КОД ИБ АКАДЕМИЯ

Штабные киберучения

Дмитрий Кузнецов

Positive Technologies

Коротко обо мне

Окончил Московский Государственный Университет, в информационной безопасности с 1999 г.. Последние 13 лет работаю в Positive Technologies, представляю компанию в экспертных группах ФСТЭК, ФСБ, Банка России

Активно консультирую коллег в профильных Telegram-каналах:

- «КИИ 187-ФЗ» (https://t.me/KII187FZ)
- «Все ФЗ» (https://t.me/vseFZ)
- «ИБ в Финсекторе» (https://t.me/FinSecurity)

Подготовка

Группа реагирования на инциденты

Мы создаем в подразделении ИБ группу реагирования на инциденты кибербезопасности

С чего начнем?

Первый подход к снаряду

Инцидент на химическом производстве

12:00 - Включились сирены локальной системы оповещения о ЧС
12:30 - Ответственный по гражданской обороне сообщил, что включение сирен было самопроизвольным

Инцидент или нет?
Если инцидент, то что делаем?

Типичные ошибки

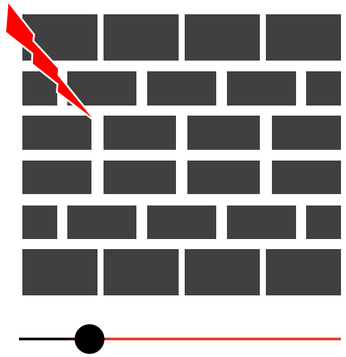
- Не знаем заранее, считать ли событие инцидентом
- Не знаем объект, на котором произошло событие
- Не знаем, к чему может привести событие
- Не имеем готового плана действий

Недопустимые события

ВСЕГДА ЕСТЬ СОБЫТИЯ, КОТОРЫЕ НЕДОПУСТИМЫ ДЛЯ ПРЕДПРИЯТИЯ

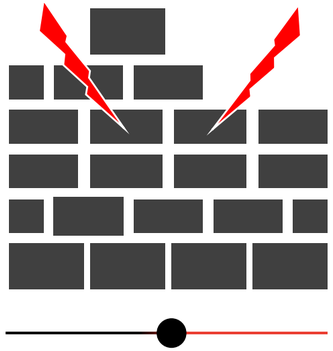
делающие **невозможным достижение** операционных и стратегических **целей** или приводящие к **длительному нарушению** его основной **деятельности,**
в том числе в результате кибератак

Выполняет все свои функции



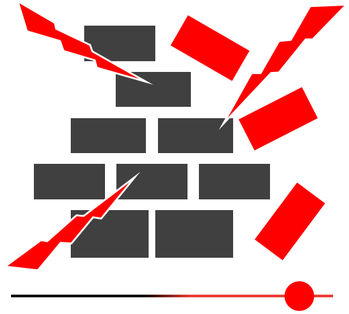
допустимый ущерб

Выполняет свои функции частично



значительный ущерб

Не выполняет свои функции

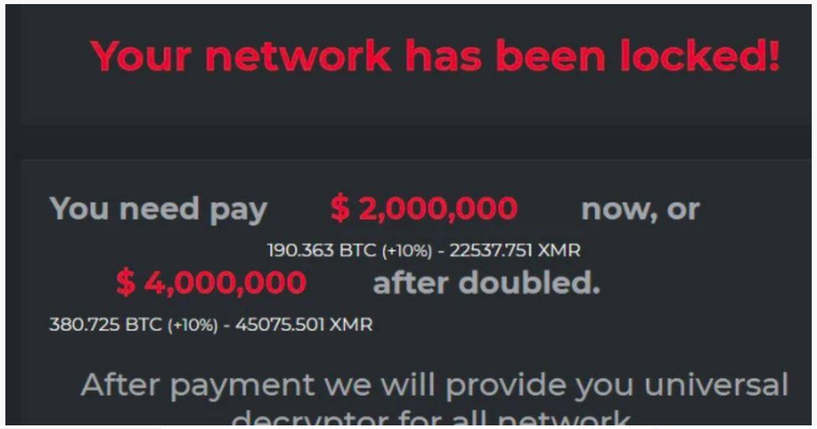


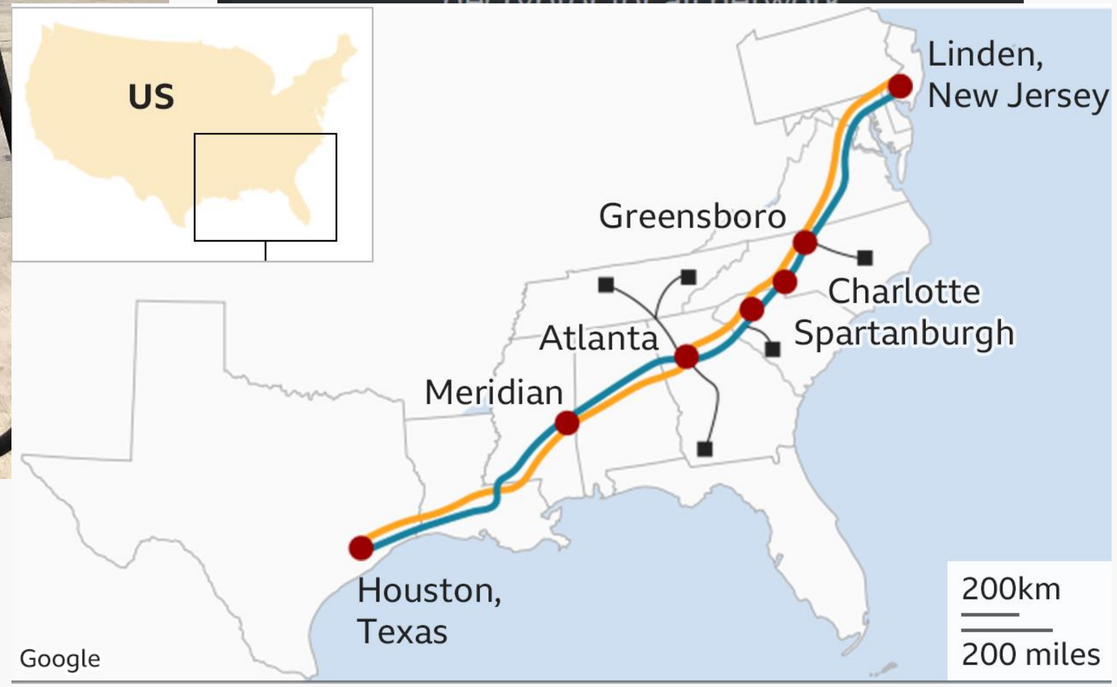
недопустимый ущерб

- ПУБЛИЧНЫЕ СУДЕБНЫЕ РАЗБИРАТЕЛЬСТВА
- СРЫВ КОНТРАКТНЫХ ОБЯЗАТЕЛЬСТВ
- ОСТАНОВКА ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ
- КРУПНЫЕ ФИНАНСОВЫЕ ПОТЕРИ
- ПОТЕРЯ ДОЛИ РЫНКА

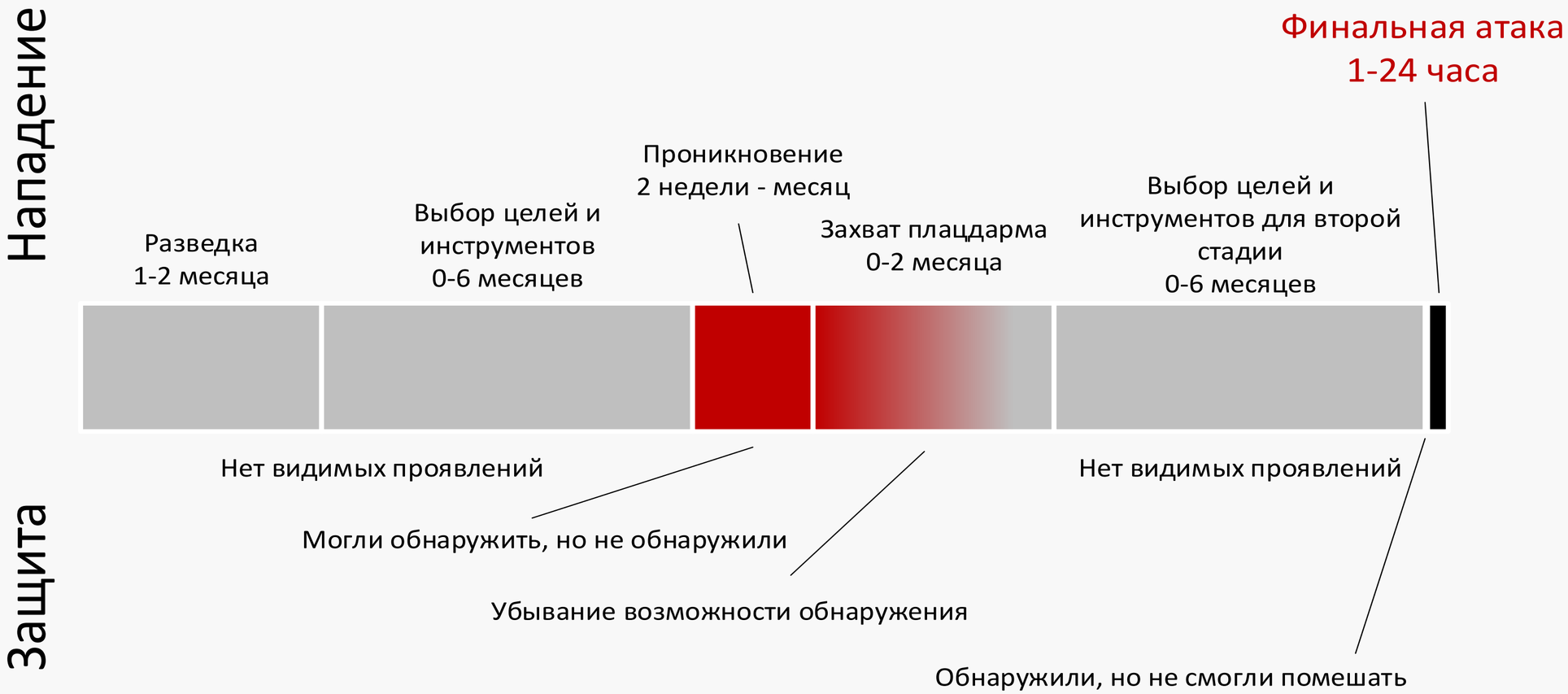
06.05.2021 – обнаружена подозрительная активность
07.05.2021 – коллапс IT-инфраструктуры, остановлена прокачка нефтепродуктов
08.05.2021 – уплачен выкуп
12.05.2021 – возобновление работы трубопровода

Когда инцидент произошел, реагировать уже поздно!





“Своевременно” – это...



Второй подход к снаряду

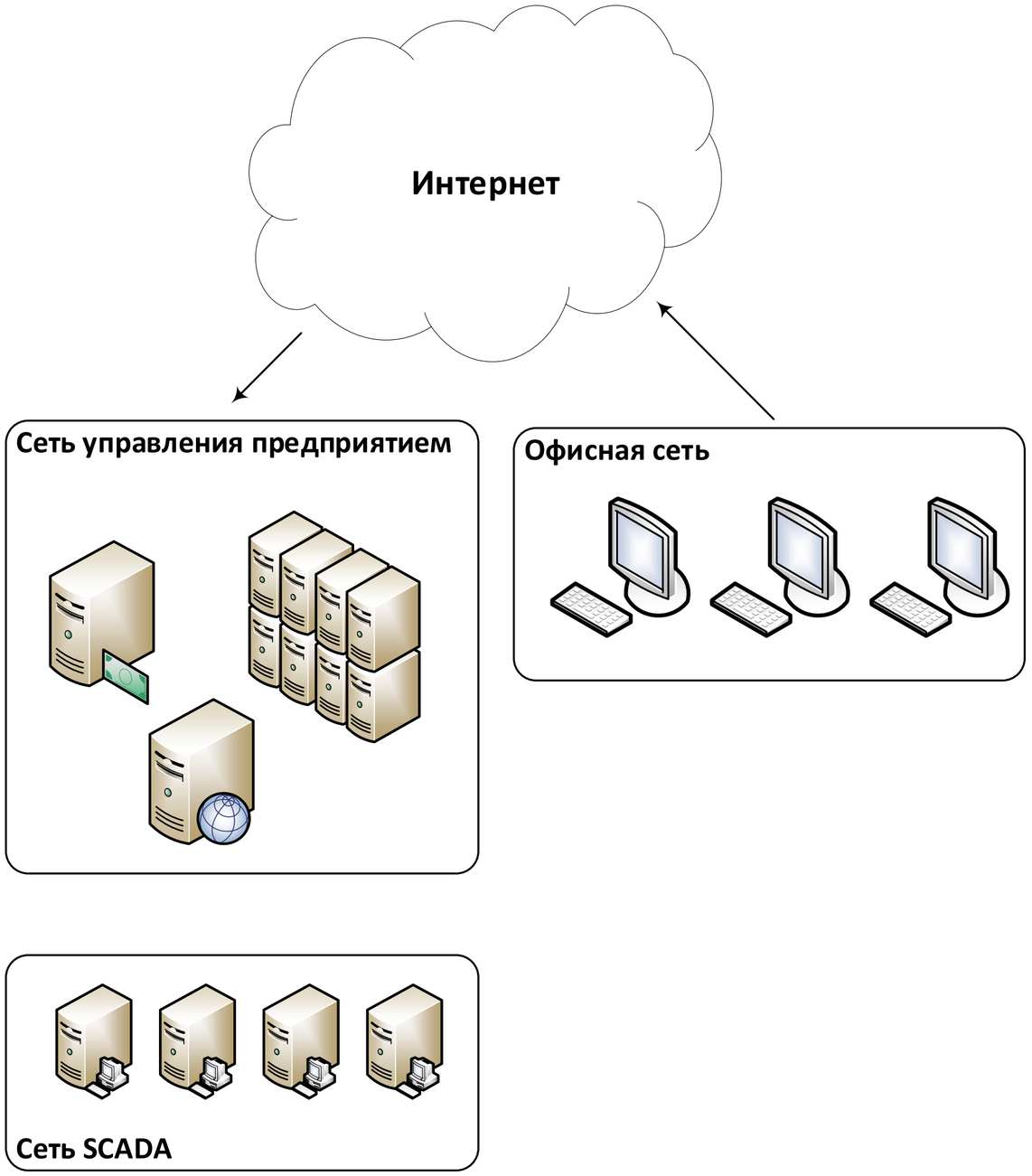
Этапы реагирования

1. Признать существование проблемы
2. Локализовать проблему
3. Выяснить, что произошло
4. Устранить проблему
5. Nevermore!

Те же,

там же,

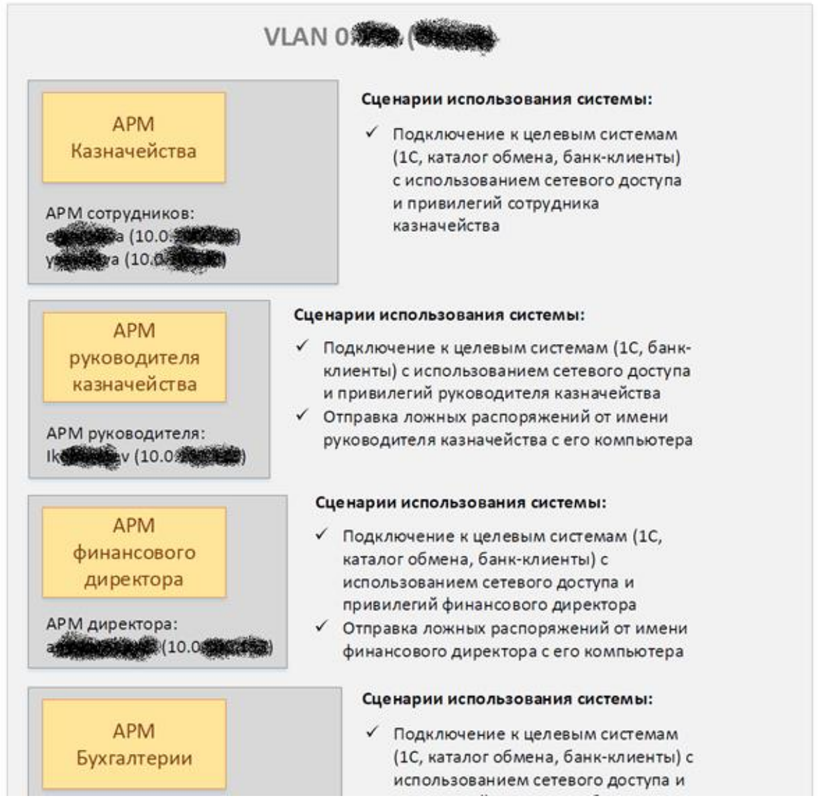
тогда же

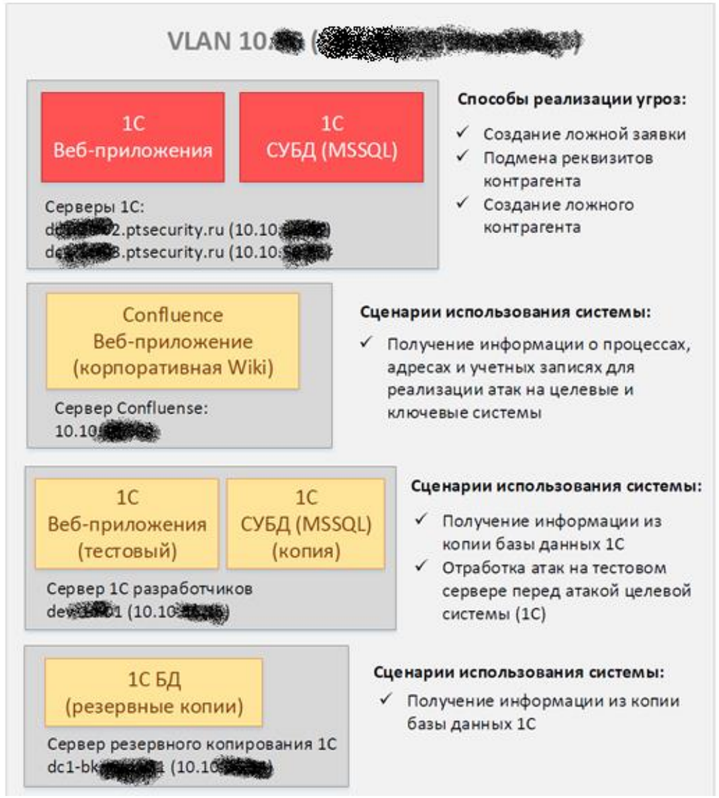


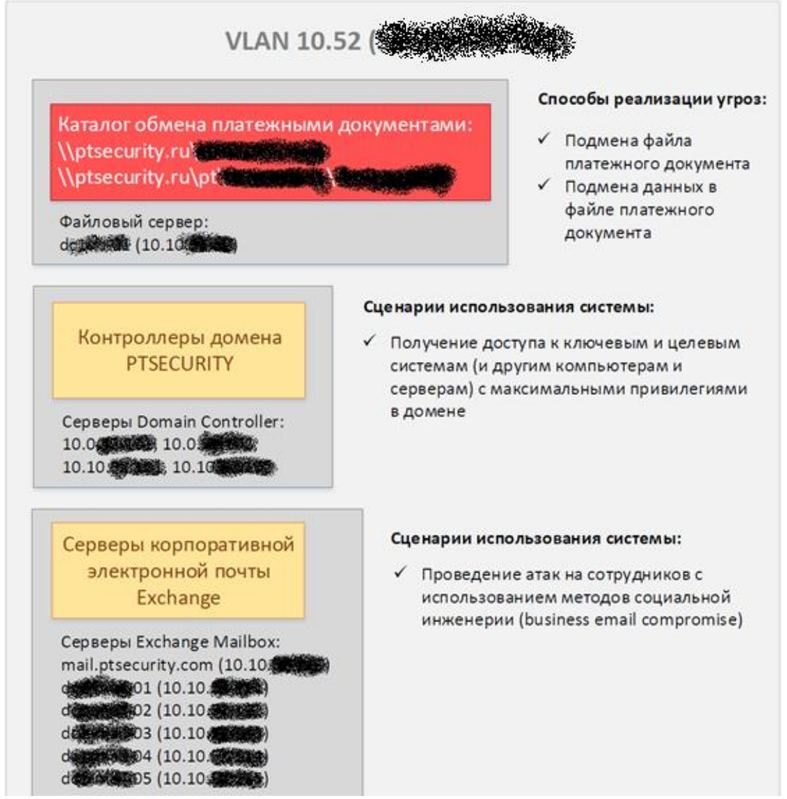
Типичные ошибки

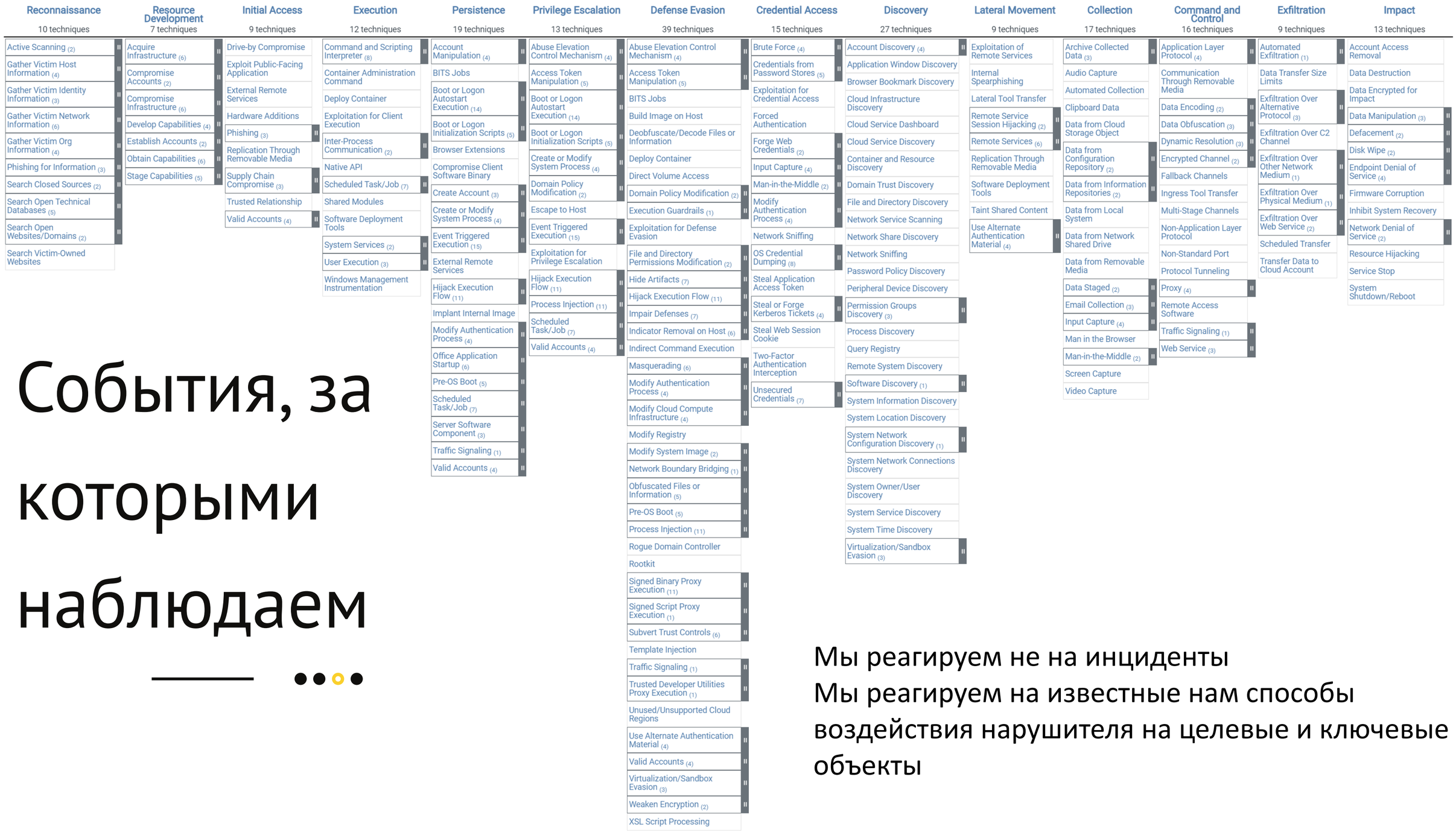
- Не знаем заранее, за чем наблюдать
- Не знаем заранее, как будем изолировать зону поражения
- Не имеем развернутых инструментов
- Не имеем готового плана действий

Объекты, за которыми наблюдаем









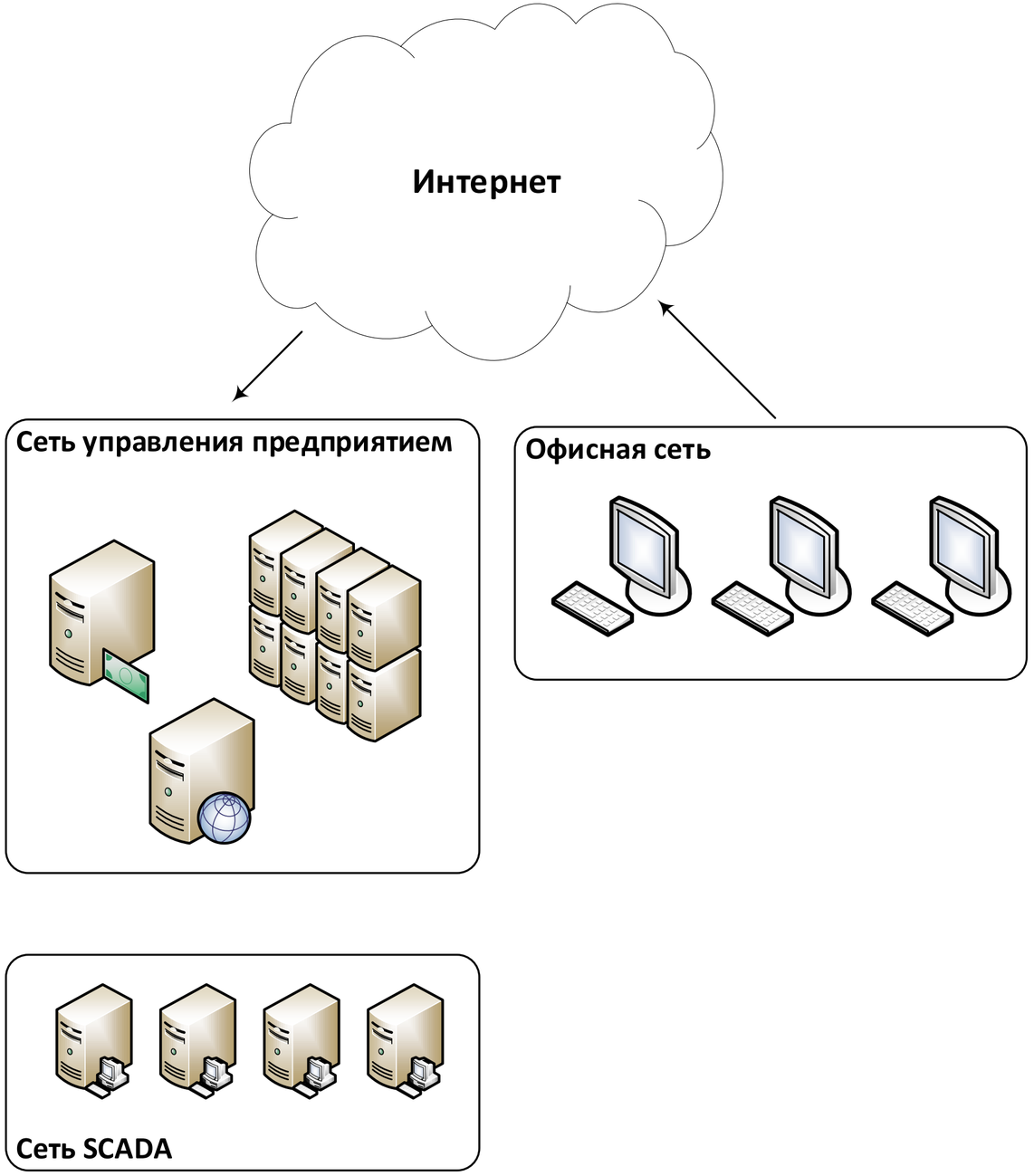
События, за которыми наблюдаем

Мы реагируем не на инциденты
Мы реагируем на известные нам способы воздействия нарушителя на целевые и ключевые объекты

План реагирования

- Какие события недопустимы?
- Какие объекты являются целевыми и ключевыми?
- Какие действия нарушителя с этими объектами нужно обнаруживать?
- Чем и как эти действия обнаруживать?
- Что делать при обнаружении?

Подготовка к реагированию



Инструменты реагирования

- SIEM
- CMDB (если этого не умеет SIEM)
- Анализаторы трафика
- WAF
- Песочницы
- Базы знаний

Что в итоге

Реагирование на инциденты vs. ИБ

- Нужно знать потребности бизнеса
- Нужно знать приемы нарушителя
- Нужно ставить под сомнение собственную защищенность
- Нужен инструментарий, не предусмотренный нормативными требованиями

Готов ответить
на ваши вопросы

E-mail
malotavr@gmail.com

Telegram
@malotavr