**Threat Intelligence Feeds and Agent**

Руководство системного администратора

Версия 1.0

АННОТАЦИЯ

Настоящий документ содержит описание программного обеспечения TI Feeds and Agent (далее – ПО, агент) для системного администратора.

Содержание

[1 Общие сведения о программе 4](#_Toc193708793)

[1.1 Наименование программы 4](#_Toc193708794)

[1.2 Назначение и область применения 4](#_Toc193708795)

[2 Требования к составу и параметрам технических средств 5](#_Toc193708796)

[2.1.1 Требования к автоматизированному рабочему месту пользователя 5](#_Toc193708797)

[2.1.2 Требования к устанавливаемому общесистемному программному обеспечению 5](#_Toc193708798)

[2.2 Требования к квалификации персонала 5](#_Toc193708799)

[3 Скачивание и инсталляция установочных файлов 6](#_Toc193708800)

[4 Запуск и проверка функционирования 7](#_Toc193708801)

# Общие сведения о программе

## Наименование программы

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.

# Требования к составу и параметрам технических средств

Для обеспечения стабильной и надежной работы TI Feeds and Agent, необходимо учитывать аппаратные требования, которые могут варьироваться в зависимости от масштаба и нагрузки на систему. В данном пункте представлены рекомендуемые требования для автоматизированного рабочего места пользователя.

### Требования к автоматизированному рабочему месту пользователя

Агент играет ключевую роль в обработке поступающих индикаторов. Он может быть установлен как на персональный компьютер, так и на виртуальную машину. Рекомендуемые аппаратные требования:

* Процессор: 4 vCPU.
* Оперативная память: 8 ГБ vRAM.
* Диск: 50 ГБ HDD.
* Количество запросов: 100 RPS.

### Требования к устанавливаемому общесистемному программному обеспечению

Для обеспечения корректного функционирования на рабочее место пользователя должно быть установлено следующее общесистемное программное обеспечение:

* Операционная система: РЕД ОС 7+, Debian 11+, Astra 1.6.
* Платформа контейнеризации: Docker 22+.
* Программа архиватор (форматы rar, zip, tar).

## Требования к квалификации персонала

Персонал должен изучить документацию TI Feeds and Agent, иметь навыки работы с ПО Docker, Docker Compose.

# Скачивание и инсталляция установочных файлов

Агент доступен в виде образа docker контейнера. В комплект поставки входит конфигурационный файл, с помощью которого можно настраивать агента без внесения изменений в программный код. Для запуска агента должно быть установлена платформа контейнеризации Docker версии 22+.

Для получения установочного комплекта необходимо обратиться к специалистам по сопровождению TI Feeds and Agent по контактным данным, указанным в п. 1.1 данного документа.

Установочный комплект включает в себя следующие файлы:

* Docker-образ агента в файле solar-4rays-ti-feeds-agent.tar.
* Файл docker-compose.yml.
* Файл конфигурации агента config.toml.

Необходимо сохранить в одной папке все полученные файлы (solar-4rays-ti-feeds-agent.tar, docker-compose.yml, config.toml) и создать папку work/data на своем компьютере.

Для получения JWT и выдачи прав на получение эндпоинтов необходимо обратиться к специалистам по сопровождению по контактным данным, указанным в п. 1.1 данного документа.

Далее необходимо вписать полученый JWT в переменную TIC\_AGENT\_API\_TOKEN в файле docker-compose.yml.

Для загрузки Docker-образа агента необходимо ввести команду:

$ docker load -i “solar-4rays-ti-feeds-agent.tar”

Для проверки того, что контейнер успешно загружен введите команду:

$ docker image list

Если в консоли появилась информация о контейнере solar-4rays/ti-feeds-agent, значит контейнер с агентом успешно загружен.

# Запуск и проверка функционирования

Для запуска агента необходимо перейти в директорию, в которой был распакован установочный комплект и ввести в командную команду:

$ docker-compose up

После запуска контейнера на консоль будет выводится служебная информация о работе агента. Для того, чтобы посмотреть результаты работы агента, необходимо зайти в поддиректорию work/data, находящуюся в директории из которой был запущен агент. Там размещаются файлы формата csv содержащие результаты работы агента. Если в файлы пишется информация о работе агента, то он функционирует правильно.

Для остановки агента нажмите сочетание клавиш Ctrl+C.