CTT THREAT FEED

СБОР ИНДИКАТОРОВ КОМПРОМЕТАЦИИ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ

СБОР, ОБОГАЩЕНИЕ, ОЧИСТКА, РАНЖИРОВАНИЕ

Для эффективного предотвращения кибератак необходимо использовать актуальные знания о текущих угрозах.

Киберсообщество формирует обширную базу знаний об актуальных индикаторах компрометации. Десятки TI-отчетов, открытых постов исследователей в социальных сетях со всего мира содержат массу чрезвычайно ценной информации о киберугрозах. Но она не структурирована, не проверена, не готова к использованию.

Сервис CTT Threat Feed агрегирует эти данные из всех доступных открытых источников TI по всему миру, нормализует, фильтрует, обогащает и ранжирует каждый индикатор в соответствие с его опасностью и актуальностью.

CTT Threat Feed включает основные типы IoC: IP, DOMAIN, URL, HASH и предоставляет готовую интеграцию с наиболее распространенными средствами защиты, таких классов как: SIEM, SOAR, NGFW, TIP.

Ключевые возможности

- Сбор IoC из открытых источников
- Очистка индикаторов
- Обогащение контекстом
- Минимизация False Positive
- Определение уровня опасности и актуальности индикатора

Коротко о CTT Threat Feed

- Более 260 источников IoC
- Более 98 источников TI-отчетов
- Анализ соцсетей
- Анализ GitHub, Pastebin
- Анализ TI-отчетов
- Анализ Online-песочниц
- Интеграция со всеми популярными SIEM, SOAR, NGFW, TIP

ООО «ТЕХНОЛОГИИ КИБЕРУГРОЗ»

e-mail: info@cyberthreattech.ru

НАШИ КАНАЛЫ В TELEGRAM:
TI-отчеты: https://t.me/aptreports
TI-тренды: https://t.me/threatinteltrends