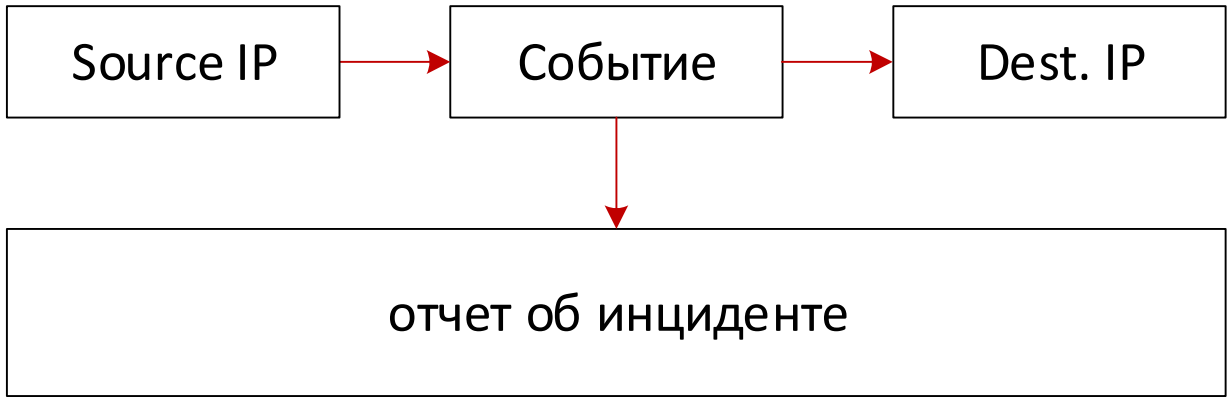
Источники контекста о внешних атаках или как понять, кто и зачем атакует ваши публичные сервисы

БЕЛЯКОВ ИГОРЬ

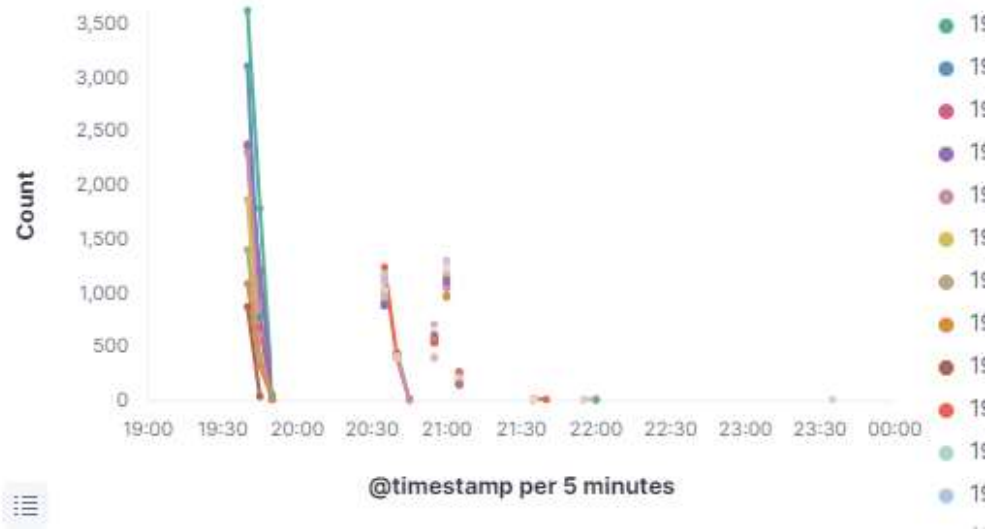
Что мы знаем об источнике угрозы?



Проблема: угрозы и инциденты часто анализируются в отрыве от других событий и контекста

Как обосновать бюджет?

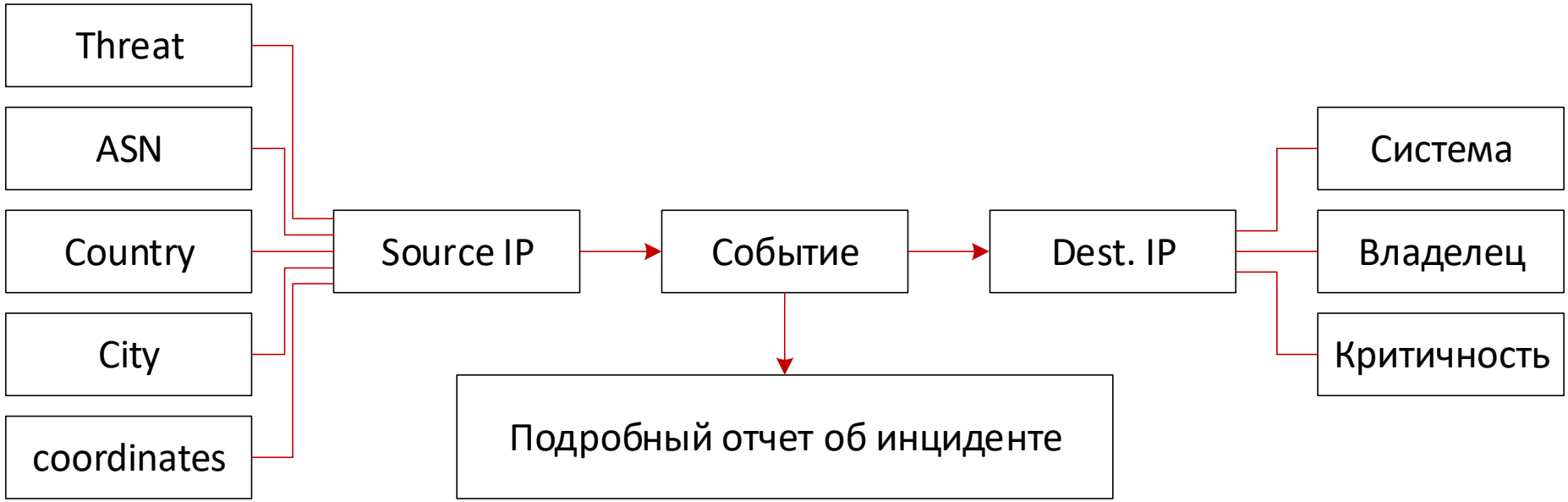
Пример атаки



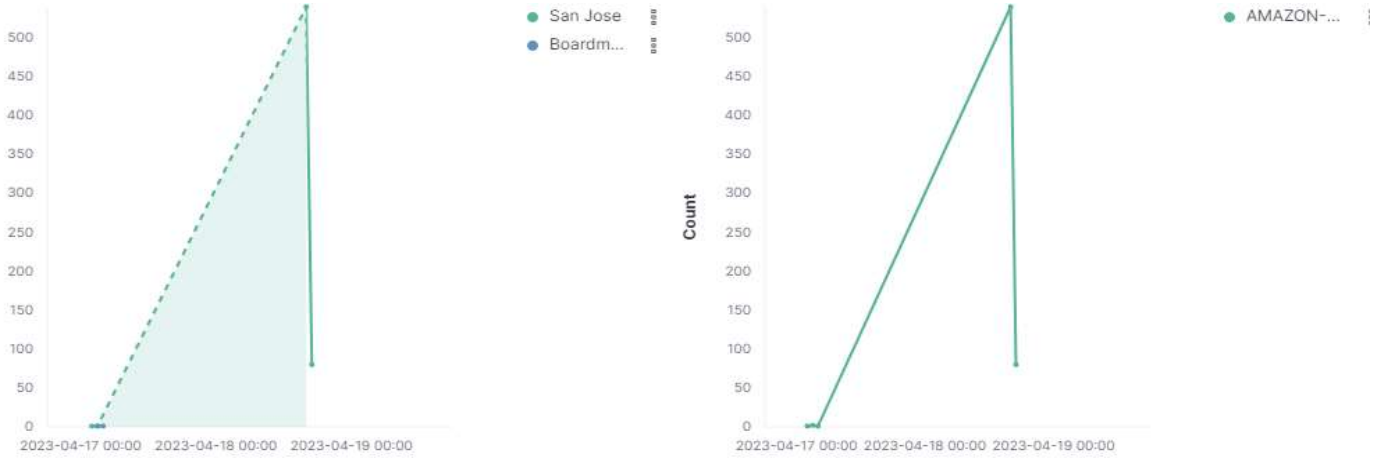
Что нам скажет IDS

Type	Name	Count	SRC	DST
IPS	Nmap Scripting Engine Scanner Over HTTP Request	24	1	15

Что мы можем узнать об источнике угрозы?

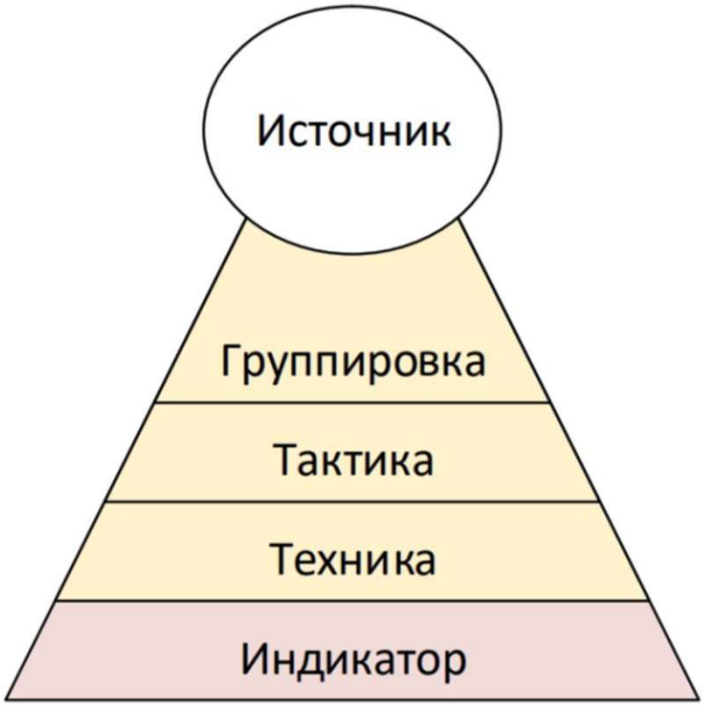


Что нам скажет база ASN



1. Кто владеет ресурсами, с которых осуществляется атака.
2. Какие еще адреса из данной подсети участвуют в атаке?
3. Есть ли аномалия по стране или городу?

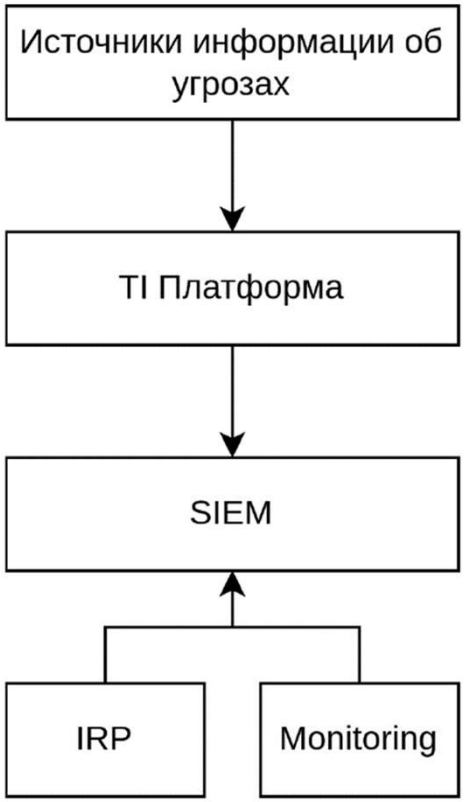
threat intelligence



Контекст — дополнительная информация для анализа индикаторов компрометации, которая позволяет ответить на вопросы, кто, как и зачем использовал угрозу, 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 хеш-сумма файла вируса-вымогателя.

threat intelligence

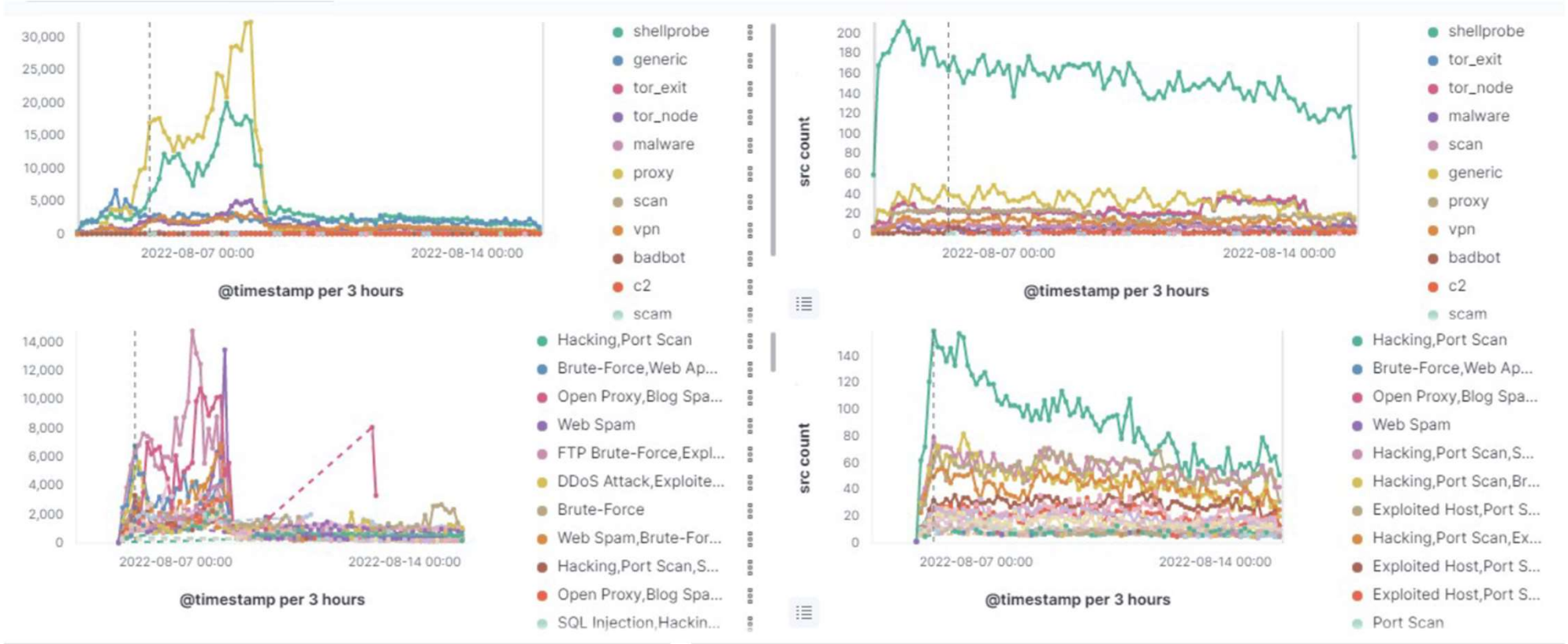


Много исследователей. Различные площадки. Различные форматы. Объемные отчеты об атаках

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

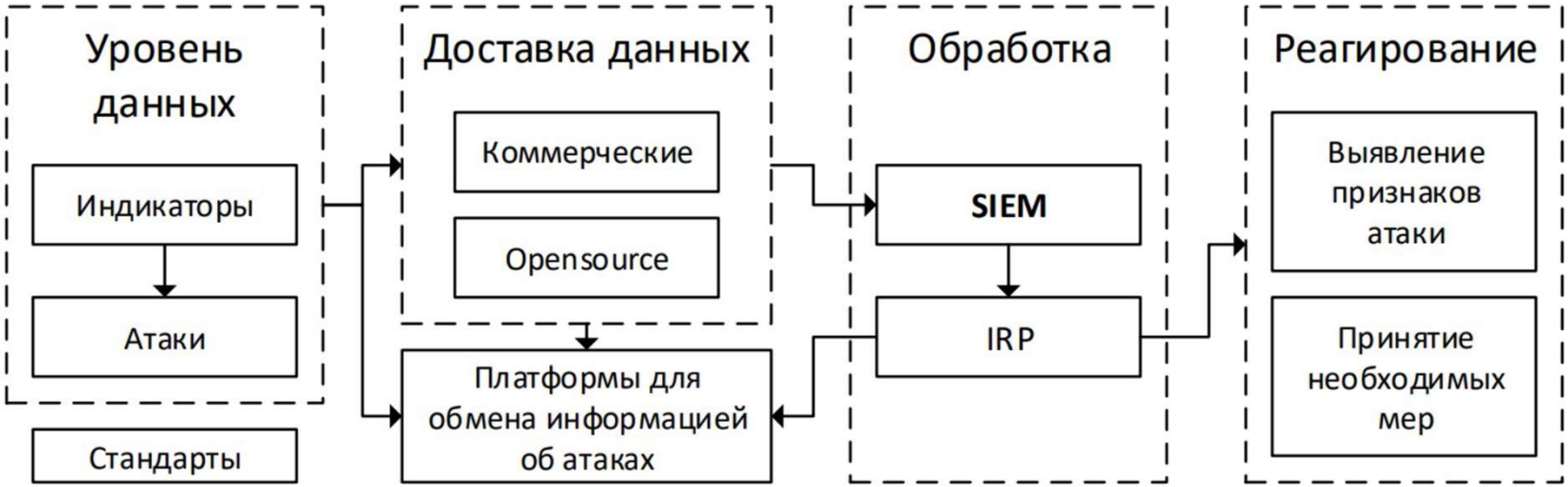
Выявление индикаторов. Обогащение входящих соединений
Решение 2 задач:
1. Выявление индикаторов компрометации
2. Выявление связанных угроз и техник во внешних коммуникациях

Что нам скажет TI

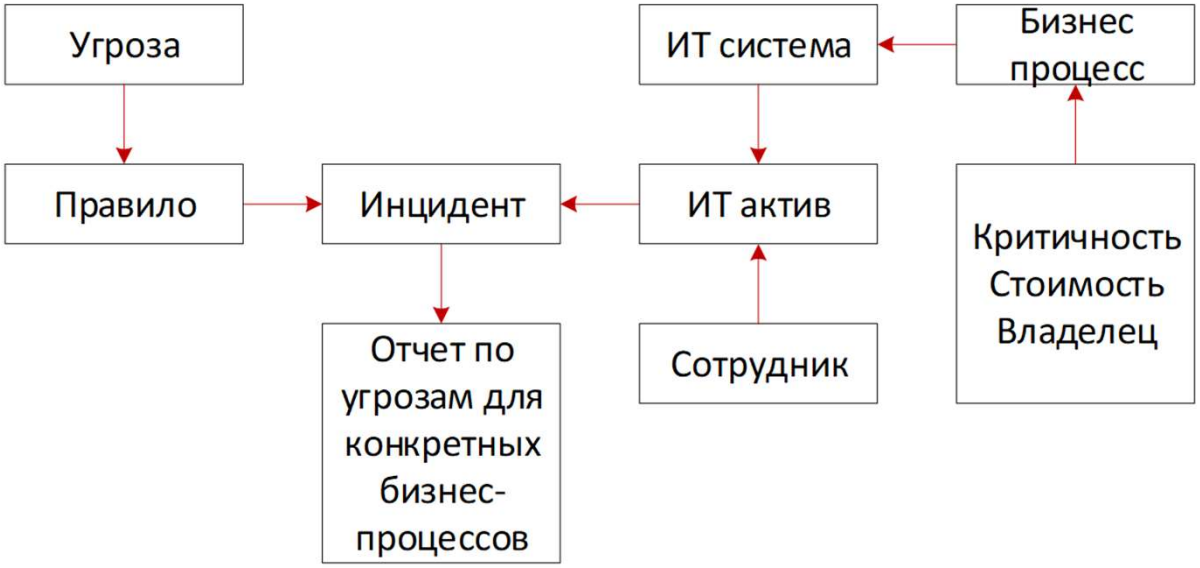


Как подключить TI

Загрузка информации об актуальных угрозах



CMDB, зачем атакуют ресурс?



В итоге получаем список угроз признаки которых были замечены в ИТ активах, реализующих конкретные бизнес процессы

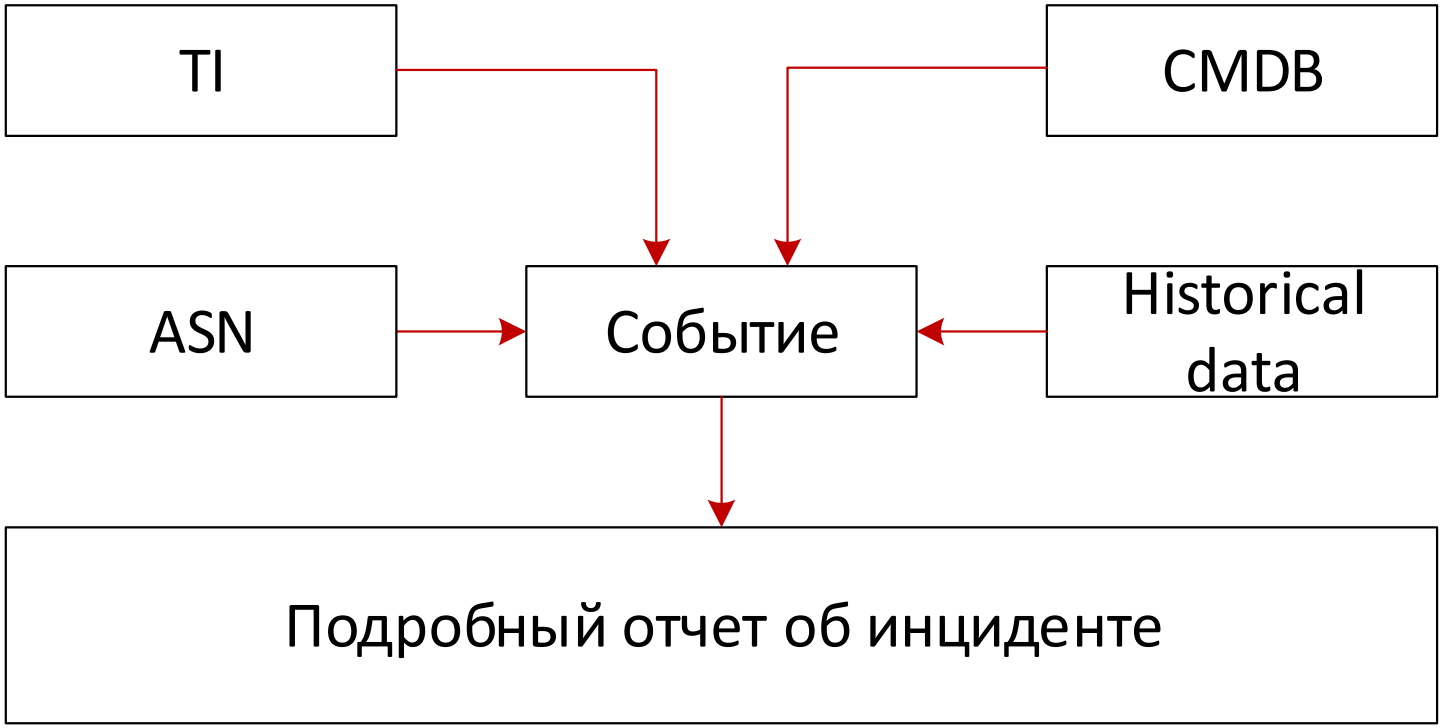
Пример обычного инцидента

Сообщение об инциденте
Дата и время: 18 апреля 2023
Категория: Внешняя атака
Название: Сканирование ресурсов
Описание: Сканером Nmap просканировано
Критичность: Средняя
Источник: фаерволл

Чем дополнить

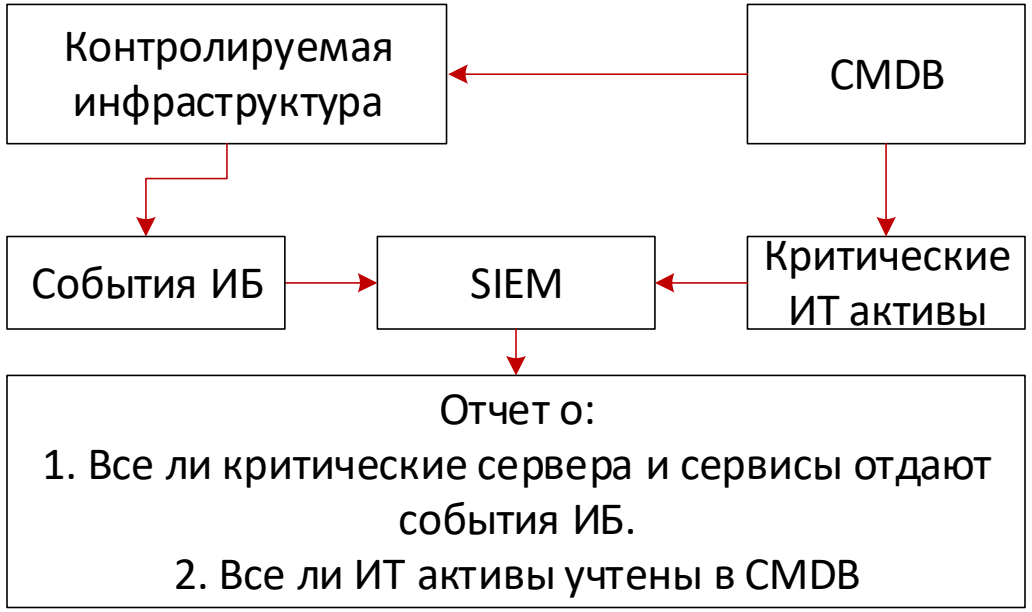
Сообщение об инциденте
Дата и время: 18 апреля 2023
Категория: Внешняя атака
Название: Сканирование ресурсов
Описание: Использование NMap
Название системы: VPN шлюз
Критичность системы: Высокая
Критичность: ~~Средняя~~ Высокая
Источник: фаерволл
Владелец сети источника запроса: Амазон
Наличие фидов: tor node

Источники контекста о внешних атаках



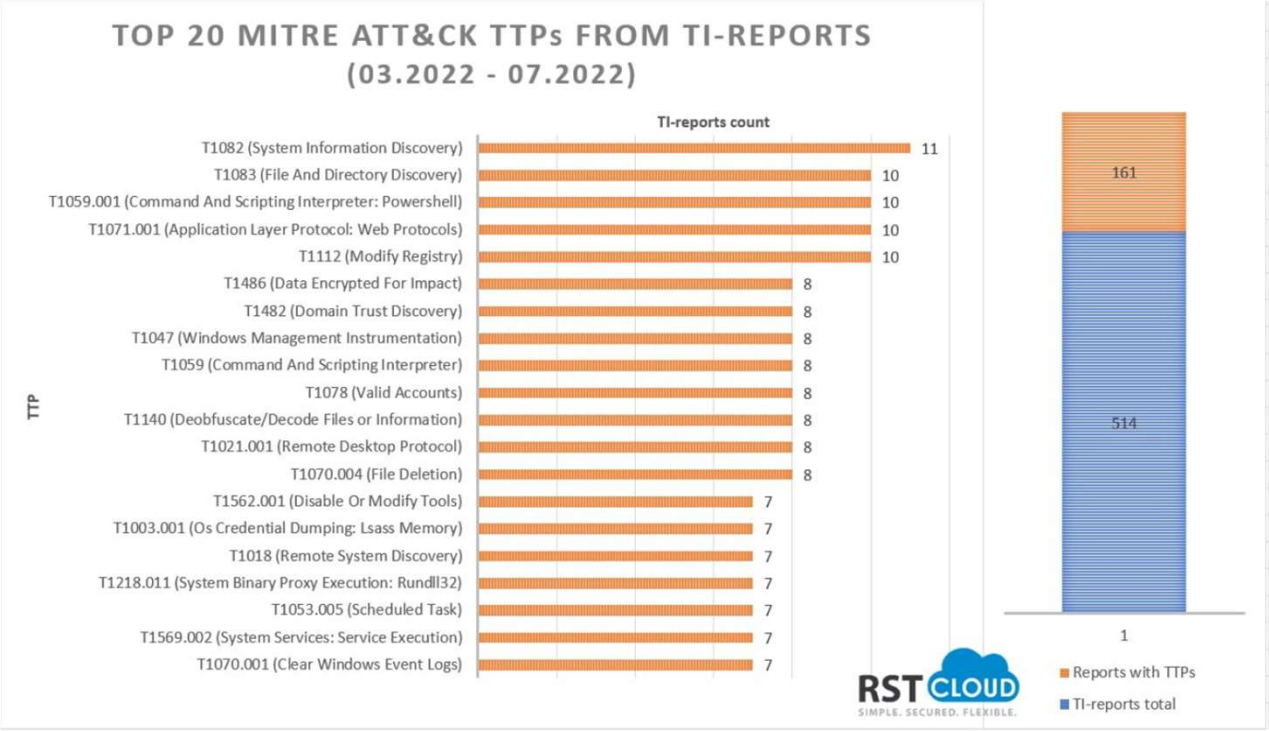
дополнительно
CMDB: полнота мониторинга

Все ли критические сервера и сервисы контролируются ИБ??



дополнительно
TI: Знаем как атакуют других

Вы же читаете все отчеты об атаках?



Заключение

Источник	Преимущества
База ASN	1. Позволяет понять, с чьих ресурсов идет атака 2. Позволяет выявить геозависимость атаки
TI	1. С какими угрозами связан source ip 2. Какие угрозы популярны в мире
CDBM	1. Какую систему атакуют (понятен вектор атаки) 2. Критичность атакуемой системы (для приоритизации инцидентов) 3. Корреляция инцидентов по атакованной системе (позволяет понять успешность атаки)
Исторические данные	1. White list на случай включения экстренных мер защиты

Спасибо за внимание

ВОПРОСЫ?