

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

Настройки определения источников



⚠ После того, как вы примените измененный набор полей, все ранее определенные источники будут удалены. Необходимо перезапустить коллекторы для корректного определения источников после изменения конфигурации.

Группирующие поля для определения источника*

DeviceProduct x DeviceHostName x DeviceAddress x DeviceProcessName x 1 x v

Набор полей должен быть уникальным в рамках инсталляции продукта. Поле TenantID указывать не требуется, оно будет учтено автоматически при определении источников.

↺ Применить сопоставление по умолчанию

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.

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

СубетTrace

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Источники событий

Список источников событий

Политики мониторинга

Включить политику

Выключить политику

Удалить источник событий

Сохранить в CSV

Параметры

Не обновлять

Показано 2 из 2

katalksmg

Статус	Название ↑	Имя хоста или IP-адрес	Политика мониторинга	Поток	Нижний порог	Верхний порог	Тенант
	KSMG[ksmg]45[ksmg]Main	ksmg/45		< 0.5 EPS	0		Main
	Kaspersky Anti Targeted Attack Platform[katal]126[Main]	kata/126		< 0.5 EPS	0		Main

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:

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

СубетTrace

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Источники событий

Список источников событий

Политики мониторинга

Добавить политику

Удалить политику

Название ↑	Нижний порог	Верхний порог	Интервал	Тип	Тенант
High bounds policy	1000		1ч	byEPS	Main
Low bounds policy	1		1ч	byEPS	Main
Middle bounds policy	100		1ч	byEPS	Main

- 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, работает политика мониторинга.
 - Если в течение этого времени одна из проверок (проводимых один раз в минуту) зафиксировала, что поток соответствует норме, политика мониторинга не работает и подсчет результатов проверок начнется заново.
 - Если вы не укажете регулярность замеров, политика мониторинга работает 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.

Создание политики

×

Название политики*

Отсутствуют события от источника в течение часа

1

Тенант*

Main

2

▼

Тип политики*

количество поступивших событий

3

▼

Нижний порог*

1

4

Верхний порог

Период подсчета (максимум 14 дней)*

1

5

час

6

▼

Отправлять уведомления

+

Адрес электронной почты

administrator@truecompany.lo...

✕

✕

Сбросить

7

8

Добавить

Отмена

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**.

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры

Состояние источников 1

Метрики

Источники событий

Список источников событий

Политики мониторинга

Включить политику

Выключить политику

Удалить источник событий

Сохранить в CSV

Параметры Не обновлять Показано 2 из 2 katakmsg

Статус	Название ↑	Имя хоста или IP-адрес	Политика мониторинга	Поток	Нижний порог	Верхний порог	Тенант
✓ 3	▶ KSMG[ksmg1] 45[ksmg]Main	ksmg/10.10.10.10		< 0.5 EPS	0		Main
✓	▶ Kaspersky Anti Targeted Attack Platform[katal] 126[Main	kata/10.10.10.10		< 0.5 EPS	0		Main

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

Включение политики

Отсутствуют события от источника в течение часа

Отмена

ОК

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

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

СубетТrace

Диспетчер задач

Параметры

Состояние источников1

Метрики

Источники событий

Список источников событий

Политики мониторинга

Включить политику

Выключить политику

Удалить источник событий

Сохранить в CSV

Параметры

Не обновлять

Показано 2 из 2

kata|ksmg

Статус	Название ↑	Имя хоста или IP-адрес	Политика мониторинга	Поток	Нижний порог	Верхний порог	Тенант
●	KSMG ksmg 192.168.1.45 ksmg Main	ksmg/192.168.1.45	Отсутствуют события от источника в течение часа	0	1		Main
●	Kaspersky Anti Targeted Attack Platform kata 192.168.1.126 Main	kata/192.168.1.126	Отсутствуют события от источника в течение часа	0	1		Main

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.

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События1

Активы

Отчеты

Источники событий

Список источников событий

Политики мониторинга

Включить политику

Выключить политику

Удалить источник событий

Сохранить в CSV

Параметры

Не обновлять

Показано 2 из 2

kata|ksmg

Статус	Название ↑	Имя хоста или IP-адрес	Политика мониторинга	Поток	Нижний порог	Верхний порог	Тенант
●	KSMG ksmg 192.168.1.45 ksmg Main	ksmg/192.168.1.45	Отсутствуют события от источника в течение часа	0	1		Main
●	Kaspersky Anti Targeted Attack Platform kata 192.168.1.126 Main	kata/192.168.1.126	Отсутствуют события от источника в течение часа	0	1		Main

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События1

Активы

Отчеты

События

Не обновлять

Последние 24ч

[OOTB] Storage (Main...)

1 SELECT *
2 FROM "events"
3 WHERE Type = 5
4 ORDER BY Timestamp
5 DESC LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TSV

Tenant...	Timestamp	Name	DeviceProduct	DeviceHostName	Message	Type
Main	25.03.2026 17:48:10:253	Monitoring policy bounds were violated	KSMG	ksmg	Отсутствуют события от источника в течение часа	Monitoring
Main	25.03.2026 17:48:10:253	Monitoring policy bounds were violated	Kaspersky Anti Targeted Attack Platform	kata	Отсутствуют события от источника в течение часа	Monitoring