

Панель мониторинга

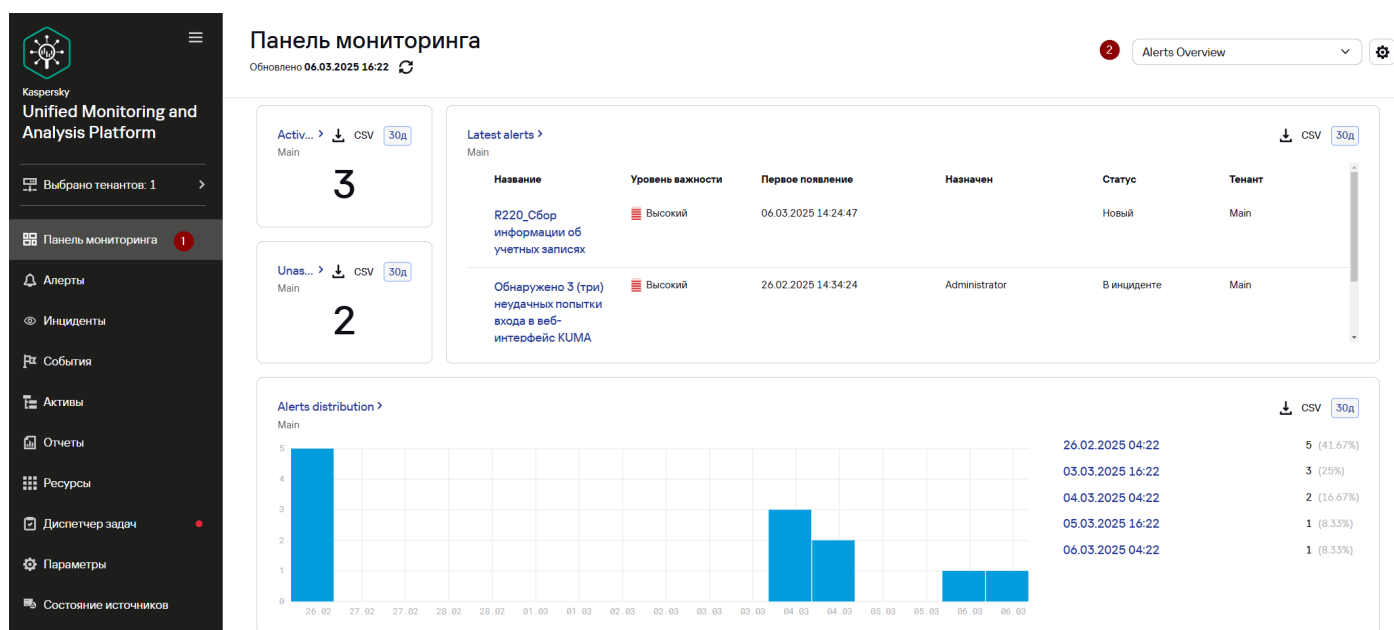
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в онлайн-справке на продукт: <https://support.kaspersky.ru/kuma/4.0/217855>

Видео «Типовые операции с панелями мониторинга и отчетами»:
<https://rutube.ru/video/304bc4fd81bae7219ade8c3a3d717213/>

Панель мониторинга представляет собой набор виджетов, которые визуализируют статистику по собранным/обработанным данным.

Набор виджетов, используемых на панели мониторинга, называется макетом. Вы можете создавать макеты вручную или воспользоваться предустановленными макетами (<https://support.kaspersky.ru/kuma/4.0/222445>). Параметры виджетов в предустановленных макетах можно редактировать при необходимости. По умолчанию на панели мониторинга отображается предустановленный макет **Alerts Overview**.



Создавать, редактировать и удалять макеты могут только пользователи с ролями Главный администратор, Администратор тенанта, Аналитик второго уровня и Аналитик первого уровня. Пользователи с учетными записями всех ролей могут просматривать макеты и

назначать макеты по умолчанию. Если макет назначен по умолчанию, этот макет отображается для учетной записи при каждом переходе в раздел **Панель мониторинга**.

Информация на панели мониторинга обновляется в соответствии с расписанием, заданным в параметрах макета. При необходимости вы можете обновить данные принудительно, нажав на  .

Для удобства представления данных на панели мониторинга вы можете включить режим ТВ. В этом случае вы перейдете в режим полноэкранного просмотра панели мониторинга в FullHD-разрешении. В режиме ТВ вы также можете настроить показ слайд-шоу для выбранных макетов.



Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга 1

Алерты

Инциденты

События

Панель мониторинга

Обновлено 06.03.2025 16:22

Alerts Overview

3

2

Название	Уровень важности	Первое появление	Назначен	Статус	Тенант
R220_Сбор информации об учетных записях	Высокий	06.03.2025 14:24:47		Новый	Main
Обнаружено 3 (три) неудачных попытки входа в веб-интерфейс KUMA	Высокий	26.02.2025 14:34:24	Administrator	В инциденте	Main

Параметры

Режим ТВ

Включено 1

Слайд-шоу

Включено 2

Время ожидания

00:05

3

Очередь

Если вы хотите определить очередь - перетащите макеты в очередь из левой таблицы, либо переместите выбранные элементы с помощью кнопки, в ином случае - отображаться будет в соответствии со списком из первой колонки.

> Добавить в очередь

☐ Все макеты

☐ Alerts Overview

☐ Incidents Overview

☐ Network Overview

☐ [OOTB] KATA & EDR

☐ [OOTB] KSC

☐ [OOTB] KSMG

☐ [OOTB] KWTS

✕ Удалить

Очередь макетов



Пусто

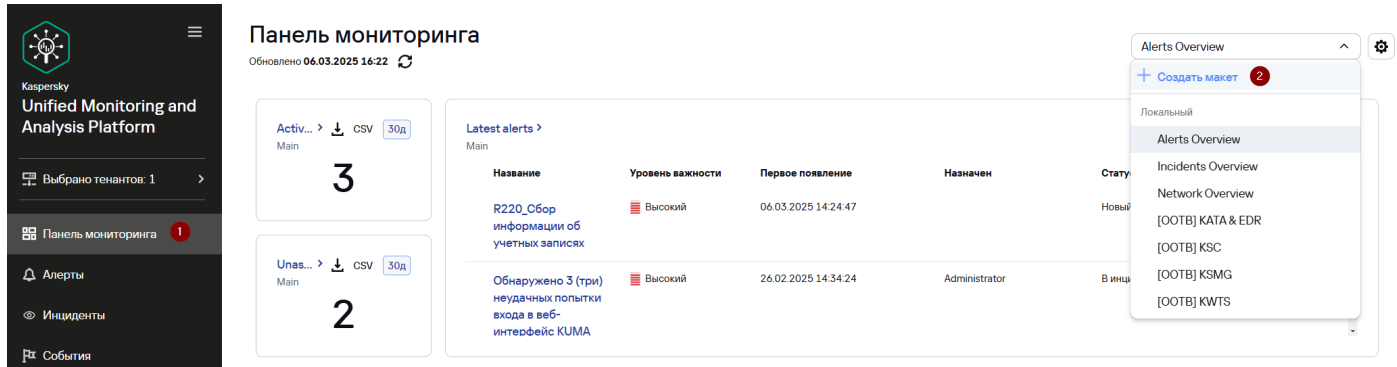
Сохранить

Отмена

В качестве примера создадим «кастомный» макет со статистикой по KUMA.

Чтобы создать макет:

- Перейдите в раздел **Панель мониторинга**.
- Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите **Создать макет**.

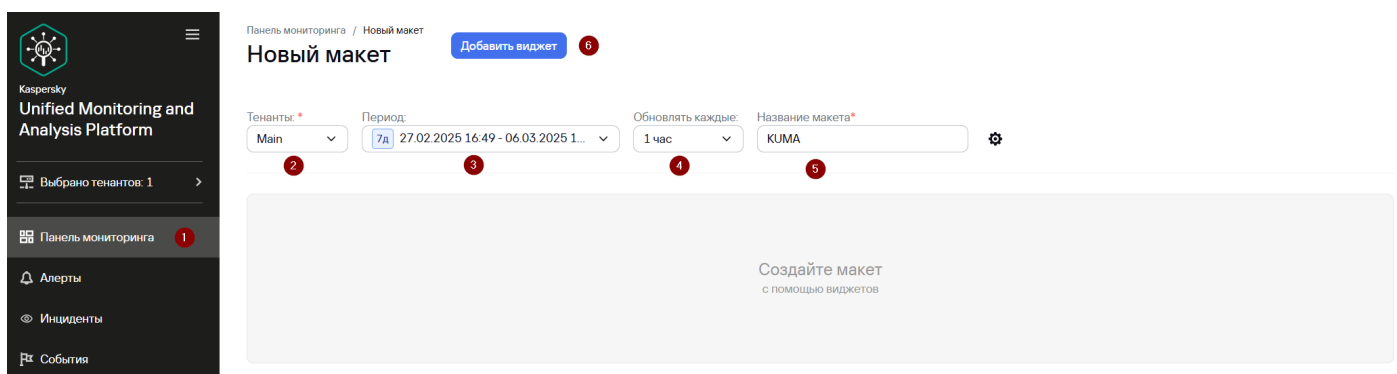


- Откроется окно **Новый макет**.
- В раскрывающемся списке **Тенанты** выберите тенанты (в нашем примере **Main**), которым будет принадлежать создаваемый макет и данными из которых будут наполняться виджеты макета.
- В раскрывающемся списке **Период** выберите период времени, по которому требуется аналитика. В нашем примере – 7 дней.
- В раскрывающемся списке **Обновлять каждые** выберите частоту обновления данных в виджетах макета. В нашем примере 1 час.
- В поле **Название макета** укажите название макета.

Первым создадим виджет со статистикой по количеству нормализованных событий от каждого типа источника за неделю.

Чтобы добавить виджет:

- В раскрывающемся списке **Добавить виджет** выберите виджет **События**. Данный тип виджета будет строится на основе событий из хранилища.



- В появившемся окне справа укажите:

- Во вкладке :
 - **График** – Круговая диаграмма
 - **Тенант** – Main
 - **Период** – Как на макете
 - Хранилище – выберите сервис Хранилища. В нашем примере [OOTB] **Storage**.
 - В поле SQL-запроса (т.е. данные на основании, которых будет строиться виджет) укажите следующий поисковый запрос:

```
SELECT count(ID) AS `metric`, DeviceProduct AS `value` FROM `events` WHERE DeviceProduct != ''  
GROUP BY DeviceProduct ORDER BY metric DESC LIMIT 10
```

- Нажмите **Предварительный просмотр**, чтобы убедиться, что SQL-запрос корректен и выполняется успешное построение виджета.

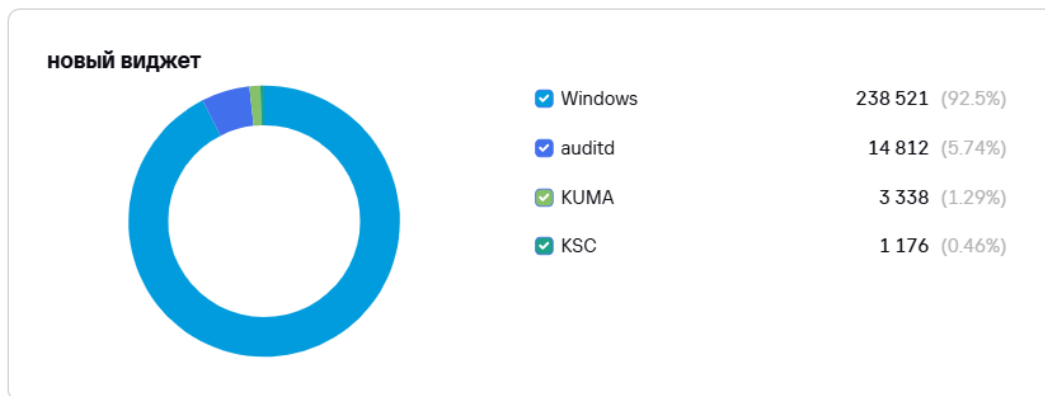


График: Круговая диаграмма 1

Тенант: Main 2

Период: Как на макете 3

Хранилище*: Хранилище: [OOTB] Storage 4

Максимальное количество значений, которые могут отображаться в круговых диаграммах в форматах PDF и HTML: 20. Для просмотра полных данных скачайте отчет в формате CSV.

5

```
SELECT count(ID) AS `metric`, DeviceProduct AS `value` FROM `events` WHERE DeviceProduct != '' GROUP BY DeviceProduct ORDER BY metric DESC LIMIT 10
```

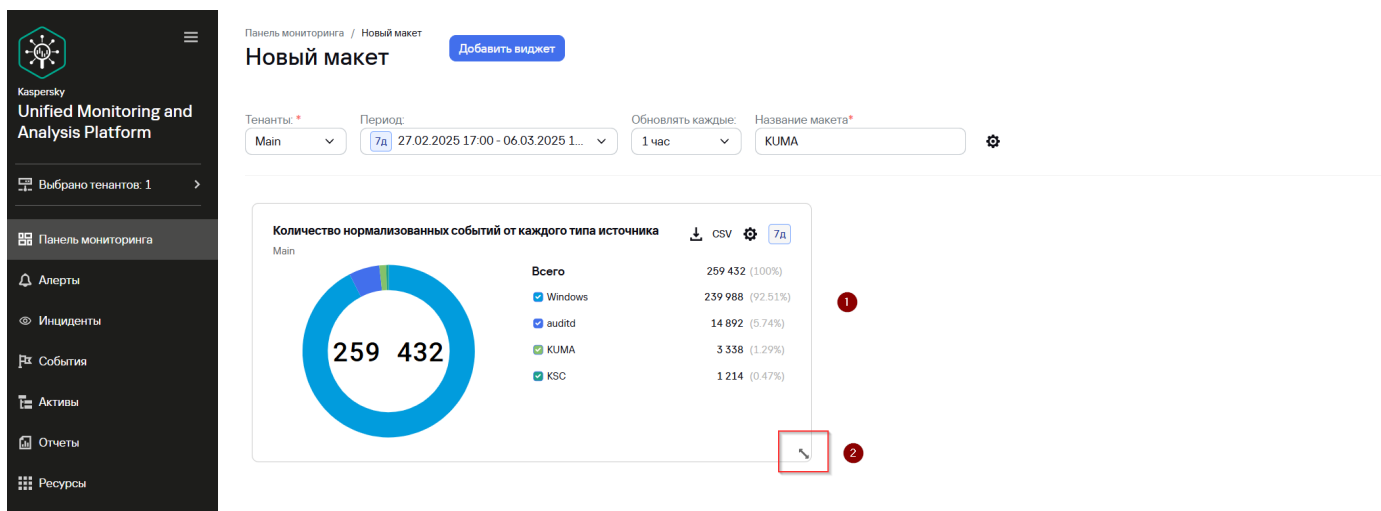
6

Предварительный просмотр

Добавить

Отмена

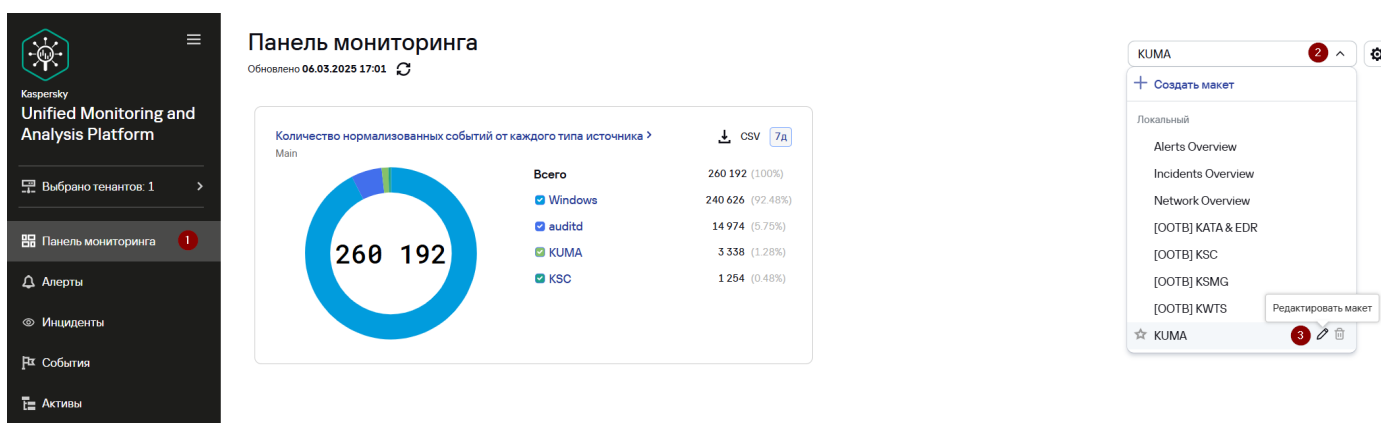
- Во вкладке :
 - Укажите **Название виджета**. В нашем примере **Количество нормализованных событий от каждого типа источника**.
 - Активируйте параметр **Итоговые значения**.
 - Нажмите **Добавить**.
- Виджет будет добавлен на макет. Виджеты можно перетаскивать по окну и изменять их размер с помощью кнопки , которая появляется при наведении указателя мыши на виджет.



Вторым создадим виджет со статистикой по количеству и типу действий пользователей в KUMA.

Чтобы добавить новый виджет на макет KUMA:

- Откройте раскрывающийся список в правом верхнем углу окна **Панель мониторинга** и выберите макет KUMA.
- Нажмите **Редактировать макет**.



- В раскрывающемся списке **Добавить виджет** выберите виджет **События**.
- В появившемся окне справа укажите:
 - Во вкладке :
 - **График** – Столбчатая диаграмма
 - **Тенант** – Main
 - **Период** – Как на макете
 - **Хранилище** – выберите сервис Хранилища. В нашем примере [OOTB] Storage.
 - Возле поля SQL-запроса нажмите на кнопку  для формирования SQL-запроса с помощью конструктора.
 - В появившемся окне **Формирование SQL-запроса** заполните поля как на скриншоте ниже и нажмите **Применить**.

Формирование SQL-запроса



Поля событий, указанные в блоках SELECT и WHERE, будут добавлены в таблицу событий в качестве столбцов. Поля событий из блока WHERE помещаются в таблицу, только если для них выбран оператор, отличный от "=".



SELECT

[-]

ID

▼

metric

count

▼

[-]

DeviceAction

▼

value

1

FROM

events

WHERE

AND

Добавить условие

Добавить группу

⋮

Type

▼

=

▼

Audit

▼

×

2

GROUP BY

DeviceAction

▼

3

ORDER BY

[-]

metric

▼

↓ DESC

▼

LIMIT

50

4

При нажатии на кнопку Применить текущий SQL-запрос будет перезаписан.



5

Применить

Запрос по умолчанию

- Сформированный запрос из конструктора появится в поле SQL-запроса.



```
SELECT count(ID) AS `metric`, DeviceAction AS `value` FROM `events` WHERE Type = 4  
GROUP BY DeviceAction ORDER BY metric DESC LIMIT 50
```

- Нажмите **Предварительный просмотр**, чтобы убедиться, что SQL-запрос корректен и выполняется успешное построение виджета.

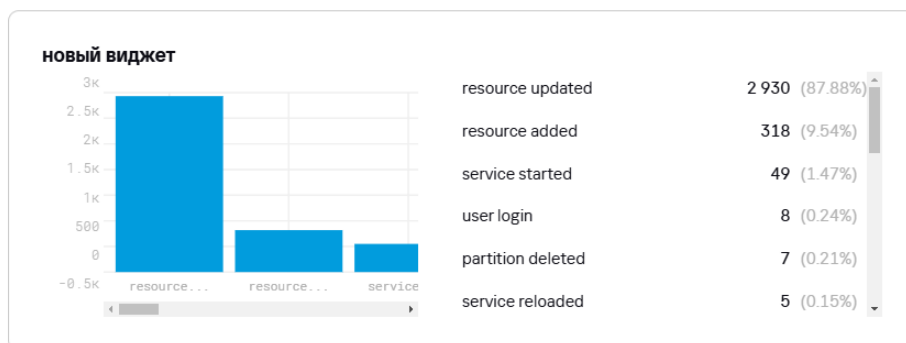


График: Столбчатая диаграмма 1

Тенант: Main 2

Период: Как на макете 3

Показывать данные за предыдущий период: ☐

Хранилище*: Хранилище: [OOTB] Storage 4

Максимальное количество значений, которые могут отображаться в столбчатых и календарных диаграммах в форматах PDF и HTML: 40. Для просмотра полных данных скачайте отчет в формате CSV.

`SELECT count(ID) AS `metric`, DeviceAction AS `value` FROM `events` WHERE Type = 4 GROUP BY DeviceAction ORDER BY metric DESC LIMIT 50` 5

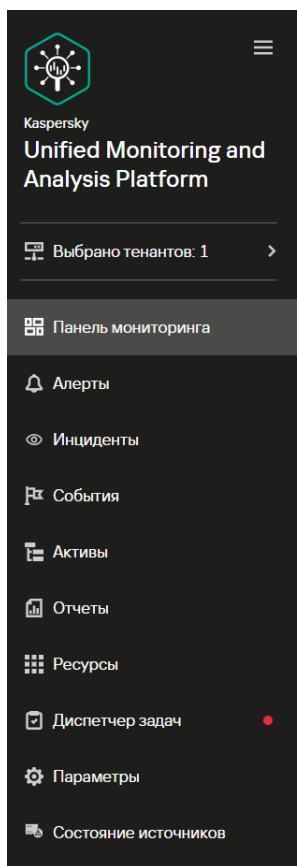
6

Предварительный просмотр

Добавить

Отмена

- Во вкладке :
 - Укажите **Название виджета**. В нашем примере **Действия пользователей в KUMA**.
 - Активируйте параметр **Итоговые значения**.
 - Нажмите **Добавить**.
- Виджет будет добавлен на макет. Виджеты можно перетаскивать по окну и изменять их размер с помощью кнопки , которая появляется при наведении указателя мыши на виджет.



Панель мониторинга / Настройка макета

Настройка макета

Добавить виджет

Тенанты: *

Main

Период:

7д

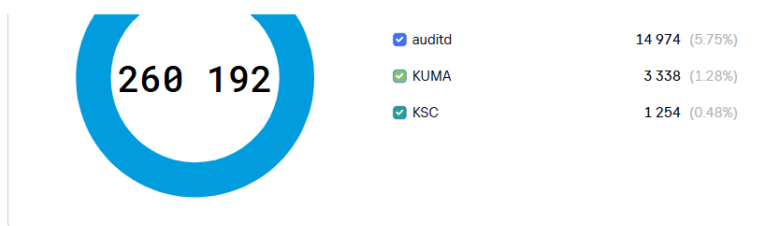
27.02.2025 17:19 - 06.03.2025 1...

Обновлять каждые:

1 час

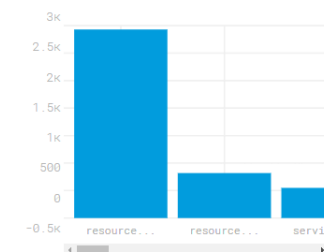
Название макета*

KUMA



Действия пользователей в KUMA

Main



Всего

3 334 (100%)

resource updated

2 930 (87.88%)

resource added

318 (9.54%)

service started

49 (1.47%)

user login

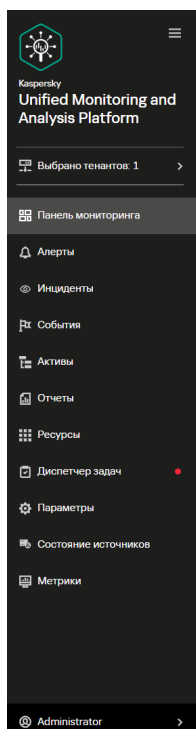
8 (0.24%)

partition deleted

7 (0.21%)

service reloaded

5 (0.15%)



Панель мониторинга / Настройка макета

Настройка макета

Добавить виджет

Тенанты: *

Main

Период:

7д

27.02.2025 17:20 - 06.03.2025 1...

Обновлять каждые:

1 час

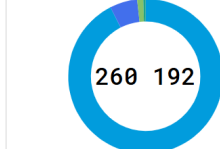
Название макета*

KUMA



Количество нормализованных событий от каждого типа источника

Main



Всего

260 192 (100%)

Windows

240 626 (92.48%)

auditd

14 974 (5.75%)

KUMA

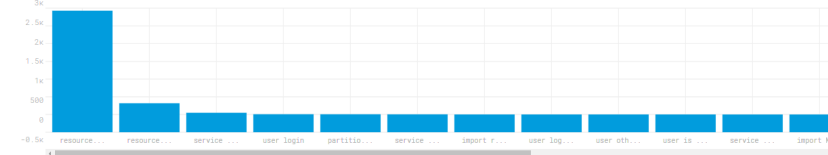
3 338 (1.28%)

KSC

1 254 (0.48%)

Действия пользователей в KUMA

Main



Всего

3 334 (100%)

resource updated

2 930 (87.88%)

resource added

318 (9.54%)

service started

49 (1.47%)

user login

8 (0.24%)

partition deleted

7 (0.21%)

service reloaded

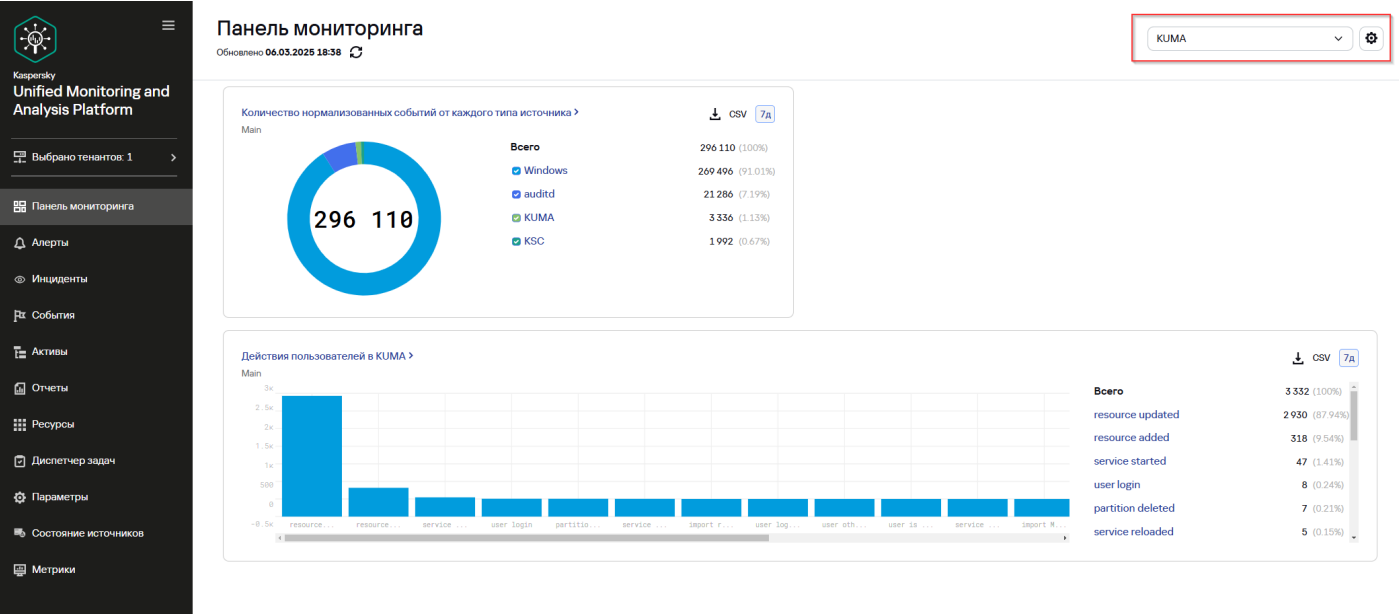
5 (0.15%)

Сохранить

Отмена

- Нажмите **Сохранить** для сохранения макета.

Новый макет создан и отображается в разделе **Панель мониторинга** веб-интерфейса KUMA.





Касперский
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События 1

Активы

Отчеты

Ресурсы

Диспетчер задач

Параметры

Состояние источников

Метрики

События

Не обновлять

7d 28.02.2025 13:02:13 - 0...

[OOTB] Storage (Main...

...

1 SELECT * FROM 'events' WHERE Type = 4 AND DeviceAction = 'user login' ORDER BY Timestamp DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	DeviceHostName	DeviceAction	SourceAddress	SourceUserName	EventOutcome
Main	07.03.2025 11:35:39.484	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	admin	succeeded
Main	06.03.2025 14:23:04.369	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	admin	succeeded
Main	05.03.2025 18:00:13.666	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.32.46.142	admin	succeeded
Main	05.03.2025 16:58:42.524	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.32.46.142	admin	succeeded
Main	04.03.2025 13:21:06.022	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	admin	succeeded
Main	03.03.2025 19:05:21.718	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	admin	succeeded
Main	03.03.2025 15:24:18.500	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	borisov	succeeded
Main	28.02.2025 17:24:55.657	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	admin	succeeded
Main	28.02.2025 14:26:22.487	Kaspersky	KUMA	kuma-aiot.truecompany.local	user login	10.16.58.77	borisov	succeeded

Revision #2
Created 2026-08-12 17:12:55 UTC by Dmitry Borisov
Updated 2026-08-12 17:33:20 UTC by Dmitry Borisov