БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Поддержание системы защиты в актуальном состоянии за счет эффективной работы с угрозами

Система защиты информации

Система защиты информации должна обеспечивать защиту от актуальных угроз.

Наиболее этапы работы с угрозами

Обмен опытом

Выявление актуальных угроз

Выявление применимых угроз

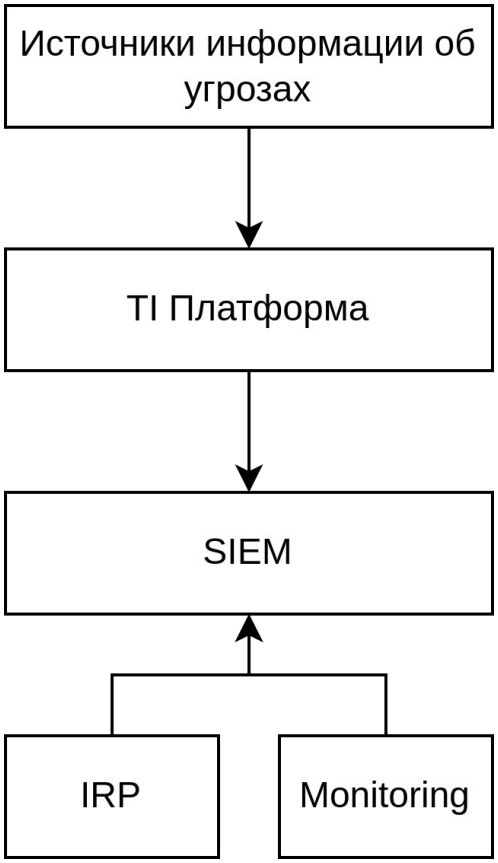
Работа с уязвимостями

Зачем важен обмен опытом

Отбили атаку и хорошо? А готовы ли вы к новой атаке?

Обязательно необходимо выяснить, кто атаковал и зачем.

Как обмениваться опытом



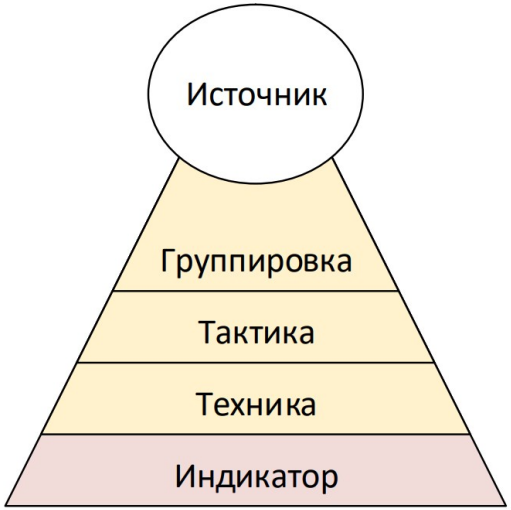
Много исследователей. Различные площадки. Различные форматы

Единая платформа. Единый формат. Данные проходят предварительную очистку и проверку

Выявление индикаторов. Обогащение входящих соединений

Решение 2 задач:
1. Выявление индикаторов компрометации
2. Выявление связанных угроз и техник во внешних коммуникациях

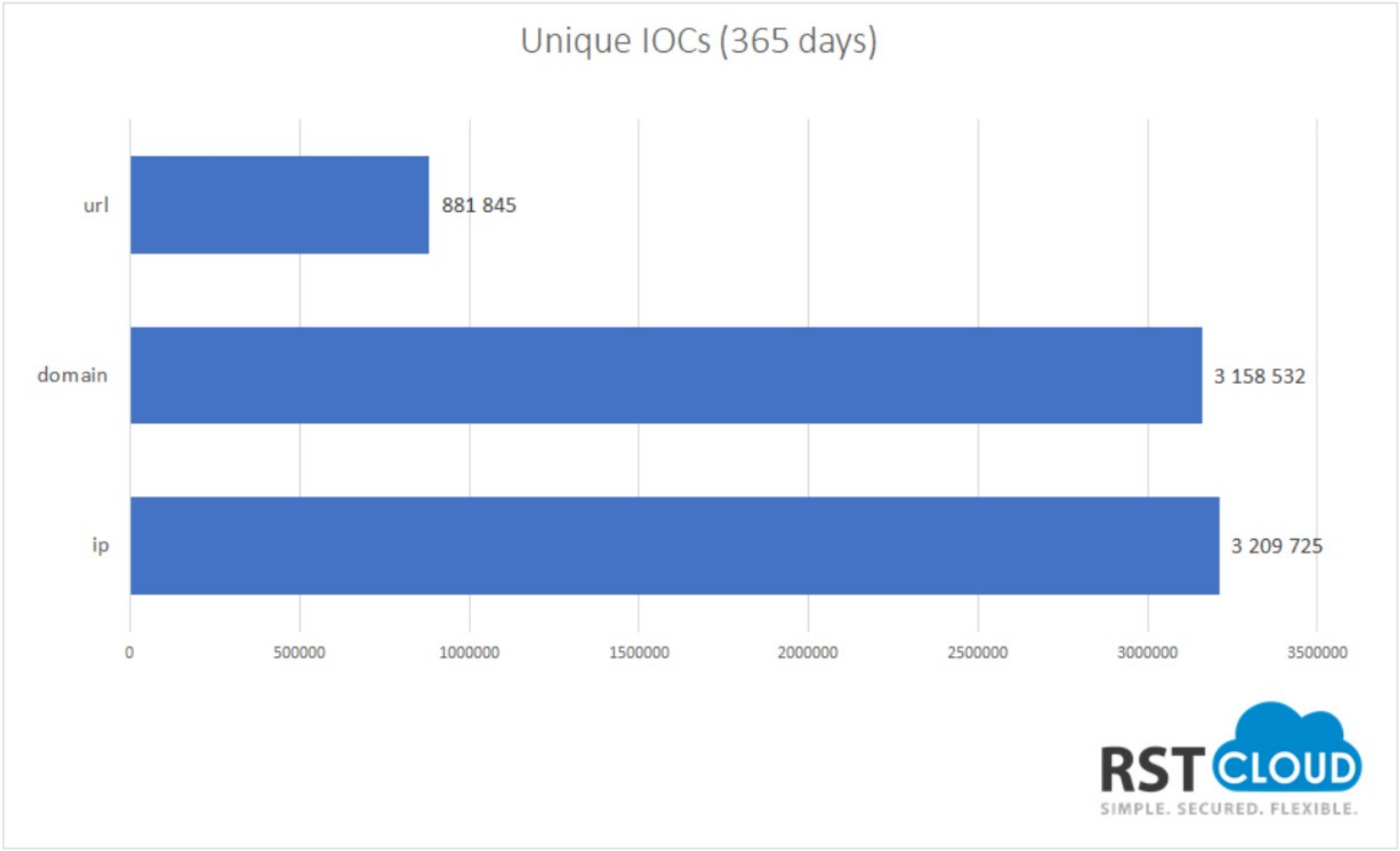
Как обмениваться опытом. Атрибуция



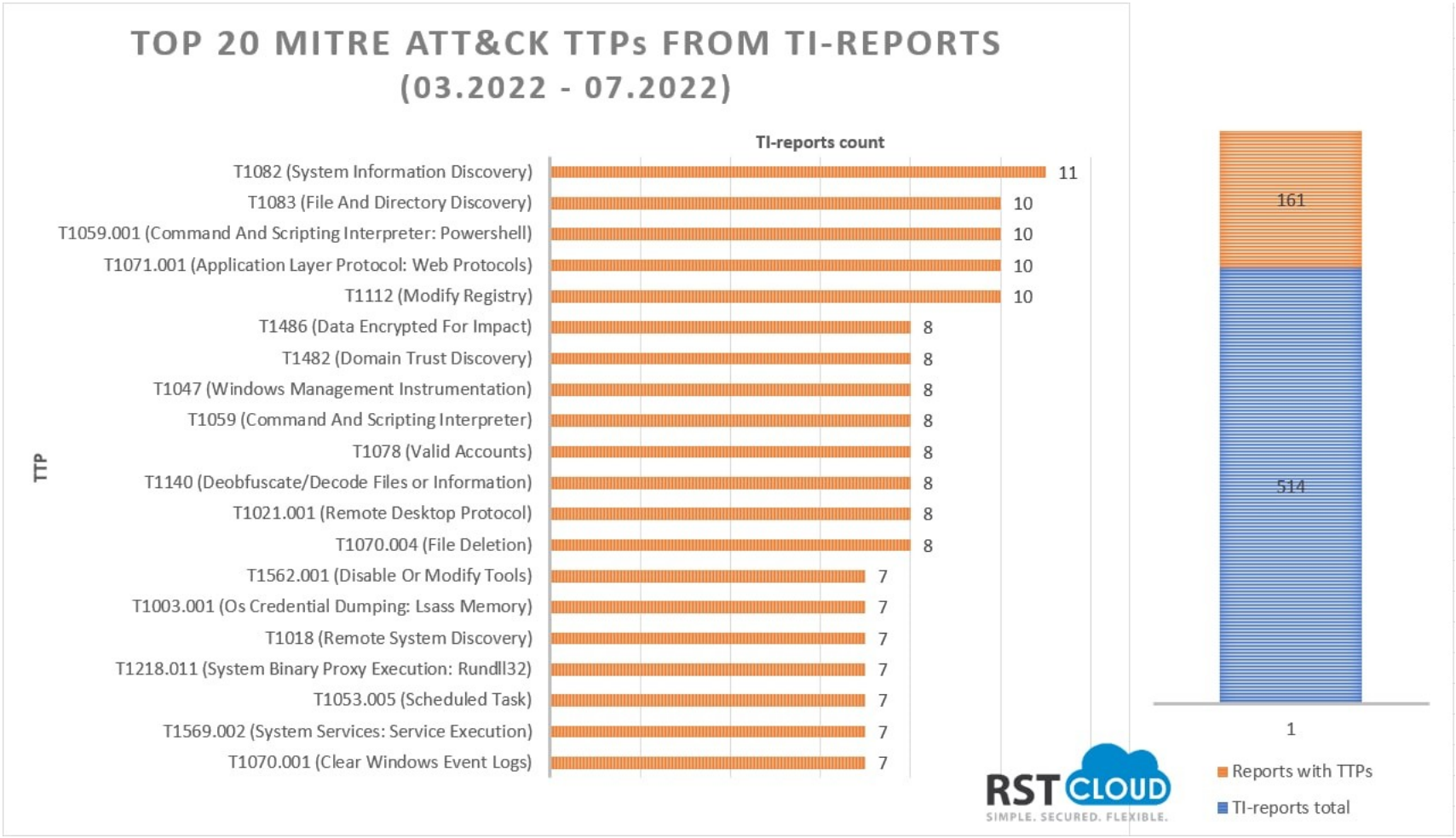
Контекст — дополнительная информация для анализа индикаторов компрометации, которая позволяет ответить на вопросы, кто как и зачем использовал какую-то технику, на которую указывает данный индикатор.

Индикатор компрометации — базовый технический признак атаки. Например, IP-адрес, с которого была зафиксирована рассылка управляющих команд в ботнет-сеть, или хешсумма файла вируса-вымогателя.

Как обмениваться опытом. Статистика

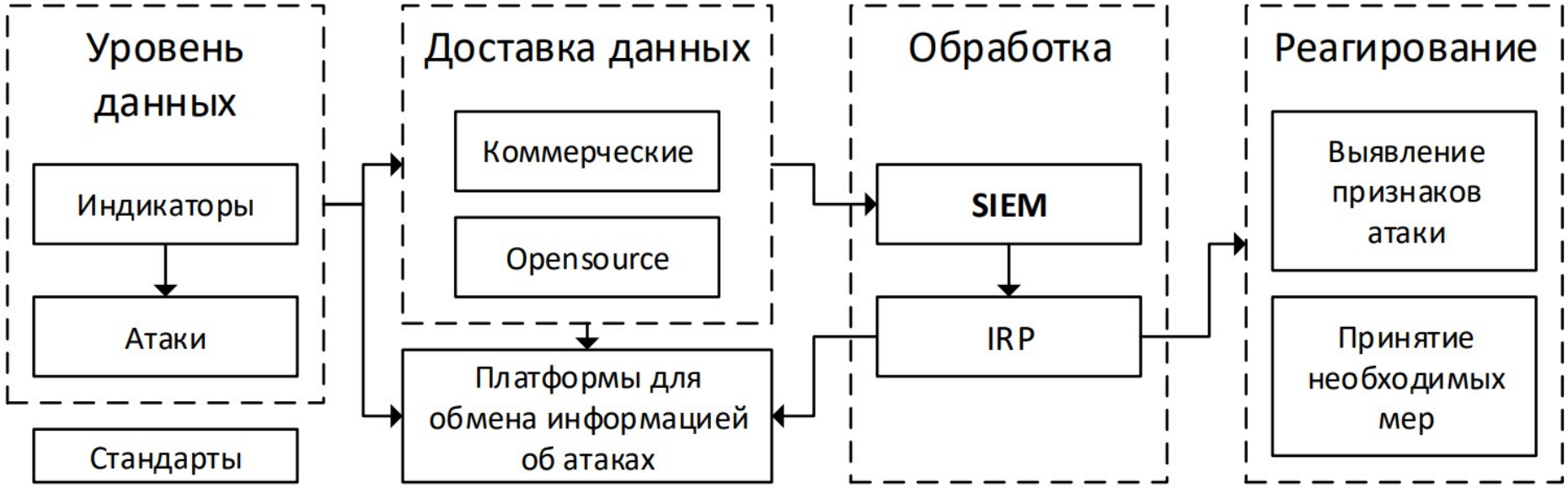


Как обмениваться опытом. Статистика



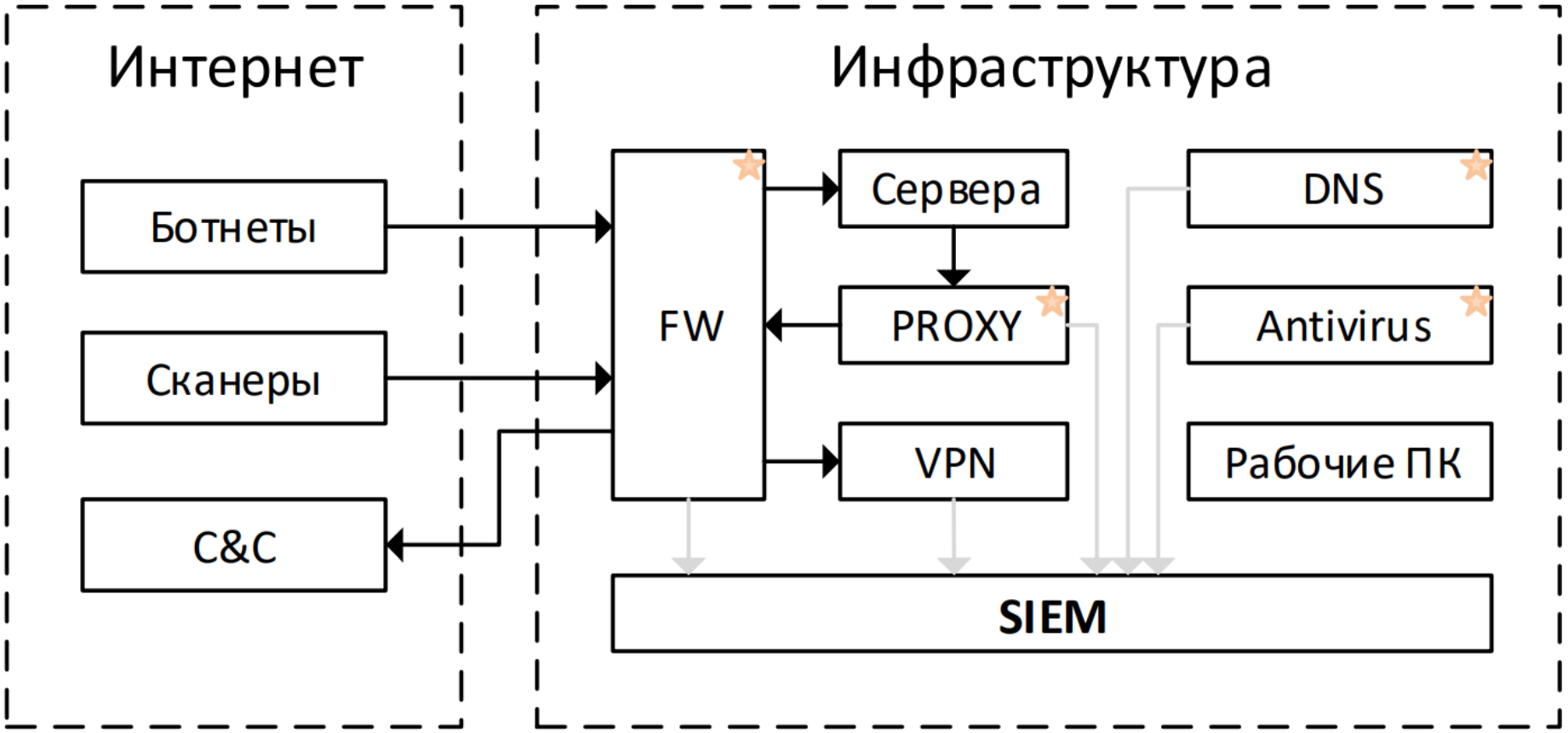
Выявление актуальных угроз. Подготовка

Загрузка информации об актуальных угрозах



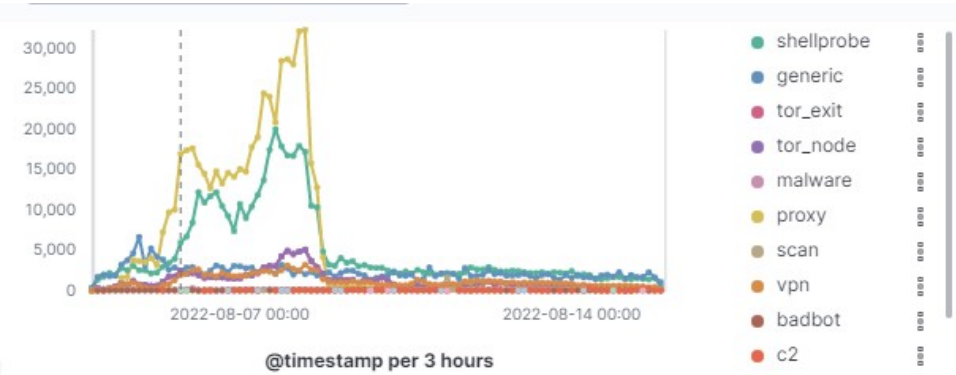
Выявление актуальных угроз. Подготовка

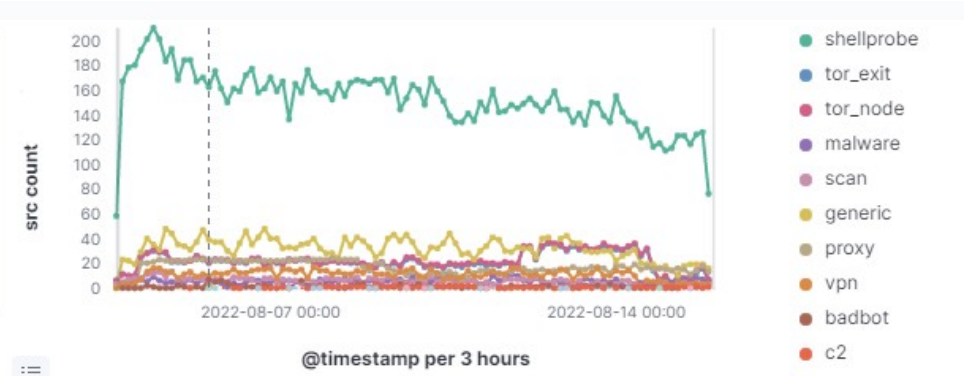
Настройка обогащения данных в SIEM

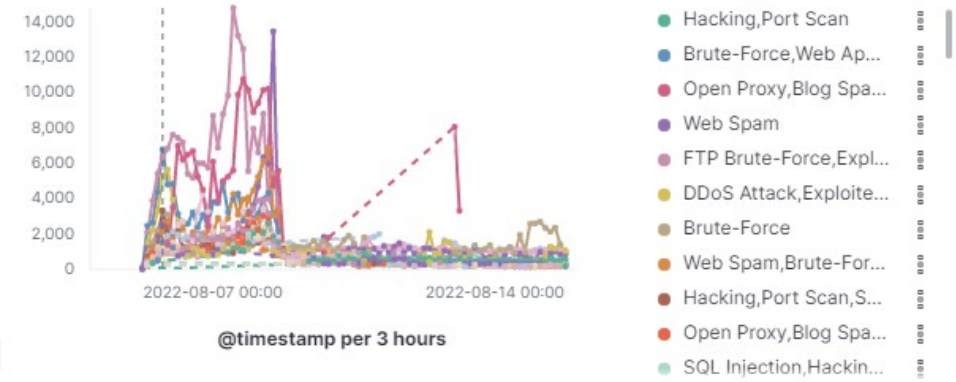


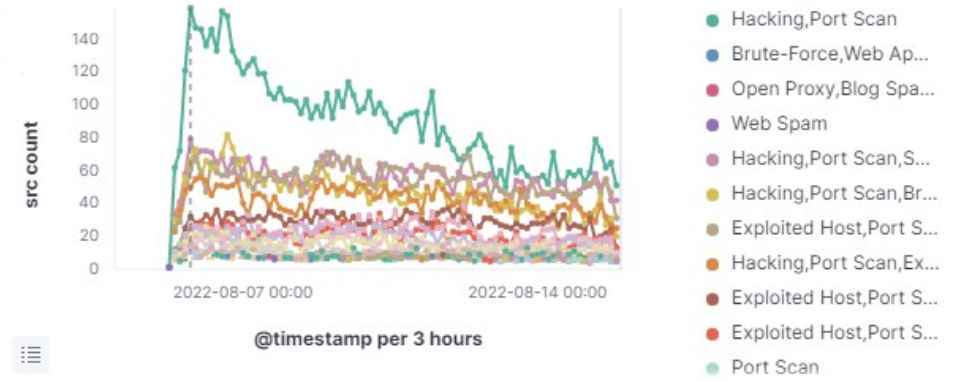
Выявление актуальных угроз

Покрытие атакующих узлов — примерно 10%



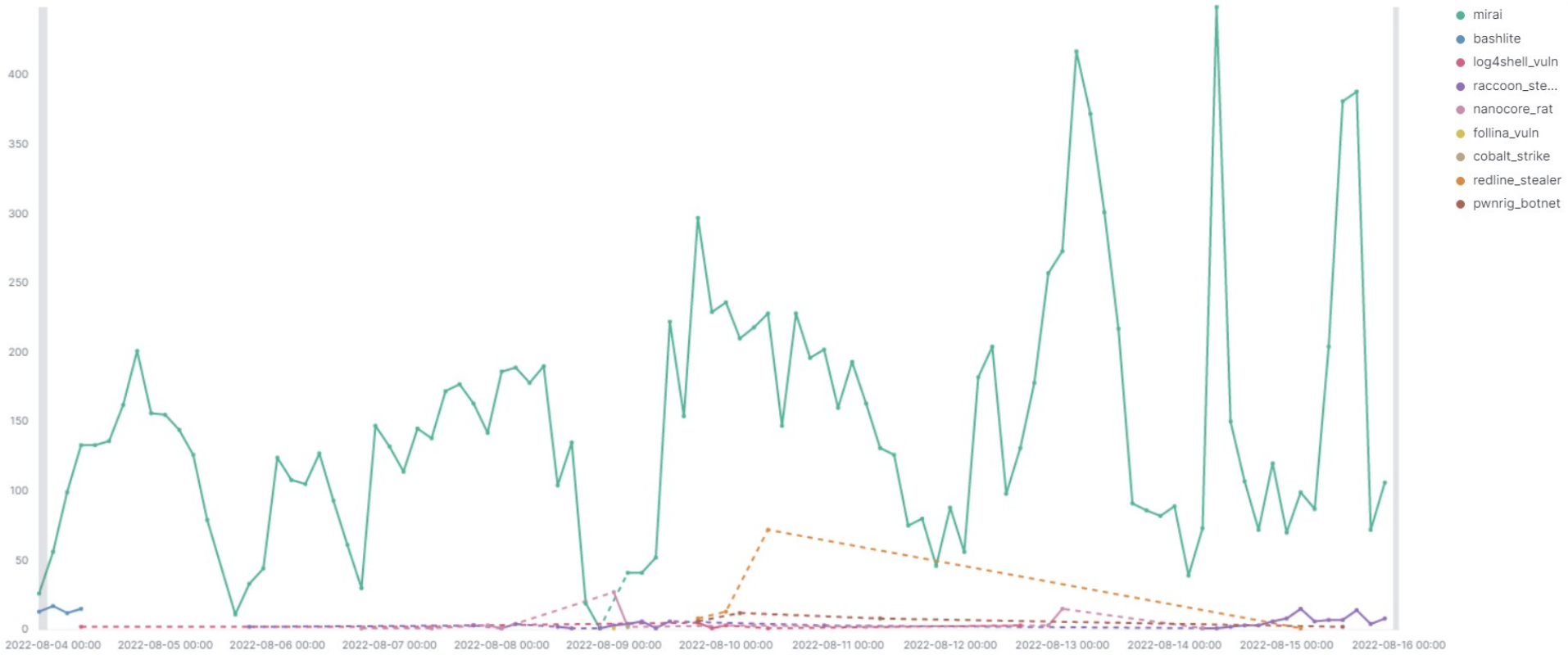






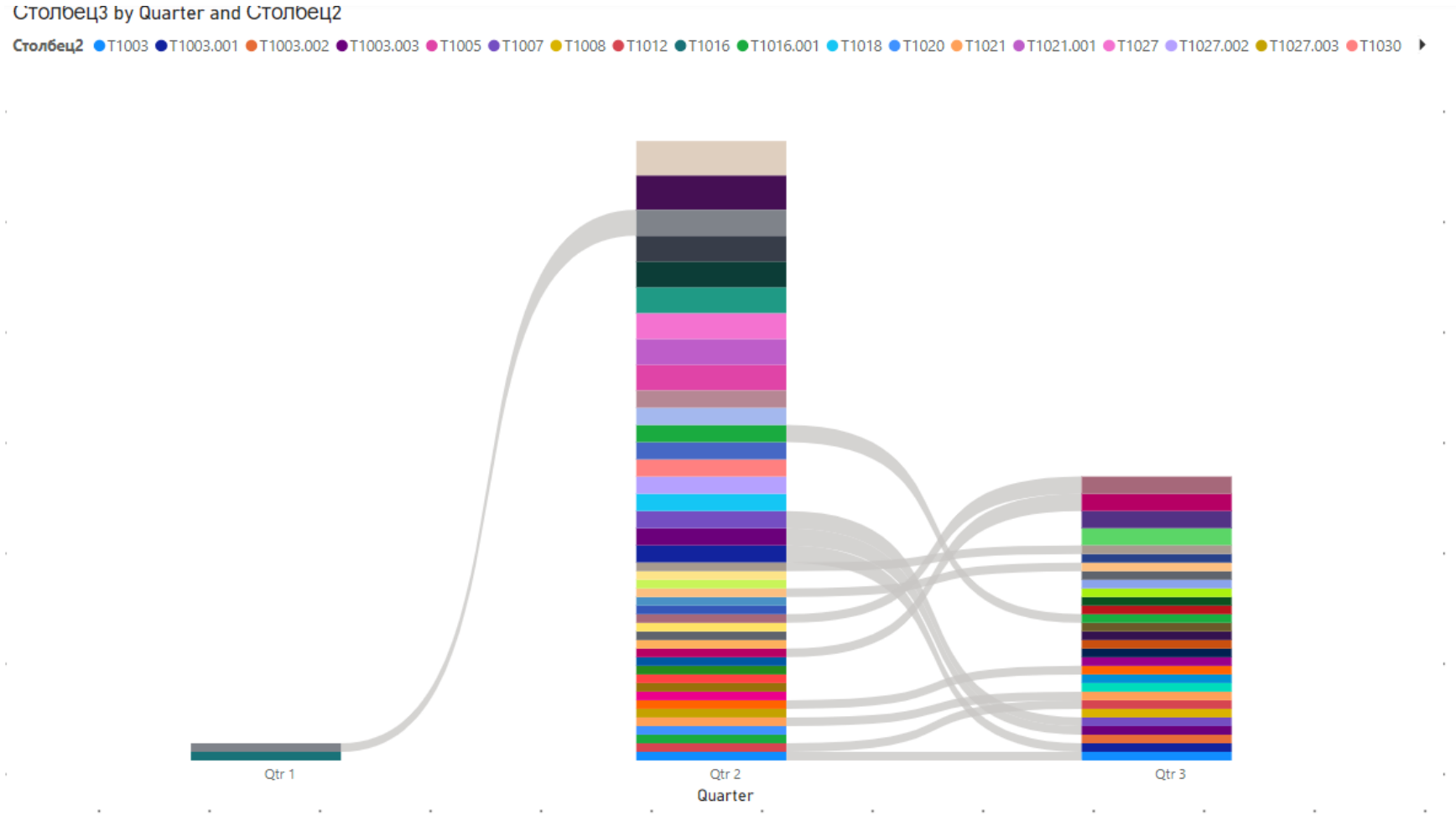
Выявление актуальных угроз

Если верить данным, на наибольшую угрозу представляют остатки mirai



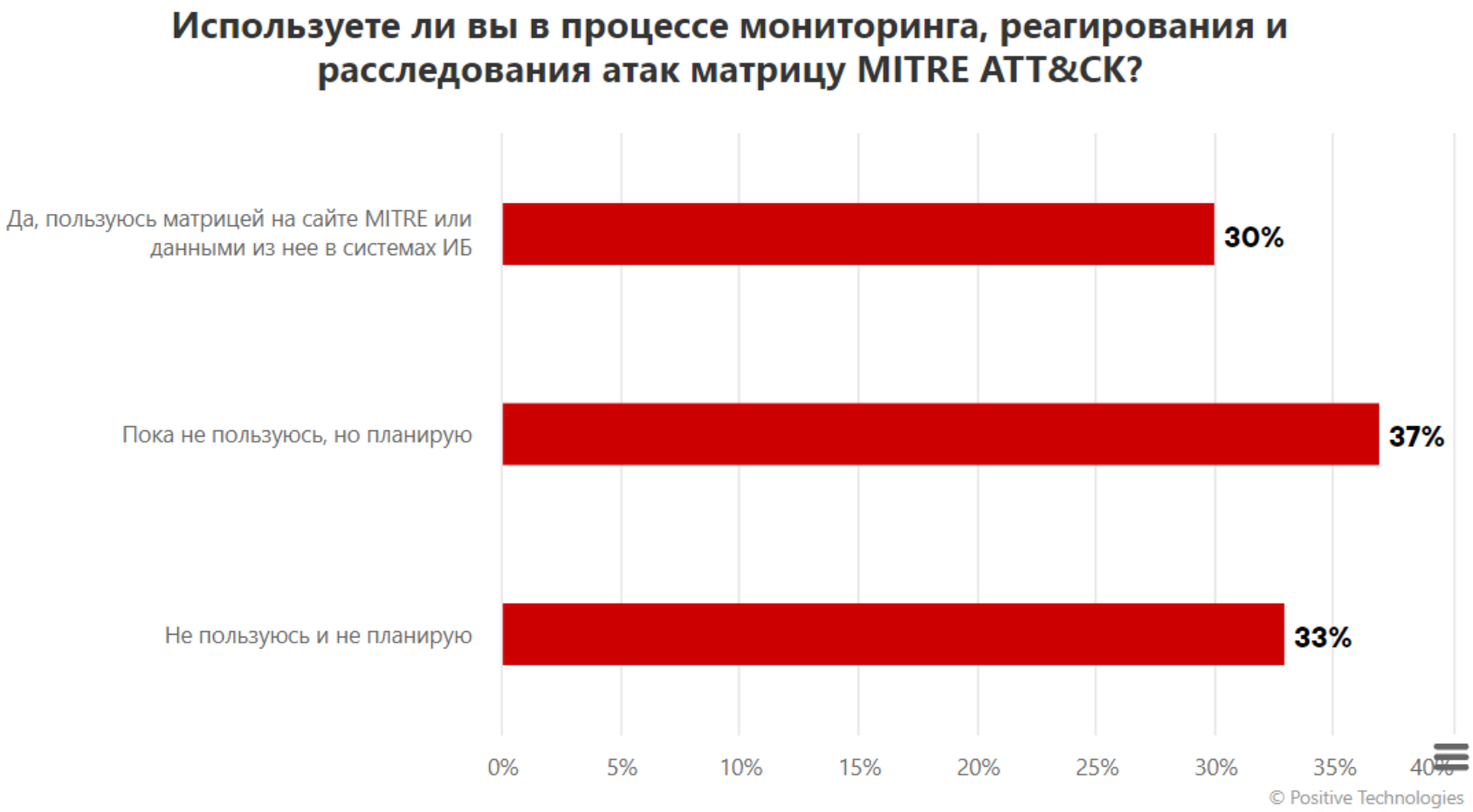
Выявление актуальных угроз

Динамика распределения техник по кварталам (данные RST-Cloud)



БАНК САНКТ-ПЕТЕРБУРГ

Выявление актуальных угроз

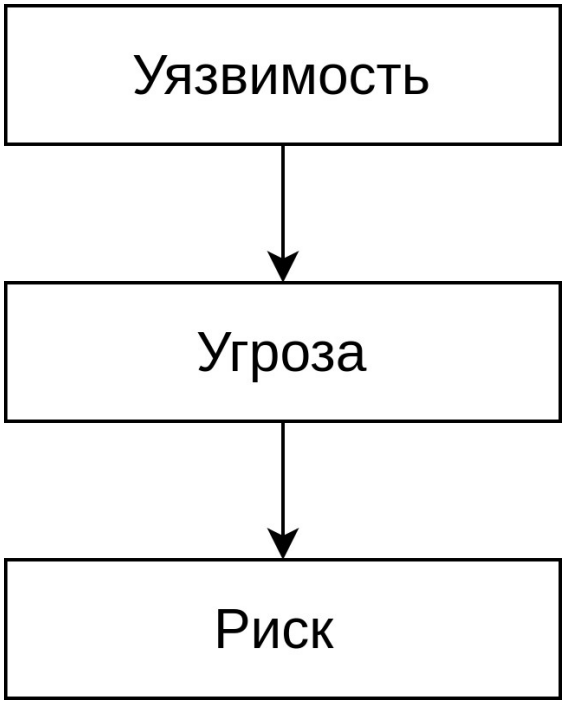


Выявление применимых угроз

Выявление признаков свершившихся угроз через связь «Инцидент-угроза»

Выявление угроз, которые актуальны для инфраструктуры компании (Пентест)

Работа с уязвимостями



Процесс зрелый, но существует большой потенциал и определении угроз, связанных с уязвимостью.

Что делать с угрозами

Выявление актуальных угроз

Оценка рисков

План минимизации рисков

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!