Сценарии использования CyberTrace

> **CyberTrace** - платформа для управления данными о киберугрозах
> В статье описаны основные два сценария использования:
> 1. **Поиск IoC**: интеграции по TCP/API, а также ретроскан
> 2. **TIP**: получение, распространение IoC и графы расследования

1. Поиск IoC

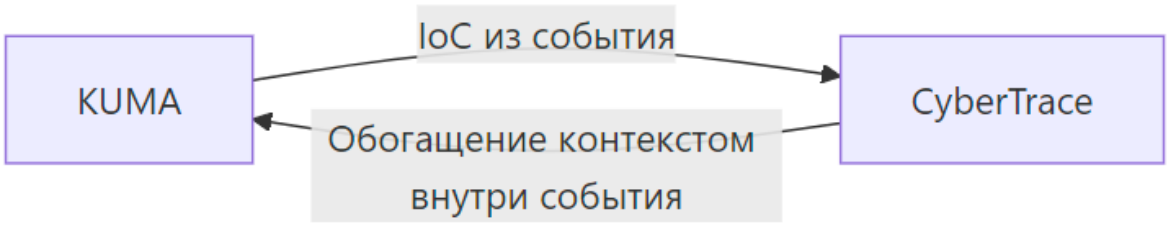
1.1 События от SIEM

1.1.1 KUMA (TCP / API)

KUMA нативно интегрируется с CyberTrace. На стороне KUMA настраивается правило обогащения:

- `cybertrace` -- события отправляются по TCP/9999 (при необходимости порт переопределяется)
- `cybertrace-http` -- события отправляются по HTTP/443 (**рекомендуемый способ**)

Схема взаимодействия:



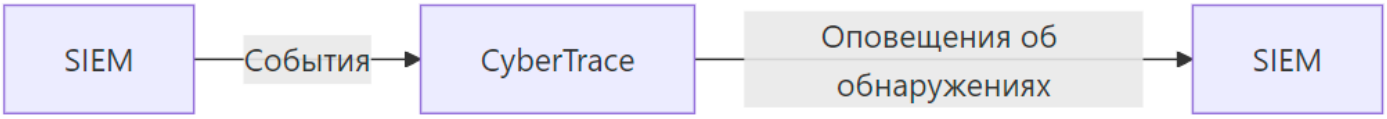
Пример обогащения:

Type	Base
Индикатор TI	[redacted]
Категория индикатора	Enrichment_KTIP_MD5
Категория индикатора	**KL_Malicious_Hash_MD5**
MD5	[redacted]
SHA1	[redacted]
SHA256	[redacted]
file_names	p003, заявка_гув_5_03д.zip, inbox, trash, ���_��5_03�zip, спам, sent-1
file_size	7314021
file_type	PE
first_seen	11.03.2025 13:13
id	25694532123
industry	Manufacturing, Construction
last_seen	21.05.2026 13:49
mitre	TA0005:T1036.008
popularity	2
threat	Exploit.Win32.ShellCode.cafg

1.1.2 Другие SIEM

Список поддерживаемых SIEM:

Схема взаимодействия:



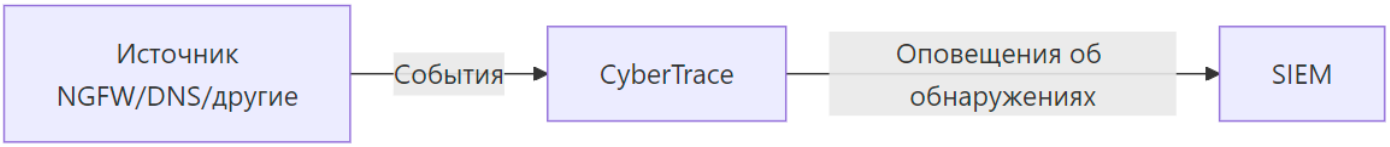
Пример интеграции:

- На стороне SIEM настраивается форвардинг событий на TCP/9999 (при необходимости порт переопределяется)
- На стороне CyberTrace выбирается SIEM/настраиваются регулярки
- На стороне CyberTrace определяется формат отправки сообщения и address:port назначения
- На стороне SIEM производится дальнейшая обработка события

1.2 Другие события отправленные по TCP

В CyberTrace не лицензируется поток EPS, поэтому, если какой-то источник флудит событиями, то возможен сценарий, когда CyberTrace обрабатывает поток, а сработки отправляет сработки в SIEM

Схема взаимодействия:



К минусам такого подхода можно отнести необходимость писать регулярные выражения под кастомный источник. Но часть этих выражений уже описаны в справке

1.3 Ретроскан

Пример использования ретроскана в сочетании с KUMA

Ретроскан помогает выявить IoC, которые на момент получения события не считались вредоносными, но спустя n-время были добавлены в фиды. После обновления фидов CyberTrace повторно проверяет сохраненные события и обнаруживает такие совпадения

CyberTrace может хранить события либо в течение заданного количества дней, либо до достижения заданного объема дискового пространства

2. TIP

2.1 Получение IoC

Способ получения:

- Файловая система
- HTTP/HTTPS
- Электронная почта (IMAP/POP3)

Формат получения IoC:

- CSV
- JSON
- STIX (1.x, 2.0, 2.1)
- XML

- PDF
- MISP

Если сторонний поставщик предоставляет фиды через TAXII, то CyberTrace считается совместимым с ними

2.2 Распространение IoC

Также можно рассмотреть CyberTrace, как поставщика фидов в сторонние решения

2.2.1 Коробочный функционал

Из коробки поддерживаются следующие форматы экспорта:

- Универсальный экспорт в CSV
- Check Point NGFW
- Cisco Firewall Management Center
- FortiGate NGFW
- Palo Alto NGFW
- Sophos NGFW
- Security Code NGFW (Код Безопасности)
- UserGate NGFW
- Broadcom (Symantec) ProxySG

2.2.2 Утилиты

Также с помощью утилит возможно экспортировать фиды в другие СЗИ по API. Они реализованы для:

- Категорий KSC
- PT NAD
- PT WAF
- PT SB

Данные утилиты предоставляются по запросу

2.3 IoC Pivoting

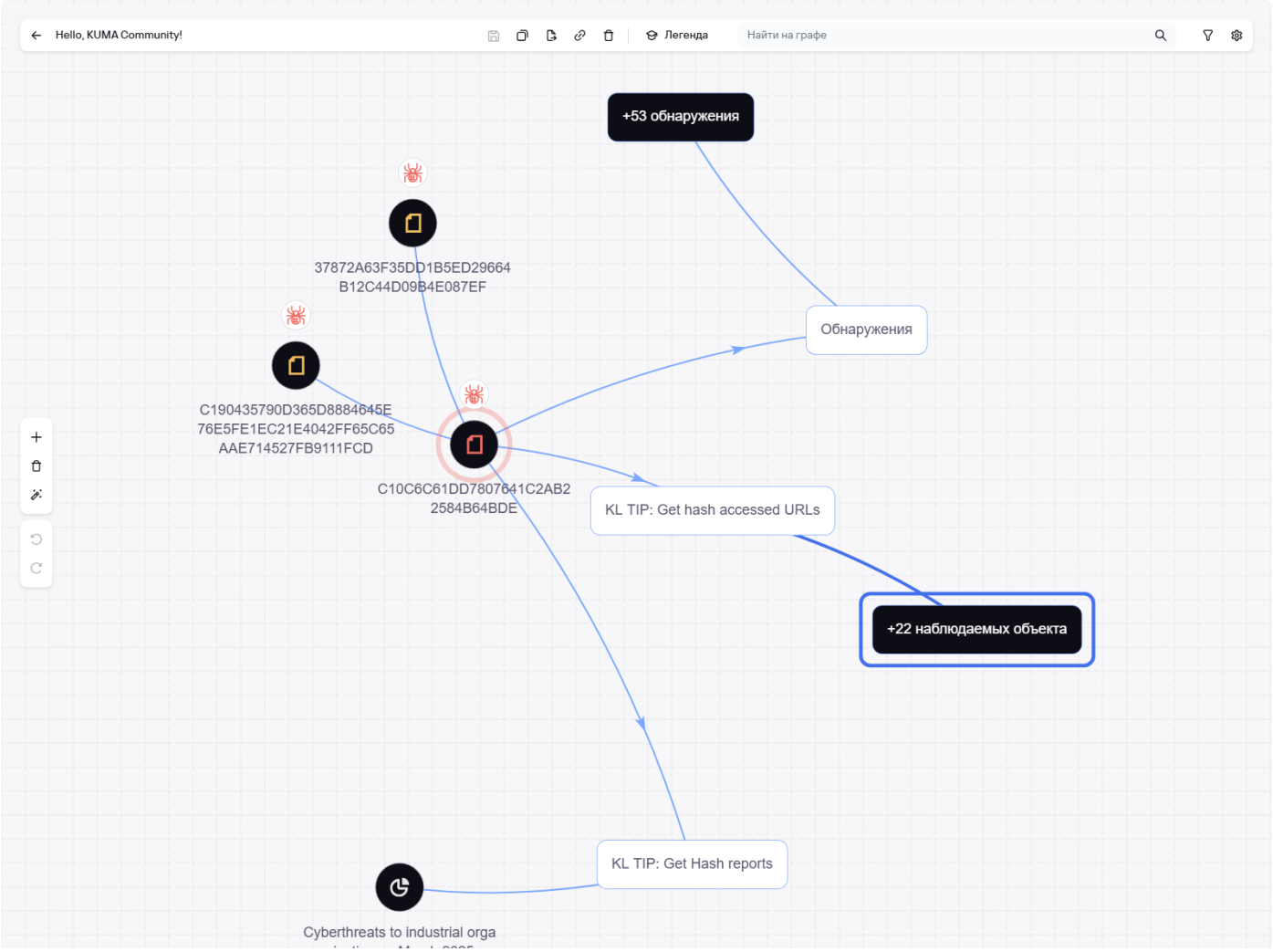
2.3.1 Граф расследования

Графы расследования визуализируют информацию об IoC и их взаимосвязях. Для получения расширенной информации по IoC CyberTrace интегрируется с:

- Kaspersky TIP
- VirusTotal

Описание трансформаций, которые поддерживаются в CyberTrace

Пример графа:



2.3.2 Kaspersky Threat Lookup

Позволяет сделать запрос по IoC и автоматически добавить его в фиды CyberTrace. Также по данному IoC предоставляется весь контекст из TIP (File downloaded from web addresses and domains, Similar files и др.)

Revision #9
Created 2026-07-14 11:45:31 UTC by lithium
Updated 2026-07-14 13:50:13 UTC by lithium