**Threat Intelligence Feeds and Agent**

Описание функциональных характеристик ПО

Версия 1.0

АННОТАЦИЯ

Настоящий документ содержит информацию о функциональных характеристиках программного обеспечения TI Feeds and Agent (далее – ПО, агент).

Содержание

[1 Общие сведения о программе 4](#_Toc192063848)

[2 Назначение и область применения 5](#_Toc192063849)

[2.1 Получение индикаторов из облака 5](#_Toc192063850)

[2.2 Обработка индикаторов 5](#_Toc192063851)

[2.3 Нотификация 5](#_Toc192063852)

# Общие сведения о программе

Полное наименование программы: Threat Intelligence Feeds and Agent.

Сокращенное наименование программы: TI Feeds and Agent. В рамках настоящего документа употребляются также термины: ПО, агент.

Контакты технических специалистов, которые могут проконсультировать по процессу развёртывания и настройки ПО и его функционирования: специалисты по сопровождению, адрес электронной почты: [support.tic@rt-solar.ru](mailto:support.tic@rt-solar.ru).

# Назначение и область применения

Программный комплекс TI Feeds and Agent предназначен для периодической загрузки полного списка фидов, получения изменений с момента последнего запуска и получения изменений по нотификациям. Он обеспечивает взаимодействие с различными источниками индикаторов компрометации информационных систем, поставляемых облаком TI Feeds для формирования централизованной базы знаний об угрозах информационной безопасности и индикаторах компрометации информационных систем.

Основные функциональные возможности TI Feeds and Agent:

* Получение индикаторов из облака.
* Обработка индикаторов.
* Нотификация о новых или измененных IoC.

## Получение индикаторов из облака

* Получение актуального состояния индикаторов IPv4 адресов.
* Получение актуального состояния индикаторов IPv6 адресов.
* Получение актуального состояния индикаторов URL.
* Получение актуального состояния индикаторов Domain.
* Получение актуального состояния индикаторов hash MD5.
* Получение актуального состояния индикаторов hash SHA1.
* Получение актуального состояния индикаторов hash SHA256.

## Обработка индикаторов

* Использование агента для периодической загрузки полного списка фида.
* Использование агента для получения изменений с момента последнего запуска.
* Использование агента для получения изменений по нотификациям.
* Использование агента для обработки полученных фидов.
* Использование агента для сохранения полученных фидов.

## Получение фидов

* Получение динамических фидов по категориям индикаторов.
* Получение файла IDS сигнатур (или правил).
* Получение категорий доменов с хешированным FQDN.

## Нотификация

* Нотификация о новых или измененных IoC из внешних источников.