Предчувствуя взлом: Реагирование на инциденты в неспокойное время

POSITIVE TECHNOLOGIES

ptsecurity.com

Целенаправленные атаки – актуальная проблема

POSITIVE TECHNOLOGIES

20 Russian high-profile organizations attacked by spy malware in coordinated op – FSB

Scarab attackers took aim at select Russian targets since 2012

NetTraveler APT Targets Russian, European Interests

Chinese Cyberspies Pivot To Russia In Wake Of Obama-Xi Pact

Roaming Tiger Hackers targets Russian organizations for espionage

December 24, 2015 By Pierluigi Paganini

September 17, 2015

News Alert: APTs target Russian military personnel and telecoms employees

NEWS

'Lurid' malware hits Russia, CIS countries

APT?

APT Goes Mainstream on TV

- **Advanced**
  - Использование 0day
  - Сложное ВПО
  - Адаптируются к изменениям
- **Persistent**
  - Атака продолжается пока не достигает успеха
  - “Low and Slow”
  - Доступ на годы вперёд
- **Threat**
  - Правительства
  - Серьёзный криминал
  - Обеспечены ресурсами

Как они это делают?

- **Разведка**

OSINT. Сбор данных о сотрудниках и организации. Поиск слабых мест.

- **Точка входа**

Исходная компрометация. Spear phishing, watering hole, взлом через веб

- **Lateral Movement**

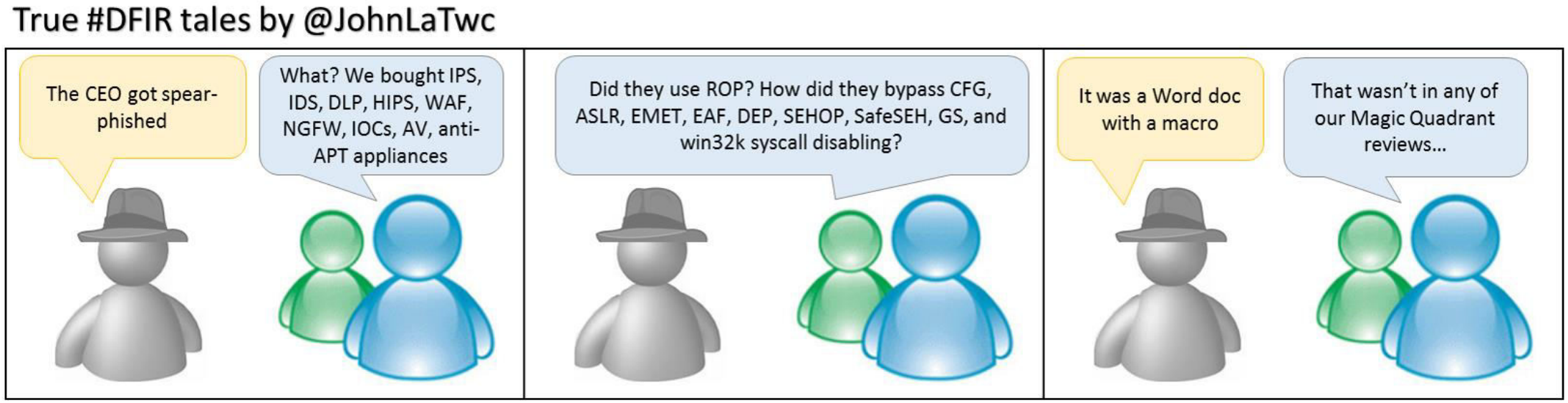
Закрепление в сети. Сбор учётных данных, повышение привилегий, сканирование портов, компрометация дополнительных машин.

- **Кража данных**

Сбор и выгрузка данных. Туннелирование. Заметание следов

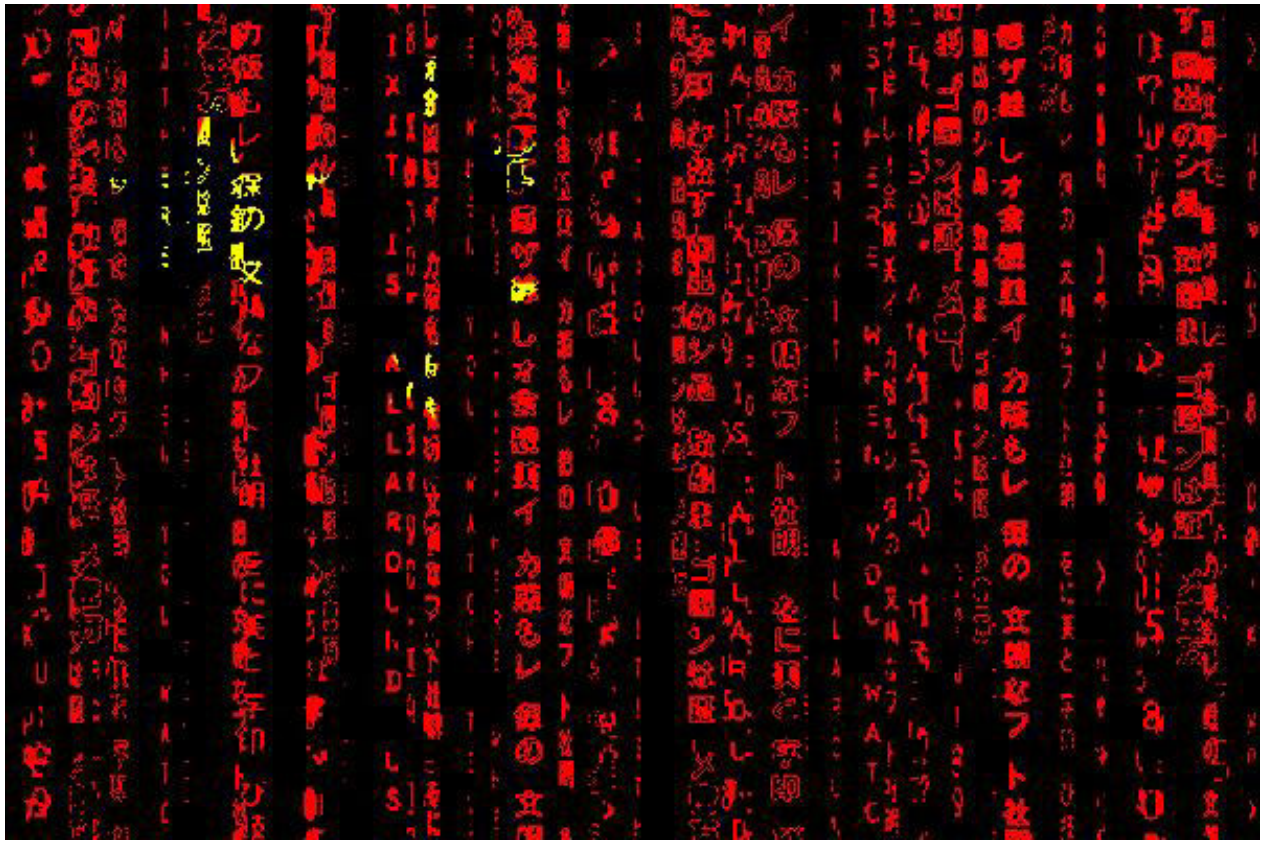
Наша практика

POSITIVE TECHNOLOGIES



- **Среднее время присутствия – 5 лет**
- **Способ обнаружения – внешний(90%)**
- **Самый популярный вектор – Spear-phishing**
- **В каких случаях использовалось ВПО? – 100%**
- **Типичный результат – полная компрометация сети**

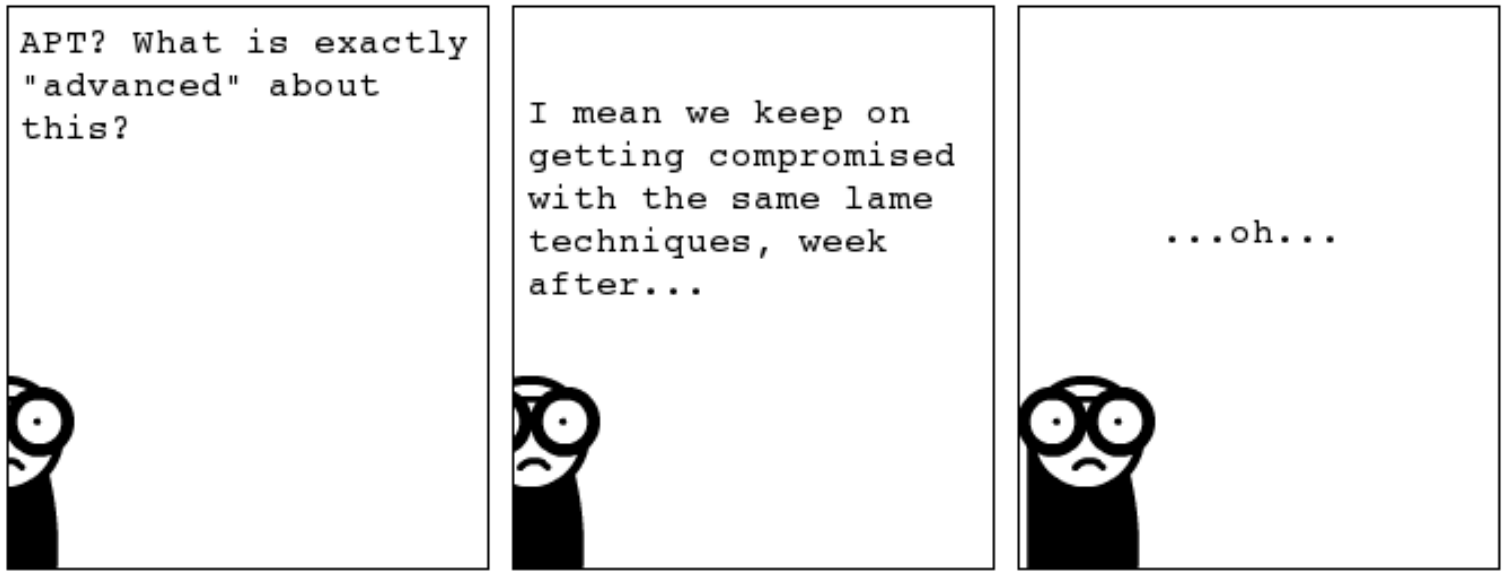
Пример



- **Кто?**
  - Roaming Tiger/NetTraveler/APT21
  - Китай
  - Вероятно state-sponsored
- **Как?**
  - Spear-phishing
  - PlugX, NetTraveler RAT
  - CVE-2014-1761, CVE-2012-0158
- **Кто жертва?**
  - Компания энергетического сектора
  - Скомпрометирована в 2011 году
- **Lateral Movement**
  - MS14-068
  - Mimikatz, pass-the-hash

Типичные проблемы

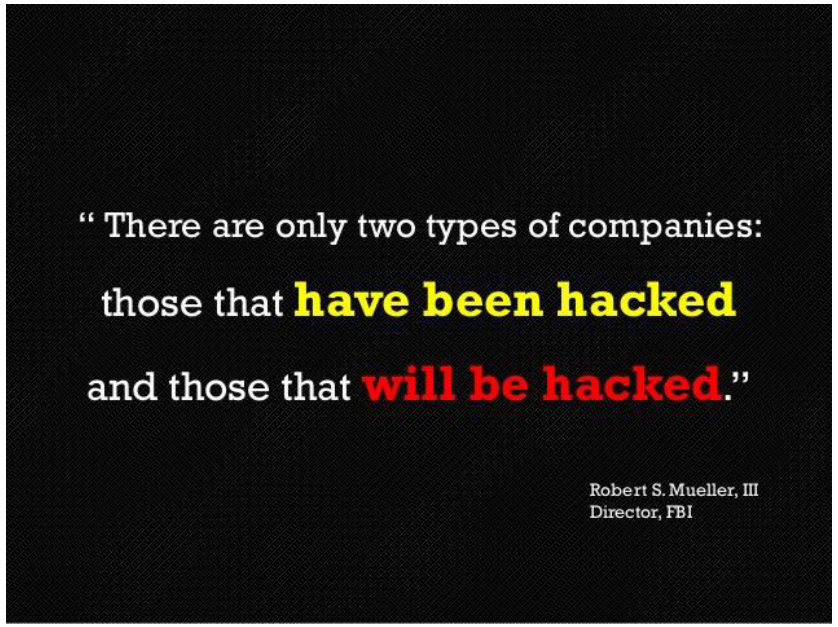
POSITIVE TECHNOLOGIES



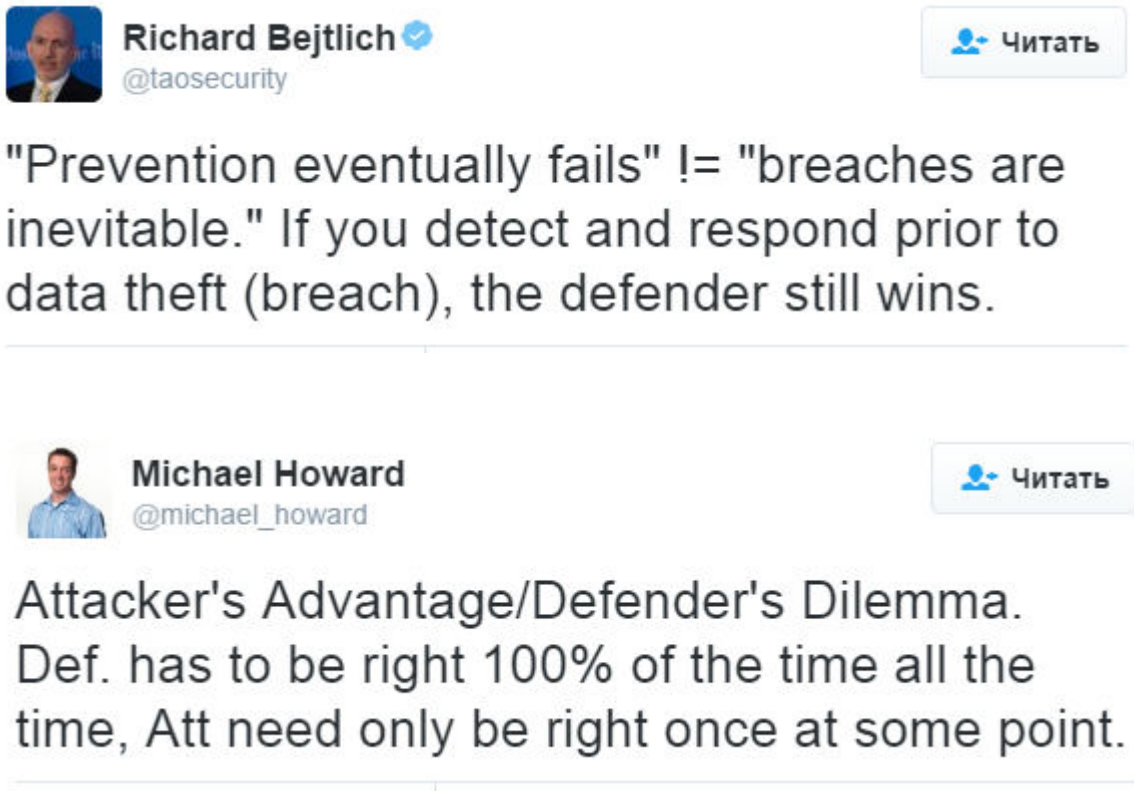
- Устаревшее ПО
- Отсутствие мониторинга
- Отсутствие квалифицированных сотрудников ИБ
- Отсутствие сегментации сети
- Незнание собственной инфраструктуры
- Отсутствие контроля за привилегированными учётными записями
- Отсутствие современных средств защиты
- …

Смена парадигмы

POSITIVE TECHNOLOGIES



- “Assume breach”
- Вас взломают, вопрос только когда вы это обнаружите
- Всё сводится к повышению стоимости атаки



О необходимости реагирования

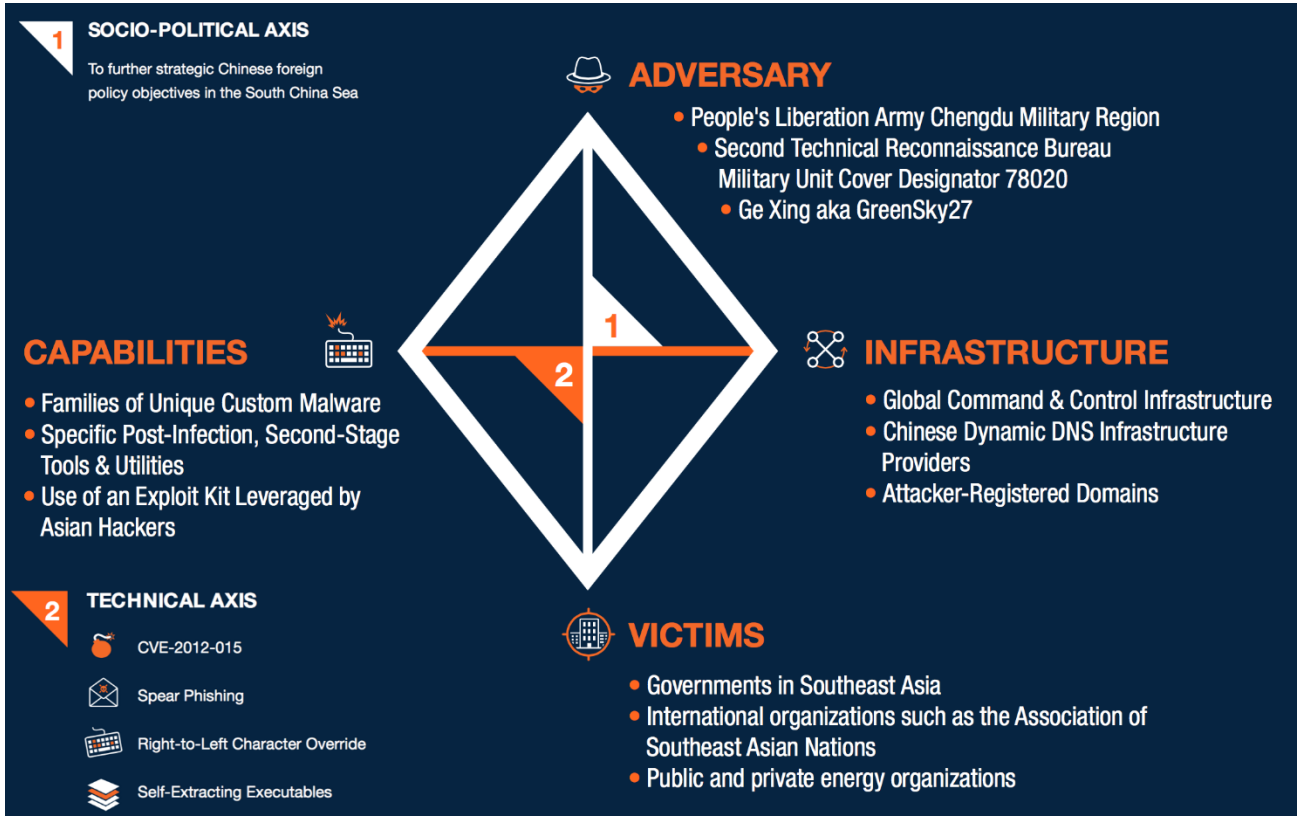
POSITIVE TECHNOLOGIES

- **Подготовка**
  - Моделирование угроз
  - Оценка защищённости
  - Люди, процессы, средства
- **Выявление**
  - Постоянный мониторинг
  - Аномалии
  - Ретроспективный анализ
- **Сдерживание и восстановление**
  - Удаление ВПО
  - Блокировка скомпрометированных УЗ
  - Восстановление или пересоздание систем
- **После инцидента**
  - “Lessons learned”

Зачем это нужно?

POSITIVE TECHNOLOGIES

Diamond Model



- **Threat Intelligence**
  - Кто, как, когда и почему
  - Проактивная защита
  - TTP
- **Своевременное обнаружение**
  - Нельзя реагировать если ты этого не видишь
  - Повышение эффективности
  - Определение «слепых зон»
- **Корректное восстановление**
  - Оценка границ
  - Установление причин
  - План восстановления

BYOC(Bring your own CSIRT)

POSITIVE TECHNOLOGIES

Build vs Buy

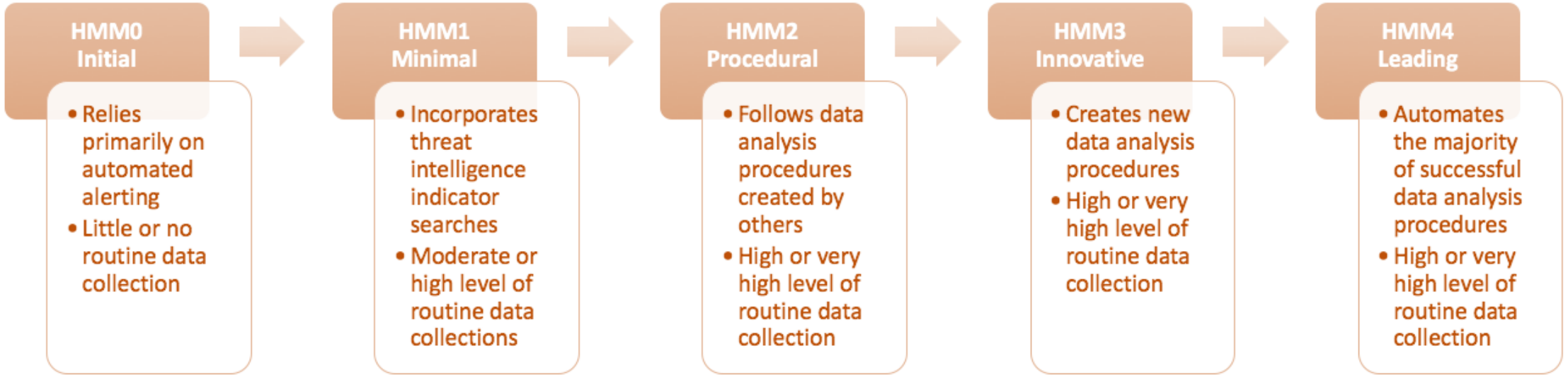
- **Плюсы**
  - Хорошо знают вашу организацию
  - Всегда «под рукой»
- **Минусы**
  - Дорого
  - Может не хватать экспертизы
  - «Замыленный глаз»
  - Может не быть налаженных связей с сторонними организациями
  - Может не хватать экспертизы
  - «Замыленный глаз»

- **Плюсы**
  - Широкая экспертиза
  - Дешевле
  - Налаженные контакты со сторонними организациями
  - Threat Intelligence
- **Минусы**
  - Необходимо время чтобы адаптироваться к вашей инфраструктуре
  - Не могут уделять 100% времени вашей организации
  - Качество может отличаться

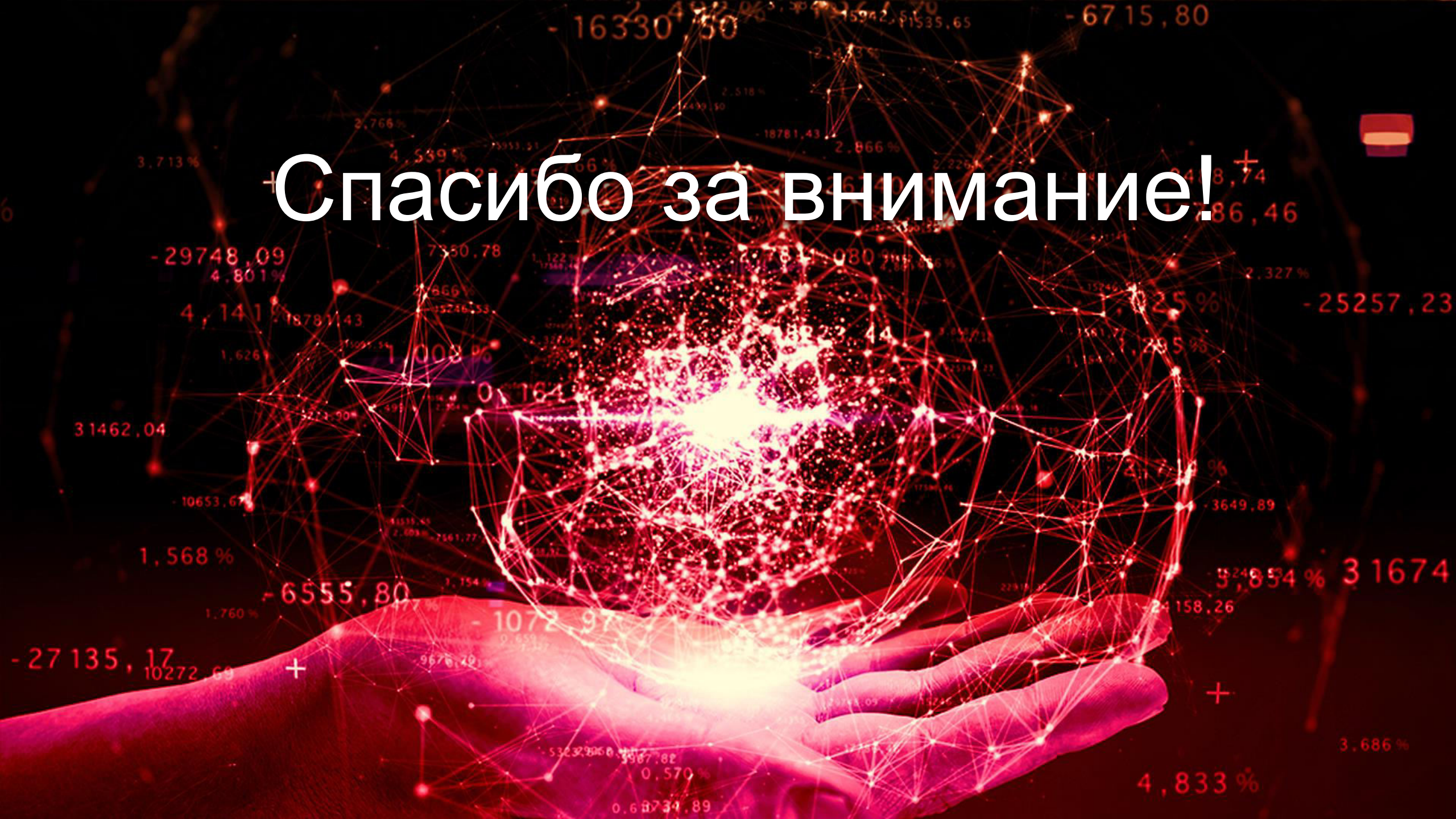
Что дальше?

POSITIVE TECHNOLOGIES

Threat Hunting Maturity Model



- **Threat Hunting**
  - IOC Sweeps
  - Data mining
  - Аномалии
- **Threat Intelligence**
  - Тактики, техники и процедуры
  - Аналитика
  - Обмен данными об угрозах
- **Purple Team**
  - Не просто пентестеры
  - Adversary Simulation
  - Работают с защитниками


Спасибо за внимание!