

Интеграция CyberTrace с KUMA

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.com/help/KUMA/3.2/ru-RU/217924.htm>

Ссылка на актуальный дистрибутив CyberTrace :
<https://support.kaspersky.com/datafeeds/download/15920#block0>

Системные требования для CyberTrace

Минимальные системные требования (обработка ~4K EPS): 8 vCPU; 20 RAM; 200 HDD

- ОС – Linux x64 (CentOS 7.x/8.x или RedHat 7.x предпочтительно, но зависит от стандартов и политик организации)
- RAM – как минимум 16 ГБ должно быть свободно для использования только СТ
- HDD – не менее 100ГБ доступных в /opt (без использования Retroscan, для продуктивного сервера потребуется около 1ТБ)
- Network – сетевой интерфейс 1Гбит/с со статическим IP

Подробнее: <https://support.kaspersky.com/help/CyberTrace/4.4/ru-RU/270383.htm>

Для загрузки фидов Лаборатории Касперского нужен доступ до <https://wlinfo.kaspersky.com> (TCP/443). Важно: **НЕ** должен подменяться сертификат (SSL inspection) на периметре при доступе к ресурсу. Для загрузки других фидов может потребоваться доступ, в зависимости от их размещения.

Установка CyberTrace на Linux

Распаковать загруженный архив:

```
tar -C /opt -xvzf CyberTrace-rpm.tar.gz --no-same-owner
```

Переход в папку установки:

```
cd /opt/cybertrace
```

Учетная запись пользователя, выполняющего установку DEB|RPM-пакета, должна иметь права root.

Запуск скрипта установки:

```
./run.sh install
```

Установка CyberTrace выполняется в каталог `/opt/kaspersky/ktfs`.

После установки DEB|RPM пакета скрипт установки автоматически запускает конфигуратор, в котором нужно прочитать и принять лицензионное соглашение (EULA). После этого выполняется запуск сервисов CyberTrace: `cybertrace_db` и `cybertrace`.

Вход в веб-интерфейс по адресу **https://<IP_or_Hostname>**, УЗ по умолчанию **admin / CyberTrace!1**

Отключите фаервол на ОС или откройте доступ до нужных портов для работы CyberTrace

Настройка на стороне CyberTrace

Вход в CyberTrace по: **https://<IP_or_Hostname>**, пароль по умолчанию: **admin / CyberTrace!1**

При первом входе после установки CyberTrace появится окно мастера первоначальной настройки (Initial Setup Wizard), в котором необходимо:

- Выбрать используемую SIEM-систему: в данном примере это KUMA

- Указать параметры подключения для используемой SIEM-системы: IP-адрес интерфейса сервера CyberTrace. В последнем поле указать IP-адрес интерфейса или Hostname сервера CyberTrace.

Connection settings

Specify connection parameters for Kaspersky CyberTrace

1

Service listens on: ☒ IP and port ☐ UNIX socket

2

IP address

Port

3

Service sends events to:

IP address

Port

4

Specify an external IP address, a host name assigned by a DHCP, or a DNS server for the Kaspersky CyberTrace host

IP address or host name

Back

Next

- Опционально указать настройки прокси-сервера
- Опционально импортировать файл лицензионного ключа и файл сертификата для возможности загрузки коммерческих потоков данных об угрозах
- Указать потоки данных об угрозах, использование которых планируется в Kaspersky CyberTrace.

Для завершения первоначальной настройки нажать **Close**.

После завершения первоначальной настройки рекомендуется изменить пароль администратора, используемый по умолчанию.

Проверить успешность загрузки индикаторов компрометации можно следующим способом:

1. Перейдите во вкладку **Indicators** и убедитесь в наличии индикаторов компрометации
2. Перейдите во вкладку **Dashboard** -> виджет **Supplier statistics** и проверьте, что столбец **Indicators** для каждого фида отличен от 0.

Настройка на стороне KUMA

Начиная с версии [3.2](#) в KUMA доступно 2 метода интеграции с CyberTrace для потокового обогащения событий данными об индикаторах компрометации:

1. С использованием API CyberTrace
2. С помощью Kaspersky CyberTrace Service

Интеграция с использованием API CyberTrace

Данный метод позволяет отправлять большое количество объектов одним запросом на API-интерфейс CyberTrace. Рекомендуется применять в системах с большим потоком событий. Производительность Cybertrace-http значительно превосходит показатели прежнего метода cybertrace, который по-прежнему доступен для обеспечения обратной совместимости.

В веб-интерфейсе CyberTrace создайте новую учетную запись пользователя, которая будет использоваться KUMA для подключения к API CyberTrace. Для этого перейдите в раздел **Settings -> Users** и нажмите **Add new user**. В появившемся окне **New user** укажите следующие параметры:

- **Login** - <имя учетной записи пользователя>
- **Password** - <пароль учетной записи пользователя>
- **Confirm password** - <пароль учетной записи пользователя>
- **Role** - Analyst

Нажмите **Add**.

Далее в веб-интерфейсе KUMA создайте секрет для подключения к API CyberTrace: перейдите в **Ресурсы -> Секреты** и нажмите **Добавить**. В появившемся окне укажите следующие параметры:

- **Название** - <название секрета>
- **Тенант** - <название тенанта, например, Main>
- **Тип** - credentials
- **Пользователь** - <Имя пользователя, созданного на предыдущем шаге>
- **Пароль** - <Пароль, созданного пользователя на предыдущем шаге>
- **Описание (опционально)**

Создание секрета



Название*	1	<input type="text" value="CyberTrace API"/>
Тенант*	2	<input type="text" value="Main"/>
Тип*	3	<input type="text" value="credentials"/>
Пользователь*	4	<input type="text"/>
Пароль* ⓘ	5	<input type="password"/>
Описание	6	<input type="text" value="Подключение к API <u>CyberTrace</u> для обогащения событий"/>

Создайте правило обогащения в веб-интерфейсе KUMA: перейдите в **Ресурсы -> Правила обогащения** и нажмите **Добавить**. В появившемся окне укажите следующие параметры:

- **Название** - <название правила обогащения>
- **Тенант** - <название тенанта, например, Main>
- **Исходный тип** - cybertrace-http
- **URL** - <IP-адрес/FQDN сервера CyberTrace>:443
- **Секрет** - <секрет, созданный на предыдущем шаге>
- **Ключевые поля** - <поля, значения которых будут передаваться в CyberTrace на анализ. Как пример, укажите поля со скриншота ниже>
- **Время ожидания** - 0
- **Максимальное кол-во событий в очереди обогащения** - 1000000
- **Описание (опционально)**
- **Параметры фильтра** - <условия срабатывания правила обогащения. В качестве примера, ниже используется набор условий, при котором правило будет срабатывать для событий обращения внутренних IP-адресов к внешним IP-адресам>

Название*

[TEST] CyberTrace API Enrichment External Connections

Тенант*

Main

Исходный тип*

cybertrace-http

URL* ⓘ

██████████:443

Секрет*

CyberTrace API

Ключевые поля*

DestinationAddress ×

DestinationHostName ×

DestinationNtDomain ×

DestinationDnsDomain ×

FileHash ×

RequestUri ×

Время ожидания

0

Максимальное кол-во событий в очереди обогащения ⓘ

1000000

Отладка

☐

Описание

Обогащение событий подключения к внешним ресурсам

Параметры фильтра

Фильтр

Создать

☐ Сохранить фильтр

Конструктор

</> Код

И ▾

+ Добавить условие

+ Добавить группу

⋮

Если е: SourceAddress inSubnet или (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

×

⋮

Если не е: DestinationAddress inSubnet или (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

×

Пример готового кода для добавления в правило обогащения:

```
SourceAddress insubnet [  
  '10.0.0.0/8',  
  '172.16.0.0/12',  
  '192.168.0.0/16'  
]  
AND NOT DestinationAddress insubnet [  
  '10.0.0.0/8',  
  '172.16.0.0/12',  
  '192.168.0.0/16'  
]
```

Указываем поля DestinationHostName | RequestURL и DestinationNtDomain | DestinationDnsDomain, потому что в событии может быть только одно поле из пары. Если есть оба поля, коннектор CyberTrace в KUMA возьмет только уникальное значение и отправит в CyberTrace на анализ

Если объекты (IP, URL, Domain, Hash) расположены в “кастомных” полях, напр., DeviceCustomString1, то можно создать отдельное правило обогащения, в котором в качестве ключевого поля будет указано необходимое "кастомное" поле/поля

Добавьте созданное правило обогащения в параметрах сервиса коллектора (или коррелятора): перейдите в **Ресурсы -> Активные сервисы** и нажмите на название сервиса коллектора . В появившемся окне **Редактирование коллектора** перейдите на шаг **Обогащение событий** и в секции справа нажмите **Добавить обогащение**.

Редактирование коллектора

×

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий **1**

Маршрутизация

Обогащение событий

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

Поле KUMA

Подпись

Примеры

DeviceAction

ApplicationProtocol

DeviceCustomIPv6Address1

DeviceCustomIPv6Address1Label

+ Добавить обогащение **2**

В поле **Правило обогащения** выберите ранее созданное правило обогащения.

Редактирование коллектора

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

Обогащение событий

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

Поле KUMA	Подпись	Примеры
DeviceAction		
ApplicationProtocol		
DeviceCustomIPv6Address1		
DeviceCustomIPv6Address1Label		

Правило обогащения

[TEST] CyberTrace API Enrichment External Conne

1

Исходный тип*

cybertrace-http

URL*

10.0.0.0/8:443

Секрет*

CyberTrace API

Ключевые поля*

DestinationAddress

DestinationHostName

DestinationNtDomain

DestinationDnsDomain

FileHash

RequestUri

Время ожидания

0

Максимальное кол-во событий в очереди обогащения

1000000

Отладка

☐

Параметры фильтра

Фильтр

Создать

☐ Сохранить фильтр

Конструктор

</> Код

И

+

Добавить условие

+

Добавить группу

Если

е:

SourceAddress

inSubnet

или (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

Если не

е:

DestinationAddress

inSubnet

или (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

После добавления правила обогащения перейдите на шаг **Проверка параметров** и нажмите **Сохранить и обновить параметры сервисов** для применения изменений конфигурации 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

Сервисы, использующие этот коллектор

Тип	Название
коллектор	

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

1

Интеграция с помощью Kaspersky CyberTrace Service

Для повышения производительности, можно изменять число рабочих процессов коллектора (1 шаг настройки) / самого правила обогащения (для асинхронных задач эффективнее работа)

В KUMA перейдите в раздел **Ресурсы - Правила обогащения**. Нажмите на кнопку **Добавить правило обогащения**. В поле URL укажите IP адрес CyberTrace, остальные поля заполните по аналогии со скриншотом ниже. Затем нажмите на кнопку **Сохранить**.

Изменить правило обогащения

*Название

CyberTracePresaleDemo

*Тенант

Main

*Тип источника данных

cybertrace

*URL

10.68.85.139:9999

?

Количество подключений

0

Запросов в секунду

5000

Время ожидания

0

*Сопоставление

Поле KUMA	Индикатор CyberTrace	
FileHash	hash	×
RequestUrl	url	×
DestinationAddress	ip	×
DeviceCustomStri...	url	×

+ Добавить сопоставление

Отладка

Выключено

Описание

Описание

Сохранить

Для снижения нагрузки на CyberTrace рекомендуется использовать фильтр на правиле обогащения, пример фильтра из пресейл пака:

<https://box.kaspersky.com/f/39a48398202543dbb9c9/>

Filter [Filter] CyberTrace

Conditions

OR + Add condition + Add group + Add filter

AND + Add condition + Add group + Add filter

If not event field FileHash = constant value

If event field FileHash match list ^[a-fA-F0-9]{32}\$, ^[a-fA-F...

AND + Add condition + Add group + Add filter

If not event field DestinationAddress = constant value

If not event field DestinationAddress inSubnet list 192.168.0.0/16, 10.0.0.0/8...

Добавьте созданное правило обогащения на нужные коллеторы или корреляторы. Ниже пример добавления в коррелятор.

- 1 Общие
- 2 Корреляция
- 3 Обогащение
- 4 Реагирование
- 5 Маршрутизация
- 6 Проверка параметров

*Правило обогащения: CyberTracePresaleDemo

*Тип источника данных: cybertrace

*URL: 10.68.85.139:9999

Количество подключений: 0

Запросов в секунду: 1000

Время ожидания: 30

*Сопоставление:

Поле KUMA	Индикатор CyberTrace
FileHash	hash
RequestUrl	url
DestinationAddress	ip
DeviceCustomStri...	url

Отладка: Выключено

Фильтр: Создать

☐ Сохранить фильтр

Условия: И + Добавить условие + Добавить группу + Добавить фильтр

После выполнения настроек необходимо сохранить и обновить (можно и перезапустить) параметры ресурса.

Сервисы, использующие этот коррелятор

Тип	Название
correlator	[Example] Correlator

Сохранить и перезапустить сервисы

Сохранить и обновить параметры сервисов

Проверка работы интеграции CyberTrace с KUMA

Подразумевается, что настроена интеграция событий с KSC на KUMA, на хосте, где будет проводиться тест установлен KES с последними обновлениями. Иначе используйте другие системы, с которыми осуществлена интеграция по событиям.

В CyberTrace в разделе Индикаторы, скопируйте любой URL из списка содержимых.

Dashboard

Search

Retroscan

Indicators

Detections

Graph

Tasks 365

Settings

Help

Indicators

AddMark as false positiveDelete

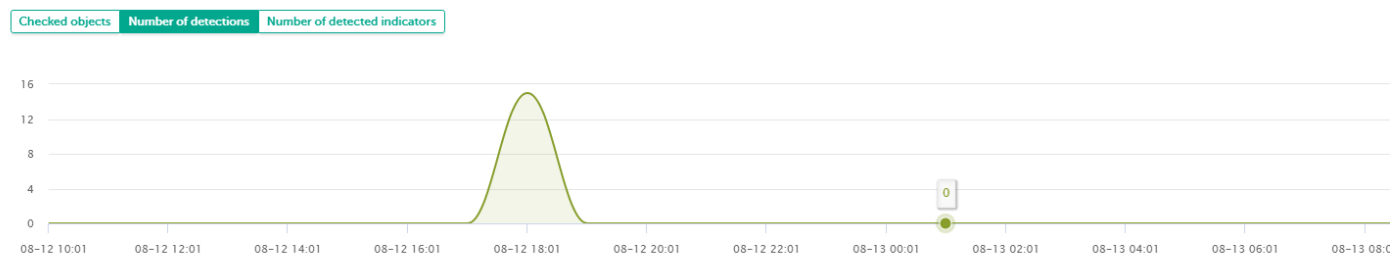
ioc_value: 192.0.2.* OR (ioc_type: md5 AND ioc_updated_date: >=01.01.2020)

Indicators selected: 0 of 3434945

<input type="checkbox"/>	Type ↓	Value ↓	Added ↓	Changed ↓	Tag	Total tag weight ↓	Suppliers
<input type="checkbox"/>	URL	8j24g0e3.ga	2022-02-10 20:30:12	2022-02-10 20:30:23	No tags	-	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed
<input type="checkbox"/>	URL	883binarynet.ga	2022-02-10 20:30:12	2022-02-10 20:30:23	No tags	-	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed
<input type="checkbox"/>	URL	erff.xyz	2022-02-10 20:30:12	2022-02-10 20:30:23	No tags	-	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed
<input type="checkbox"/>	URL	1002ch8.b-cdn.n...	2022-02-10 20:30:12	2022-02-10 20:30:23	No tags	-	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed

С хоста, где установлен KES осуществите переход в браузере по ссылке, например - <http://www.kasprsky.com/test/wmuf> и получите "отбивку" от KES. Через некоторое время появится событие от KSC. В событии будет обращение по вредоносной ссылке с дополнительным контекстом от CyberTrace, пример ниже:

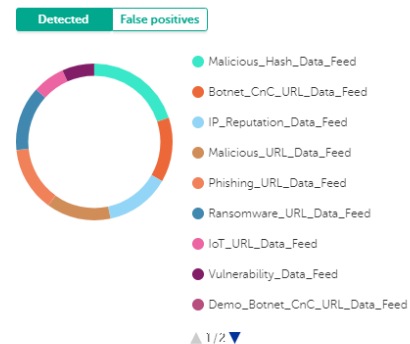
Statistics overview



Supplier statistics

Supplier name	Last update date	Indicators	False positives	Detected
Kaspersky Malicious Hash Data Feed	2023-08-15 07:04	1 622 043	0	3
Kaspersky Botnet CnC URL Data Feed	2023-08-15 09:05	584 158	0	2
Kaspersky IP Reputation Data Feed	2023-08-15 07:04	59 956	0	2
Kaspersky Malicious URL Data Feed	2023-08-15 09:05	145 213	0	2
Kaspersky Phishing URL Data Feed	2023-08-15 09:05	231 019	0	2
Kaspersky Ransomware URL Data Feed	2023-08-15 07:04	147 212	0	2
Kaspersky IoT URL Data Feed	2023-08-15 09:05	50 543	0	1
Kaspersky Vulnerability Data Feed	2023-08-15 05:05	30 843	0	1
Total		2 499 827	0	15

← Previous 1 2 Next →



В качестве упрощенного варианта проверки корректной работы обогащения CyberTrace можно отправить тестовое событие в коллектор с помощью утилиты netcat или утилиты [kuma](#). В примере ниже используется тестовое событие в формате CEF, отправленное средствами netcat.

Для коллектора с транспортом TCP:

```
nc <IP-адрес> <порт> <<< 'CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|request=<любой URL из вкладки Indicators CyberTrace>'
```

Для коллектора с транспортом UDP:

```
nc -u <IP-адрес> <порт> <<< 'CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|request=<любой URL из вкладки Indicators CyberTrace>'
```

Пример обогащенного события на скриншоте ниже

Копировать

TenantID	Main
Timestamp	15.07.2024 14:52:15:345
Name	Name
EndTime	15.07.2024 14:52:15:345
DeviceAddress	
DeviceAssetID	
DeviceEventClassID	Signature ID
DeviceProduct	Device Product
DeviceReceiptTime	15.07.2024 14:52:15:345
DeviceTimeZone	+03:00
DeviceVendor	Device Vendor
DeviceVersion	Device Version
Service	
RequestUrl	1.0077.x24hr.com
Severity	Severity
Type	Base
Индикатор TI	1.0077.x24hr.com

Категория индикатора	KL_BotnetCnC_URL
first_seen	22.06.2021 14:30
id	51569005
last_seen	20.02.2024 13:05
mask	*.0077.x24hr.com
popularity	2
threat	CnC.Win32.Generic

Для создания алертов и отслеживания обращений к IP-адресам/доменам/URL, информация о которых есть в фидах CyberTrace, необходимо привязать к коррелятору следующие правила корреляции из SOC Package:

R201_Обнаружено соединение с подозрительным IP-адресом

R202_Обнаружено обращение на подозрительный Domain

R203_Обнаружено обращение на подозрительный URL

Revision #11

Created 1 July 2024 14:37:16 by Dmitry Borisov

Updated 9 August 2024 12:33:10 by Koala