БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Использование Mitre Att&ck для проведения эффективной оценки киберрисков с учетом информации об инцидентах, атаках и уязвимостях

Оценка рисков

Threads??

facilitiesmanagementadvisor.blr.com

Оценка рисков

Чаще всего, оценка рисков используется для решения задач:

1. Для закрытия регуляторных требований
2. В качестве регуляторного рычага для

Связь с другими ИБ процессами

Threads = Techniques !?

С какими процессами можно увязать процесс оценки рисков:

1. Выявление уязвимостей
2. Мониторинг инцидентов

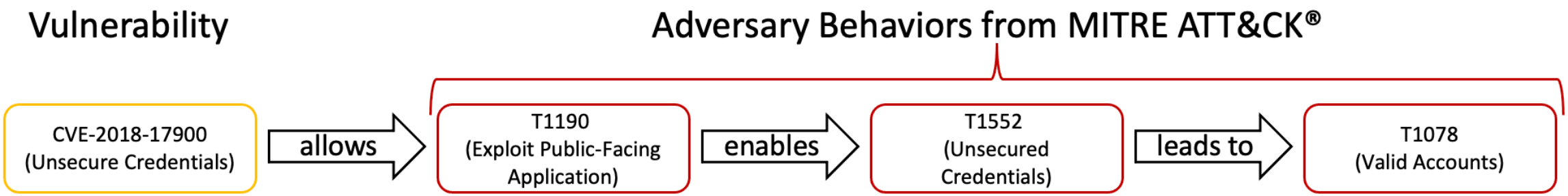
\+ дополнительно

1. Threat Intellegence
2. Тестирование на проникновение

Влияние уязвимости на вероятность

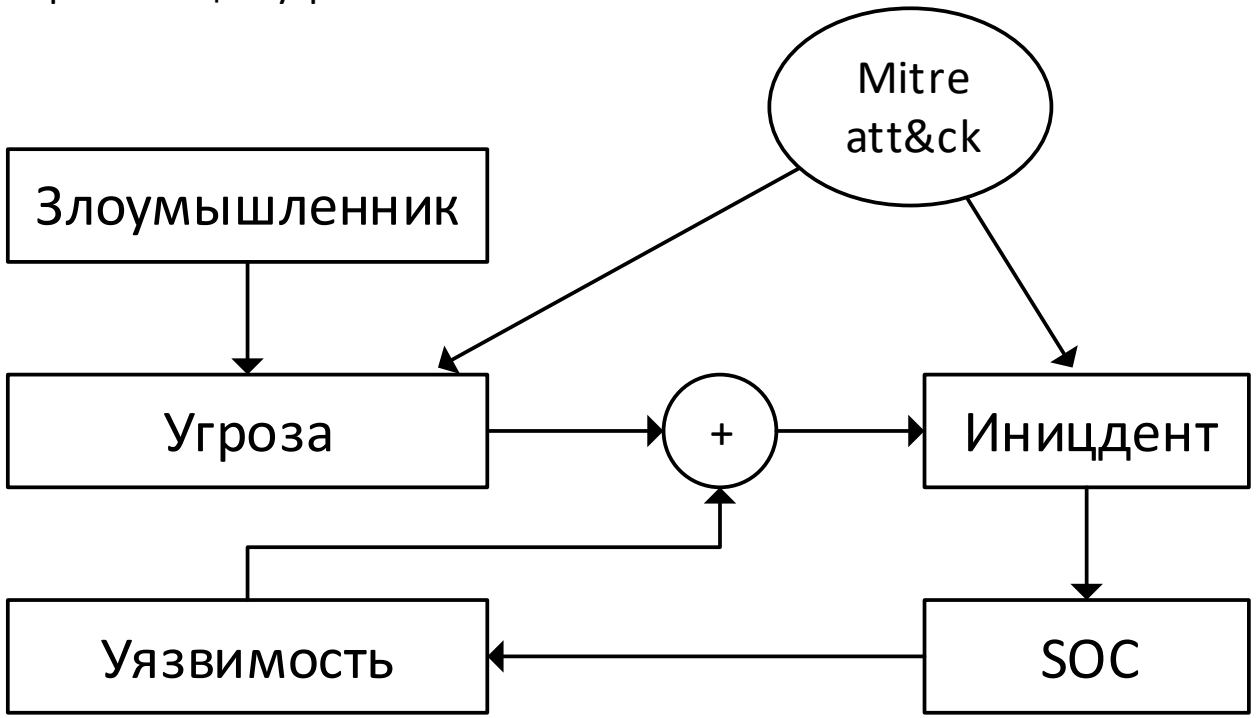
Уязвимость – причина возникновения угрозы.

Пример:



Влияние инцидентов на вероятность

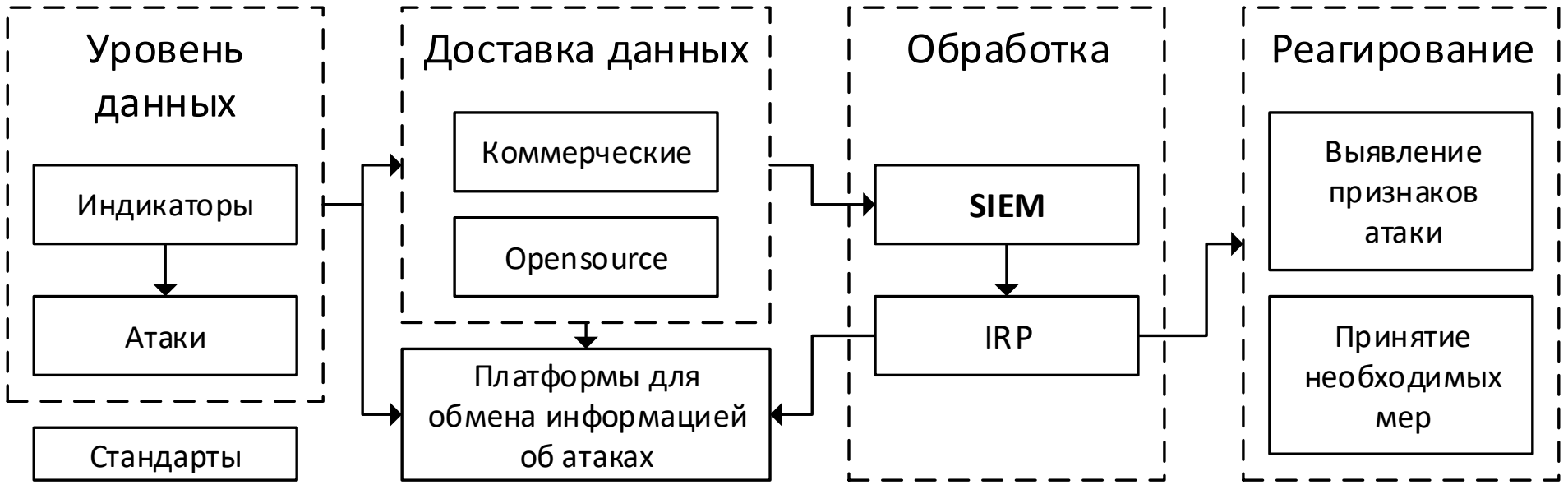
Инцидент – следствие реализации угрозы.



Использование единой базы угроз позволит провести более корректную оценку оценки рисков.

TI

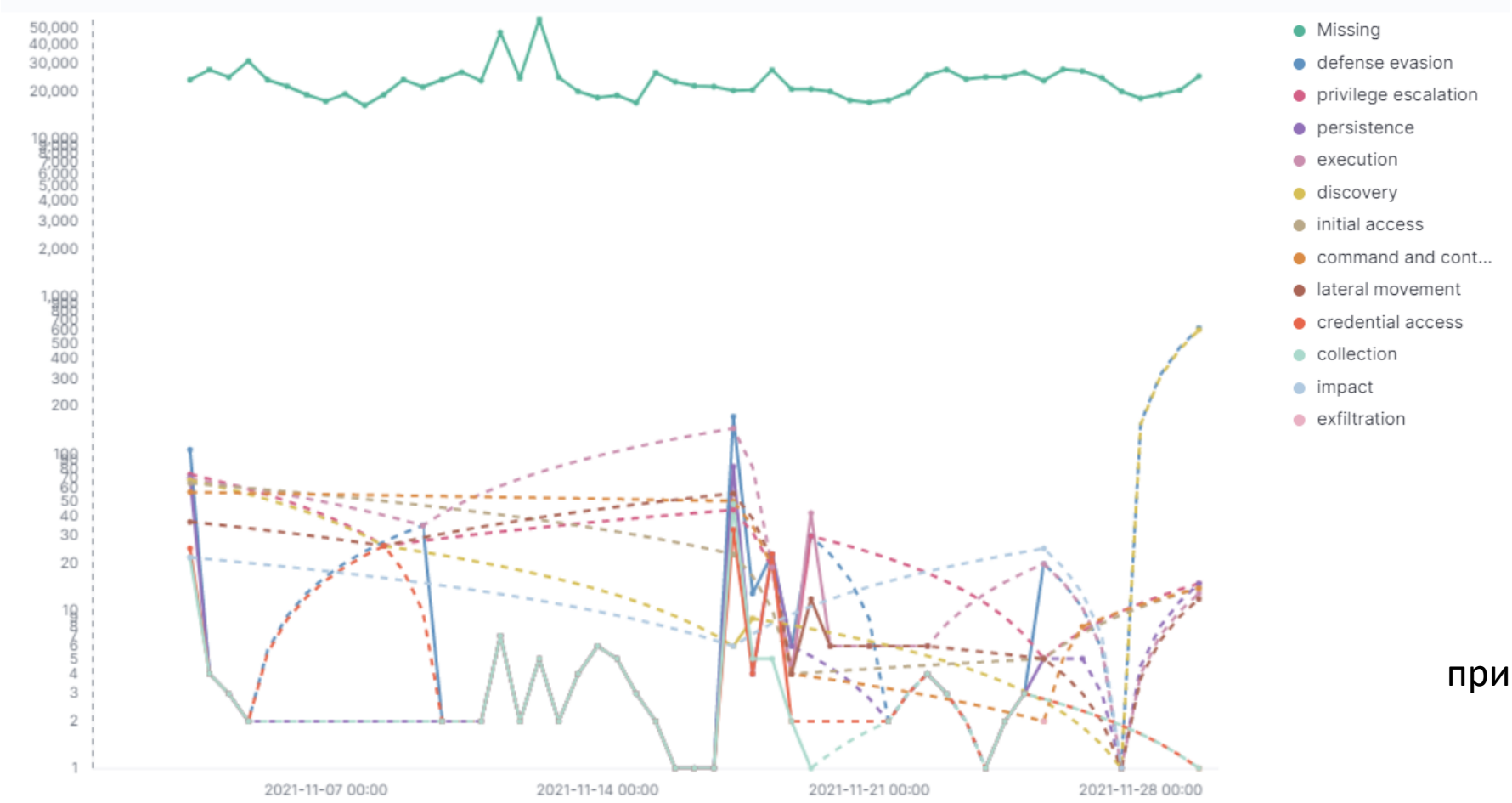
Главная цель процесса управления угрозами – обмен опытом о том, кто и как атакует другие компании.



Примерно 25% индикаторов содержат описание атаки, группировки или иную атрибуцию

TI

Статистика за ноябрь 2021



примерно 1%

Целевая схема

Преимущества

1. Более эффективный расчет вероятности возникновения угрозы.
2. Определение актуальных угроз
3. Более точное определение актуальных угроз способствует эффективному распределению ресурсов

БАНК САНКТ-ПЕТЕРБУРГ

Банк высокой культуры

Беляков И.А.
bia@bspb.ru

Спасибо за внимание!