

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 корреляционное 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** укажите 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.

Tenant EPS limit

Average tenant EPS
0

☐ Enabled

EPS limit: 50000 | Available EPS: Not set

Incoming events

Define the parameters of the socket the tenant will use to listen to incoming events.

Detection alerts

Define the parameters that will be used for outgoing alerts about detections.

Service alerts

Settings of sending service alerts that inform another software (for example, SIEM) about the state of the tenant.

☐ Enabled


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.

<<

🌙 📅

Kaspersky
CyberTrace

System >

Dashboard

Retroscan

Tasks

Settings ▾

Service

Service alerts

Users

Tenants

Feeds

Indicators export

Detections

Tags


Retroscan

Logging

Licensing

Retroscan

Settings of the retrospective scan of saved events that might contain undetected indicators.

Size of saved events Less than 1 GB 

☒ Enabled

General settings

Feeds

Regular expressions

Retroscan frequency

Every day ▾

Retention period for events (days)

30 ▴ ▾

Retention period for retroscan results (days)

90 ▴ ▾

Limit the size of saved events

☒ Enabled

Maximum size (GB)


10.0 ▴ ▾

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

<<

🌙

📄

Kaspersky
CyberTrace

☰ System >

📊 Dashboard

🔍 Retroscan

📅 Tasks

⚙️ Settings ▾

Service

Service alerts

Users

Tenants

Feeds

Indicators export

Detections

Tags

Retroscan

Logging

Licensing

Retroscan

Settings of the retrospective scan of saved events that might contain undetected indicators.

Size of saved eventsLess than 1 GB🗑️

🔵 Enabled

General settings

Feeds

Regular expressions

🔵 Select all

☐ Botnet_CnC_URL_Data_Feed.json

☐ FalsePositive.json

☒ InternalTI.json

☐ IP_Reputation_Data_Feed.json

☐ Malicious_Hash_Data_Feed.json

☐ Phishing_URL_Data_Feed.json

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.

<< Kaspersky CyberTrace

System >

Dashboard

Retroscan

Tasks

Settings ▾

Service

Service alerts

Users

Tenants

Feeds

Indicators export

Detections

Tags

Retroscan

Logging

Licensing

Retroscan

Settings of the retrospective scan of saved events that might contain undetected indicators.

Size of saved events Less than 1 GB

Enabled

General settings Feeds Regular expressions

General

Enabled

Event source: default

☒ Clear all

☒ RE_CONTEXT ☒ RE_HASH ☒ RE_IP ☒ RE_URL

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_CONTE  
XT%|KUMA_event_date=%EventReceivedDate%|outcome=%Retroscan%
```

Kaspersky CyberTrace

General

Dashboard

Search

Indicators

Detections

Research graphs

Settings

General

Service alerts

Feeds

Event sources

Detection alerts

Detection alerts

Settings of outgoing alerts about detections.

FormatFiltrationContext

We do not recommend typing the format strings manually. Instead, configure alert formats by selecting from the provided check boxes.

[View more information](#)

Service fields

Select all

☒Category—Category of the detected object

☒RecordContext—Context of the detection alert

☐Confidence—Feed confidence

☐IndicatorInfo—Link to the Kaspersky CyberTrace page that contains information about the detected indicator

☒MatchedIndicator—Detected indicator (a URL, hash, or IP address) that caused the event

☐ActionableFields—Actionable fields that are added to the detection alert

☐SourceId—Event source identifier

☐Date—Date and time when the detection was made

☒EventReceivedDate—Date and time when Kaspersky CyberTrace received the event from the SIEM system

☒Retroscan—Whether the detection was made as a result of a retroscan

Values extracted from the event

Select all

☒RE_CONTEXT

☐RE_HASH

☐RE_IP

☐RE_URL

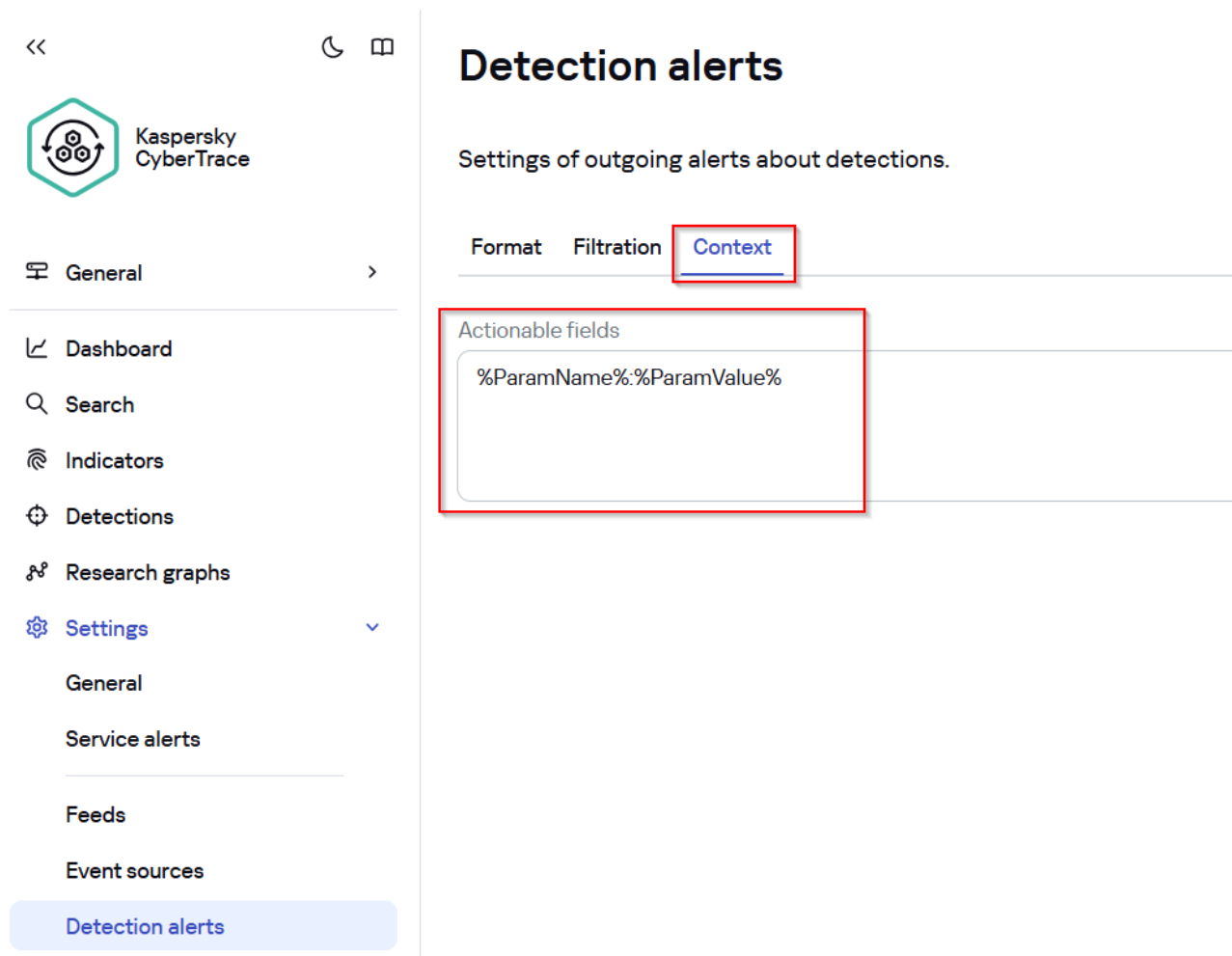
Alert format

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

Timezone: UTC+3
Kaspersky CyberTrace v5.0.0.2086

Выберите сверху **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**.

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор	<div>Создать</div>
Тип* ⓘ	<div>tcp</div>
URL* ⓘ	<div>:9998</div>
Auditd	<div><input type="checkbox"/></div>
Разделитель	<div></div>

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.

Редактирование правила корреляции

Общие

Селекторы

Действия

Корреляторы

Параметры

Локальные переменные

+ Добавить

Удалить

☐

Переменная

Значение

☐

core

"kuma.demo.lab:7220"

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 сканирования 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.

Алерты >

D016:CyberTrace:IoC Matched By Retroscan Новый

Уровень важности: Высокий

Назначить: Не назначено

Закрыть алерт

Создать инцидент

Привязать

Информация об алерте

Уровень важности правила корреляции: **Высокий**

Первое появление: 19.12.2024 10:22:58

Тенант: **Main**

Наивысшая важность категорий активов: **Нет значения**

Последнее появление: 19.12.2024 10:22:58

Правило корреляции: [D016:CyberTrace:IoC Matched By Retroscan](#)

Идентификатор алерта: 68520581-8a6e-4517-8ff2-df4c0fc77171

Связанные события

Время ↓	Информация о событии	Тенант
19.12.2024 10:22:58	DeviceCustomNumber3: 100 , DeviceCustomString5: qwe.0077.x24hr.com:443 , DeviceCustomString6: {"first_seen":"22.06.2021 14:30","id":"51569005","last_seen":"13.12.2024 16:00","mask":"*.0077.x24hr.com","popularity":1,"threat":"OnC.Win32.Generic","type":"19","whois":{"NS":"ns1.changeip.com, ns2.changeip.com, ns3.changeip.com, ns4.changeip.com, ns5.changeip.com","city":"miami","country":"United States","created":"29.06.2000","domain":"x24hr.com","email":"noc@changeip.com","expires":"29.06.2025","name-operations","org":"changeip.com","registrar_email":"abuse-contact@publicdomainregistry.com","registrar_name":"PDR Ltd. d/b/a PublicDomainRegistry.com","updated":"24.04.2024"}}, DeviceExternalID: https://kuma.demo.lab:7220/threat-hunting?search=%7B%22\$al%22%3A%22SELECT*FROM%60events%60WHERE+ID%3D%27659141b9-d1d7-42d8-a2ab-a5db89b2396c%27%22%2C%22period%22%3A%7B%22from%22%3A1734519990000%2C%22to%22%3A1734520230000%2C%22relative%22%3Anull%7D%7D	Main
19.12.2024 10:22:58	EndTime: 18.12.2024 14:09:34 , DeviceAddress: 10.0.0.1 , DeviceEventClassID: 2 , DeviceProduct: CyberTrace , DeviceReceiptTime: 18.12.2024 14:08:30 , DeviceTimeZone: +03:00 , DeviceVendor: Kaspersky , DeviceVersion: 4.4 , DeviceCustomNumber2: 1 , DeviceCustomNumber2Label: Popularity	Main
Найти в событиях: 1		Main

Информация о корреляционном событии

Копировать

Подробные сведения

TenantName: Main

Timestamp: 19.12.2024 10:22:58.613

Name: D016:CyberTrace:IoC Matched By Retroscan

StartTime: 19.12.2024 10:22:58.117

EndTime: 19.12.2024 10:22:58.117

DeviceExternalID: [https://kuma.demo.lab:7220/threat-hunting?search=%7B%22\\$al%22%3A%22SELECT*FROM%60events%60WHERE+ID%3D%27659141b9-d1d7-42d8-a2ab-a5db89b2396c%27%22%2C%22period%22%3A%7B%22from%22%3A1734519990000%2C%22to%22%3A1734520230000%2C%22relative%22%3Anull%7D%7D](https://kuma.demo.lab:7220/threat-hunting?search=%7B%22$al%22%3A%22SELECT*FROM%60events%60WHERE+ID%3D%27659141b9-d1d7-42d8-a2ab-a5db89b2396c%27%22%2C%22period%22%3A%7B%22from%22%3A1734519990000%2C%22to%22%3A1734520230000%2C%22relative%22%3Anull%7D%7D)

DeviceProduct: KUMA

DeviceTimeZone: +03:00

DeviceVendor: Kaspersky

DeviceCustomNumber3: 100

DeviceCustomString5: [qwe.0077.x24hr.com:443](#)

DeviceCustomString6: {"first_seen":"22.06.2021 14:30","id":"51569005","last_seen":"13.12.2024 16:00","mask":"*.0077.x24hr.com","popularity":1,"threat":"OnC.Win32.Generic","type":"19","whois":{"NS":"ns1.changeip.com, ns2.changeip.com, ns3.changeip.com, ns4.changeip.com, ns5.changeip.com","city":"miami","country":"United States","created":"29.06.2000","domain":"x24hr.com","email":"noc@changeip.com","expires":"29.06.2025","name":"changeip operations","org":"changeip.com","registrar_email":"abuse-contact@publicdomainregistry.com","registrar_name":"PDR Ltd. d/b/a PublicDomainRegistry.com","updated":"24.04.2024"}}, CorrelationRule: [D016:CyberTrace:IoC Matched By Retroscan](#)

Service: [Correlator](#)

BaseEventCount: 1

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.

События

Не обновлять

4m 18.12.2024 14:06:30 - 18...

Storage (Main)

1 SELECT*FROM`events`WHERE ID= '659141b9-d1d7-42d8-a2ab-a5db89b2396c'

Нажмите Ctrl + Enter, чтобы выполнить запрос

TSV

TenantID	Timestamp	Name	DeviceHostName	SourceAddress	RequestUrl
Main	18.12.2024 14:07:44:259	ICAP message processed	kwts	10.0.0.1	qwe.0077.x24hr.com:443

Revision #6

Created 18 December 2024 14:05:09 by Koala

Updated 10 March 2025 13:27:38 by Koala