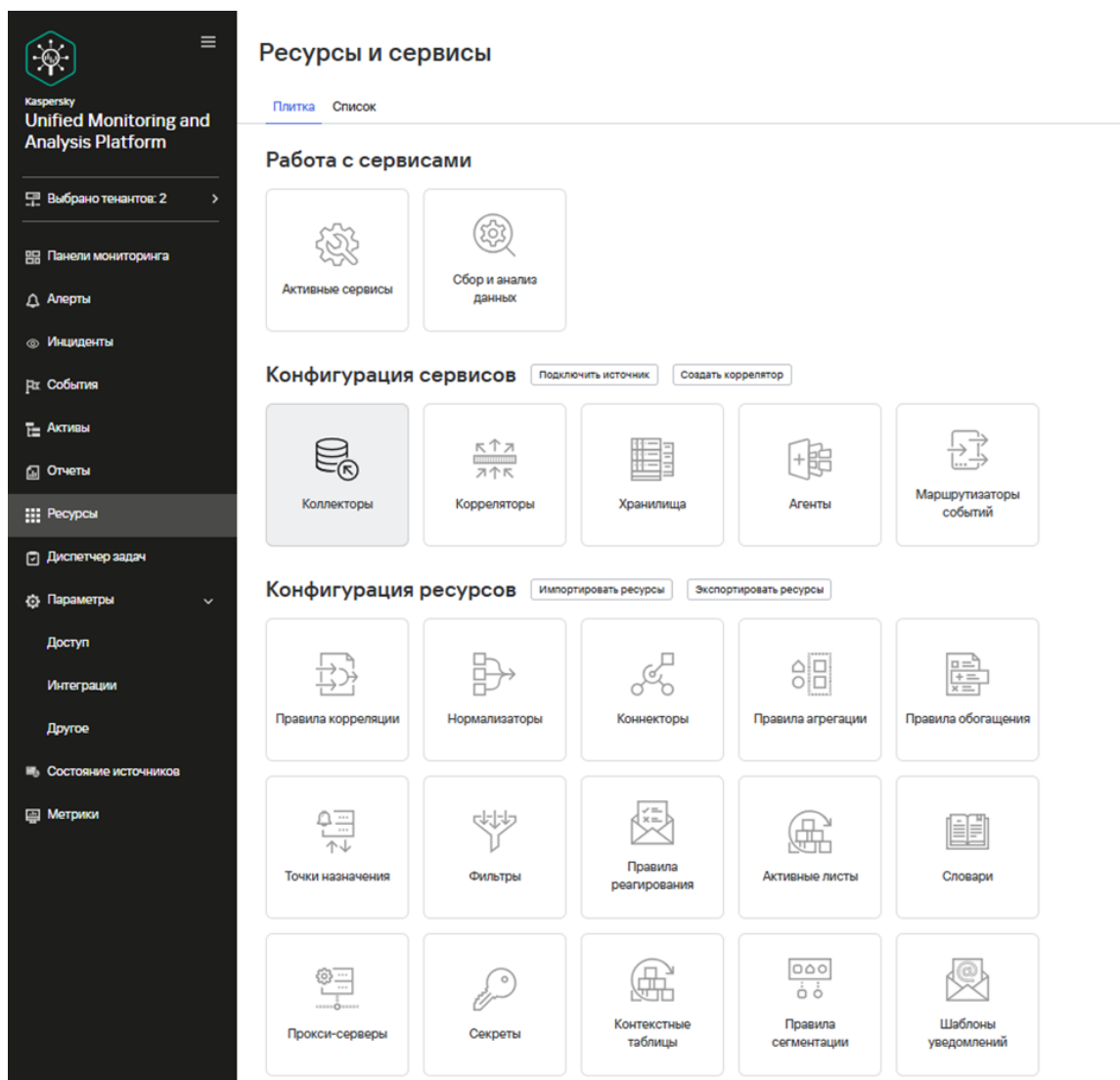


?????????? ??????????? ??????????? ?? KICS for Networks (????????? 4.3 ? 4.5) ? KUMA

Настройка интеграции выполняется в два этапа: сначала создается и настраивается коллектор в KUMA, затем создается коннектор в KICS for Networks.

Настройка KUMA

1. Перейдите в раздел «Ресурсы» и откройте вкладку «Коллекторы».



1. Нажмите кнопку «+ Создать».

Создание коллектора

Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразование их в нормализованные события, понятие KUMA. С помощью коллектора можно также отсечь ненужные события, объединить похожие события и обогатить события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. в [очках-справке](#).

Основные параметры | **Дополнительные параметры**

Название коллектора*

Тип*

Обработка

Время загрузки данных

Тип

Описание

1. В открывшемся окне укажите название коллектора. Рекомендуется использовать наименование продукта, тип подключения и порт (например, KICS_for_Networks_TCP\5160), чтобы в дальнейшем легко идентифицировать коллектор.

Создание коллектора

Подключение источников

- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

Подключение источников

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. 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](#).

[Основные параметры](#) [Дополнительные параметры](#)

Название коллектора*	<input type="text" value="KICS_for_Networks_TCP/5160"/>
Тенант*	<input type="text" value="Main"/>
Обработчики	<input type="text" value="0"/>
Время загрузки геоданных ⓘ	<input type="text"/>
Теги	<input type="text"/>
Описание	<input type="text"/>

1. На вкладке «Транспорт» укажите тип соединения (протокол) и порт, который будет использоваться для приема событий от источника.

Создание коллектора

Подключение источников

Транспорт

- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров

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="tcp"/>
URL* ⓘ	<input type="text" value=":5160"/>
Auditd	<input type="checkbox"/>
Разделитель	<input type="text"/>

1. На вкладке «Парсинг событий» - «Настройки парсинга» выберите соответствующий нормализатор для обработки входящих событий.

Создание коллектора



Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Парсинг событий

Преобразуйте полученные события в формат, понятный KUMA. Подробнее см. [в онлайн-справке](#).
Настройки парсинга доступны, если тип коннектора — http/tcp/udp.

Схемы парсинга [Настройки парсинга](#)

IP-адрес(-а)

Введите IP-адрес или несколько IP-адресов, используя запятую в качестве разделителя

Нормализатор*

+ Добавить условную нормализацию

+ Источник события

1. На вкладке «Маршрутизация» добавьте ранее созданные коррелятор и хранилище. Подробнее о разворачивании этих компонентов см. в [Справке по KUMA](#).

Создание коллектора



- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация**
- Проверка параметров

Маршрутизация

Укажите, куда следует отправлять полученные события. Подробнее см. [в онлайн-справке](#).

+ Добавить Удалить

<input type="checkbox"/>	Название	Тип	URL
<input type="checkbox"/>	[OOTB] Correlator	correlator	kuma-ics.demo.lab:7231
<input type="checkbox"/>	[OOTB] Storage	storage	kuma-ics.demo.lab:7230

1. На вкладке «Проверка параметров» нажмите кнопку «Сохранить и создать сервис».

Создание коллектора

- Подключение источников
- Транспорт
- Парсинг событий
- Фильтрация событий
- Агрегация событий
- Обогащение событий
- Маршрутизация
- Проверка параметров**

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

Сохранить и создать сервис

1. После создания коллектора скопируйте сгенерированную команду и выполните её в терминале сервера KUMA с правами администратора для развертывания сервиса.

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Проверка параметров

Настройка коллектора завершена, сервис добавлен в KUMA. Подробнее см. [в онлайн-справке](#).

Чтобы начать получать события, сервис этого коллектора необходимо установить на сервере, предназначенном для сбора событий (см. пример команды установки ниже). Обратите внимание, что должна быть обеспечена сетевая связность компонентов системы и открыты порты. Подробнее см. [в онлайн-справке](#).

Сервисы, использующие этот коллектор

Тип	Название
коллектор	KICS_for_Networks_TCP/5160

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

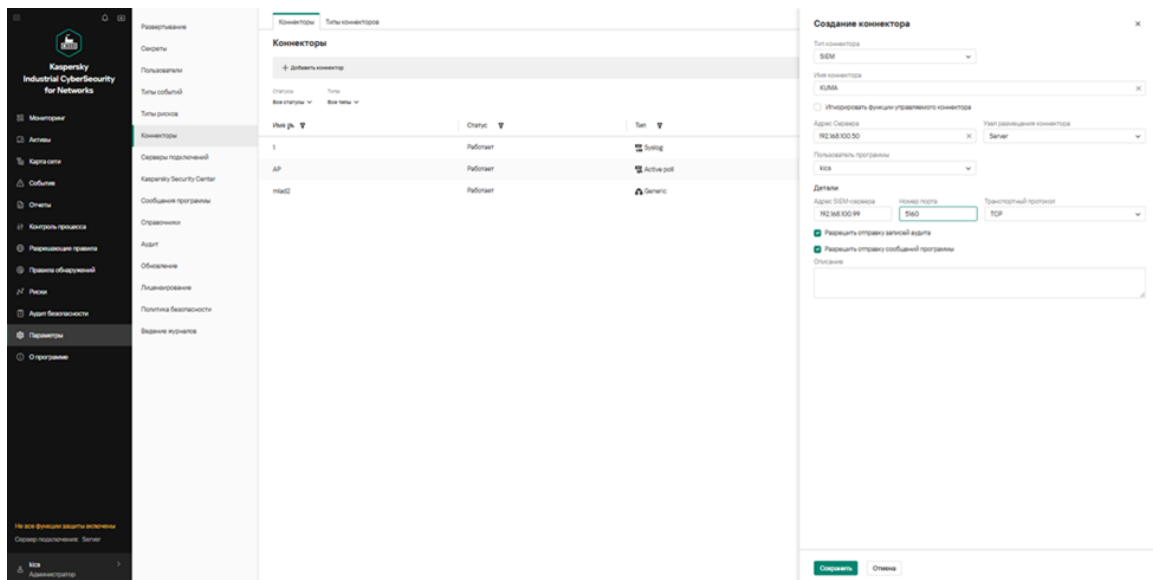
Рекомендуемая команда для установки коллектора

```
/opt/kaspersky/kuma/kuma collector --core https://kuma-ics.demo.lab:7210 --id 4800ba10-8c0f-4a18-ad48-aad7b446ebc6 --api.port 7237 --install
```






Настройка KICS for Networks

1. Перейдите в раздел «Параметры» - «Коннекторы» и нажмите кнопку «+ Добавить коннектор».
2. В карточке нового коннектора заполните поля:
 - Тип коннектора: SIEM.
 - Имя коннектора: Произвольное наименование.
 - Адрес сервера: IP-адрес узла, на котором развернут сервер KICS for Networks.
 - Узел размещения коннектора: Server.
 - Пользователь программы: Учетная запись администратора KICS for Networks.
 - Адрес SIEM-сервера: IP-адрес узла, на котором развернут сервер KUMA.
 - Номер порта: Порт, указанный при настройке коллектора KUMA (см. п. 4 раздела «Настройка KUMA»).
 - Транспортный протокол: Протокол, указанный при настройке коллектора KUMA (см. п. 4 раздела «Настройка KUMA»).



1. Нажмите кнопку «Сохранить».
2. Убедитесь, что в свойствах созданного коннектора параметры имеют следующие значения:
 - Включен: Да.
 - Статус: Работает.

 Изменить  Удалить  Выключить

Тип	SIEM	Управляемый	Да
Пользователь программы	kics	Узел размещения коннектора	Server



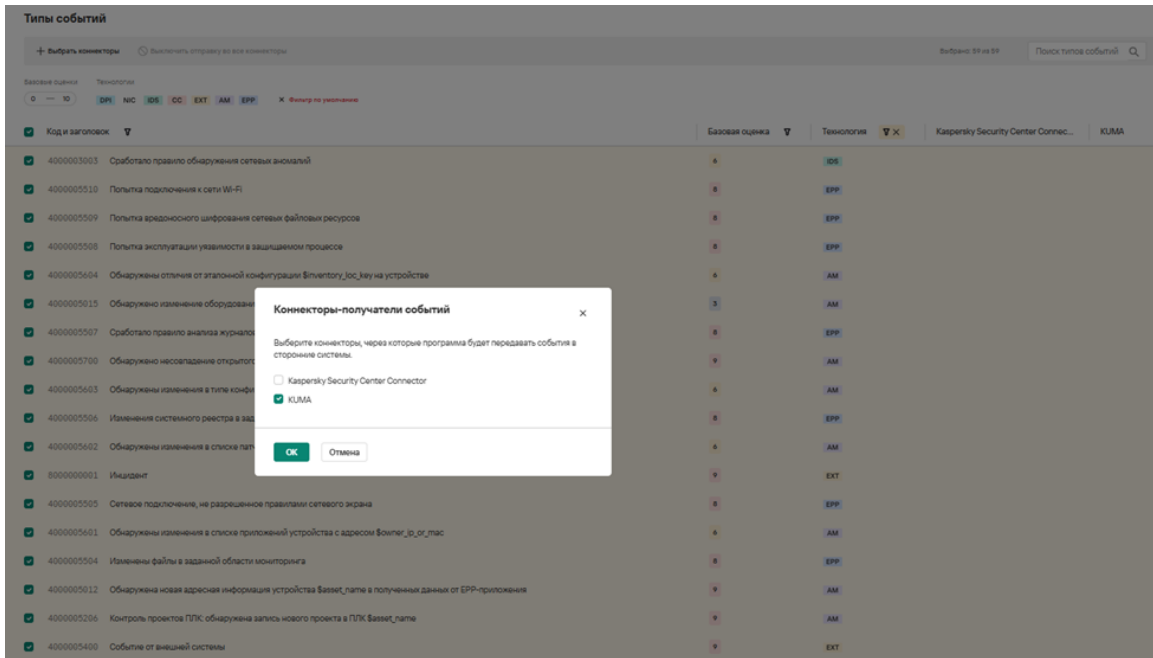
Включен	Да
Изменен	16.02.2026 12:36:45
Последнее подключение	16.02.2026 12:36:45
Статус	Работает
ID коннектора	11
ID типа	Siem
Типы событий	Не отправляются
Функциональные возможности	Отправка данных, Управляемый

Детали

Адрес SIEM-сервера	192.168.100.99
Номер порта	5160
Транспортный протокол	TCP
Разрешить отправку записей аудита	
Разрешить отправку сообщений программы	

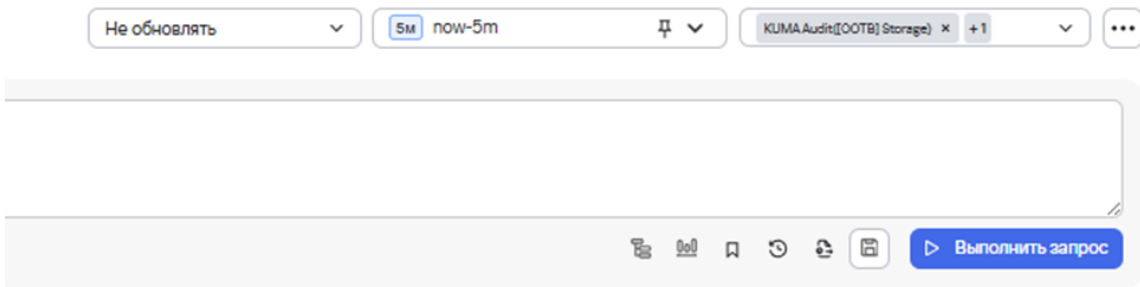
Если значения отличаются, проверьте выполненные настройки и перезапустите коннектор (выполните последовательность «Выключить» - «Включить»).

3. Перейдите в раздел «Параметры» - «Типы событий». Выберите типы событий, которые необходимо передавать в KUMA, и активируйте для них отправку через созданный коннектор.

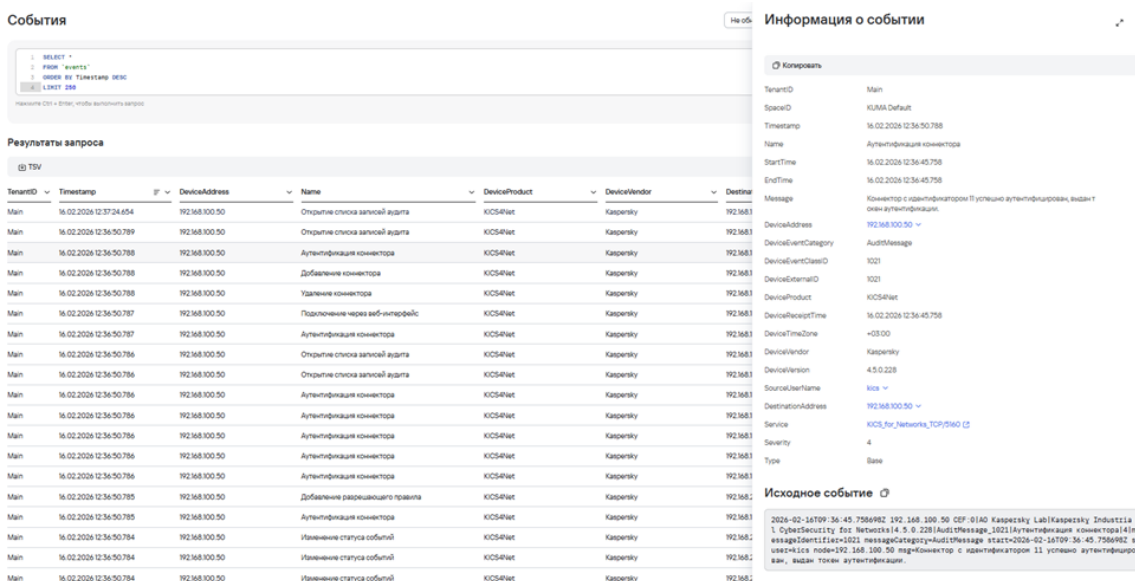


Проверка передачи событий

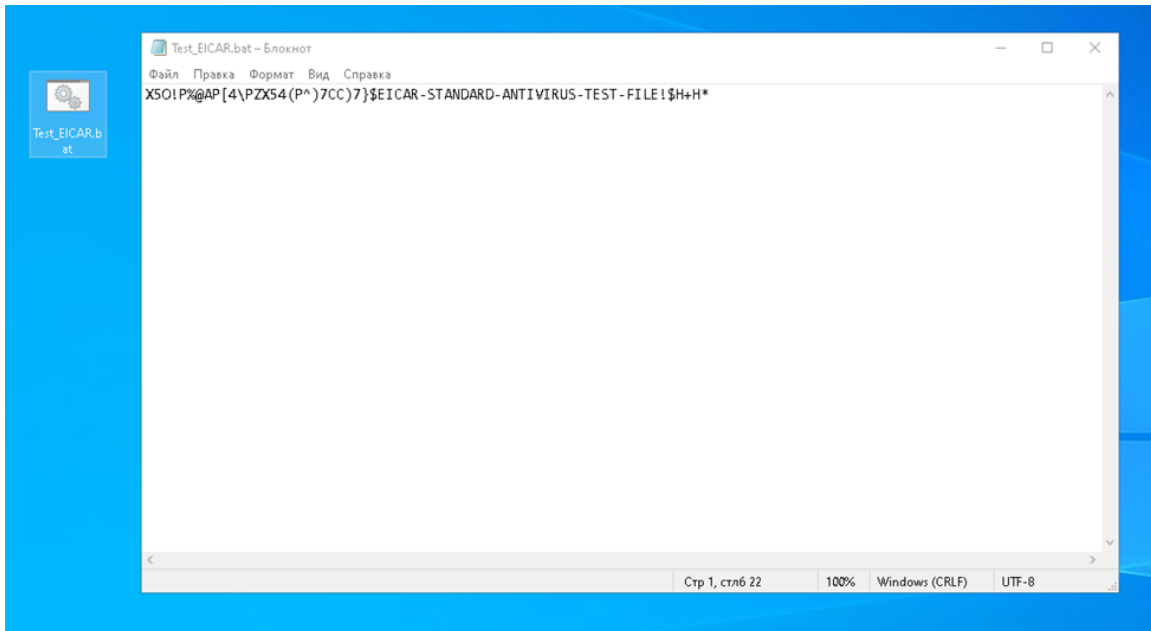
1. В интерфейсе KUMA перейдите в раздел «События» и выполните опрос источников.



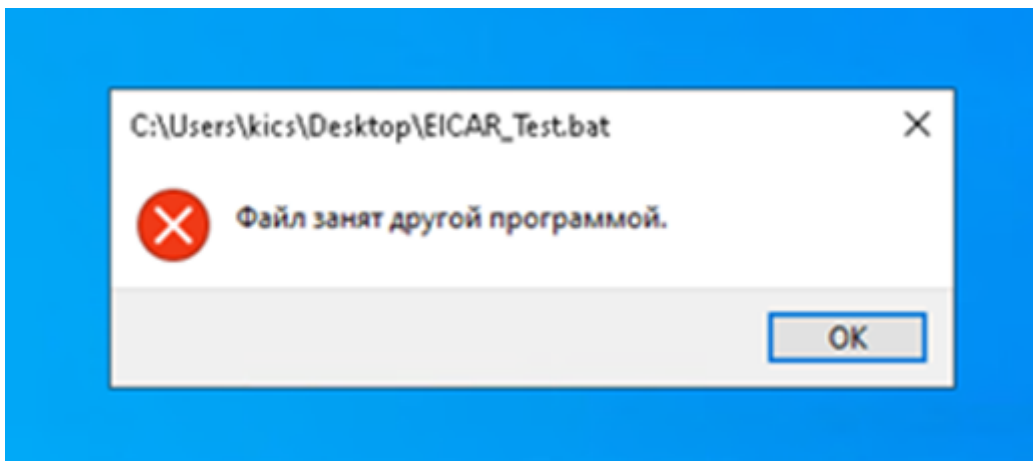
2. Убедитесь в наличии событие об успешной аутентификации коннектора, которое должно появиться в момент его создания в KICS for Networks.



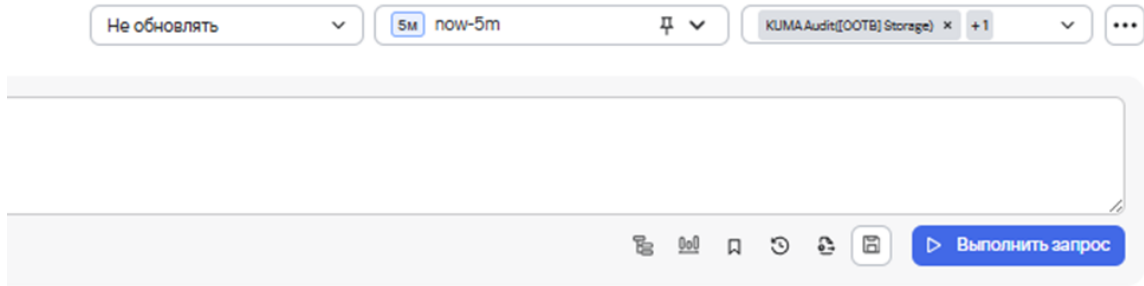
1. Воспроизведите событие безопасности, например, запустите тестовый вирус на узле, который интегрирован с KICS for Networks.



1. Убедитесь, что сработал модуль постоянной защиты KICS for Nodes (детектирование события на стороне источника).



1. В интерфейсе KUMA снова перейдите в раздел «События» и выполните опрос.



1. Убедитесь, что воспроизведенное событие безопасности успешно доставлено и отображается в KUMA.

События

```

SELECT *
FROM 'events'
ORDER BY Timestamp DESC
LIMIT 200
        
```

Нажмите Ctrl + Enter, чтобы выполнить запрос

Результаты запроса

TSV

TenantID	Timestamp	IP	DeviceAddress	Name	DeviceProduct	DeviceVendor	Destination
Main	16.02.2026 12:58:42.147		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:56:10.017		192.168.100.50	Привлечены активности вредоносной программы на у...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:33.586		192.168.100.50	C:\Users\kcor\Desktop\Tet_EICAR bat	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:39.952		192.168.100.50	С IP-адреса 192.168.100.50 часть попыток несрав...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:33.586		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:33.586		192.168.100.50	Попытки сетевых взаимодействий с IP-адресом 92...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:33.585		192.168.100.50	Обнаружено повреждение (CLOCK/ACCURACY DECRE...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:33.585		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:27.230		192.168.100.50	Попытки сетевых взаимодействий с IP-адресом 92...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:27.230		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:27.229		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:23.968		192.168.100.50	Подозрительная активность (MITRE: Unauthorized C...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:23.967		192.168.100.50	Попытки сетевых взаимодействий с IP-адресом 90.18...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:23.967		192.168.100.50	Попытки сетевых взаимодействий с IP-адресом 90.1...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:23.967		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:54:23.966		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	
Main	16.02.2026 12:52:35.138		192.168.100.50	С IP-адреса 192.168.100.50 часть попыток несрав...	KICS4Net	Kaspersky	
Main	16.02.2026 12:52:16.425		192.168.100.50	Попытки сетевых взаимодействий с IP-адресом 92...	KICS4Net	Kaspersky	
Main	16.02.2026 12:52:16.425		192.168.100.50	Попытки сетевых взаимодействий с IP-адресом 92...	KICS4Net	Kaspersky	
Main	16.02.2026 12:52:16.425		192.168.100.50	Обнаружено несоответствие (TIME CORRECTION T...	KICS4Net	Kaspersky	

Информация о событии

Копировать

TenantID	Main
SpaceID	KUMA Default
Timestamp	16.02.2026 12:56:10.017
Name	Привлечены активности вредоносной программы на ус...
StartTime	16.02.2026 12:55:48.222
EndTime	16.02.2026 12:55:48.222
DeviceAddress	192.168.100.50
DeviceEventCategory	Event
DeviceEventClassID	8000000001
DeviceProduct	KICS4Net
DeviceReceiptTime	16.02.2026 12:55:48.222
DeviceTimeZone	+03:00
DeviceVendor	Kaspersky
DeviceVersion	4.5.0.228
SourceHostName	dekstop-4725ka
DeviceCustomString1	K4N_L5_Win10
DeviceCustomString2Label	assetName
DeviceCustomString2	None
DeviceCustomString2Label	monitoringPoint
DeviceCustomString5	VMaine201
DeviceCustomString5Label	arcVendor
DeviceCustomString6	1
DeviceCustomString6Label	type
Service	KICS_for_Networks_TCP/5160_C3
ApplicationProtocol	IP
BaseEventCount	1
EventOutcome	trojan_on_host
ExternalID	45719
FlacString1	Привлечены активности вредоносной программы на ус...
FlacString1Label	technologyRule

Revision #5

Created 16 February 2026 13:34:50 by Alexey Panyukhin

Updated 18 February 2026 12:14:42 by Alexander Somonov