БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

eXtended Detection:
зачем нужна атрибуция угроз

Как было раньше

Отбили атаку и хорошо?

Обязательно необходимо выяснить, кто атаковал и зачем.

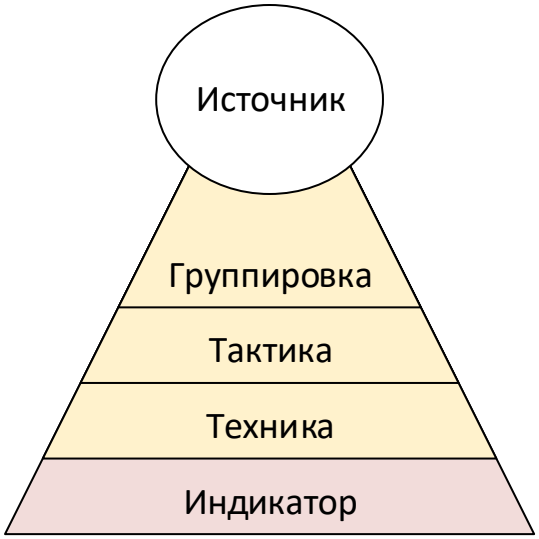
Эволюция

База сигнатур

Индикаторы компрометации

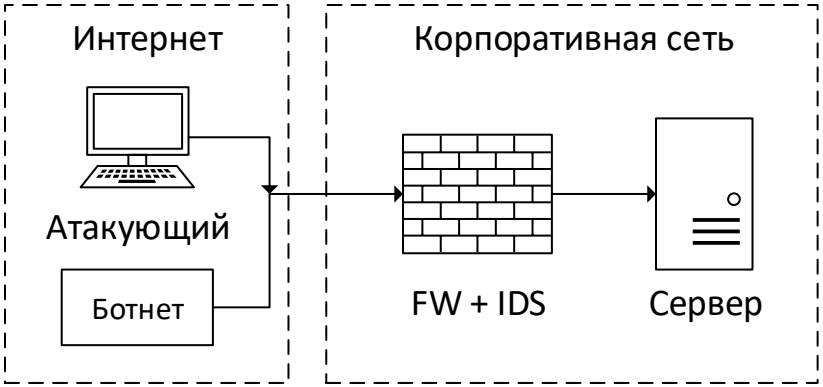
TI

Что такое атрибуция



Атрибуция – дополнительное описание индикатора компрометации, которое позволяет ответить на вопросы: кто как и зачем проводил атаку.

Пример: Внешняя атака



Контролируем:

- IP адреса атакующих
- Используемые техники атаки

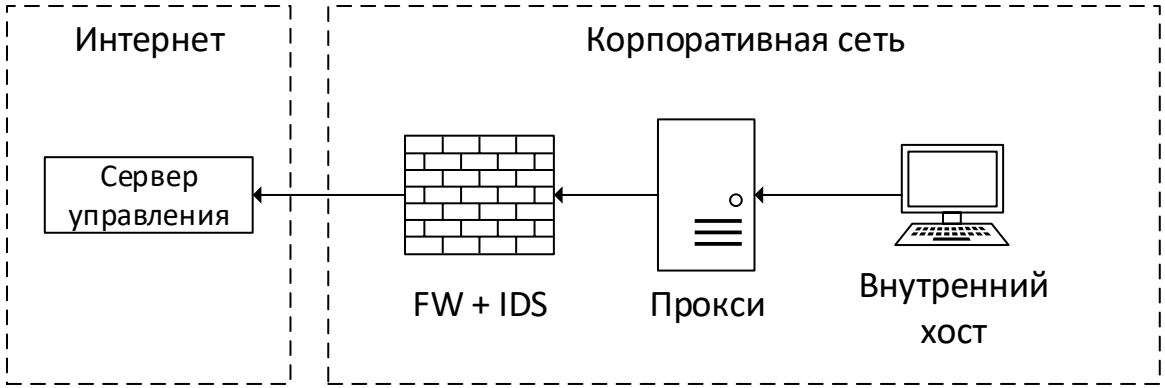
Зачем:

- Для оценки возможностей атакующего.
- Оценки вероятности использования существующих техник и для исследования новых

Пример: Обращения к сервисам атакующих

Контролируем:

- IP адреса и DNS атакующих
- Указание на тип атаки



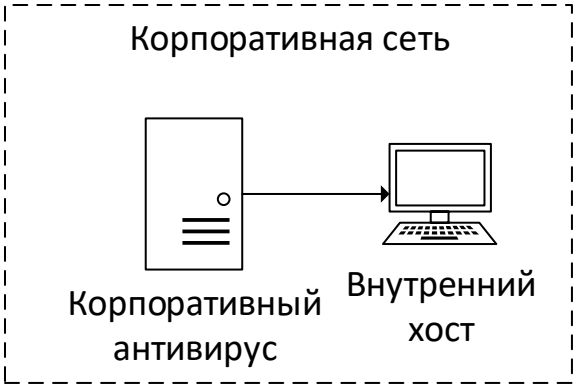
Зачем:

- Необходимо понять, кто и в рамках какой атаки пытается скомпрометировать инфраструктуру. Это даст понимание дальнейшего вектора развития атаки.

Пример: Дополнительная проверка выявленного вредоносного ПО

Контролируем:

- Вредоносное ПО (+ его сигнатуры)



Зачем:

- Для выявления признаков распространенных типов атак.

Существующие проблемы.

Отсутствие единой централизованной платформы для обмен информацией об атаках

Полнота покрытия. Не все компании сообщают о выявленных инцидентах.

БАНК
САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!