?????????? 1: ?????? ???????????? ??????

Приложение 1: Состав передаваемых данных

Информация, передаваемая о каждом обнаружении, представлена в таблице ниже.

Состав передаваемых данных об обнаружении

Параметр	Значение	Описание
`alertID`	Целочисленное значение.	Идентификатор обнаружения.
`eventTimeStamp`	Дата и время.	Время события.
`detectTimestamp`	Дата и время.	Время занесения информации об обнаружении в базу Kaspersky Anti Targeted Attack Platform.
importance	Одно из следующих значений: · `high`; · `medium`; · `low`.	Важность обнаружения.
`objectSource`	Одно из следующих значений: · `web`; · `mail`; · `endpoint`; · `external`; `dns`.	Источник обнаруженного объекта.
`technology`	Одно из следующих значений: · `am` – Anti-Malware Engine; · `sb` – Sandbox; · `yara` – YARA; · `url_reputation` – URL Reputation; `ids` – Intrusion Detection System.	Технология, с помощью которой обнаружен объект.
`objectType`	Одно из следующих значений: · `file`. · `URL`. `host` (для удаленных доменов или хостов).	Тип обнаруженного объекта.
`object`	Зависит от типа обнаруженного объекта.	Данные об обнаруженном объекте. (Полное описание приведенео в таблице ниже)
`detection`	Зависит от технологии, с помощью которой обнаружен объект.	Данные о найденных угрозах. (Полное описание приведенео в таблице ниже)

`details`	Зависит от источника обнаруженного объекта.	Данные об окружении обнаруженных объектов. (Полное описание приведенео в таблице ниже)

Данные об обнаруженных объектах

Тип	Параметр	Тип данных	Описание	Пример
file	`processedObject.MD5`	MD5	MD5-хеш файла или составного объекта, переданного на проверку.	`1839a1e9621c58dadf782e131df3821f`
	`processedObject.SHA256`	SHA256	SHA256-хеш файла или составного объекта, переданного на проверку.	`7bbfc1d690079b0c591e146c4294305da1cee857e12db40f4318598fdb503a47`
	`processedObject.fileName`	String	Имя файла или составного объекта, переданного на проверку.	`EICAR-CURE.com`
	`processedObject.fileType`	String	Тип файла или составного объекта, переданного на проверку.	`GeneralTxt`
	`processedObject.fileSize`	Integer	Размер файла или составного объекта, переданного на проверку, в байтах.	`184`
	`detectedObject.MD5`	MD5	MD5-хеш файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	`1839a1e9621c58dadf782e131df3821f`
	`detectedObject.fileName`	String	Имя файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза.	`EICAR-CURE.com`
	`detectedObject.fileSize`	Integer	Размер файла (простого объекта или файла внутри составного объекта), в котором обнаружена угроза, в байтах.	`184`
`URL`	`detectedObject`	String	URL-адрес обнаруженного объекта.	`http://example.com/link`

host	detectedObject	Array	Список доменов, к которым относятся обнаруженные объекты. Для технологии URL, а также для объектов с параметром objectSource=dns список может содержать несколько доменов.	example.org, example.net

Данные о найденных угрозах

Технология	Параметр	Описание	Тип данных	Пример
Одна из следующих технологий: · Anti-Malware Engine. · YARA. · Intrusion Detection System.	detect	Список найденных угроз.	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	dataBaseVersion	Версия баз, с помощью которых проверен файл.	Integer	201811190706
Sandbox	detect	Список найденных угроз.	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	image	Имя образа виртуальной машины, на которой был проверен файл.	String	Win7
	dataBaseVersion	Версия баз в следующем формате: <версия баз программы, с помощью которых проверен файл> / <версия баз модуля IDS>.	Integer	201902031107/ 201811190706
URL Reputation	detect	Список категорий URL Reputation для обнаруженного объекта (для объектов типа URL или host).	Array	Phishing host, Malicious host, Botnet C&C(Backdoor.Win32.Mokes)

Данные об окружении обнаруженных объектов

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/`
	`agentString`	Заголовок `User agent` из HTTP-запроса, содержащий название и версию клиентского приложения.	String	`Mozilla/4.0`
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 #3
Created 16 December 2025 22:12:40 by Владислав
Updated 6 February 2026 10:55:44 by Кирилл