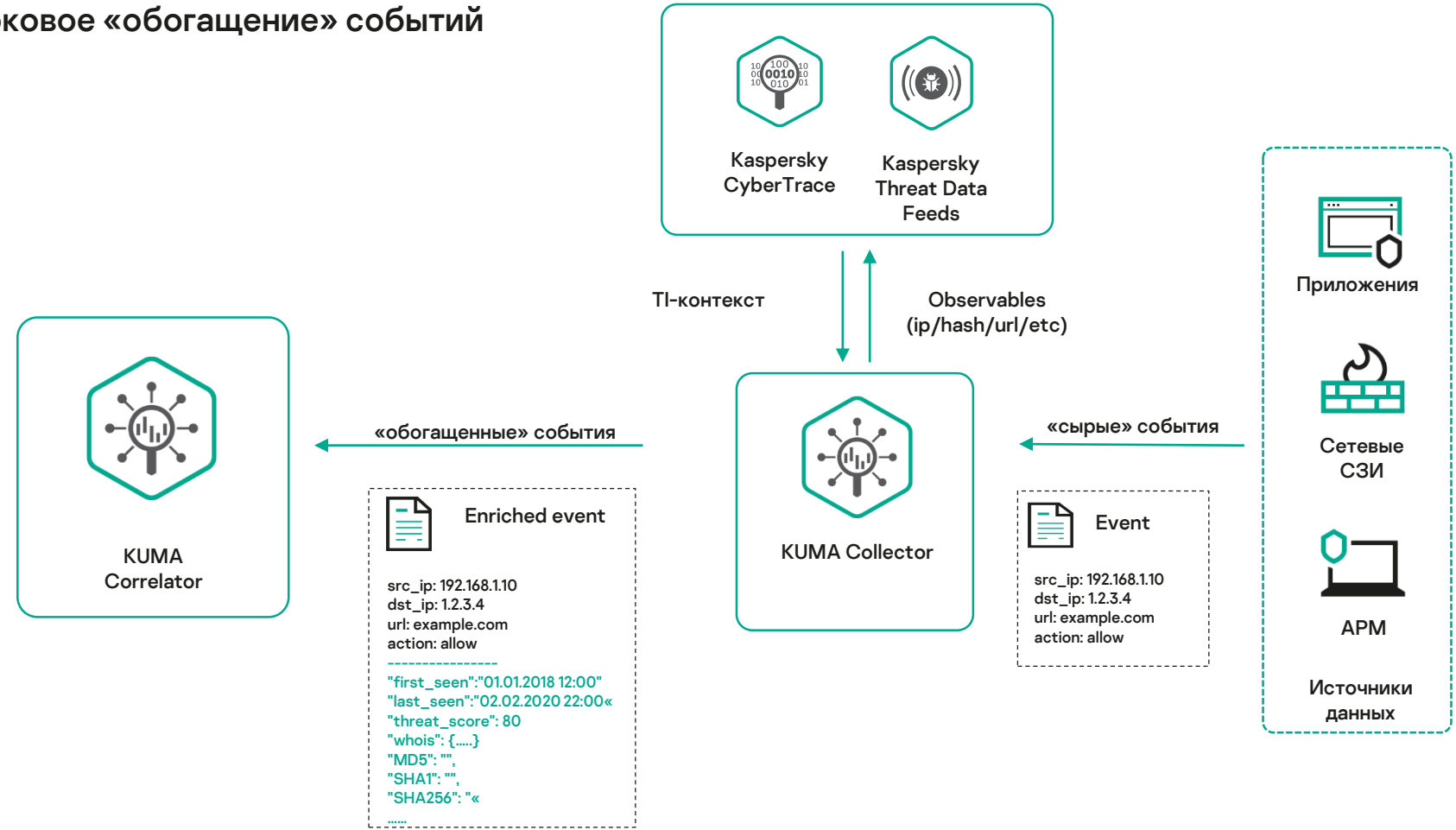
# Управление информационными активами





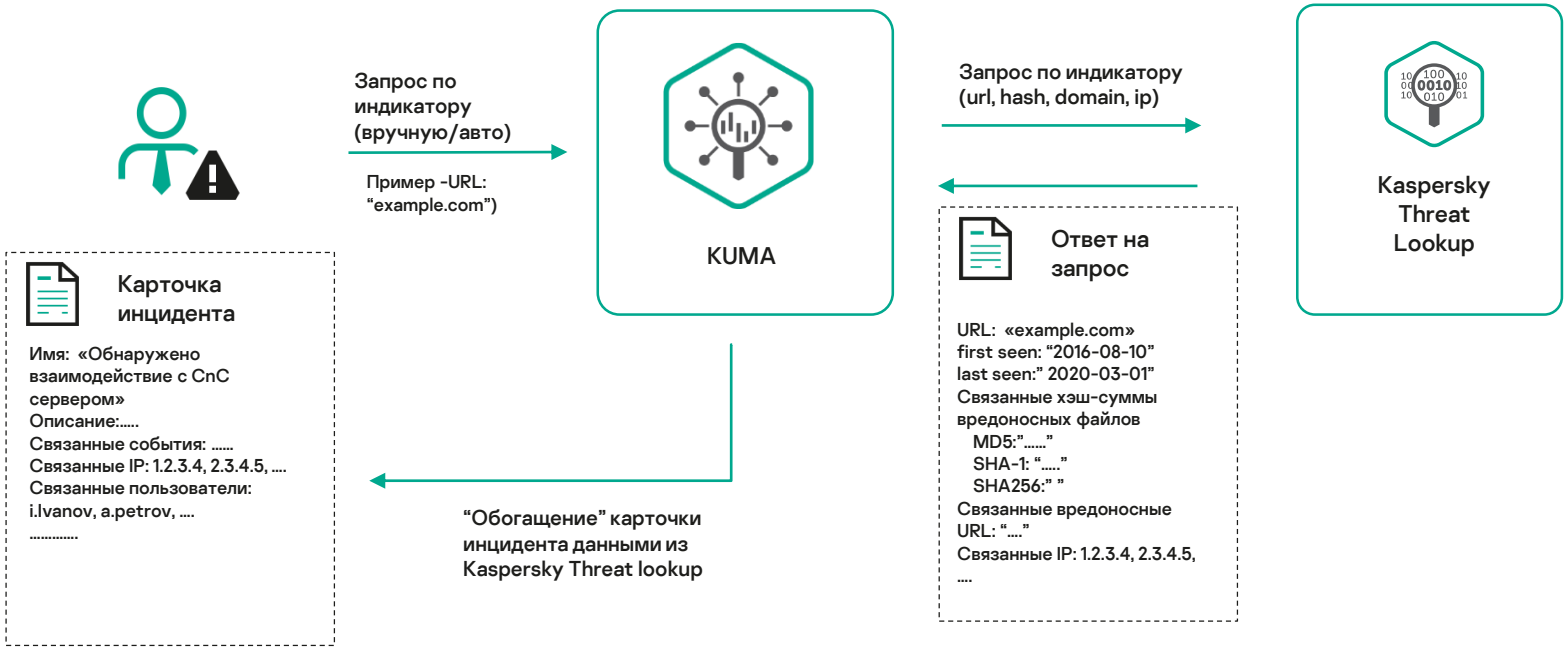
# Потоковое «обогащение» событий





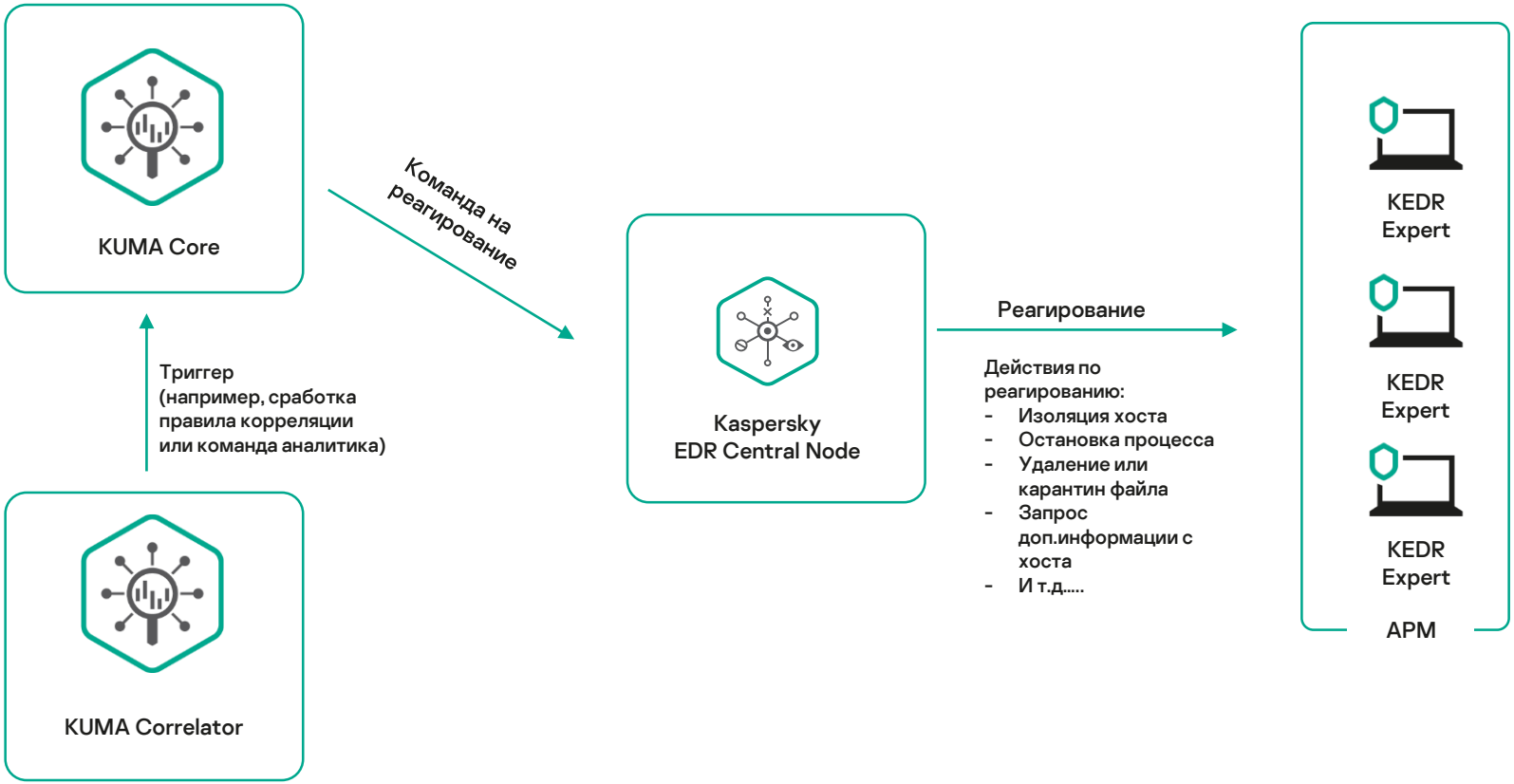
# «Обогащение» событий по запросу





# Интеграция с Kaspersky EDR





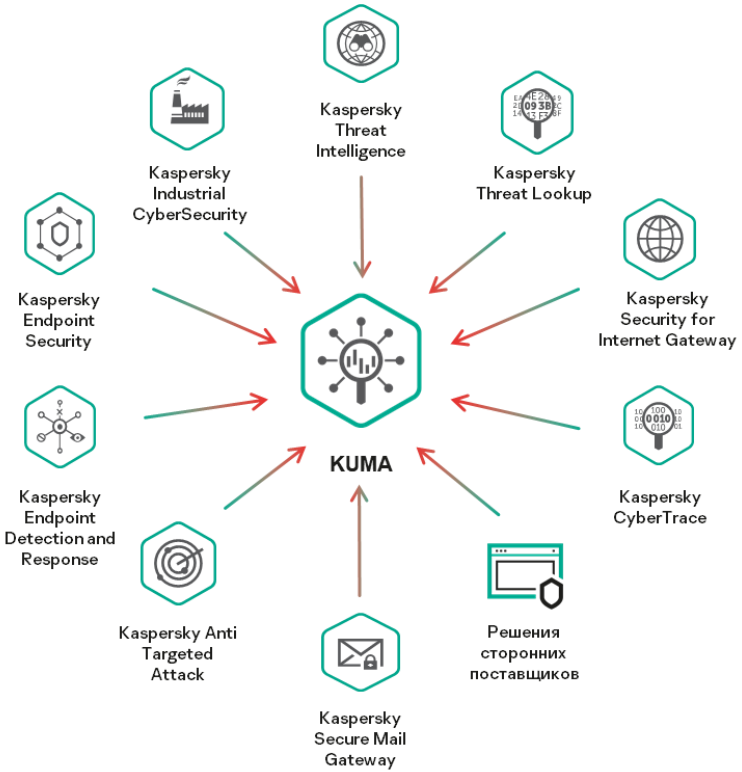
# KUMA Roadmap* 2021

(* - основные направления развития)

- Локализация UI
- Сертификация по требованиям ФСТЭК (ТУ, НДВ4)
- Реестр отечественного ПО
- Интеграция с НКЦКИ и соответствия требованиям ГосСОПКА
- Поддержка функций регистрации и учета инцидентов (case management)
- Поддержка иерархической модели развертывания SIEM (Головные и подчиненные ноды)
- Развитие функционала управления активами (asset management)
- Развитие функционала обогащения событий
- Расширение списка интеграций с решениями «Лаборатории Касперского»
- Расширение списка поддерживаемых «из коробки» источников данных
- Авто-приоритизация инцидентов с использованием методов Machine Learning и информации Threat Intelligence (ML- & TI-assisted auto triage)
- Функции автоматизированного реагирования с Kaspersky EDR и Custom scripts
- Multitenancy

# Заключение






**Единая экосистема безопасности Kaspersky**

**KUMA – ключевой компонент экосистемы**

**Релиз первой версии KUMA - декабрь 2020.**

**Демо и пилот tech preview версии возможен уже сейчас.**

# Thank you!

Subtitle

**Павел Таратынов**

**Архитектор центров информационной безопасности**

kaspersky

**pavel.taratynov@kaspersky.com**

# Примерный сайзинг



**~40k EPS**

Correlator + Collector + Core

**Коллектор:**

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

**Коррелятор:**

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

**Ядро:**

- CPU – 4 vCPU
- RAM – 8 ГБ;
- Storage – 50 ГБ

**Хранилище событий** (Elastic)

CPU– 24 vCPU

RAM – 48 ГБ;

Storage– 500* ГБ

*объем хранилища зависит от длительности хранения событий

# Мировый рынок SIEM - конкурентный и зрелый....

# Но безальтернативный.


* *Gartner Magic Quadrant 2019*

# Наш подход



Технологии

Экспертное сообщество

Консалтинг

Поддержка от экспертов «Лаборатории Касперского»