?????????? 2: EVENT API

Приложение 2: event api

API для получения внешними системами информации о событиях приложения

Kaspersky Anti Targeted Attack Platform предоставляет интерфейс API для доступа внешних систем к информации о зарегистрированных приложением событиях.

Вы можете указать в параметрах запроса фильтры, чтобы получить информацию только о тех событиях, которые удовлетворяют требуемым условиям.

При появлении новых событий приложение не отправляет информацию о них автоматически на основе предыдущих запросов. Для получения актуальной информации требуется отправить повторный запрос.

Параметры фильтрации событий. Задаются с помощью языка запросов для работы с событиями.

Язык запросов для фильтрации событий поддерживает следующие функции и операторы:

- Функции: in.
- Операторы сравнения для значений типа String или Boolean: ==, !=.
- Операторы сравнения для чисел и переменных: AND, OR, NOT, ==, !=, >, >=, <, <=.

Вы можете посмотреть список полей, по которым можно отфильтровать события, в разделе Поля для фильтрации событий. Полный перечень полей приведен в таблице ниже.

Если вы хотите получить информацию о событиях разного типа, вам нужно создать отдельный запрос для каждого типа событий.

```
EventType=='threatdetect' AND EventType=='threatprocessingresult'
```

Поддерживаются константы числового и строкового типа. Строковые константы заключаются в апострофы: 'example'. Для строковых констант поддерживаются метасимволы * и ?. Если вы не хотите использовать метасимволы, вам нужно экранировать их: *, \?. Также в строковых константах вам нужно экранировать специальные символы.

Состав передаваемых данных об окружении обнаруженных объектов в зависимости от источника объекта приведен в таблице ниже.

Источник объекта	Параметр	Описание	Тип данных	Пример
WEB	`sourceIP`	IP-адрес компьютера, установившего соединение.	IP address	`192.0.2.0`
	`sourceHostname`	Имя компьютера, установившего соединение.	String	`example.com`
	`destinationIp`	IP-адрес компьютера, с которым установлено соединение.	IP address	`198.51.100.0`
	`destinationPort`	Порт компьютера, с которым установлено соединение.	Integer	`3128`
	`URL`	URL-адрес интернет-ресурса, к которому выполнено обращение. Для обнаружений, выполненных технологией IDS, этот параметр отсутствует. Для обнаружений, выполненных технологией URL, этот параметр совпадает с параметром `detectedObject`.	String	`https://example.com:443/`
	`method`	Метод HTTP-запроса.	String	`Connect`
	`referrer`	URL-адрес, на который была выполнена переадресация.	String	`https://example.com:443/`
MAIL	`mailFrom`	Адрес электронной почты отправителя.	String	`sender@example.com`
	`mailTo`	Список адресов электронной почты получателей через запятую.	Array	`recipient1@example.com, recipient2@example.com`
	`subject`	Тема сообщения.	String	`'You are the winner'`
	`messageId`	ID сообщения электронной почты.	String	`1745028736.156014.1542897410859.JavaMail.svc_jira_pool@hqconflapp2`
Endpoint, external	`hostName`	Имя компьютера, на котором выполнено обнаружение.	String	`computername.example.com`
	`IP`	IP-адрес компьютера, на котором выполнено обнаружение.	IP address	`198.51.100.0`

☐	DNS	`sourceIp`	IP-адрес компьютера, инициировавшего соединение по протоколу DNS.	IP address	`192.0.2.0`
		`destinationIp`	IP-адрес компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	IP address	`198.51.100.0`
		`destinationPort`	Порт компьютера, с которым установлено соединение по протоколу DNS (как правило, DNS-сервера).	Integer	`3128`
		`dnsMessageType`	Тип DNS-сообщения: · `Request`. `Response`.	String	`Request`
		`dnsRequestType`	Один из следующих типов записи DNS-запроса: · `A`. · `AAA`. · `CNAME`. `MX`.	String	`MX`
		`domainToBeResolved`	Имя домена из DNS-запроса.	String	`example.com`

Revision #2
Created 16 December 2025 22:16:54 by Владислав
Updated 6 February 2026 10:55:44 by Кирилл