kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Павел Таратынов

Архитектор центров информационной безопасности, «Лаборатория Касперского», Россия

#KasperskyICS

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

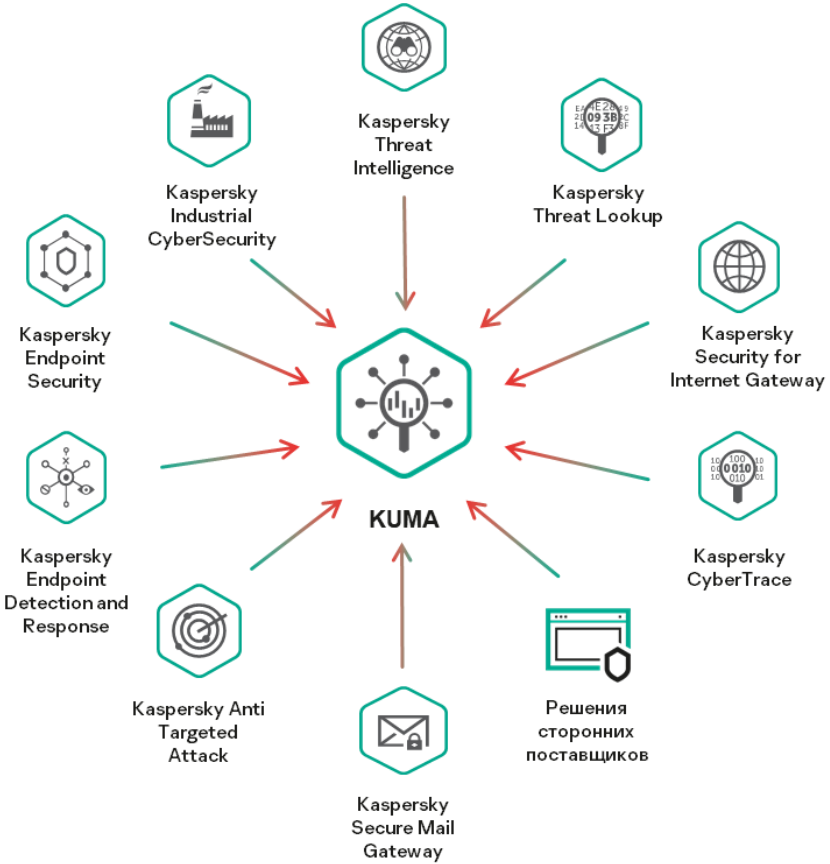
Kaspersky Industrial Cybersecurity Conference 2021

Платформа Kaspersky для мониторинга и анализа инцидентов ИБ. Обзор новых функций

Таратынов Павел,
Архитектор SOC

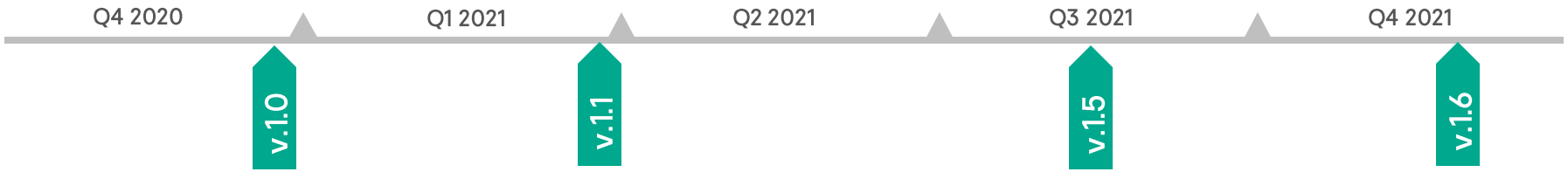
kaspersky

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Единая консоль мониторинга и анализа инцидентов ИБ

2021 RoadMap для KUMA



28.12.2020 – релиз KUMA 1.0

27.09.2020 – релиз KUMA 1.5

Q4 2020 – релиз KUMA 1.6

Ключевые преимущества

Производительность

До 300k+ EPS на один узел

Масштабируемость

Вертикальная и горизонтальная

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

Автоматическая инвентаризация сети

С помощью агентов KES

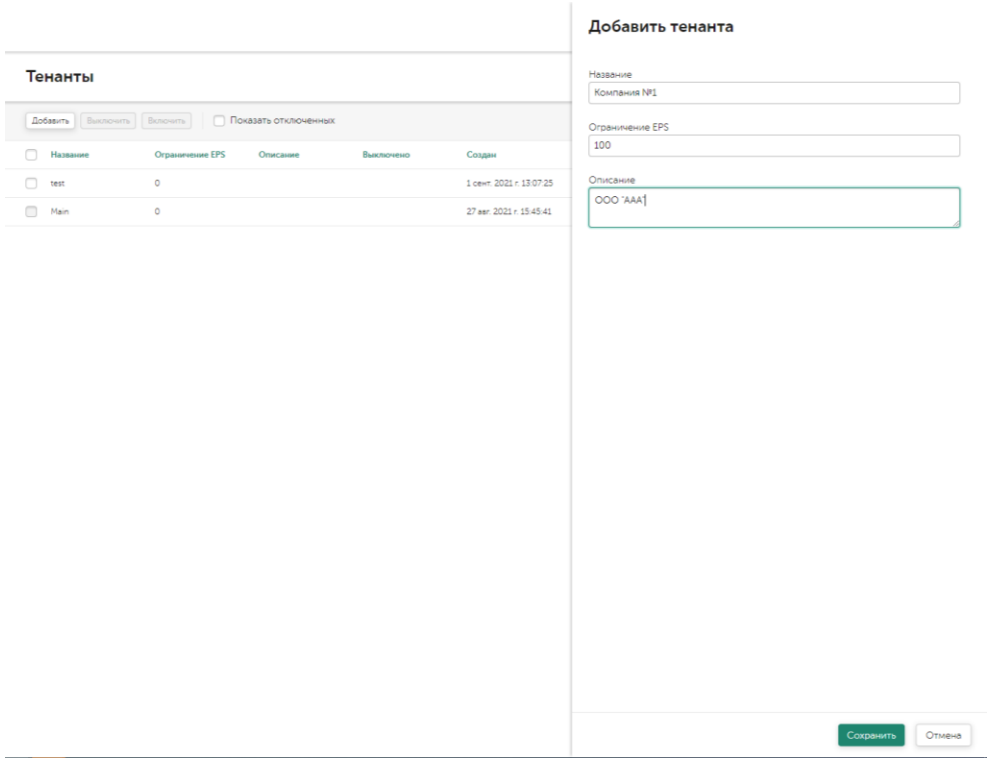
Автоматизированное реагирование

Через KSC, пользовательские скрипты
*Интеграция с KEDR**

* Будущие релизы

Обзор новых функций KUMA 1.5

Поддержка Multitenancy

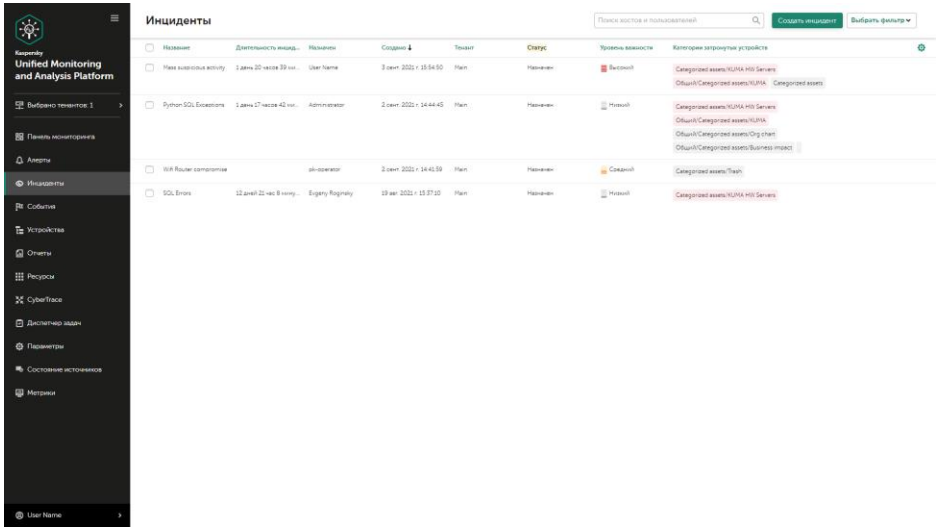


Разделение данных, конфигурации и прав доступа

Возможность ограничения EPS для каждого тенанта отдельно

Целевой сценарий для MSSP и центров Госсопка

Управление инцидентами

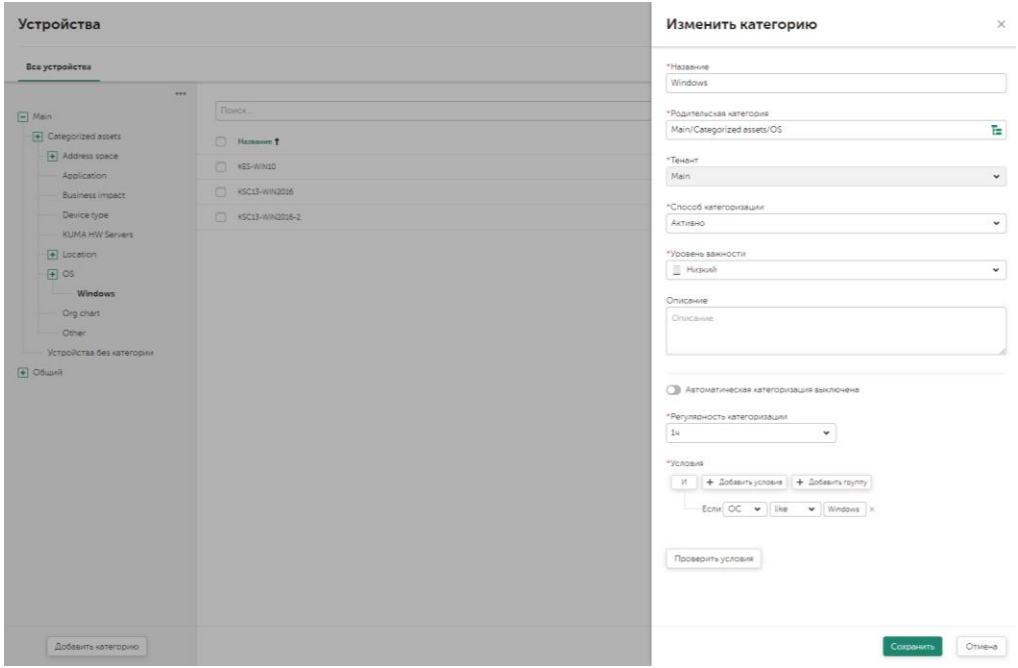


Управление инцидентами - ***назначение ответственного, изменение приоритета, эскалация, ведение истории, так далее***

Создание инцидентов автоматически или вручную

Экспорт в НКЦКИ

Динамическая категоризация активов



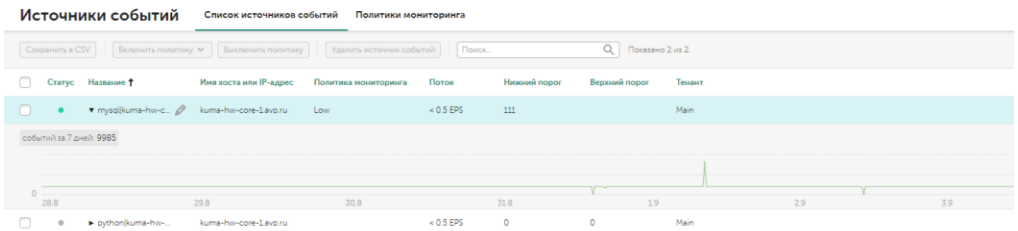
Динамическая категоризация по:

- **FQDN**
- **IP**
- **CVE**
- **ОС**
- **Версия билда ОС**

Логические операторы AND, OR, NOT и группировки

Возможность проверки условий

Мониторинг доступности источников

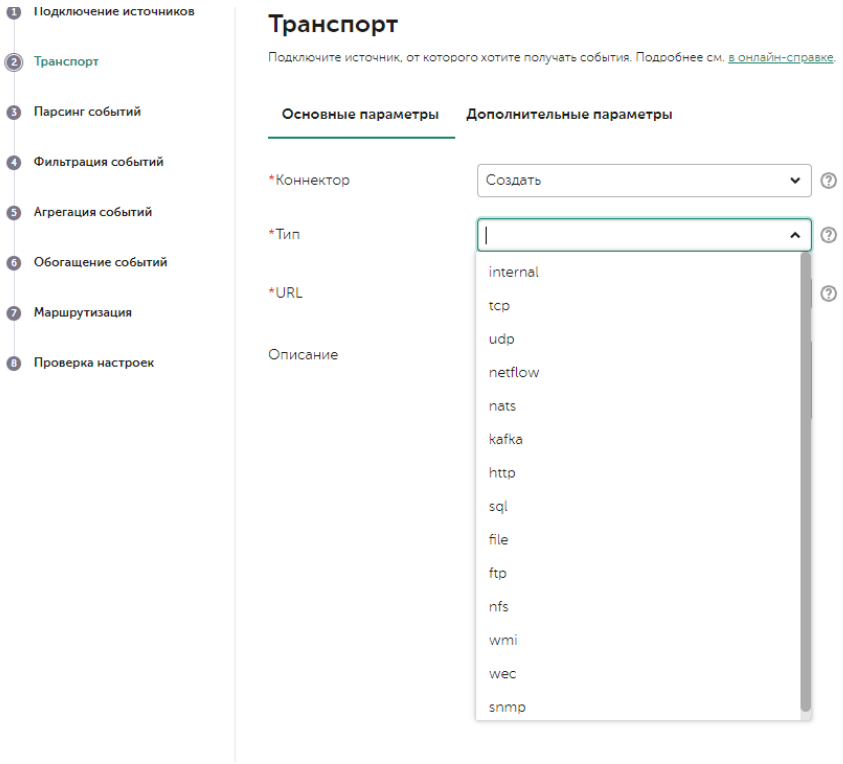


Мониторинг источников по минимальному кол-ву событий в период времени

Уведомление по почте в случае недоступности

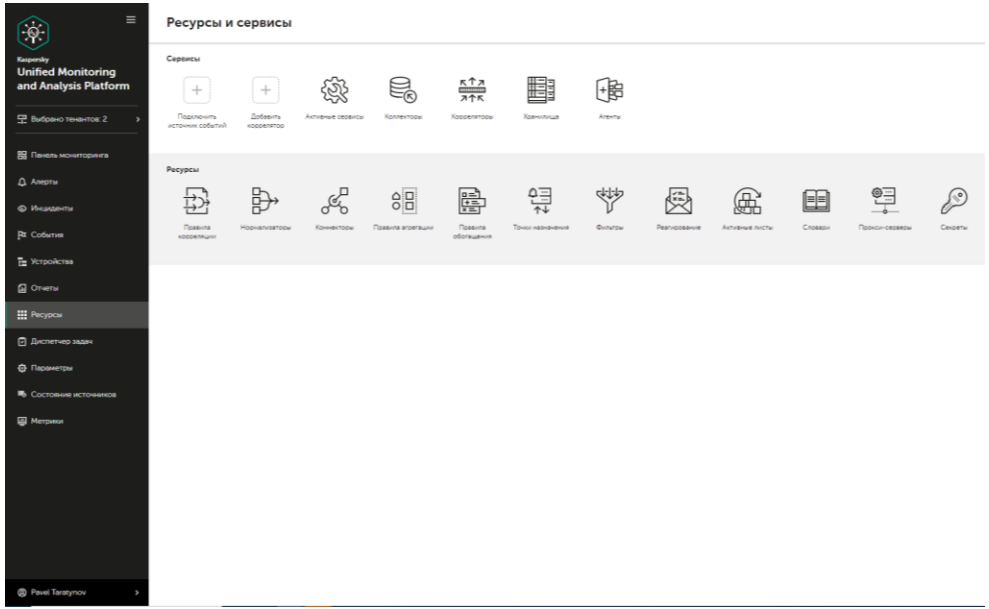
Возможность задать разные политики

Безагентский сбор Windows Event Log



Поддержка сбора событий через механизм Windows Management Instrumentation (WMI)

Переработанный интерфейс управления ресурсами и сервисами

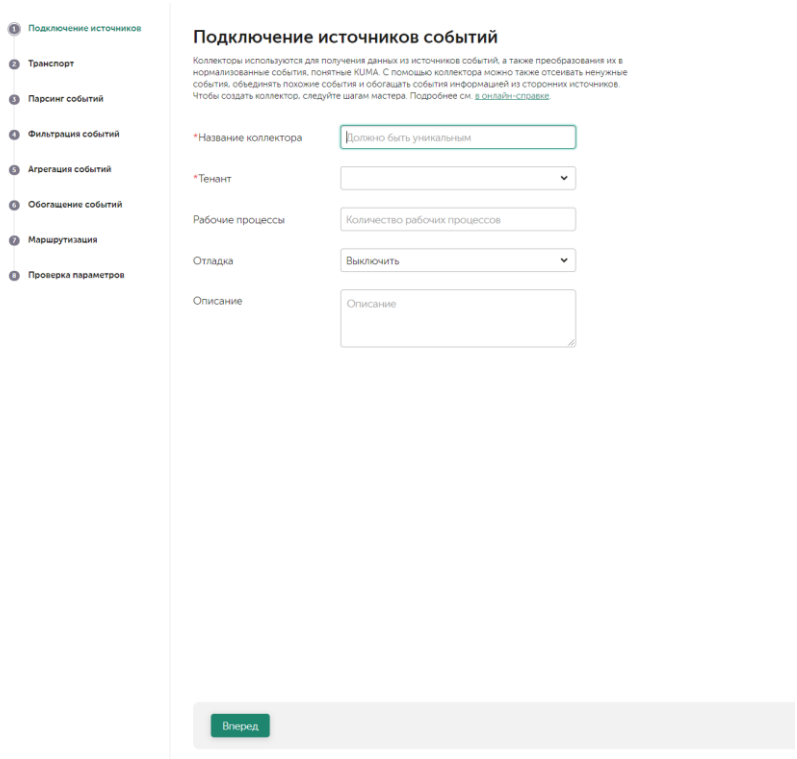


Мастер добавления нового источника

Мастер добавления/ изменения конфигурации коррелятора

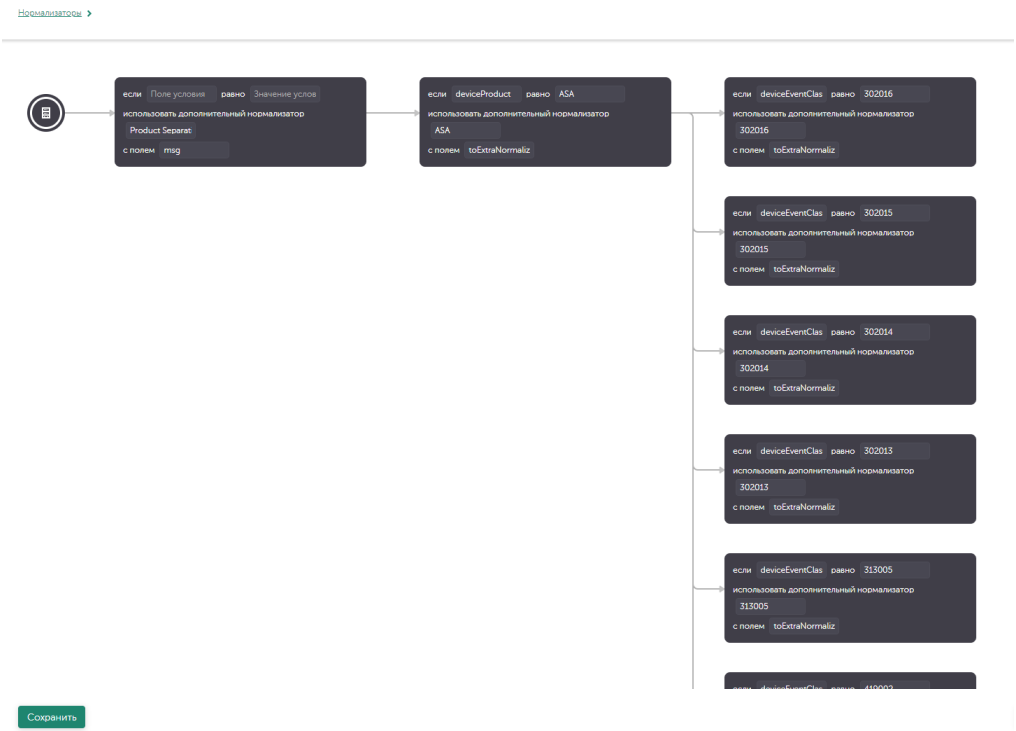
Объединенный интерфейс управления сервисами и ресурсами

Переработанный интерфейс управления ресурсами и сервисами



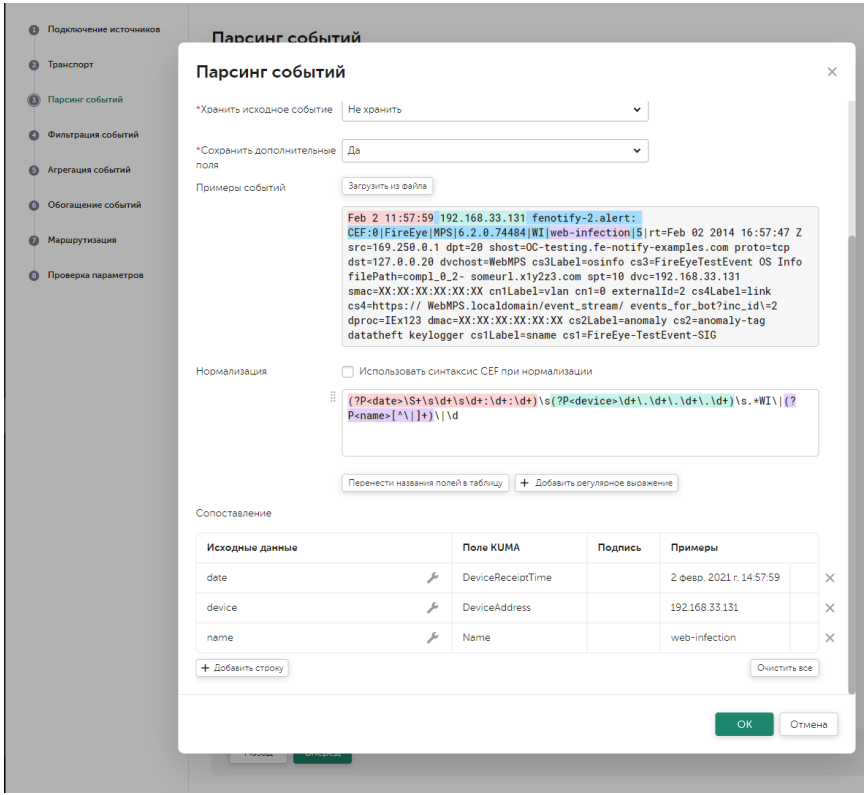
Пошаговый мастер добавления нового источника

Визуализация схемы нормализации



Визуализация иерархической нормализации

Мастер добавления нового источника



Пошаговый мастер для добавления нового источника

Проверка правил нормализации на примерах событий

RESTful API

Возможность работы с ассетами и активными списками

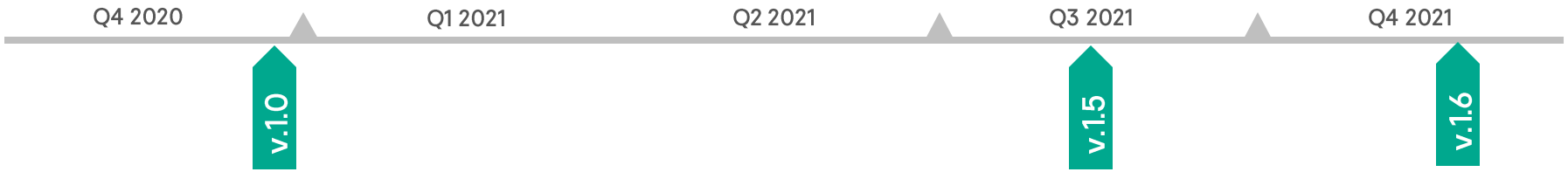
Поддержка multitenancy

Возможность работы с событиями, алертами

Другие новые функции

- Переход на Oracle Linux 8
- Новый пакет правил корреляции (+50шт)
- Поддержка новых источников данных «из коробки»
- Поддержка сбора логов из SQL базы KSC
- Улучшения UI/UX
- Возможность бэкапа и восстановления полной конфигурации
- Авторизация пользователей через AD
- Настраиваемая агрегация алертов
- Расширение списка поддерживаемых источников данных
- Замена инсталлятора на Ansible (поддерживает и распределенную установку)
- .....

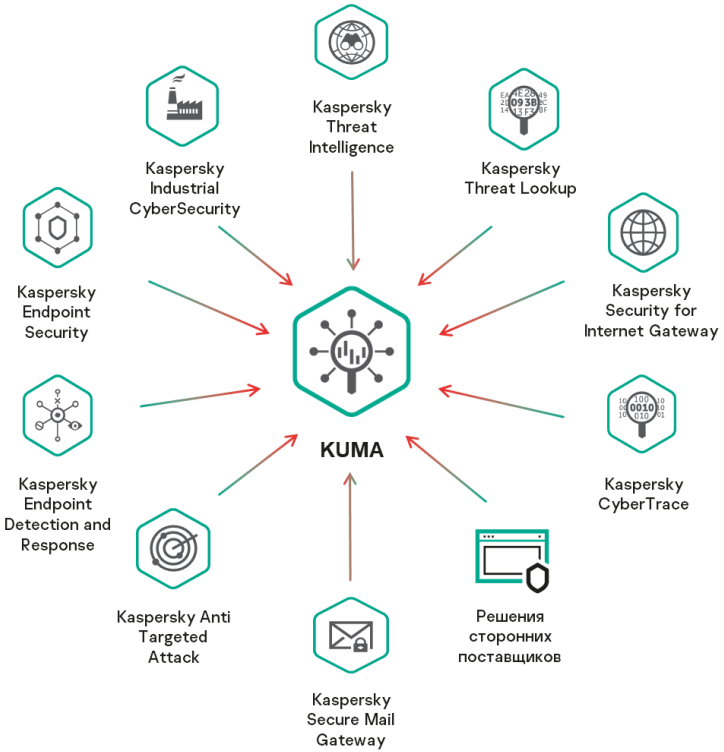
2021 RoadMap for KUMA



Релиз 1.6 (12.2021):

- Поддержка сценариев иерархического развёртывание
- Поддержка Astra Linux («Смоленск»)
- 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

Новые сценарии интеграции с KICS, KEDR, сторонними решениями

Функции оркестрации и автоматизации

Поддержка облачных сценариев

** Возможные направления дальнейшего развития*

Спасибо за внимание !

kaspersky