Отслеживание состояния источников событий

> 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/4.0/249532

> Видео «Типовые операции с панелями мониторинга и отчетами»: https://rutube.ru/video/4dae62d146a819a2044fbc45f07ac65a/

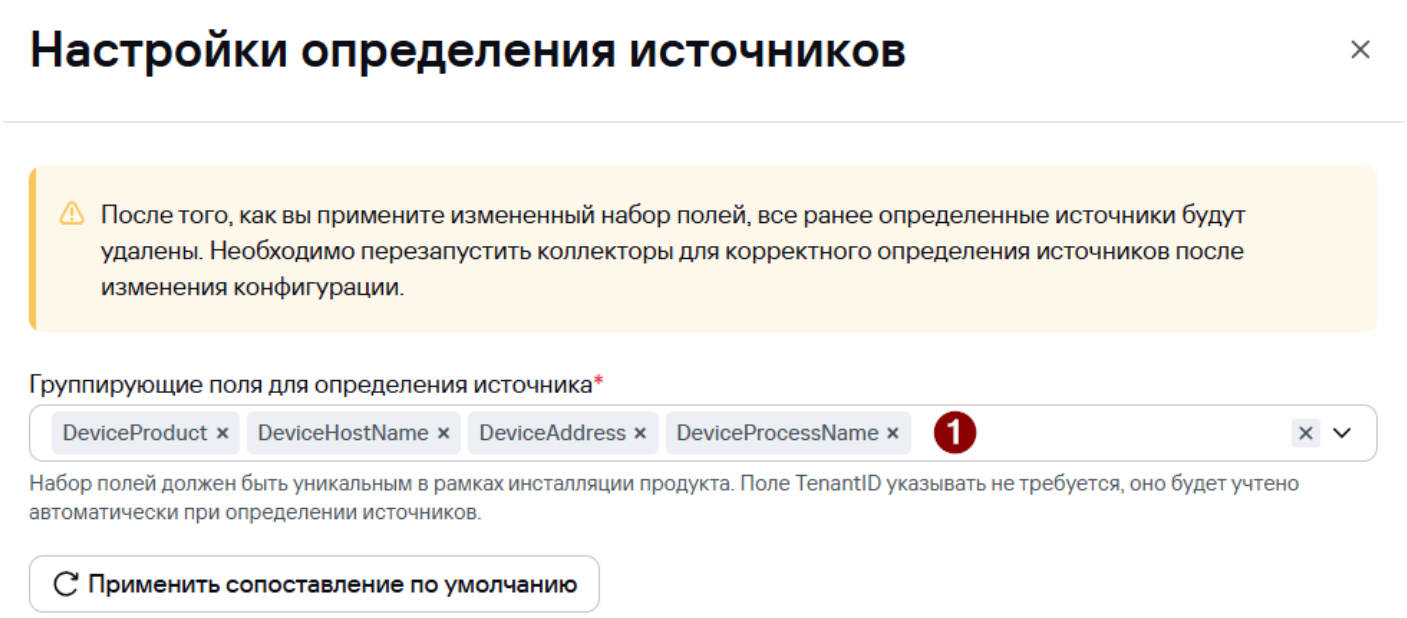
В KUMA можно контролировать состояние источников, от которых поступают события в коллекторы.

Например, можно обнаружить, когда поток событий стал аномально большим, ниже типовых значений или вообще прекратился. Для отслеживания таких ситуаций используются политики мониторинга.

Политика мониторинга применяется к источнику событий, сформированному на основании поступающих в коллекторы событий.

По умолчанию KUMA автоматически формирует список источников на основании набора полей по умолчанию:

- DeviceProduct.
- DeviceHostName.
- DeviceAddress.
- DeviceProcessName



> Источник определяется, только если в событии заполнены поля: DeviceProduct + DeviceAddress и/или DeviceHostname + TenantID.

При необходимости можно задать собственный пользовательский набор полей – от 1 до 9 полей на выбор в желаемой последовательности.

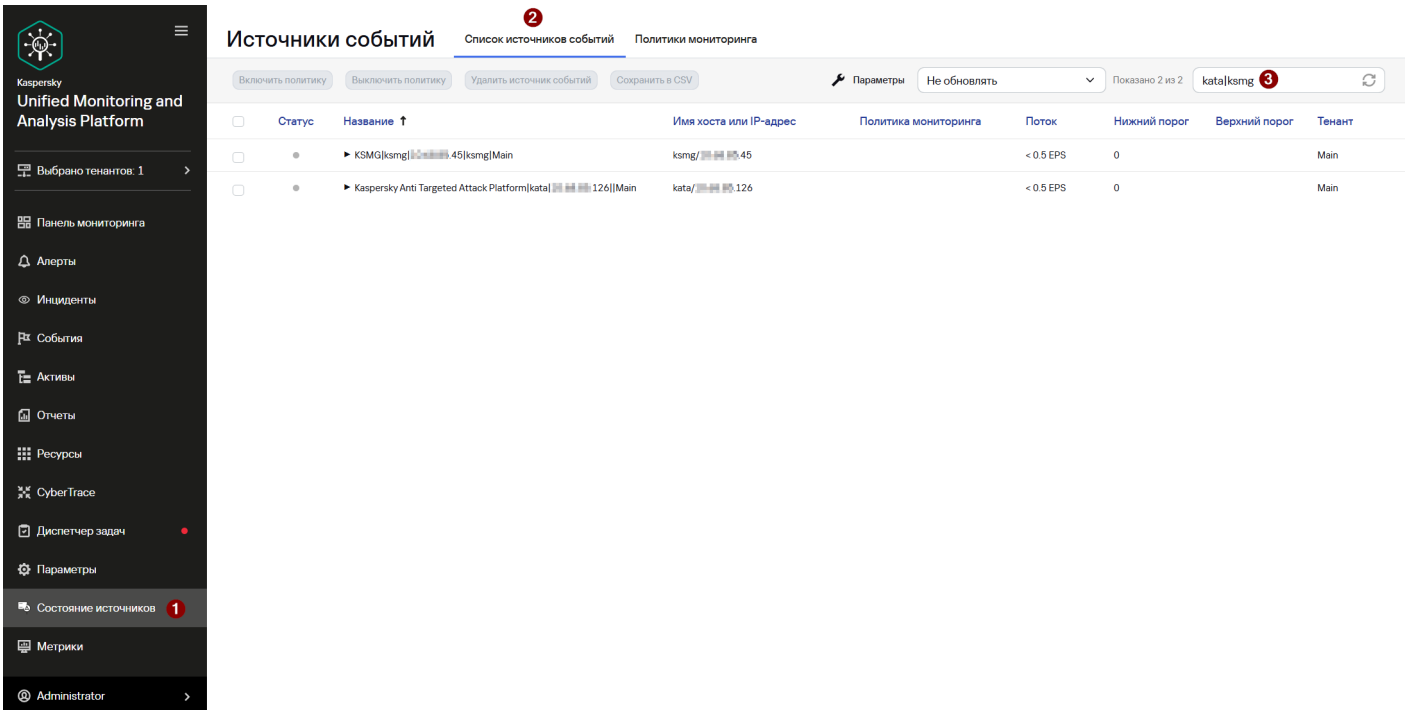
После того как вы сохраните изменения в наборе полей, ранее определенные источники событий будут удалены из веб-интерфейса KUMA и из базы данных. Чтобы измененные параметры вступили в силу и KUMA начала определять источники с учетом новых параметров, перезапустите коллекторы.

> Описание логики определения источников событий в зависимости от наличия непустых значений в полях событий:
>
> https://support.kaspersky.ru/kuma/4.0/221645?page=help

> Один набор полей действует для всей инсталляции.

Чтобы просмотреть сформированный список источников:

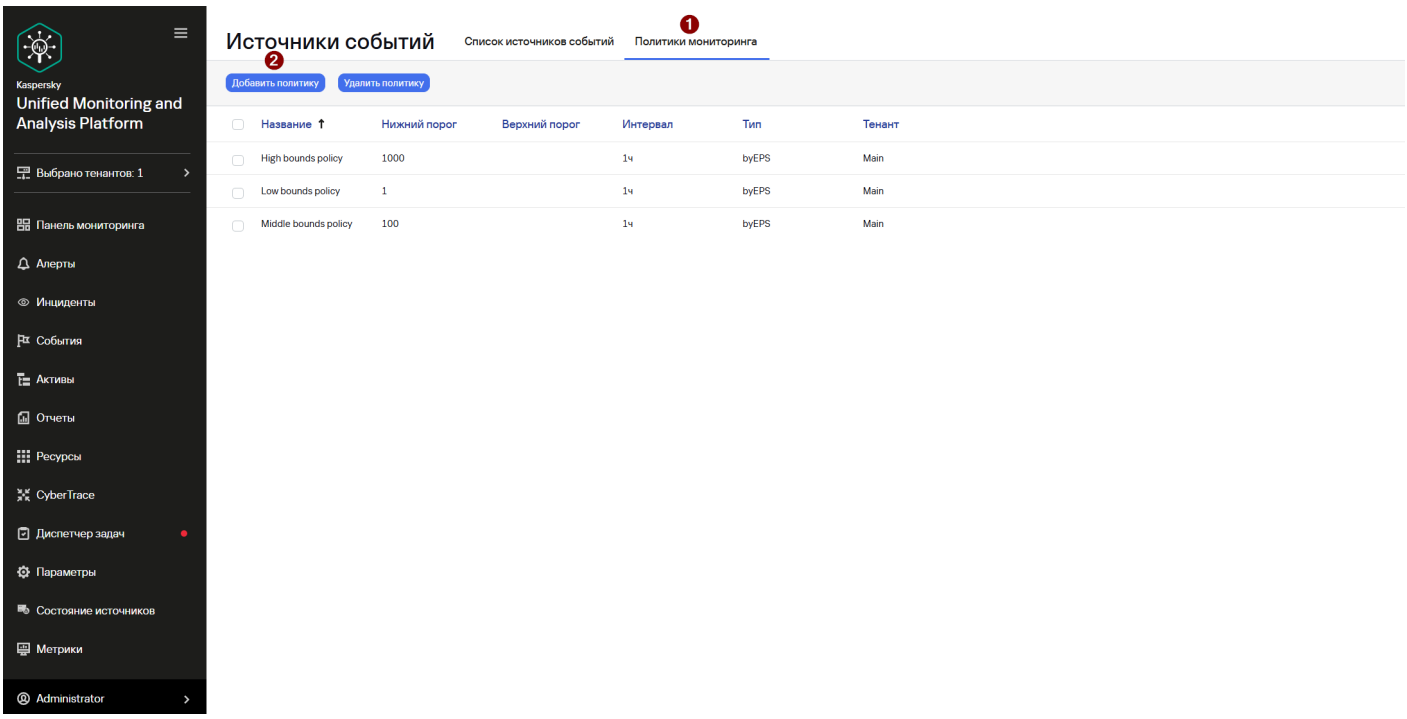
- Перейдите в раздел **Состояние источников**.
- Выберите вкладку **Список источников событий**.
- Опционально в поле **Поиск** справа укажите определенное имя источника событий.



> Описание столбцов, доступных на вкладке Список источников событий: https://support.kaspersky.ru/kuma/4.0/221773

Чтобы создать политику мониторинга:

- Перейдите в раздел **Состояние источников** → **Политики мониторинга**.
- Нажмите **Добавить политику** и в открывшемся окне **Создание политики** укажите следующие параметры:



- В поле **Название политики** введите имя создаваемой политики.

- В раскрывающемся списке **Тенант** выберите тенант, которому будет принадлежать политика. От выбора тенанта зависит, для каких источников событий можно будет включить политику мониторинга.
- В раскрывающемся списке **Тип политики** выберите один из следующих вариантов:
  - **byCount** – по количеству событий за определенный промежуток времени.
  - **byEPS** – по количеству событий в секунду за определенный промежуток времени. Считается среднее значение за весь промежуток. Можно дополнительно отслеживать скачки в определенные периоды.

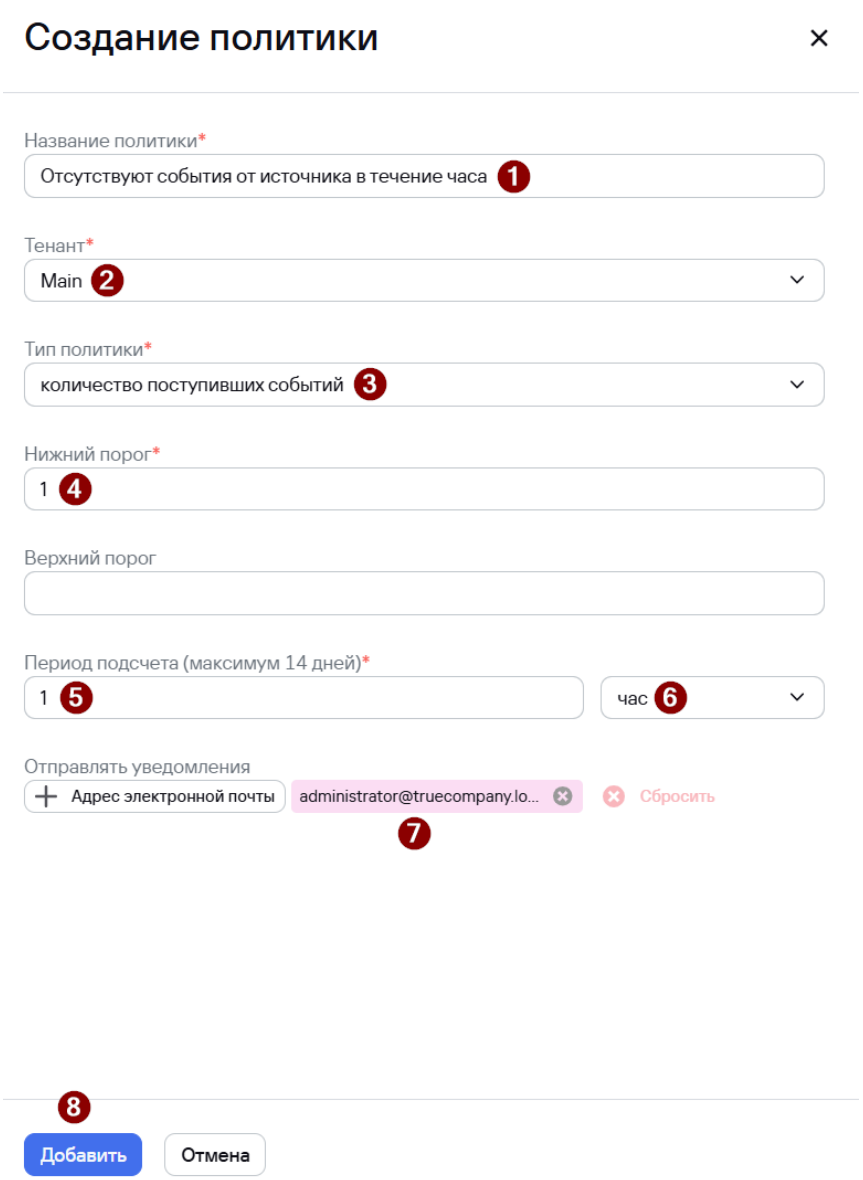
В нашем примере будет создана политика (по количеству поступивших событий), которая срабатывает в случае, если от источника в течение часа будут отсутствовать события.

- В поле **Нижний порог** и **Верхний порог** определите, выход за какие границы будет считаться отклонением от нормы, при котором политика мониторинга будет срабатывать, создавая алерт и рассылая уведомления. В нашем примере указываем только **Нижний порог** – 1 событие.
- В поле **Период подсчета** укажите, за какой период в политике мониторинга должны учитываться данные из источника мониторинга. Максимальное значение: 14 дней.
  В нашем примере указываем 1 час.
- Если вы выбрали тип политики **byEPS**, в поле **Регулярность замеров**, **мин** укажите контрольный интервал времени (в минутах), в течение которого проверки должны фиксировать отклонение числа потока событий от нормы для срабатывании политики мониторинга:
  - Если в течение этого времени все проверки (проводимые один раз в минуту) зафиксировали отклонение потока от нормы, сработает политика мониторинга.
  - Если в течение этого времени одна из проверок (проводимых один раз в минуту) зафиксировала, что поток соответствует норме, политика мониторинга не сработает и подсчет результатов проверок начнется заново.
  - Если вы не укажете регулярность замеров, политика мониторинга сработает сразу после того, как будет зафиксировано отклонение потока от нормы.
- При необходимости укажите электронные адреса, на которые следует отправить уведомления о срабатывании политики мониторинга KUMA. Для добавления каждого адреса необходимо нажимать на кнопку **Адрес электронной почты**.

> Для рассылки уведомлений необходимо настроить подключение к SMTP-серверу. См. раздел **Уведомления об алертах**.

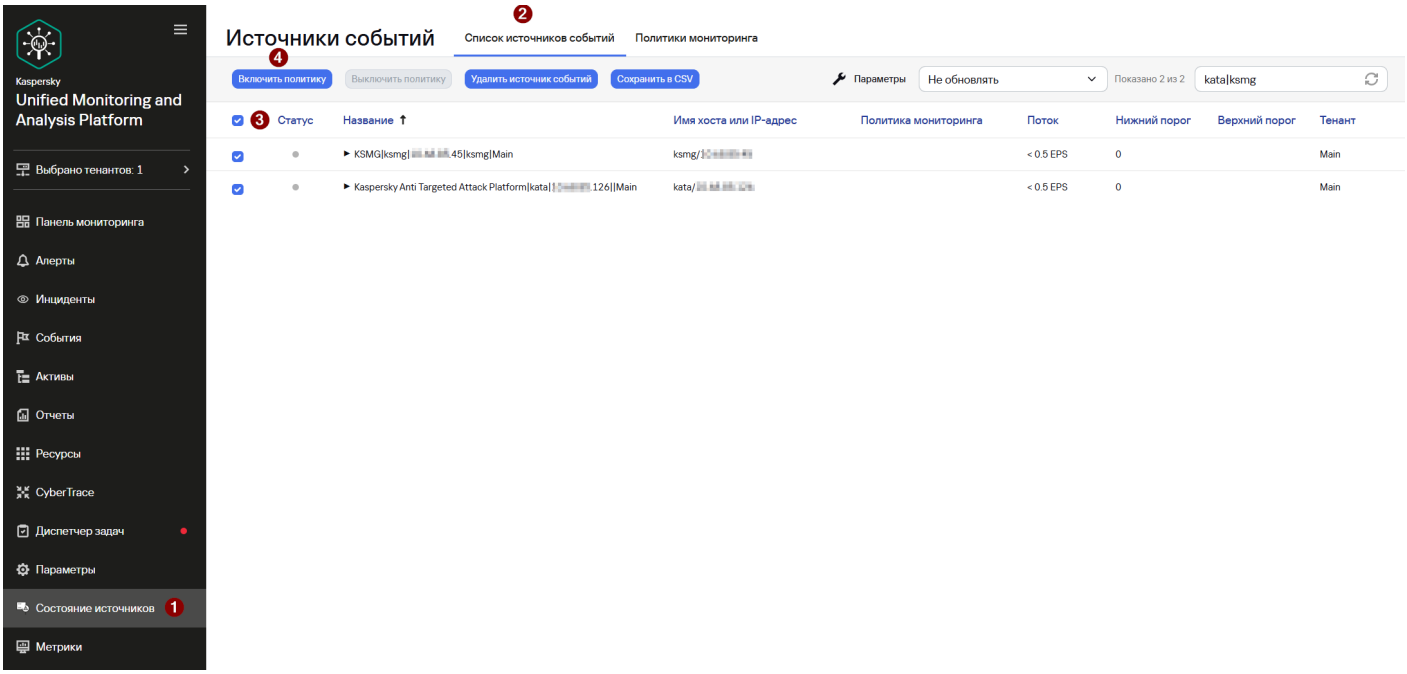
- Нажмите **Добавить**.

Политика мониторинга добавлена.

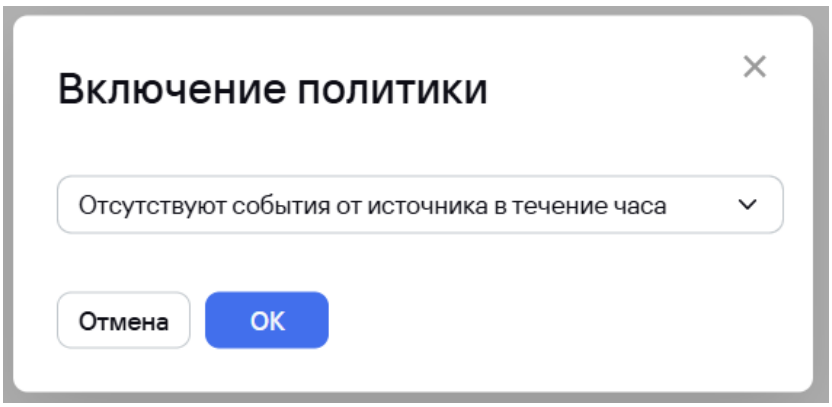


Чтобы применить политику мониторинга к источнику:

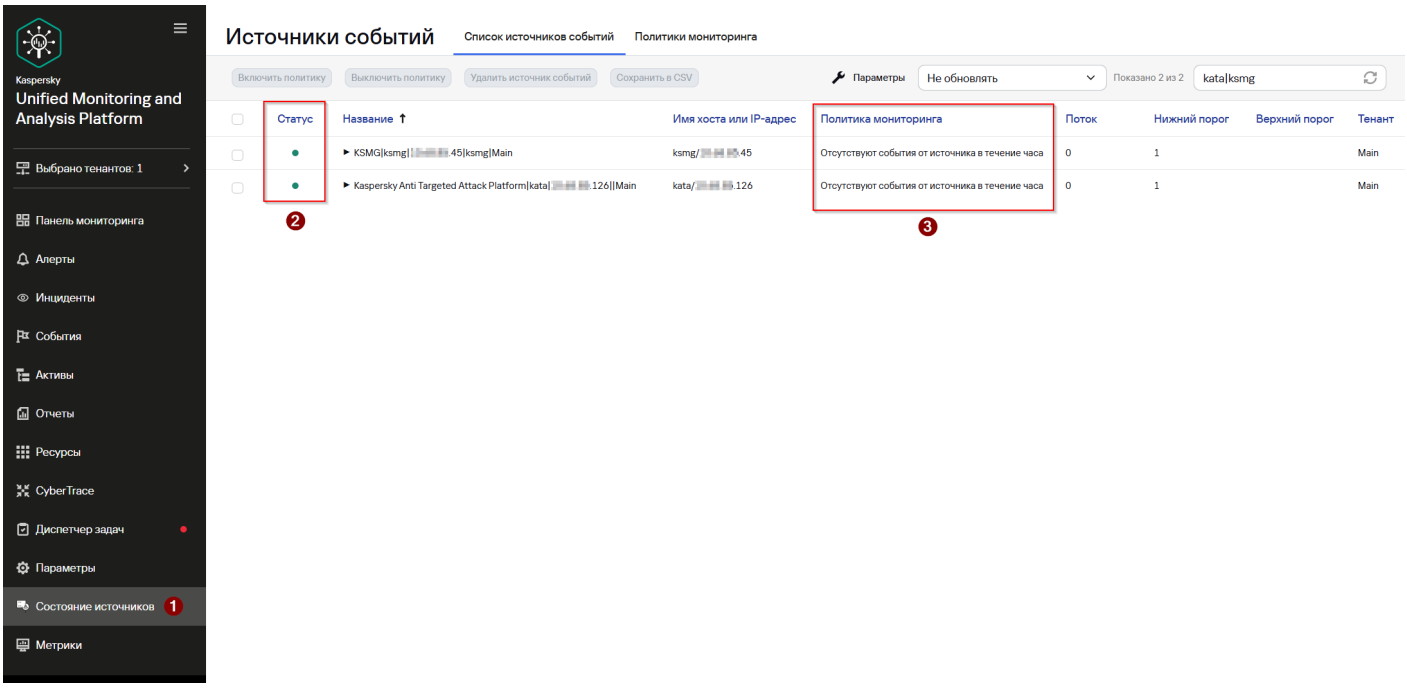
- Перейдите в раздел **Состояние источников** → вкладка **Список источников событий**.
- Выберите в списке один или несколько источников событий, установив рядом с названием источника события флажок. Также вы можете выбрать все источники событий в списке, установив флажок **Выбрать все**.
- После того как вы выберете в списке источники событий, к которым хотите применить политику мониторинга, на панели инструментов станет доступна кнопка **Включить политику**.
- Нажмите **Включить политику**.



- В открывшемся окне **Включение политики** выберите ранее созданную политику из раскрывающегося списка. Нажмите **OK**.

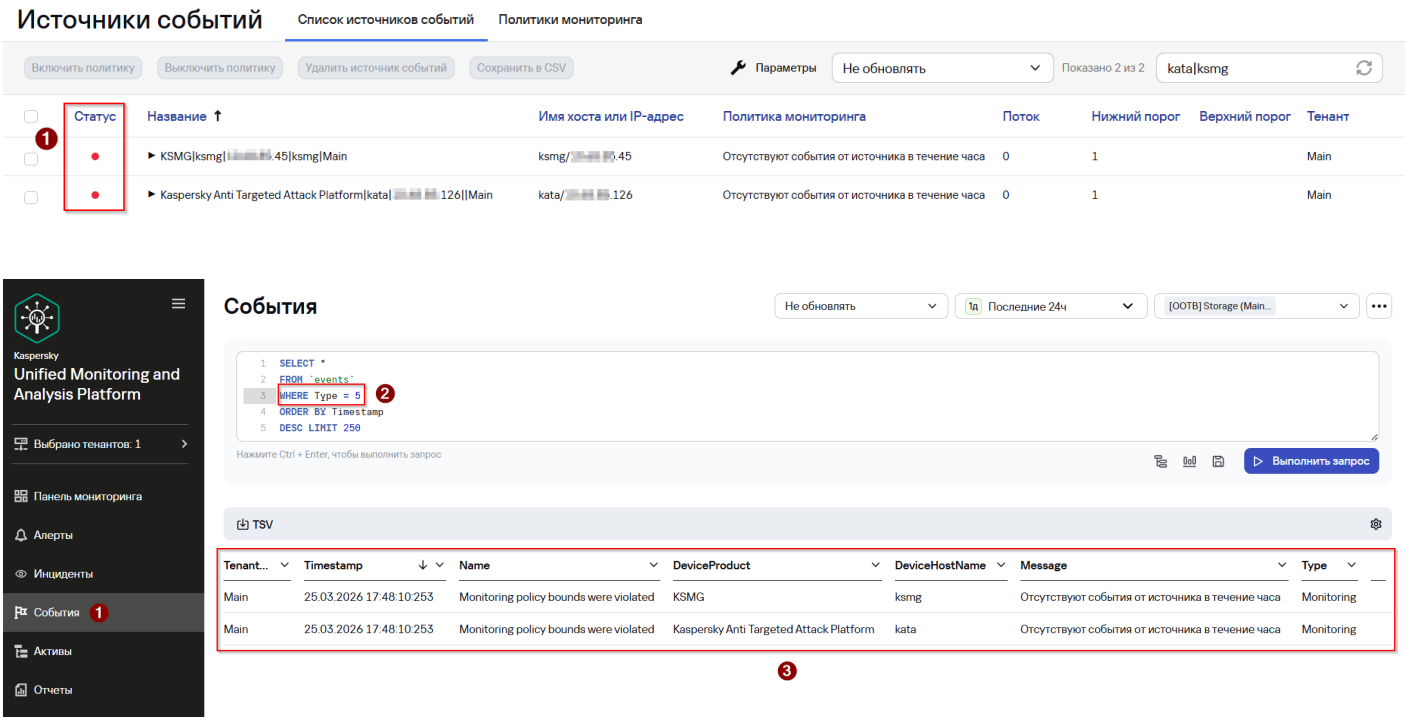


- После включения политики статус источника событий становится зеленым, столбцы **Политика мониторинга**, **Поток**, **Нижний порог** и **Верхний порог** заполняются информацией из назначенной политики.



Политика мониторинга успешно применена к выбранным источникам событий.

В случае если условия **Политики мониторинга** будут нарушены индикация столбца **Статус** изменится на красный. Кроме того, будет создано событие типа **Monitoring** и отправлено уведомление на указанные в политике почтовые адреса.



Revision #2
Created 2026-08-18 09:44:08 UTC by Dmitry Borisov
Updated 2026-08-18 09:57:21 UTC by Dmitry Borisov