



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

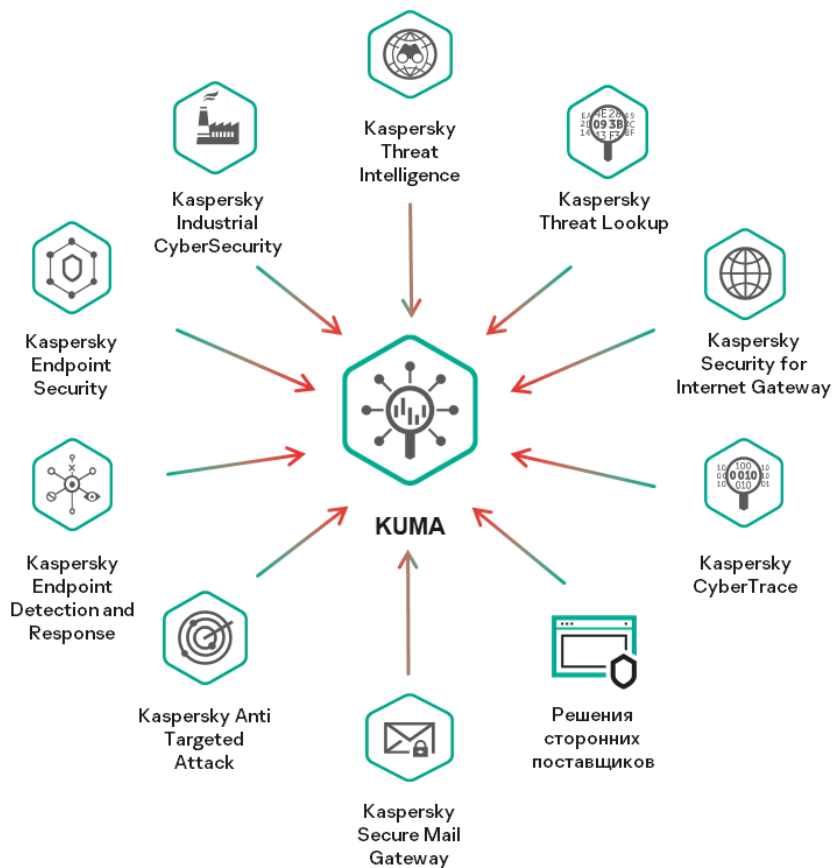
Платформа Kaspersky для мониторинга и анализа инцидентов ИБ. Обзор новых функций

Таратынов Павел,
Архитектор SOC

kaspersky

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

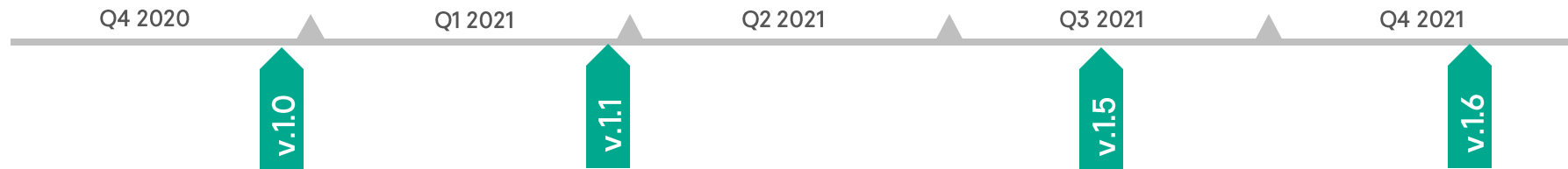
4



Единая консоль
мониторинга и анализа
инцидентов ИБ

2021 RoadMap для KUMA

5



28.12.2020 – релиз KUMA 1.0

27.09.2020 – релиз KUMA 1.5

Q4 2020 – релиз KUMA 1.6



Производительность

До **300k+ EPS** на один узел



Масштабируемость

Вертикальная и
горизонтальная



Низкие системные требования



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**

Обзор новых функций KUMA 1.5



Поддержка Multitenancy

Тенанты

Показать отключенных

<input type="checkbox"/>	Название	Ограничение EPS	Описание	Выключено	Создан
<input type="checkbox"/>	test	0			1 сент. 2021 г. 13:07:23
<input type="checkbox"/>	Main	0			27 авг. 2021 г. 15:45:41

Добавить тенанта

Название

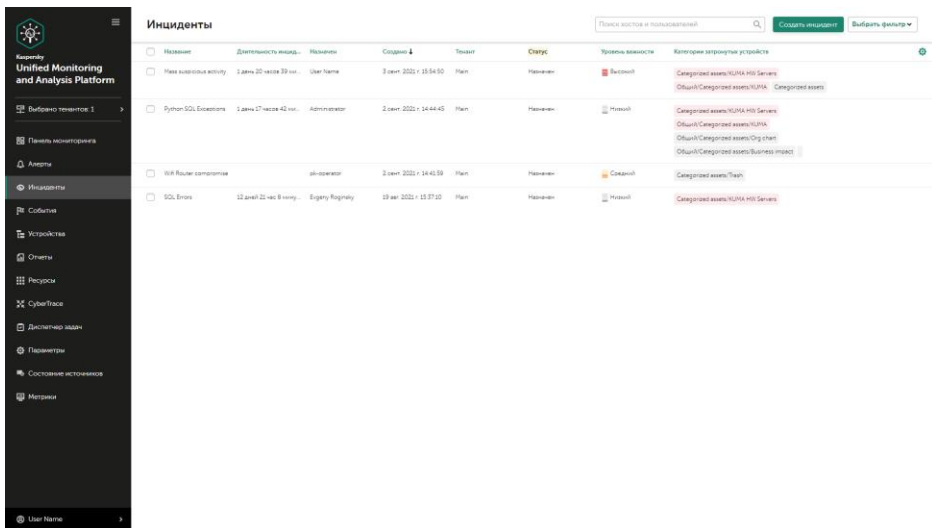
Ограничение EPS

Описание

**Разделение данных,
конфигурации и прав доступа**

**Возможность ограничения
EPS для каждого тенанта
отдельно**

**Целевой сценарий для MSSP
и центров Госсопка**



The screenshot displays the 'Инциденты' (Incidents) section of the Unified Monitoring and Analysis Platform. The interface includes a search bar at the top with the text 'Поиск по названию и пользователям', a 'Создать инцидент' button, and a 'Выбрать фильтр' dropdown. Below the search bar is a table listing incidents with columns for 'Название', 'Длительность инцидента', 'Название пользователя', 'Создан', 'Теги', 'Статус', 'Уровень важности', and 'Категория затронутых устройств'. The table contains five rows of incident data.

Название	Длительность инцидента	Название пользователя	Создан	Теги	Статус	Уровень важности	Категория затронутых устройств
Массовый выход	1 день 20 часов 39 мин.	User Name	3 сен 2022 в 15:54:50	Plan	Назначен	Высокий	Сегрегированность/УСМ/УСМ Серверы Общ./УСМ/Сегрегированность/УСМ/УСМ Серверы
Рухнул SQL Базы данных	1 день 27 часов 42 мин.	Администратор	2 сен 2022 в 14:44:45	Plan	Назначен	Низкий	Сегрегированность/УСМ/УСМ Серверы Общ./УСМ/Сегрегированность/УСМ/УСМ Серверы Общ./УСМ/Сегрегированность/УСМ/УСМ Серверы Общ./УСМ/Сегрегированность/УСМ/УСМ Серверы Общ./УСМ/Сегрегированность/УСМ/УСМ Серверы
WSR Выход компьютера		администратор	3 сен 2022 в 14:41:59	Plan	Назначен	Средний	Сегрегированность/УСМ/УСМ Серверы
SQL Errors	12 дней 22 час 8 мин.	Владимир Рогачев	02 сен 2022 в 13:37:10	Plan	Назначен	Низкий	Сегрегированность/УСМ/УСМ Серверы

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

**Создание инцидентов
автоматически или вручную**

Экспорт в НКЦКИ

The screenshot displays the 'Устройства' (Devices) management interface. On the left, a tree view shows 'Все устройства' (All devices) with categories like 'Categorized assets', 'Address space', 'Application', 'Business impact', 'Device type', 'КЦМА HW Servers', 'Location', 'OS', 'Org chart', and 'Other'. The 'OS' category is expanded, showing 'Windows' and 'Общий' (General). A search bar and a list of assets are visible. On the right, the 'Изменить категорию' (Change category) dialog is open, showing fields for 'Название' (Name), 'Родительская категория' (Parent category), 'Тенит' (Tenant), 'Способ категоризации' (Categorization method), and 'Уровень важности' (Importance level). Below these fields, there are options for 'Автоматическая категоризация выключена' (Automatic categorization is disabled), 'Регулярность категоризации' (Categorization frequency), and 'Условия' (Conditions). The conditions are set to 'Если ОС [И] [или] Windows' (If OS [AND] [OR] Windows). Buttons for 'Сохранить' (Save) and 'Отмена' (Cancel) are at the bottom.

Динамическая категоризация по:

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

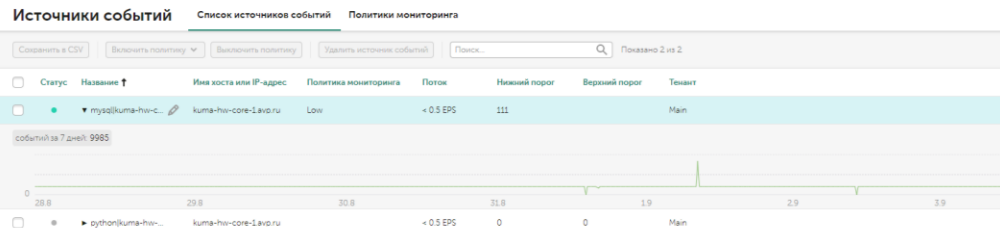
Логические операторы AND, OR, NOT и группировки

Возможность проверки условий

Мониторинг доступности источников

15

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

16

- 1 Подключение источников
- 2 **Транспорт**
- 3 Парсинг событий
- 4 Фильтрация событий
- 5 Агрегация событий
- 6 Обогащение событий
- 7 Маршрутизация
- 8 Проверка настроек

Транспорт

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

Основные параметры

Дополнительные параметры

*Коннектор	<input type="text" value="Создать"/>	?
*Тип	<input type="text" value=""/>	?
*URL	<input type="text" value=""/>	?
Описание		

internal

tcp

udp

netflow

nats

kafka

http

sql

file

ftp

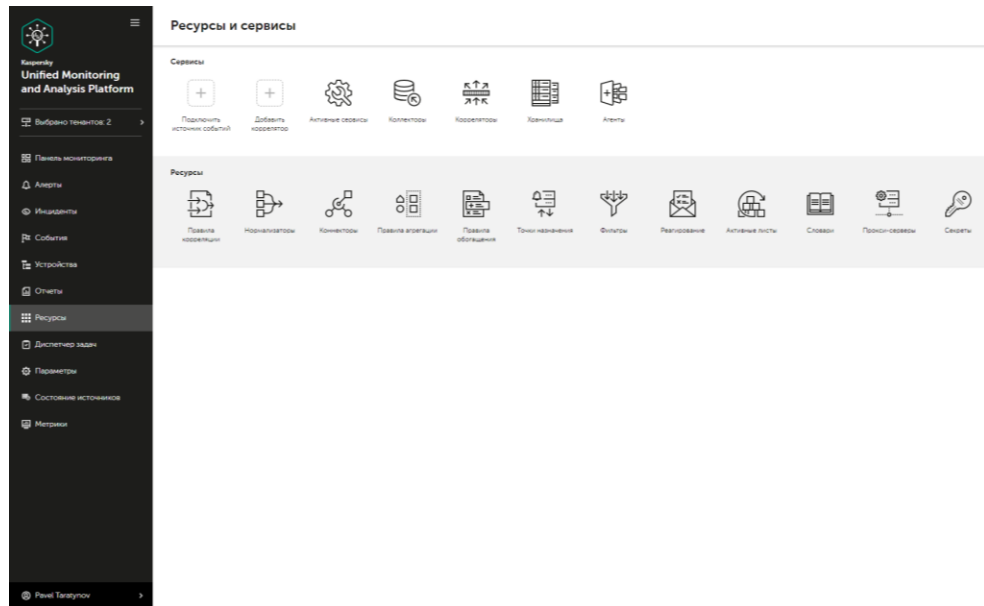
nfs

wmi

wec

snmp

**Поддержка сбора событий
через механизм Windows
Management Instrumentation
(WMI)**



Мастер добавления нового источника

Мастер добавления / изменения конфигурации коррелятора

Объединенный интерфейс управления сервисами и ресурсами

1 Подключение источников

2 Транспорт

3 Парсинг событий

4 Фильтрация событий

5 Агрегация событий

6 Обогащение событий

7 Маршрутизация

8 Проверка параметров

Подключение источников событий

Коллекторы используются для получения данных из источника событий, а также преобразования их в нормализованные события, понятные ЦИМД. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. в [онлайн-справке](#).

*Название коллектора

*Тенант

Рабочие процессы

Отладка

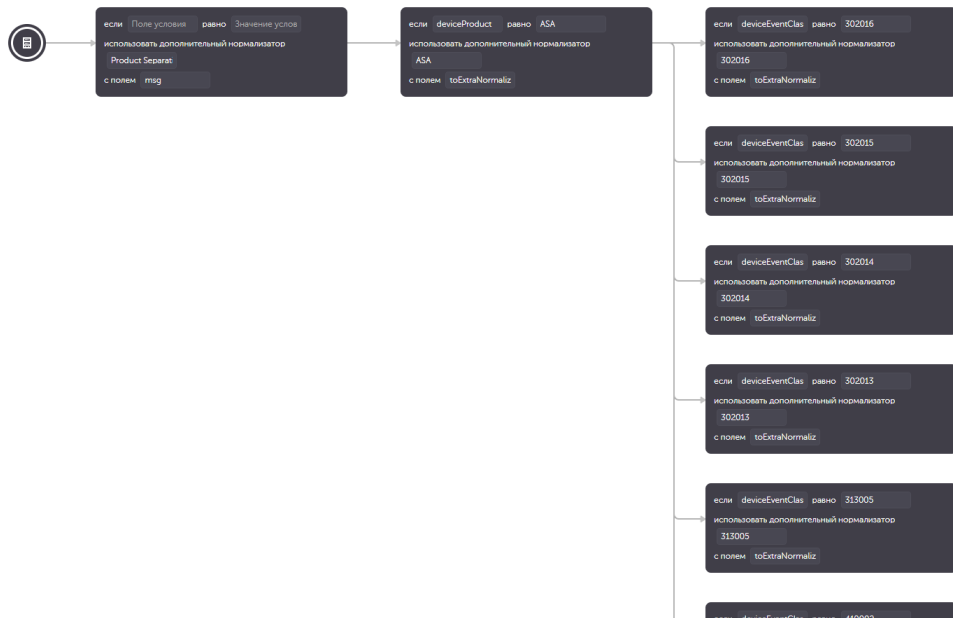
Описание

Вперед

Пошаговый мастер добавления нового источника

Визуализация схемы нормализации

[Настройка](#) >



Визуализация иерархической нормализации

Сохранить

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Парсинг событий

Хранить исходное событие: Не хранить

Сохранить дополнительные поля: Да

Примеры событий: Загрузить из файла

```
Feb 2 11:57:59 192.168.33.131 fenotify-2.alert:
CEF:0|FireEye|MPS|6.2.0.74484|WI|web-infection|S|rt=Feb 02 2014 16:57:47 Z
src=169.258.0.1 dpt=20 shost=0C-testing.fe-notify-examples.com proto=tcp
dst=127.0.0.20 dvchost=WebMPS cs3Label=osinfo cs3=FireEyeTestEvent OS Info
filePath=comp1_0_2- someurl.x1y2z3.com spt=10 dvc=192.168.33.131
smac=XX:XX:XX:XX:XX:XX cn1Label=vlan cn1=0 externalId=2 cs4Label=link
cs4=https:// WebMPS.localdomain/event_stream/ events_for_bot?inc_id=2
dproc=IEx123 dmac=XX:XX:XX:XX:XX cs2Label=anomaly cs2=anomaly-tag
datatheft keylogger cs1Label=sname cs1=FireEye-TestEvent-SIG
```

Нормализация

Использовать синтаксис CEF при нормализации

```
(?P<date>)\s+(\d{4}|\d{2}|\d{1})\s+(?P<device>\d{1}.\d{1}.\d{1})\s.*WI\|(?
P<name>[^\|]+)\| \d
```

Перенести названия полей в таблицу + Добавить регулярное выражение

Сопоставление

Исходные данные	Поле KUMA	Подпись	Примеры	
date	DeviceReceiptTime		2 фев. 2021 г. 14:57:59	X
device	DeviceAddress		192.168.33.131	X
name	Name		web-infection	X

+ Добавить строку Очистить все

OK Отмена

Пошаговый мастер для добавления нового источника

Проверка правил нормализации на примерах событий

RESTful API

Возможность работы с
ассетами и активными
списками

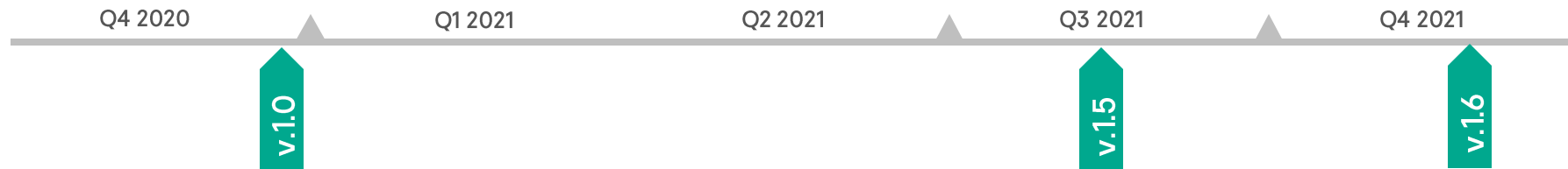
Поддержка multitenancy

Возможность работы с
событиями, алертами

- 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

23

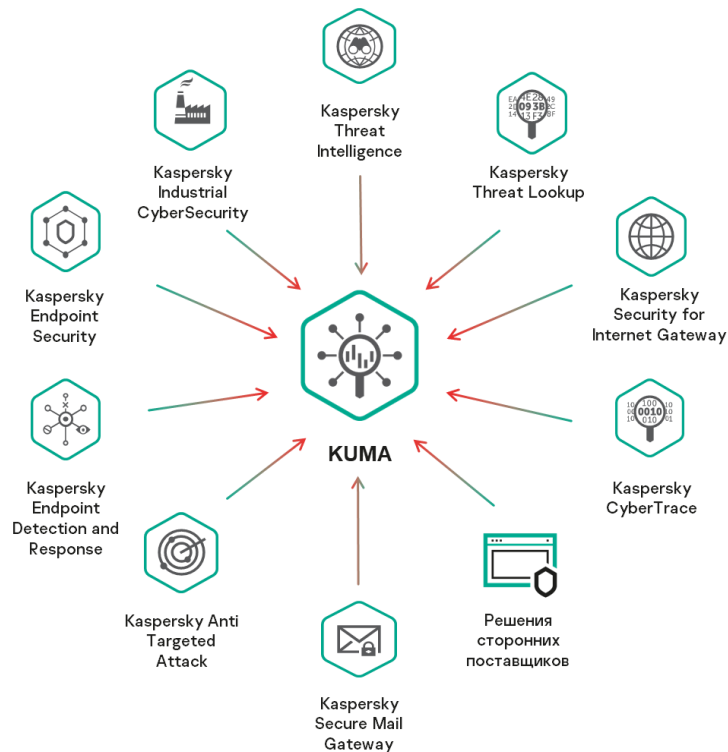


Релиз 1.6 (12.2021):

- Поддержка сценариев иерархического развёртывание
- Поддержка Astra Linux («Смоленск»)
- Утилита для конвертации sigma-правил в ресурсы KUMA
- Расширение списка поддерживаемых источников логов
- Расширение набора правил корреляции

Дальнейшее развитие решения*

24



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