Ретроспективная проверка IoC с помощью KUMA и CyberTrace

Введение

> Описанный ниже сценарий применим для версии **CyberTrace 4.4** и выше. Ресурсы, поставляемые для данного сценария в **KUMA** применимы к версии **3.2** и выше, но могут быть сделаны аналогичные для версий **2.1+**.

В данном сценарии рассматривается автоматизация ретроспективной проверки по IoC с использованием интеграции KUMA и CyberTrace.

Сценарий позволяет:

1. По расписанию выполнять ретроспективную проверку на стороне CyberTrace

2. Получать событие в KUMA по результатам ретроспективной проверки

3. Создавать корррреляционное событие и алерт на основании такого события, а также добавлять в корреляционное событие кликабельную ссылку на исходное событие, на которое сработал ретроскан.

Настройка CyberTrace

Подключитесь к CyberTrace от имени пользователя с правами администратора.

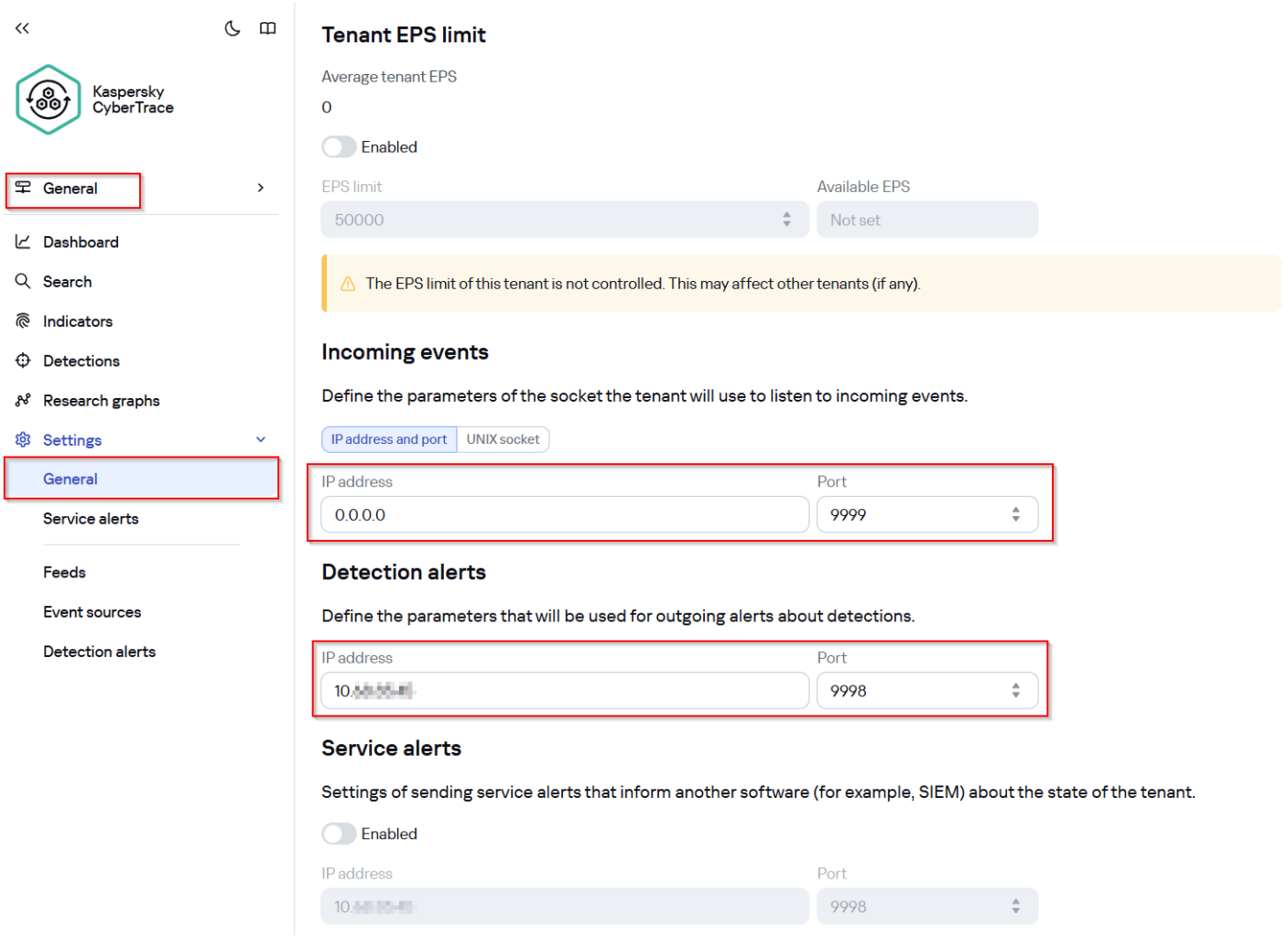
Настройка получения и отправки событий

Перейдите в раздел **Settings** - **General.**

В графе **Incoming events** выберите **IP address and port**, в поле **IP address** укажие адрес CyberTrace, на котором он будет принимать индикаторы от KUMA (запись **0.0.0.0** означает, что CyberTrace будет принимать соединения на всех адресах), а в поле **Port** задайте порт, на котором CyberTrace будет принимать индикаторы.

В графе **Detection alerts** в поле **IP address** укажите адрес коллектора KUMA, а в графе **Port** - порт коллектора KUMA.

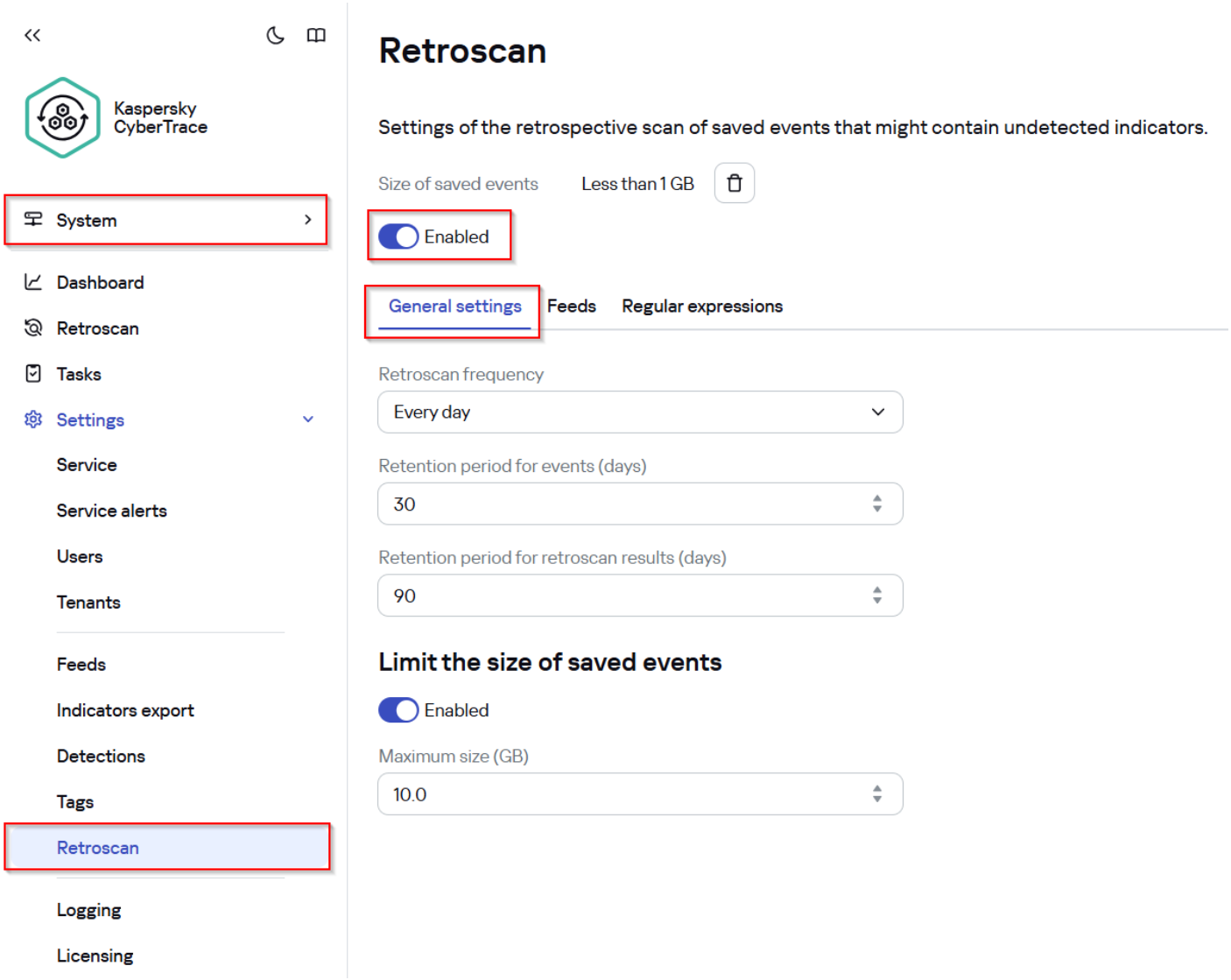
По завершении настройки нажмите кнопку **Save** внизу экрана.



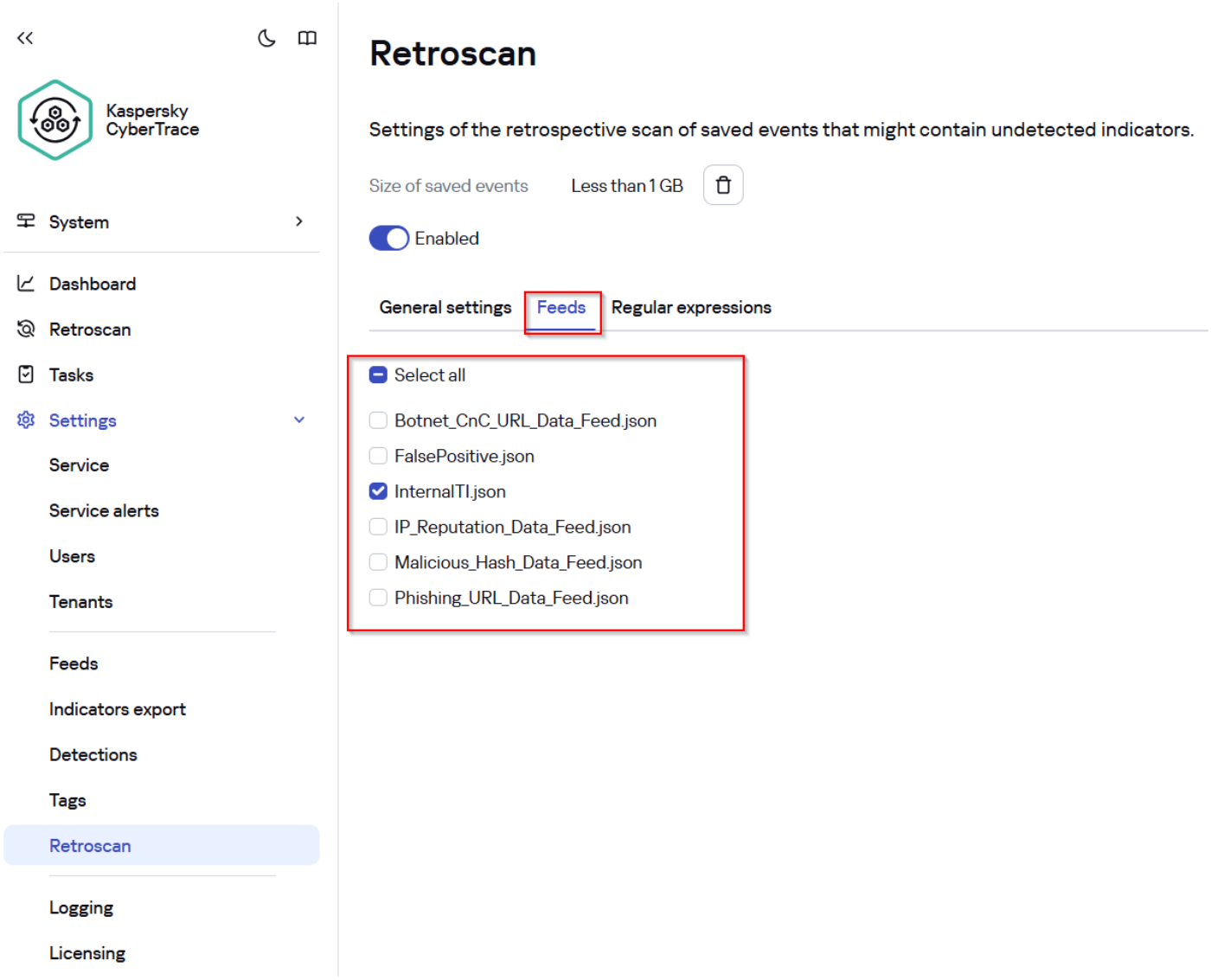
Настройка ретроспективной проверки

Перейдите в раздел **Settings - Restroscan**

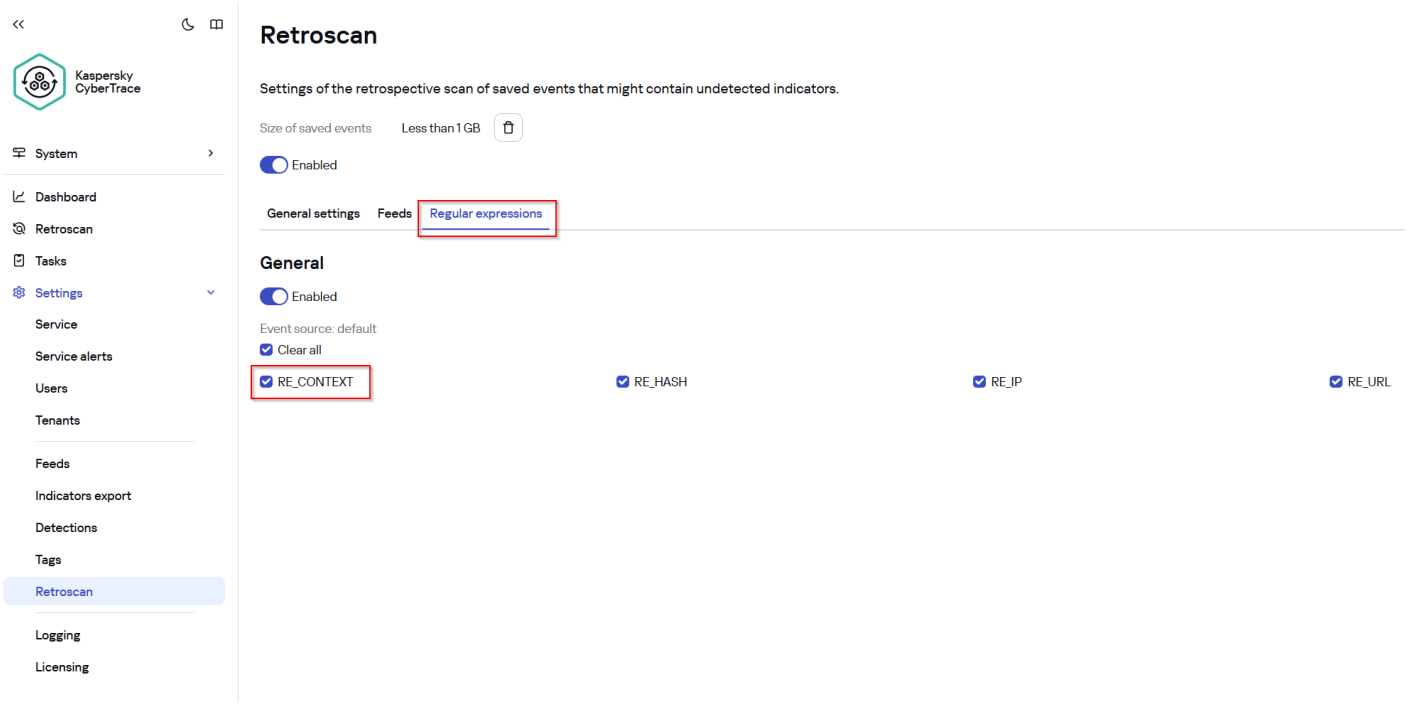
Включите ретроскан ползунком **Enabled**. На вкладка **General settings** задайте необходимые настройки регулярности ретроспективной проверки и другие параметры.



Находясь в том же разделе, перейдите на вкладку **Feeds** и включите необходимые фиды для ретроспективной проверки.



Находясь в том же разделе, перейдите на вкладку **Regular expressions** и выберите **RE_CONTEXT** (обязательно в данном сценарии), а также те индикаторы, по которым планируется ретроспективная проверка.



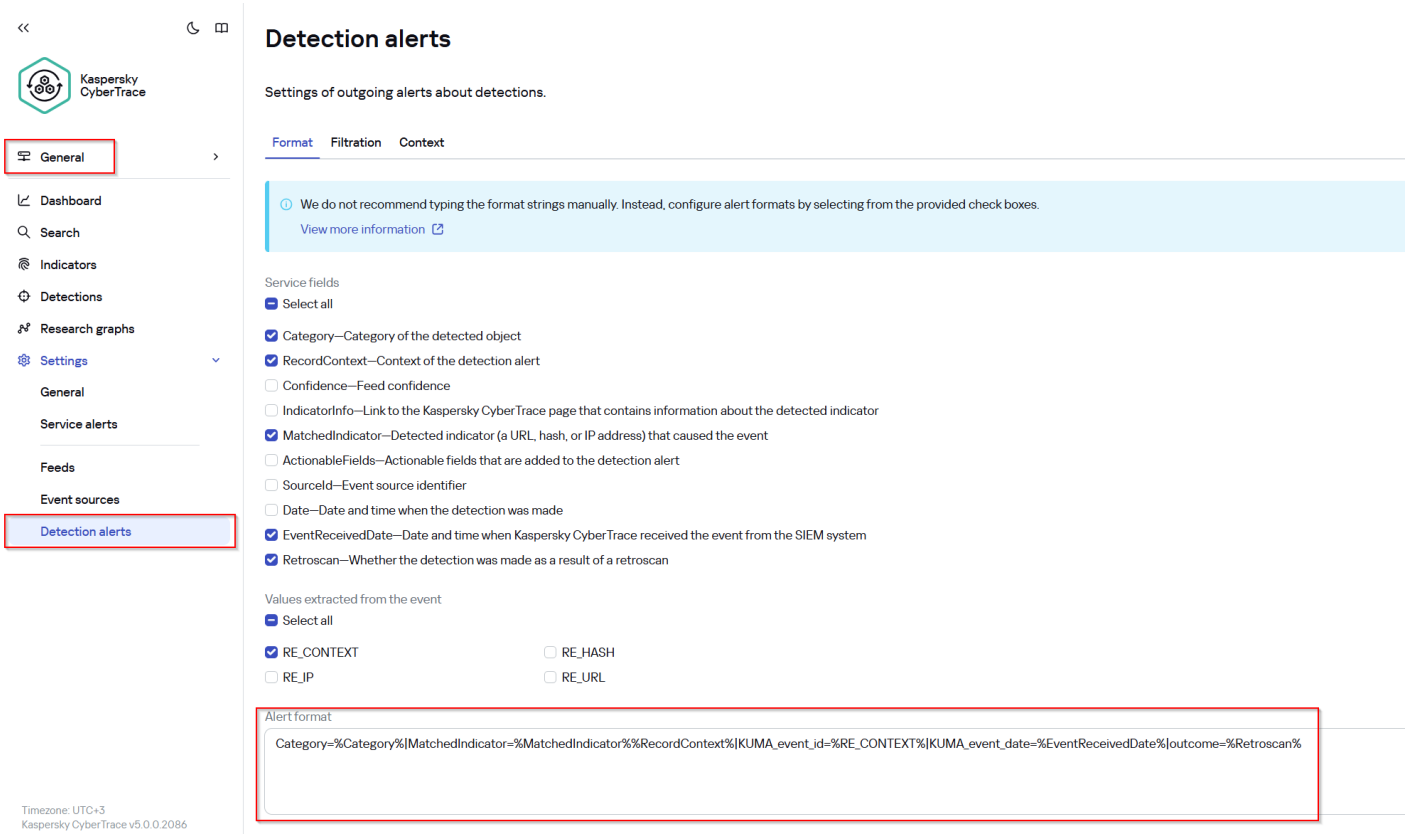
По окончании настройки нажмите кнопку **Save**.

Настройка формата событий

Перейдите в раздел **Settings - Detection alerts**

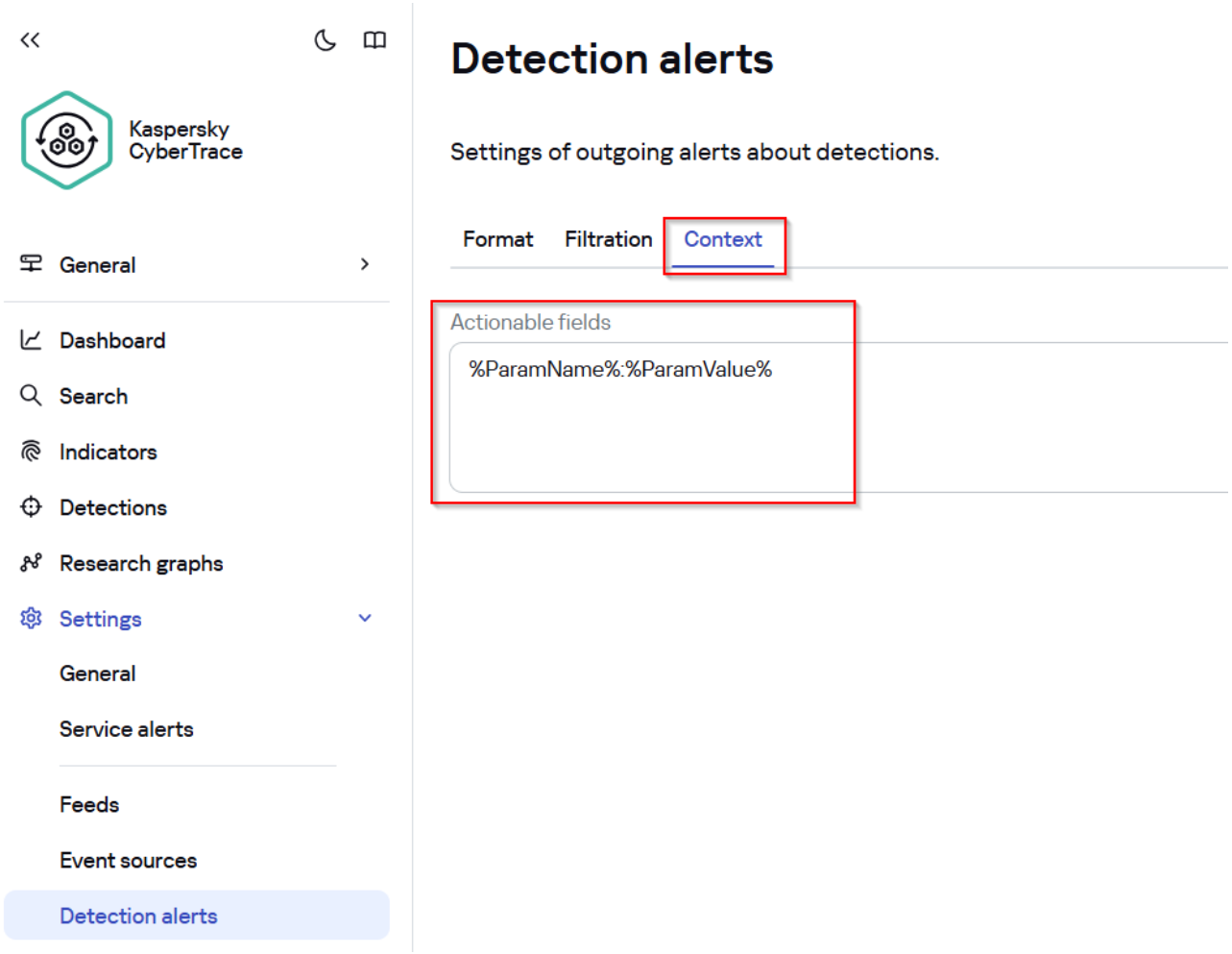
Заполните **Alert format**, как показано в примере.

```
Category=%Category%|MatchedIndicator=%MatchedIndicator%%RecordContext%|KUMA_event_id=%RE_CONTEXT%|KUMA_event_date=%EventReceivedDate%|outcome=%Retroscan%
```



Выберите вверху **Context** и заполните **Actionable fields**, как в примере ниже.

```
"%ParamName%":"%ParamValue%"
```



Пролистайте в самый низ страницы и нажмите кнопку **Save**.

Настройки для **Service alerts** можете оставить по умолчанию или изменить по своему усмотрению. В данном сценарии рассматривается и требуется взаимодействие только с **Detection alerts**.

Настройка KUMA

1. Скачайте набор ресурсов (нормализатор и правило корреляции) по **ссылке** и импортируйте в KUMA.

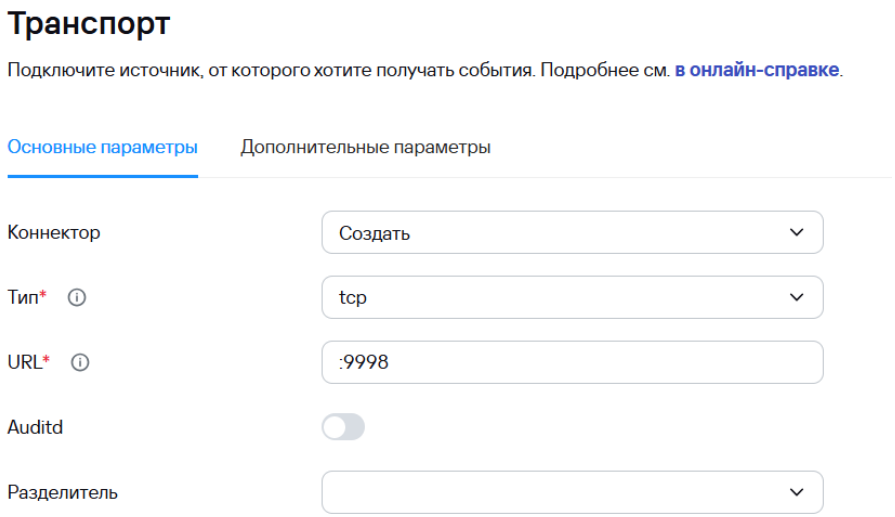
Настройка обогащения

> **Важно!** Обогащение должно выполняться именно методом **cybertrace**. Метод **cybertarce-http** не применим в данном случае, т.к. в CyberTrace до 5.0 версии включительно обогащение по API не доступно для ретроспективной проверки и отображения в детектах.

1. Настройте обогащение на коллекторах, где это требуется по инструкции из соответствующего **раздела**.

Настройка коллектора

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне **CyberTrace**.



2. На шаге **Парсинг** событий выберите нормализатор **[DEMO] CyberTrace**.

3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- Хранилище. Для отправки обработанных событий в хранилище.
- Коррелятор. Для отправки обработанных событий в коррелятор.
Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.

5. Скопируйте появившуюся команду для установки коллектора KUMA.

Настройка корреляции

1. Откройте на редактирование правило корреляции **D016;CyberTrace;IoC Matched By Retroscan** (или **D016;CyberTrace;Обнаружение IoC в ходе ретроспективной проверки**)

2. Перейдите в Селекторы - Локальные переменные

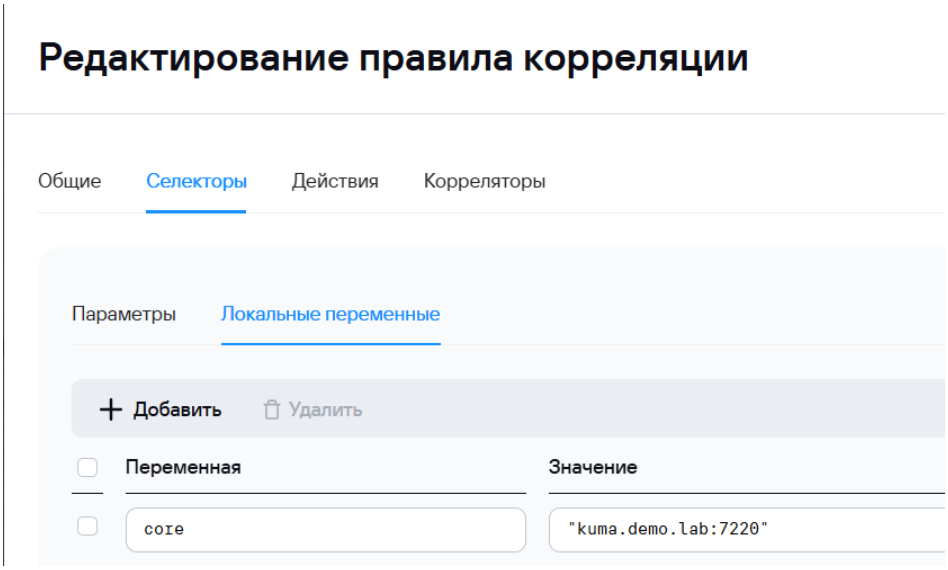
3. Отредактируйте значение переменной **core** подставив свой FQDN или IP-адрес ядра

> Важно! FQDN для данного сценария не должен превышать 18 символов! В случае более длинного FQDN следует использовать IP-адрес.

Пояснение ограничения

Ссылка на событие KUMA (переменная **url**), которая будет помещена в корреляционное событие, находится в поле **DeviceExternalID**. Максимальная длина данных в этом поле **255** символов. Пустой запрос без FQDN содержит **237** символов, что дает возможность указать FQDN меньше или равным **18** символам.

При необходимости, можно изменить мапинг ссылки на событие на другое поле, например, Message. Но в таком случае ссылка будет "не кликабельная" и нужно будет копировать ее из события и вставлять в строку браузера.



4. Сохраните правило корреляции.

5. Привяжите к коррелятору правило корреляции **D016;CyberTrace;IoC Matched By Retroscan**

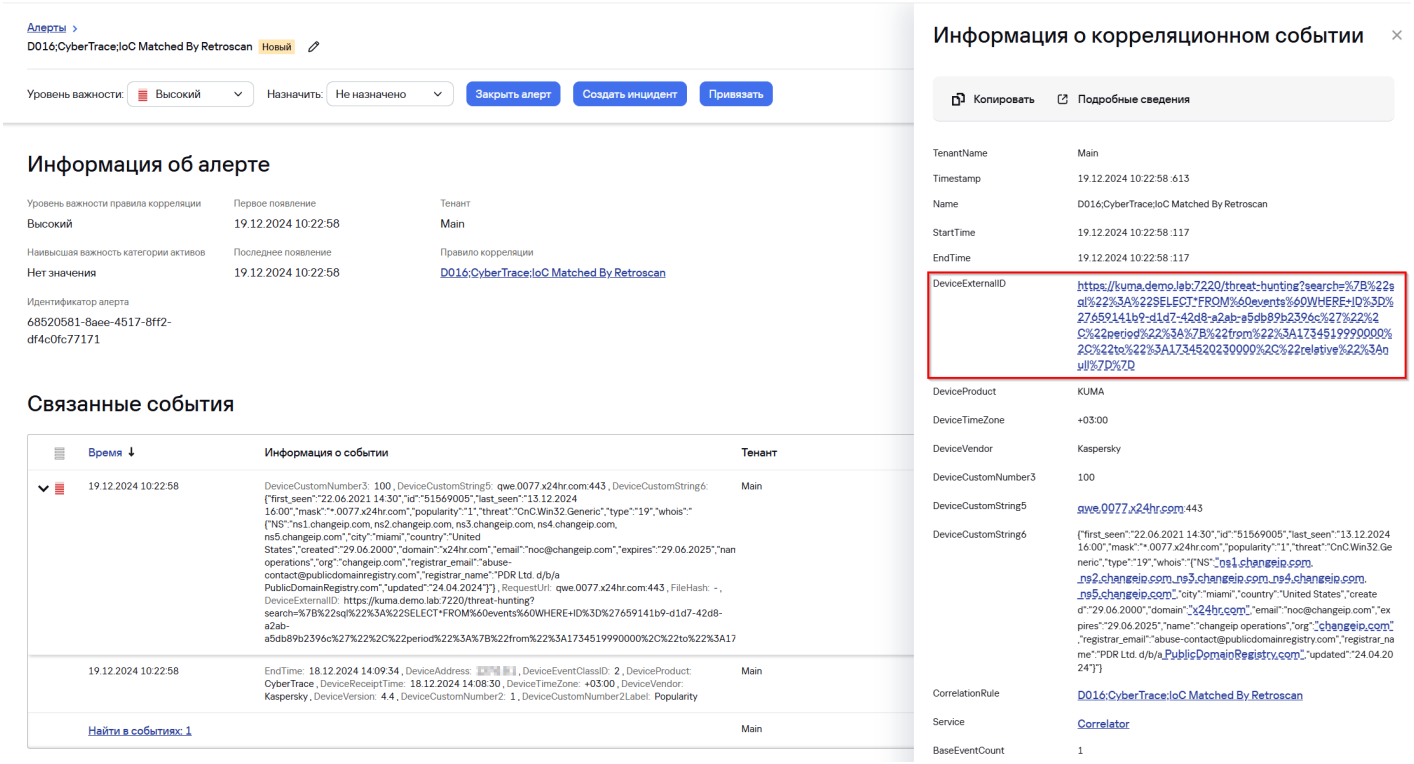
6. Обновите параметры сервиса коррелятора.

Результат

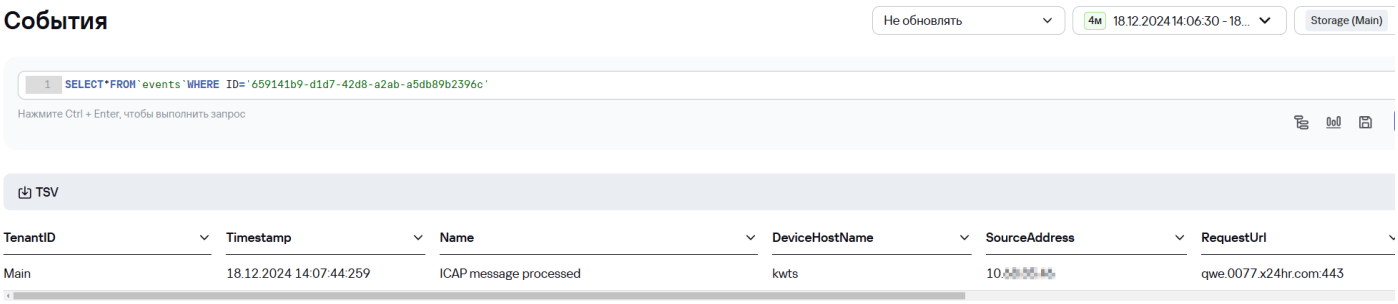
В результате по обнаружению в результате ретроспективного скнаирования в KUMA будет отправлено соответствующее обнаружение.

На основании данного обнаружения с помощью правила корреляции будет возведен алерт, в котором в поле **DeviceExternalID** будет доступна ссылка на событие KUMA, в котором было

обнаружено совпадение.



При нажатии на ссылку откроется окно с событиями с подготовленным поиском и временным окном. Для отображения события требуется только нажать на кнопку Выполнить запрос. В результате отобразится событие KUMA, в котором с помощью ретроскана CyberTrace было найдено совпадение по индикатору.



Revision #6
Created 18 December 2024 14:05:09 by Koala
Updated 10 March 2025 13:27:38 by Koala