

Ретроспективная проверка

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/4.0/217979>

В обычном режиме коррелятор работает только с событиями, поступающими от коллекторов в реальном времени, выполняя потоковую корреляцию.

Ретроспективная проверка позволяет применять правила корреляции к историческим событиям, уже сохранённым в хранилище. Это удобно, если вы внесли изменения в существующие правила корреляции или загрузили новые и хотите проверить наличие вредоносной активности или инцидентов в ранее сохранённых событиях.

С помощью поискового запроса можно определить список исторических событий, для которых будет выполнена ретроспективная проверка, задать период поиска и указать хранилище, в котором следует искать события. Также можно настроить задачу так, чтобы во время ретроспективной проверки создавались алерты и применялись правила реагирования.

Для тестирования ретроспективной проверки:

- Создайте правило корреляции Неудачная попытка входа в веб-интерфейс KUMA (см. **Создание правила корреляции типа Simple**).
- Выполните неудачную попытку входа в веб-интерфейс KUMA.
- Перейдите в **Алерты** и закройте алерт **Неудачная попытка входа в веб-интерфейс KUMA** (при наличии).

Kaspersky

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

1

Инциденты

События

Активы

Отчеты

Ресурсы

СубетПасе

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты

Неудачная

Найдено 1

Фильтры

Название	Статус	Назначен	Инцидент	Первое появление	Последнее появление	Категория затрону...	Тенант
Неудачная попытка входа в веб-интерфейс KUMA	Новый			26.02.2025 14:28:04	03.03.2026 15:40:01	Без категории	Main

Выбрано: 1

Уровень важности: Средний

Назначить: Не назначено

Закреть алерт

Создать инцидент

Привязать

Чтобы выполнить ретроспективную проверку:

- Перейдите в раздел **События** и сформируйте необходимую выборку событий:
 - Выберите хранилище.
 - Укажите поисковый запрос.
 - Задайте необходимый временной период.
- Нажмите **Выполнить запрос**.

События

Не обновлять

15m Последние 15м

[OOTB] Storage (Main...

1

...

1

SELECT * FROM `events` WHERE Type = 4 ORDER BY Timestamp DESC LIMIT 250

2

4

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

SELECT * FROM `events` WHERE Type = 4 ORDER BY Timestamp DESC LIMIT 250

- В раскрывающемся списке

...

 выберите **Ретроспективная проверка**.

События

Не обновлять

15m Последние 15м

[OOTB] Storage (Main...

1

...

1

SELECT * FROM `events` WHERE Type = 4 ORDER BY Timestamp DESC LIMIT 250

2

Ретроспективная проверка

Статистика

4

Нажмите Ctrl + Enter, чтобы выполнить запрос

Выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct	DeviceAction	SourceUserName	EventOutcome	Type
Main	03.03.2026 16:12:00:150	Kaspersky	KUMA	user login	admin	succeeded	Audit
Main	03.03.2026 16:11:27:465	Kaspersky	KUMA	user login	admin	failed	Audit

- В появившемся окне **Ретроспективная проверка**:
 - В раскрывающемся списке **Коррелятор** выберите сервис коррелятора, в который будут загружены выбранные события.

- В раскрывающемся списке **Правила корреляции** выберите правила корреляции, с помощью которых необходимо обработать выбранные события. Если на этом шаге не выбрано ни одного правила, проверка будет выполнена с применением всех правил корреляции.
- Если необходимо, чтобы в процессе обработки событий срабатывали правила реагирования, включите переключатель **Выполнить правила реагирования**.
- Если необходимо, чтобы в процессе обработки событий создавались алерты, включите переключатель **Создать алерты**.
- Нажмите на кнопку **Создать**.

Ретроспективная проверка



Коррелятор*

[OOTB] Correlator

1



Правила корреляции

Неудачная попытка входа в веб-интерфейс KUMA x

2



Выполнить правила реагирования

☐

Создать алерт



3

4

Создать

Отмена

В разделе **Диспетчер задач** создана задача ретроспективной проверки.

Чтобы просмотреть результаты проверки:

- Перейдите в **Диспетчер задач**.

- Нажмите на созданную задачу **Ретроспективная проверка** и в раскрывающемся списке выберите **Перейти к событиям**.



Kaspersky
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры

Состояние источников

Метрики

Диспетчер задач

☒ Отображать только свои

Статус	Задача	Создал	Создана	Последнее обновление	Тенант
Завершено	Ретроспективная проверка	Administrator	03.03.2026 16:13:41	03.03.2026 16:13:41	Main
Завершено	Ретроспективная проверка	Administrator	03.03.2026 15:40:01	03.03.2026 15:40:01	Main

- Откроется новая вкладка браузера с таблицей корреляционных событий, созданных в процессе ретроспективной проверки исторических событий. Корреляционные события, содержат дополнительное поле **ReplayID**, в котором хранится уникальный идентификатор выполнения ретроспективной проверки.



Kaspersky
Unified Monitoring and
Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты

Инциденты

События

Активы

Отчеты

Ресурсы

CyberTrace

Диспетчер задач

Параметры

Состояние источников

Метрики

События

1 SELECT * FROM 'events' WHERE ReplayID = 'a651c3b7-9151-42bc-8b90-a126700e4628' LIMIT 250

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

TenantID	Timestamp	DeviceVendor	DeviceProduct
Main	03.03.2026 16:13:41.345	Kaspersky	KUMA

Информация о корреляционном событии

☐ Копировать ☒ Подробные сведения

TenantIDMain

Timestamp03.03.2026 16:13:41.345

NameНеудачная попытка входа в веб-интерфейс KUMA

StartTime03.03.2026 16:11:27.465

EndTime03.03.2026 16:11:27.465

MessageОбнаружена неудачная попытка входа в веб-интерфейс KUMA под учетной записью admin с IP-адреса 10.16.59.71

DeviceActionuser login

DeviceProductKUMA

DeviceTimeZone+03:00

DeviceVendorKaspersky

SourceAddress10.16.59.71

SourceUserNameadmin

CorrelationRuleНеудачная попытка входа в веб-интерфейс KUMA

Service[OOTB] Correlator

BaseEventCount1

EventOutcomefailed

PriorityСредний

ReplayIDA651c3b7-9151-42bc-8b90-a126700e4628

TypeCorrelated

Также в ходе ретроспективной проверки будет создан алерт **Неудачная попытка входа в веб-интерфейс KUMA** (если переключатель **Создать алерты** был активирован).

Карантэку

Unified Monitoring and Analysis Platform

Выбрано тенантов: 1

Панель мониторинга

Алерты 1

Инциденты

События

Активы

Отчеты

Ресурсы

СубетTrace

Диспетчер задач

Параметры

Состояние источников

Метрики

Administrator

Алерты >

Неудачная попытка входа в веб-интерфейс KUMA Новый 2

Уровень важности: Средний

Назначить: Не назначено

Заккрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции

Средний

Первое появление

03.03.2026 16:13:41

Тенант

Main

Наивысшая важность категории активов

Нет значения

Последнее появление

03.03.2026 16:13:41

Правило корреляции

Неудачная попытка входа в веб-интерфейс KUMA 3

Идентификатор алерта

9968d057-e584-48db-8adc-b2e4192fc2d7

Связанные события

Скачать события

Найти в событиях

Время	Информация о событии	Тенант
03.03.2026 16:13:41	DeviceAction: user login, SourceAddress: 10.16.59.71, SourceUserName: admin, EventOutcome: failed, ReplayID: a651c3b7-9151-42bc-8b90-a126700a4628 4	Main

Всего: 1

Связанные активы

Скачать активы

Поиск по IP или FQDN...

Количество	Актив	Категории	Тенант
------------	-------	-----------	--------

Всего: 0

Таким образом, в ходе ретроспективной проверки выборки исторических событий было выявлено событие неудачной попытки входа в веб-интерфейс KUMA, что привело к срабатыванию правила корреляции.