SOC
FORUM
2023

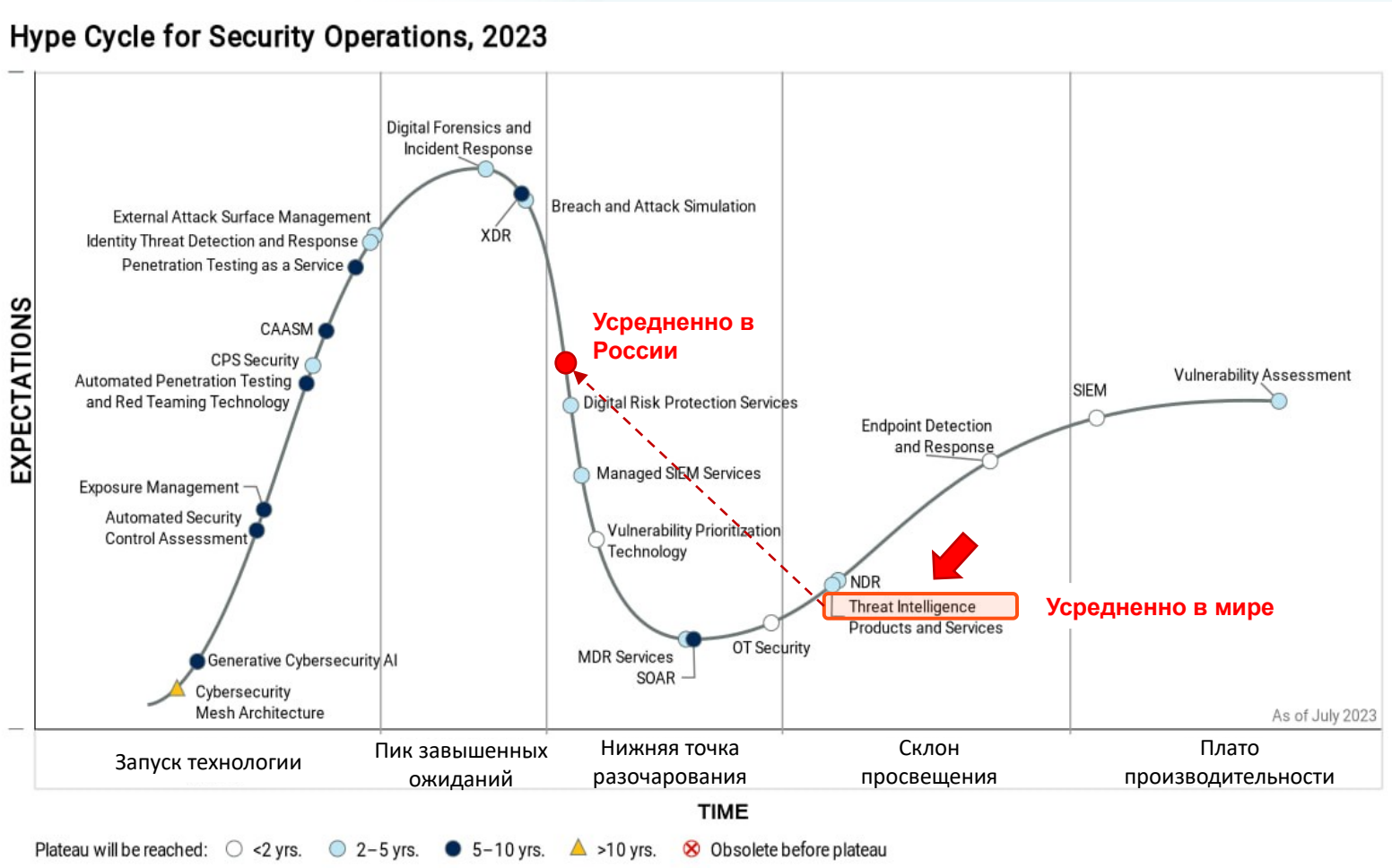
Открытые источники Threat Intelligence. Ожидания и реальность.

Николай Арефьев
Генеральный директор ООО "Технологии киберугроз" (бренд RST Cloud)

RST CLOUD
ТЕХНОЛОГИИ КИБЕРУГРОЗ

Понимание задач Threat Intelligence

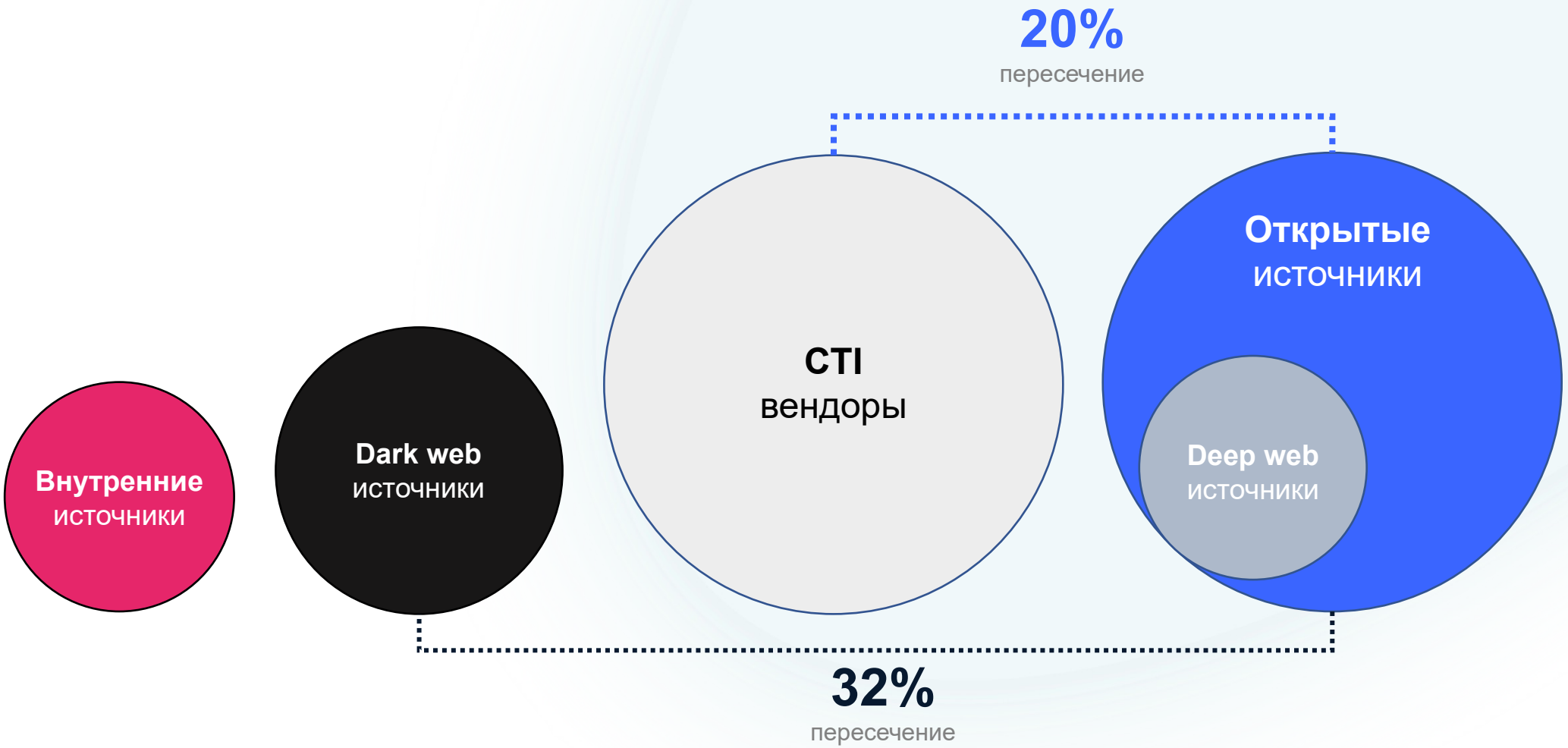
SOC FORUM 2023



Gartner

Источники Threat Intelligence

SOC FORUM 2023



Форматы данных в открытых источниках

SOC FORUM 2023

1. **Отчеты**
   - Неструктурированные (pdf, html)
   - STIX/MISP (json)

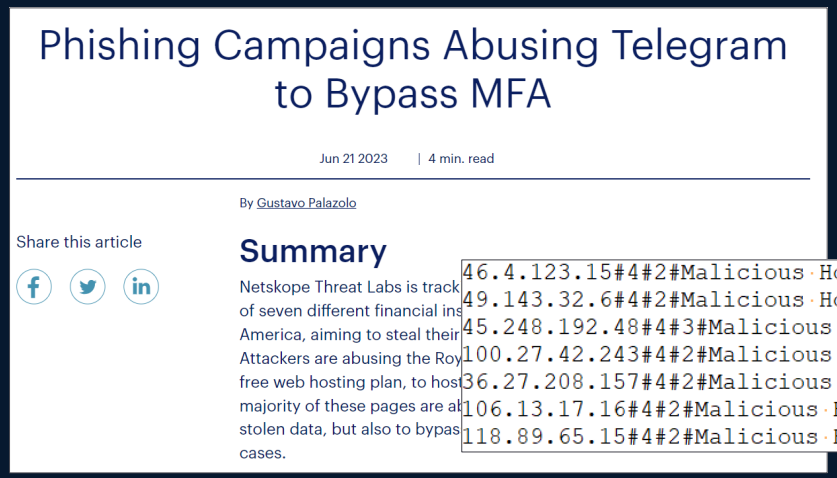
   Стратегический
   Операционный
   Тактический
   Технический

2. **Соцсети, репозитории**
   (txt, csv, json, html)
   - Twitter
   - Telegram

   Тактический
   Технический

3. **Песочницы** (csv, json, html)
4. **Фиды** (txt, c(t)sv, json, html)

   Технический


Phishing Campaigns Abusing Telegram to Bypass MFA

Jun 21 2023 | 4 min. read

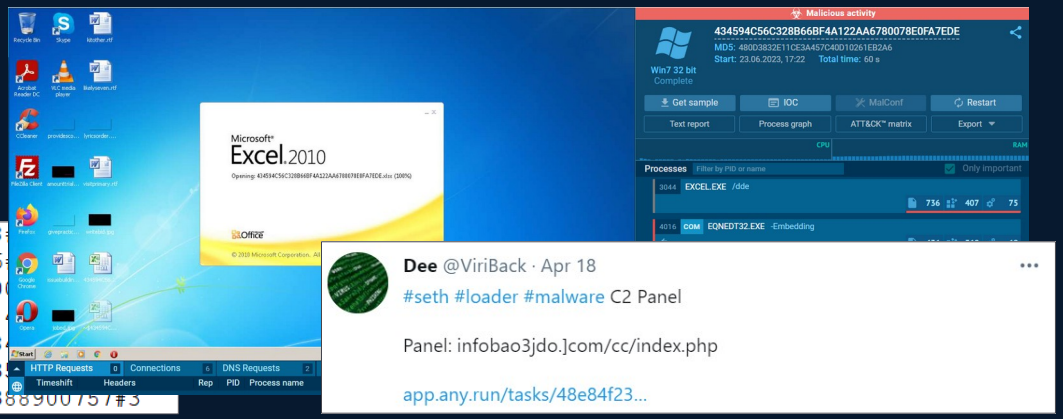
By Gustavo Palazolo

Share this article

Summary

Netskope Threat Labs is track
of seven different financial ins
America, aiming to steal their
Attackers are abusing the Roy
free web hosting plan, to host
majority of these pages are al
stolen data, but also to bypas
cases.


46.4.123.15#4#2#Malicious Host#DE##51.2993011475,9.49100017548
49.143.32.6#4#2#Malicious Host#KR##37.5111999512,126.974098206
45.248.192.48#4#3#Malicious Host#IN#Sikar#27.6166992188,75.150
100.27.42.243#4#2#Malicious Host#US#Ashburn#39.0480995178,-77.
36.27.208.157#4#2#Malicious Host#CN##30.2936000824,120.1613998
106.13.17.16#4#2#Malicious Host#CN##39.9289016724,116.388298035
118.89.65.15#4#2#Malicious Host#CN#Beijing#39.9287986755,116.38890075?#3



SOC FORUM 2023

Ожидание № 1

Там просто надо пару скриптов написать

С чем столкнемся в реальности
Ключевые проблемы

SOC FORUM 2023

Общие

- Множество источников в разных форматах.
- Часто нет контекста.
- Нет очистки индикаторов.

Отчеты

- Необходима ручная валидация результатов
- Индикаторы на скриншотах
- Сложность извлечения связей IoC
- IoC, которые не IoC

Соцсети

- Нельзя обойтись только регулярными выражениями, необходимо понимать, в какой части текста ожидать IoC
- Множественные способы экранирования (hxxp, p:, s:, [:], [.], \., \\, unicode)
- Синтаксические ошибки, ошибки в IoC

Фиды

- Вольное трактование форматов
- Поломанные форматы
- Ошибки в IoC

С чем столкнемся в реальности

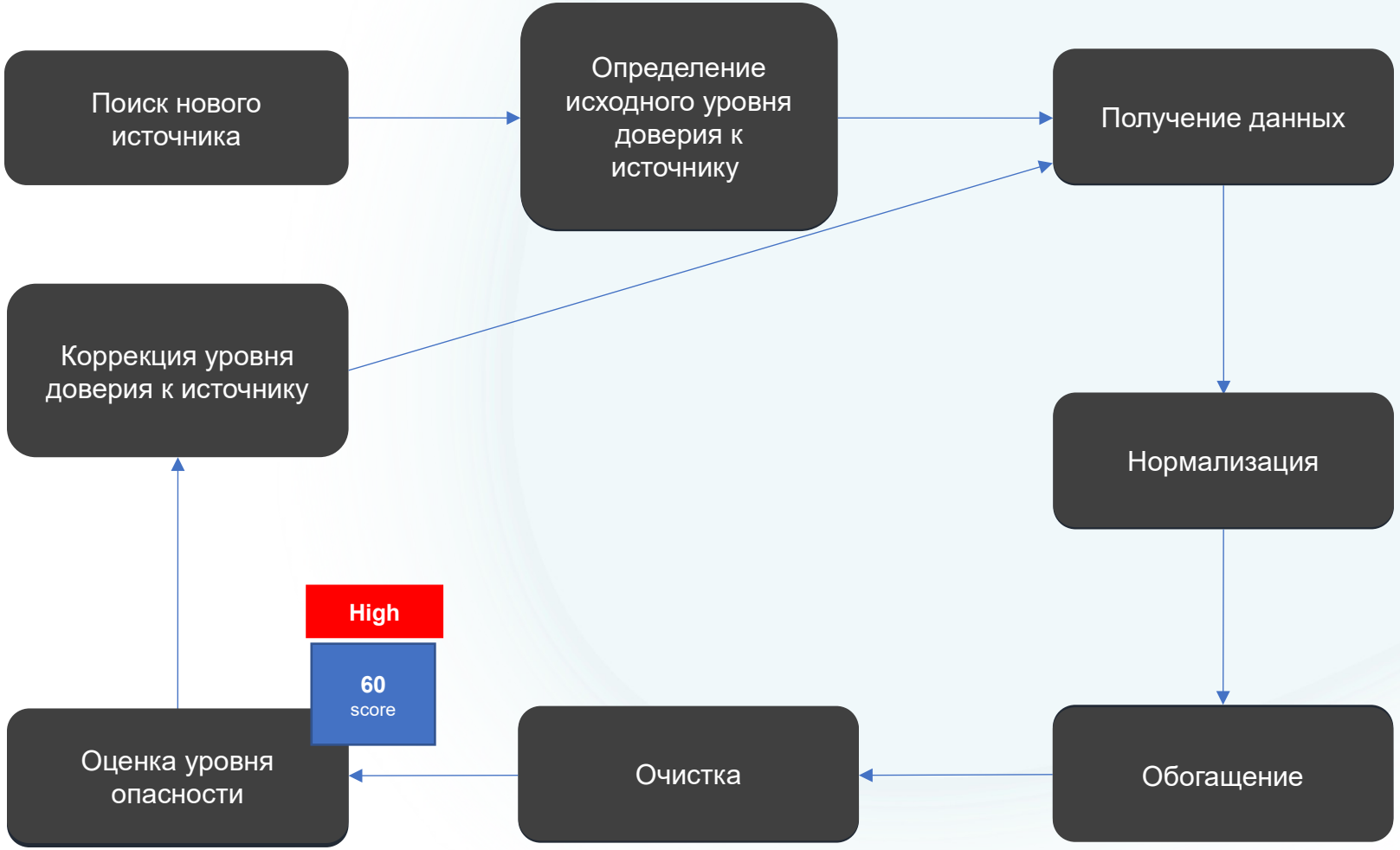
SOC FORUM 2023

1. **Необходимы:**
   - транспорты для источников;
   - свои парсеры для разных форматов;
   - механизмы обработки данных, учитывающие специфику источников.
2. **Это не пара скриптов.**
3. **Необходима поддержка созданных механизмов.**

Аналогия: Подключение новых источников к SIEM

Подход к решению

SOC FORUM 2023



SOC FORUM 2023

Ожидание № 2

Количество переходит в качество

С чем столкнемся в реальности
Количество индикаторов

SOC FORUM 2023

260
источников

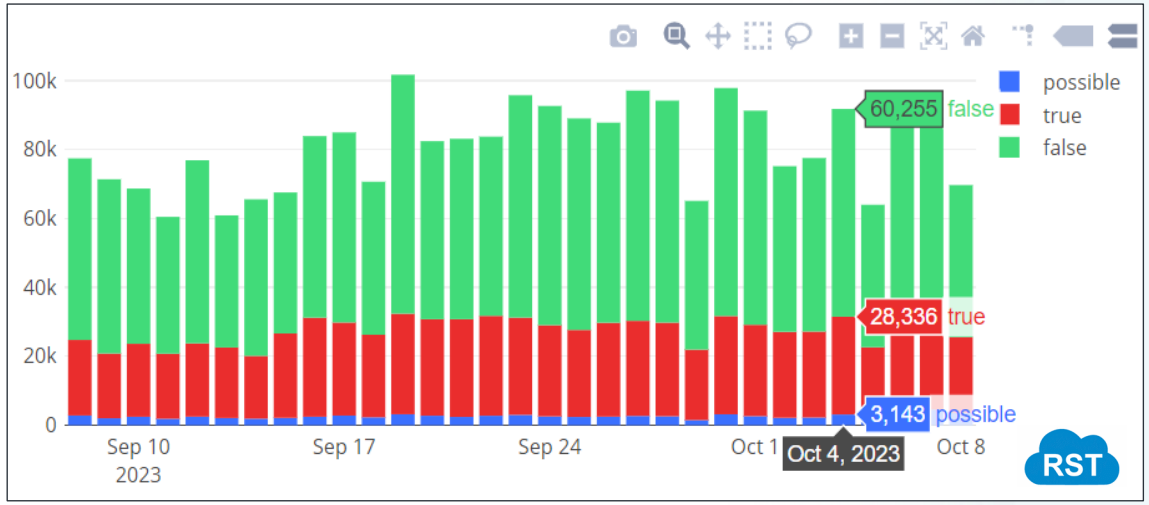
~10M
уникальных в год

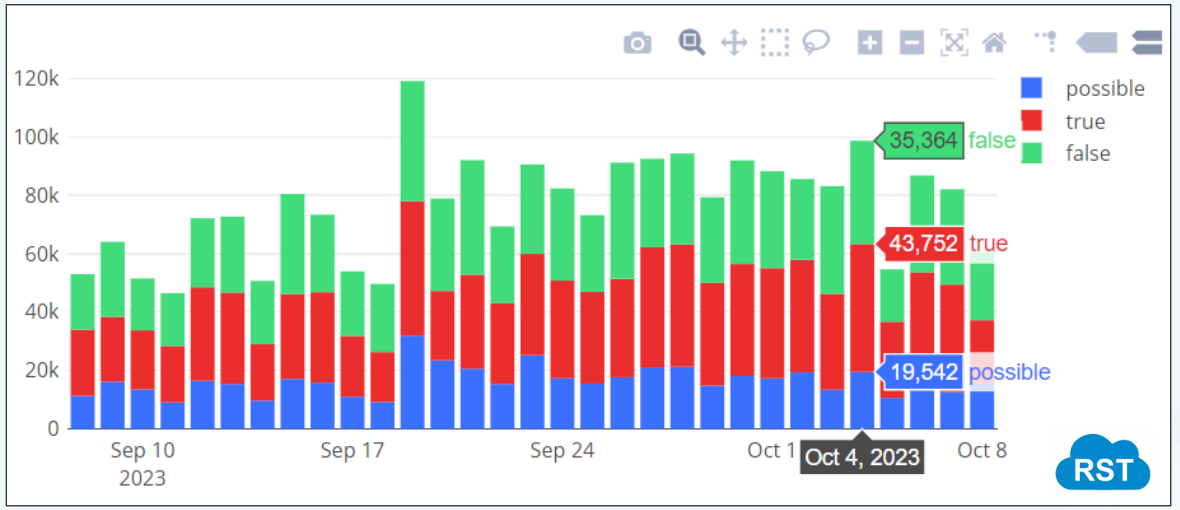
~200K
IOC в день

~120K
с атрибуцией

С чем столкнемся в реальности
False Positive

SOC FORUM 2023





IP

91K
всего в день

60K
очищенные

28K
False Positive

3K
потенциальный FP

34%
FP данных

Domain

98K
всего в день

35K
очищенные

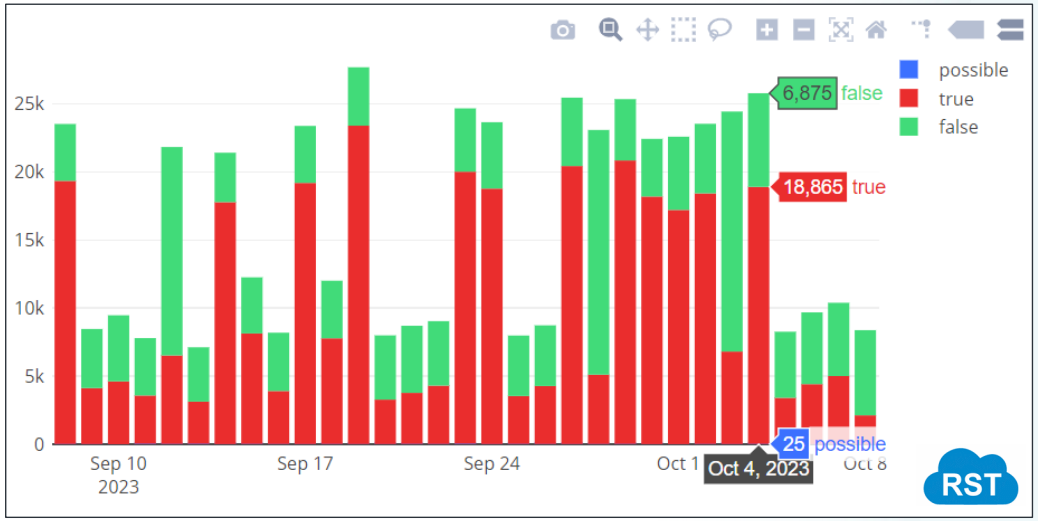
44K
False Positive

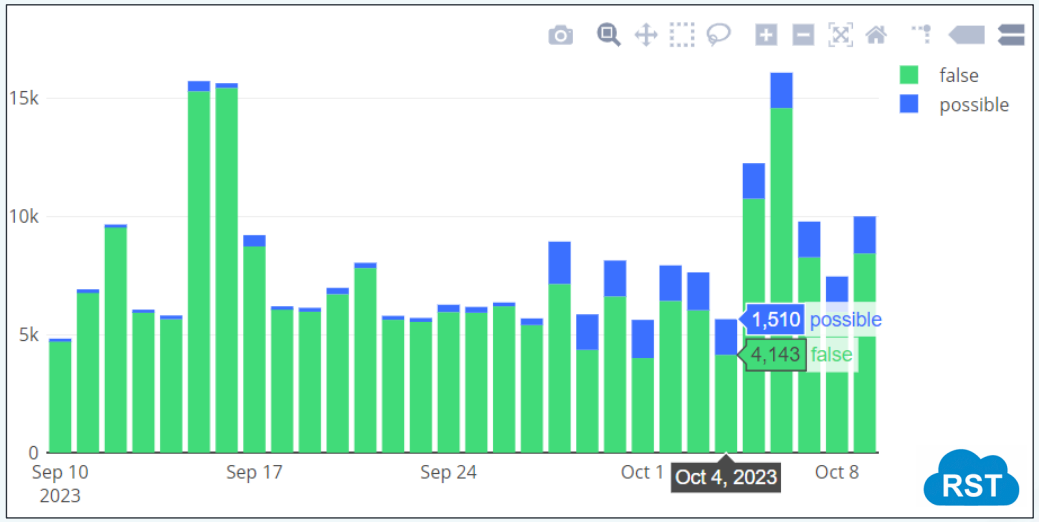
19K
потенциальный FP

64%
FP данных

С чем столкнемся в реальности
False Positive

SOC FORUM 2023





URL

26K
всего в день

7K
очищенные

19K
False Positive

25
потенциальный FP

73%
FP данных

Hash

5K
всего в день

4K
очищенные

0
False Positive

1K
потенциальный FP

20%
FP данных

Подход к решению

SOC FORUM 2023

1. Определить что мы будем считать исключением.
2. **Необходимы:**
   a) Движок для проверки исключений, поддерживающий:
      - полное совпадение;
      - вхождение в диапазон;
      - совпадение по подстроке;
      - проверку по списку из регулярных выражений.
   b) Списки исключений и процесс их пересмотра и обновления:
      - статические;
      - динамические.
        (IP Googlebot, hash системных файлов и т.д.)

SOC FORUM 2023

Ожидание № 3

Что-то многовато IoC и фолсят здорово, тогда мы будем работать только с TI-отчетами.

С чем столкнемся в реальности
Виды сообщений

SOC FORUM 2023

- Репост важных новостей.
- Новости о компании.
- Новости о продуктах компании.
- Новости о том, как продукт помогает решить проблему.

Сообщений

45 625 в год

~125 в день

- Заметки про анализ.
- Компактный отчет по анализу.
- Расширенный отчет по анализу.

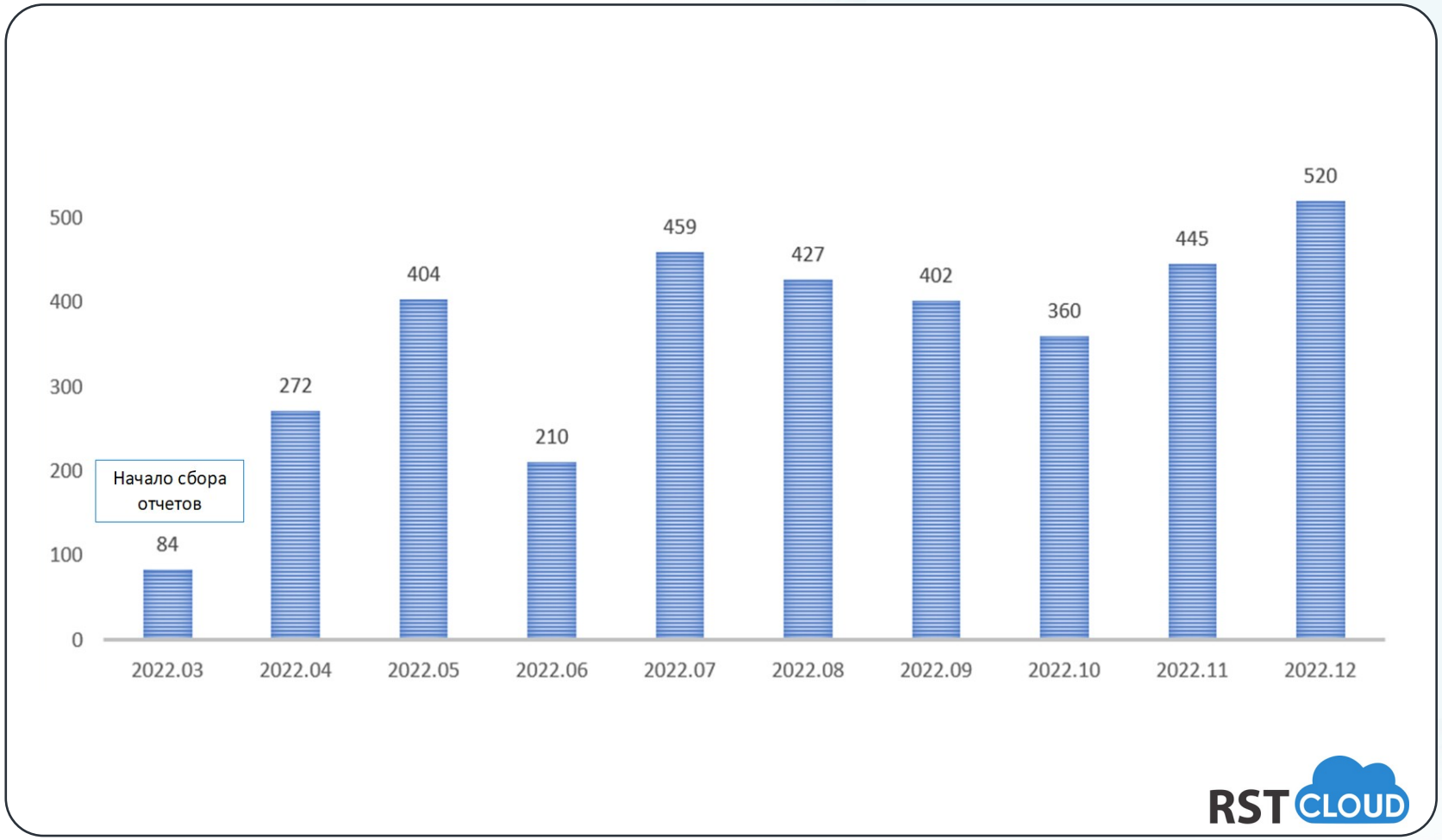
Операционный
Тактический
Технический

- Информационный бюллетень.
- Топ угроз.
- Статистика за период.
- Прогноз на следующий год.

Стратегический

С чем столкнемся в реальности
Количество отчетов

SOC FORUM 2023



Технический, Тактический, Операционный

3583 в год

~12 в день

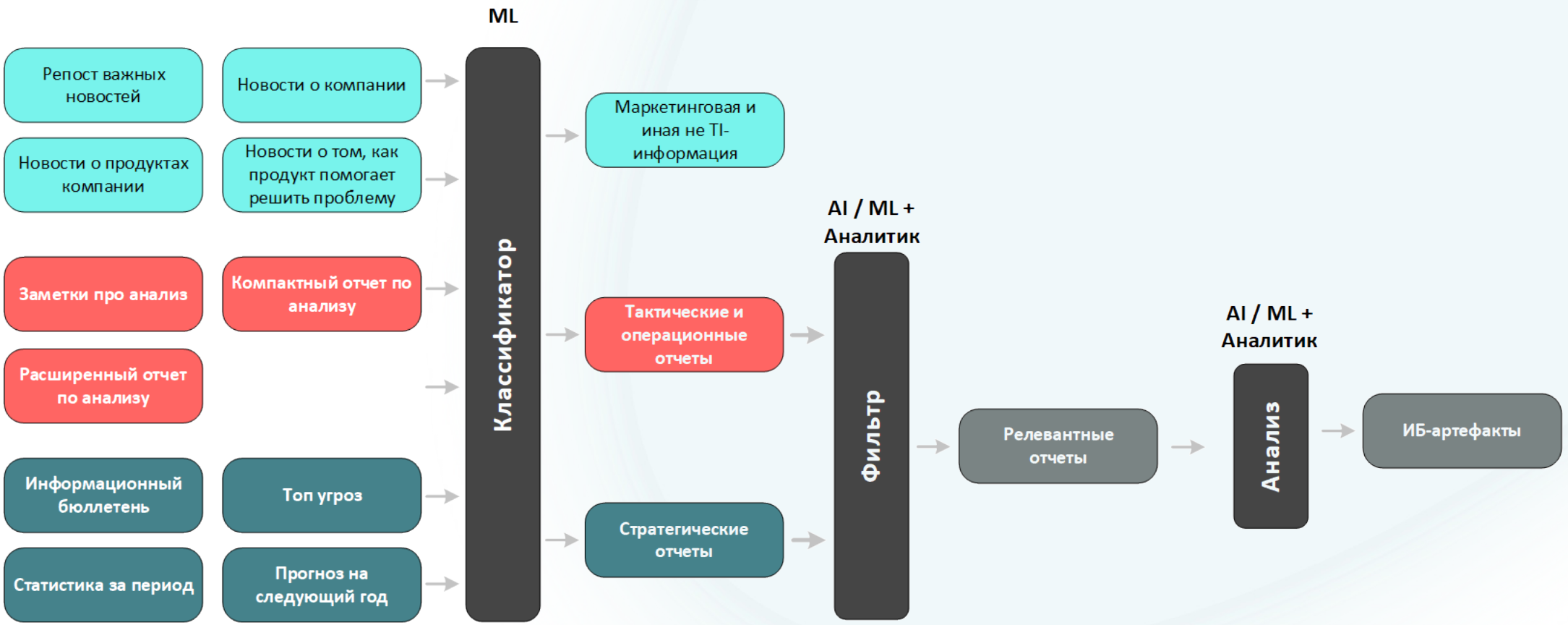
Стратегический

350 в год

~1 в день

Подход к решению

SOC FORUM 2023



SOC FORUM 2023

Ожидание № 4

Мы просто поставим бесплатную TIP.

С чем столкнемся в реальности

SOC FORUM 2023

1. Выбор очень небольшой: **MISP**, **OpenCTI**.
2. Малое количество источников "из коробки".
   ~30% от доступных в открытом доступе
3. Скудная поддержка TI-отчетов.
4. Сторонние интеграции с Online-песочницами, соцсетями.
5. Скудный список исключений.
6. Архитектурные проблемы:
   - **MISP**: умирает на 50-100К IOC в день.
   - **OpenCTI**: долгая загрузка IOC.
7. TIP многокомпонентная и каждая часть требует мониторинга и поддержки.

OPENCTI

Подход к решению

SOC FORUM 2023

Бесплатный TIP - хороший старт, но необходимо обеспечить:

1. Постоянное наполнения данными.
2. Дописывание собственных коннекторов.
3. Наполнение списков исключений.
4. Мониторинг.
5. Собственную поддержку.

   часто необходимы знания ЯП для доработки и устранения багов

Необходима небольшая команда с навыками разработки ПО.

SOC FORUM 2023

Ожидание № 4

У нас есть SIEM / NGFW / WAF, в них и загрузим IoC-и

С чем столкнемся в реальности

SOC FORUM 2023

1. Решение просто не умеют загружать в себя фид.
2. Надо купить отдельное решение для работы с TI.
3. TIP не поддерживает формат данных/протокол СЗИ.
4. В решение не поступают данные для работы с TI.

   пример: в SIEM не приходят логи с нужными полями
5. Нет структур для хранения всего контекста.

   есть только поле для индикатора
6. Нет механизма для обновления данных.

   можно только полностью перезагрузить список
7. Ограничение на кол-во записей.

   особенно для сетевых СЗИ
8. Отсутствие нормального логирования по тому сколько загрузилось, а сколько нет и в чем причины ошибок.

Подход к решению

SOC FORUM 2023

Необходимо заранее проверить, что СЗИ обладает рядом функциональных возможностей.

SIEM / SOAR

Списки

- Табличные, или Ключ-Значение
- TTL для записей
- UPSERT при вставке
- Персистентность
- Возможность хранить хотя бы 200К записей

Заполнение списков (или)

- Из событий
- Через API
- Ручное добавление/удаление записей

Работа со списками

- Чтение из правил корреляции/обогащения
- Работа из правил с несколькими списками одновременно.

Подход к решению

SOC FORUM 2023

Сетевые СЗИ

- Аутентификация при запросе списка индикаторов на внешнем ресурсе:
  - токен в кастомном HTTP-заголовке.
  - Base.
- Обновление списка индикаторов по расписанию.
- Политика блокировки и/или оповещения по сработке правил проверки IoC.

SOC FORUM 2023

Выводы

Открытые источники - это бесплатно, но дорого.

1. Желательно использовать в рамках TIP, либо придется написать свой.
2. У вас должна быть выделенная команда, занимающаяся TI.
3. В команде обязательно должно быть хотя бы пара человек, которые с ЯП на "ты".
4. У них должно быть время для сопровождения механизмов работы с открытыми источниками.
5. Можно переложить часть задач на поставщика TI.

SOC FORUM 2023

info@cyberthreattech.ru

RST CLOUD

ТЕХНОЛОГИИ КИБЕРУГРОЗ