

Solar TI Feeds

Solar Threat Intelligence Feeds — сервис поставки потоков данных (фидов) об актуальных киберугрозах для усиления SOC и раннего обнаружения и реагирования

НАПОЛНЕНИЕ

Уникальные данные

Сведения от сенсоров в сети крупнейшего телеком-оператора «Ростелеком»

Экспертиза сервисов крупнейшего центра противодействия Solar JSOC

Результаты собственной киберразведки и 200+ расследований Solar 4RAYS

ЗНАНИЯ О ВРЕДОНОСНЫХ КАМПАНИЯХ 24/7

Более 3 лет ежедневно фиксируются и обрабатываются:

- 200+ млрд событий на сенсорах
- 3+ млн алертов
- 1+ млн действий хакеров

В результате проверки остаются сведения о самых опасных угрозах:

- Индикаторы компрометации (адреса, хеши)
- Сигнатуры в формате Suricata для обнаружения ВПО в сетевом трафике
- Правила детектирования атак (Sigma, YARA, ModSec)

ПРИЗНАКИ, ЧТО КОМПАНИИ НУЖНЫ ДАННЫЕ THREAT INTELLIGENCE

- 01 У компании есть собственный SOC, или она его строит
- 02 Необходимо улучшить качество детектирования угроз и повысить эффективность процессов
- 03 Используемые источники TI Feeds генерируют много нерелевантной информации и фолзов
- 04 SOC перегружен количеством обрабатываемых инцидентов, команда тратит слишком много времени на ручной анализ угроз и обогащение событий
- 05 Входит в число наиболее атакуемых отраслей: финансовый сектор, госсектор, ИТ, телеком, промышленность, нефтегазовый сектор

Наличие 2 и более признаков означает острую потребность в TI-данных.

Пилот Solar TI Feeds

30—60 дней

до 3 СЗИ

ЧТО ВХОДИТ

Несколько срезов данных

Промежуточный разбор срабатываний

До 3 сценариев* использования фидов

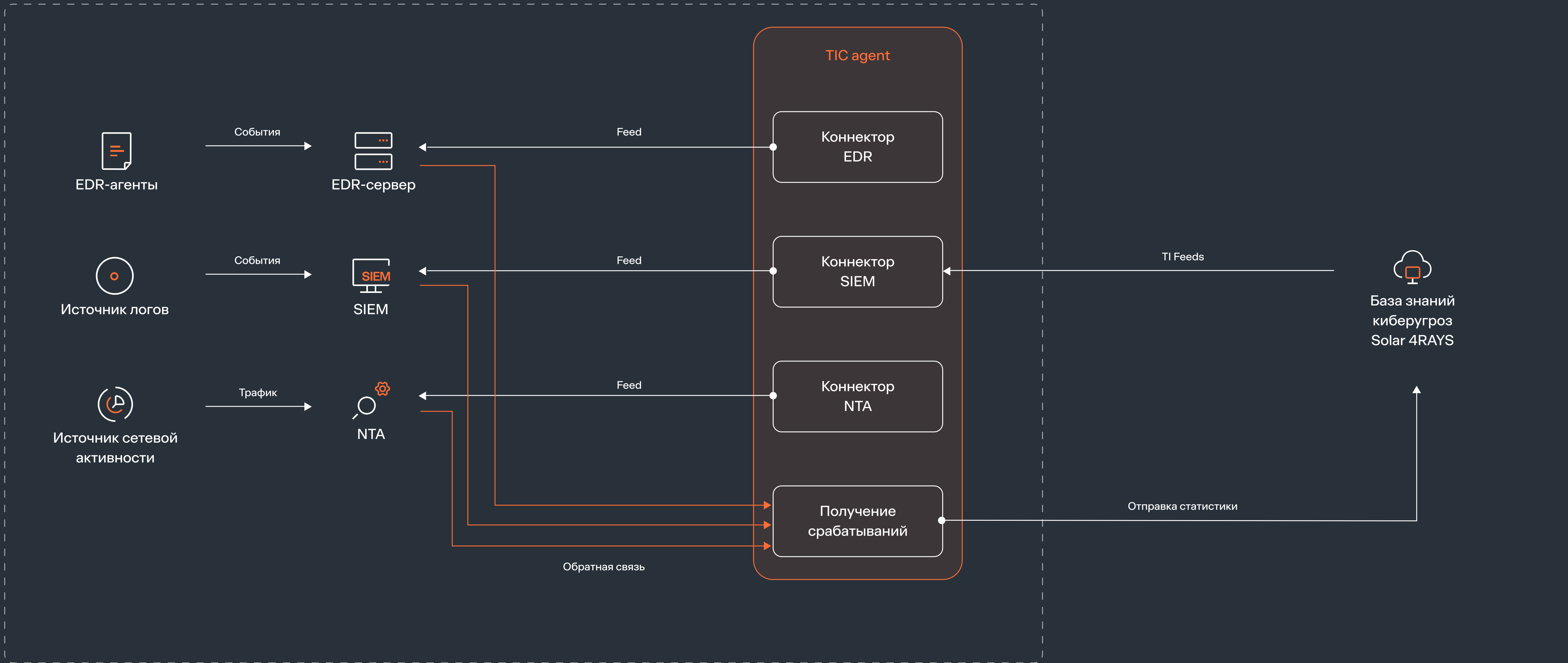


* Примеры сценариев

Определение критериев успеха

Отчет о результатах испытания

ПОДКЛЮЧЕНИЕ ОТ 2 ДНЕЙ



ИНТЕГРАЦИЯ СЕРВИСА ЧЕРЕЗ TI AGENT

- Легковесный Docker-образ, минимальные затраты на инфраструктуру
- Поддержка режима инициатора загрузки
- Настройка частоты запросов данных — от инкрементальных обновлений до полного актуального набора данных в моменте
- Любой формат данных: список, CSV, TSV, JSON; выгрузка всех или выборочных полей
- Поддержка передачи данных в Kafka



Готовые комплекты под ключевые сценарии



Сервис Solar TI Feeds
ГК «Солар»