ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ

КАК Red Team тестирования могут помочь вашему SOC.

Максим Чудаков,
Руководитель группы внутреннего аудита и защиты

Whoami

- Руководитель группы технического аудита и защиты в ЦФТ
- Внедряю SOC ~ 3 года
- Red&Blue Teamer
- OSCP, CISA, ECSA и другие наборы букв

Twitter: @Mchudakov
Telegram: @i223t

Prevention vs Detection&Response

Исторически:

- Акцент на защиту периметра.
- Антивирус и IPS не дадут хулиганам шанса.
- Злоумышленник не может получить доступ к системам.

Как итог:

- Отсутствие функции мониторинга событий ИБ
- Отсутствие плана реагирования при инциденте

Статистика Positive Technologies по пентестам за 2017 год

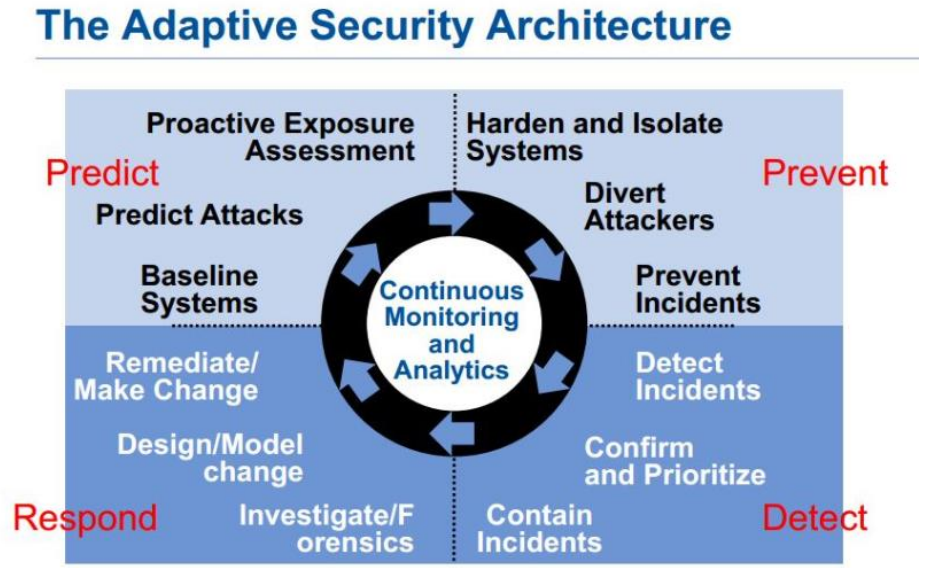
- 68% - преодолен внешний сетевой периметр (внешний нарушитель)
- 100% - компрометация инфраструктуры (внутренний нарушитель)
- 60% - наличие уязвимости ms17-010 (WannaCry)
- 26% сотрудников осуществляют переход по ссылке на фишинговый веб-ресурс
- 15% сотрудников запустят вложение в почте
- 75% - возможно получить доступ в сеть через взлом Wi-Fi

APT

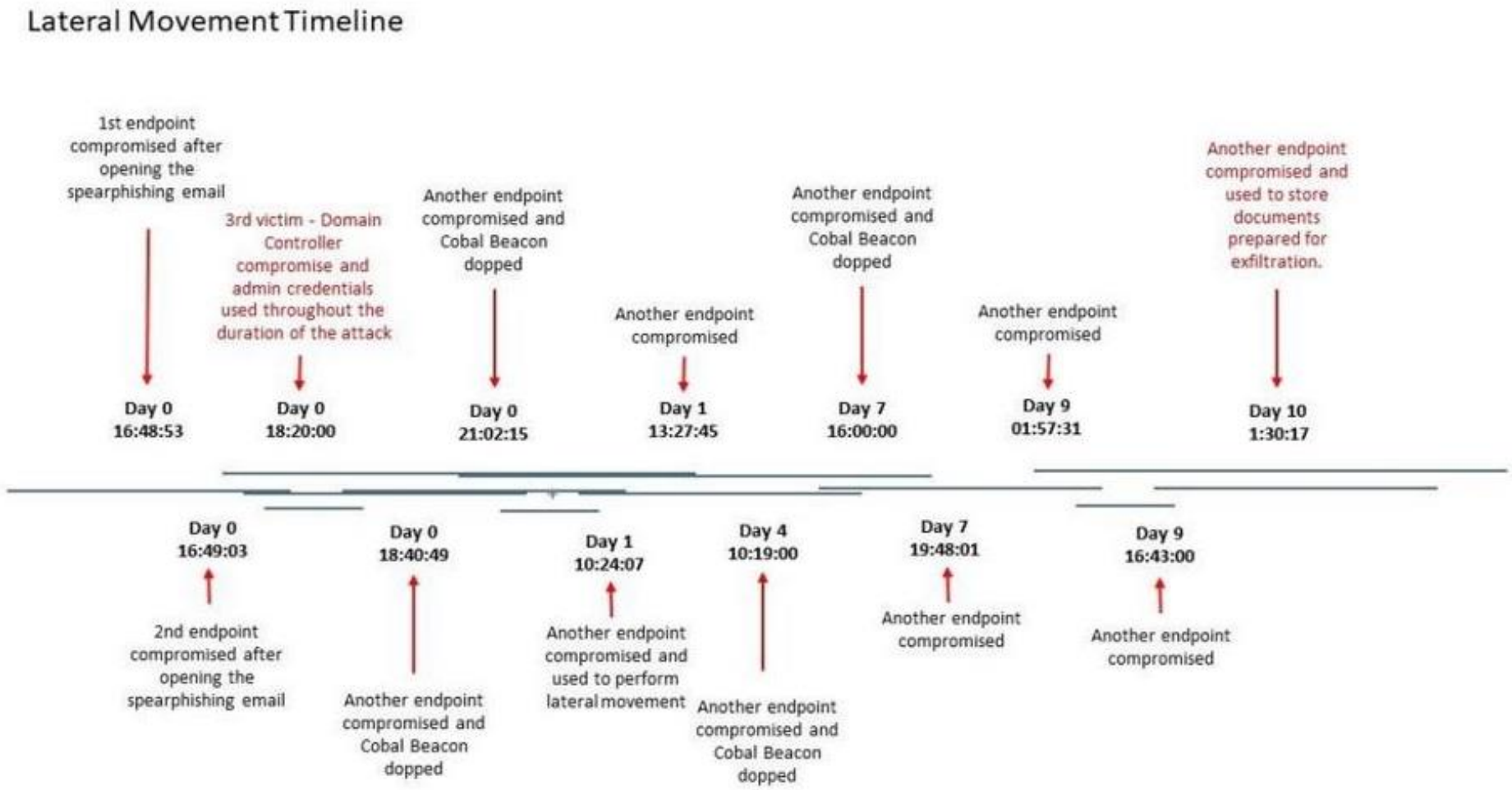
- **Advanced**
  - Использование 0-day
  - Сложное ВПО
  - Адаптируются к изменениям
- **Persistent**
  - Атака продолжается, пока не достигает успеха
- **Неограниченные ресурсы**
  - Правительство
  - Серьёзный криминал

Assume Breach Model

1. Вашу инфраструктуру взломают. Вопрос лишь в том, когда это произойдет и сможете ли вы вовремя отреагировать (узнаете ли вообще?).
2. Превентивные меры должны рассматриваться отдельно от детективных.

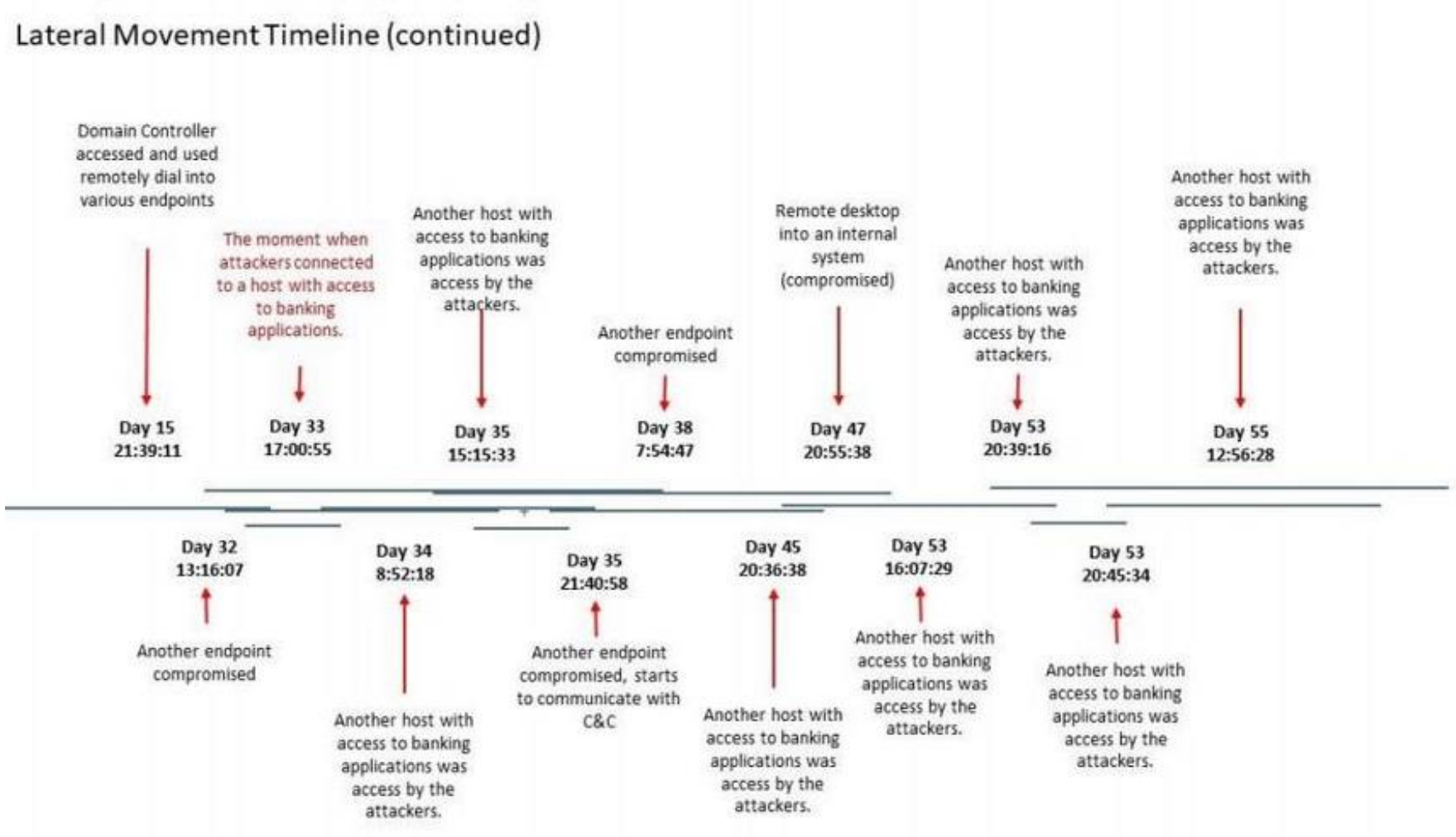


Attack Timeline. Carbanak



https://www.zdnet.com/article/hollywood-lie-bank-hacks-take-months-not-seconds/

Attack Timeline. Carbanak (продолжение)



https://www.zdnet.com/article/hollywood-lie-bank-hacks-take-months-not-seconds/

Логичный вывод: Внедряем SOC

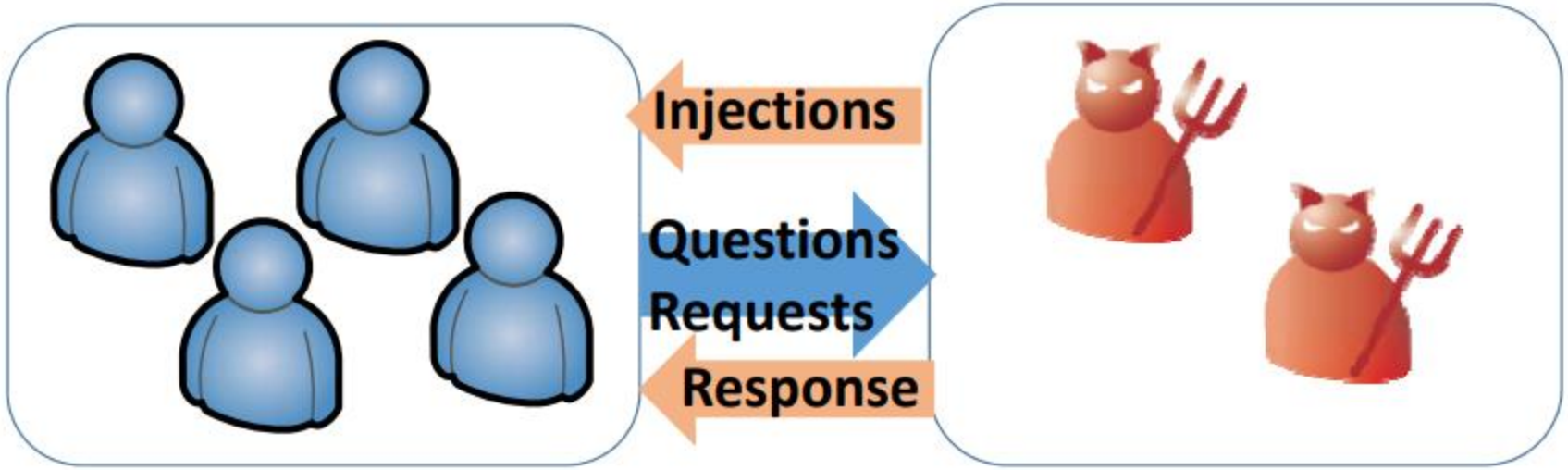
SOC. Оценка эффективности

Как оценить готовность к реальным атакам?

- Аудиты на соответствие лучшим практикам
- Tabletop Exercise
- Red Team Exercise (Full Live)

Tabletop Exercises

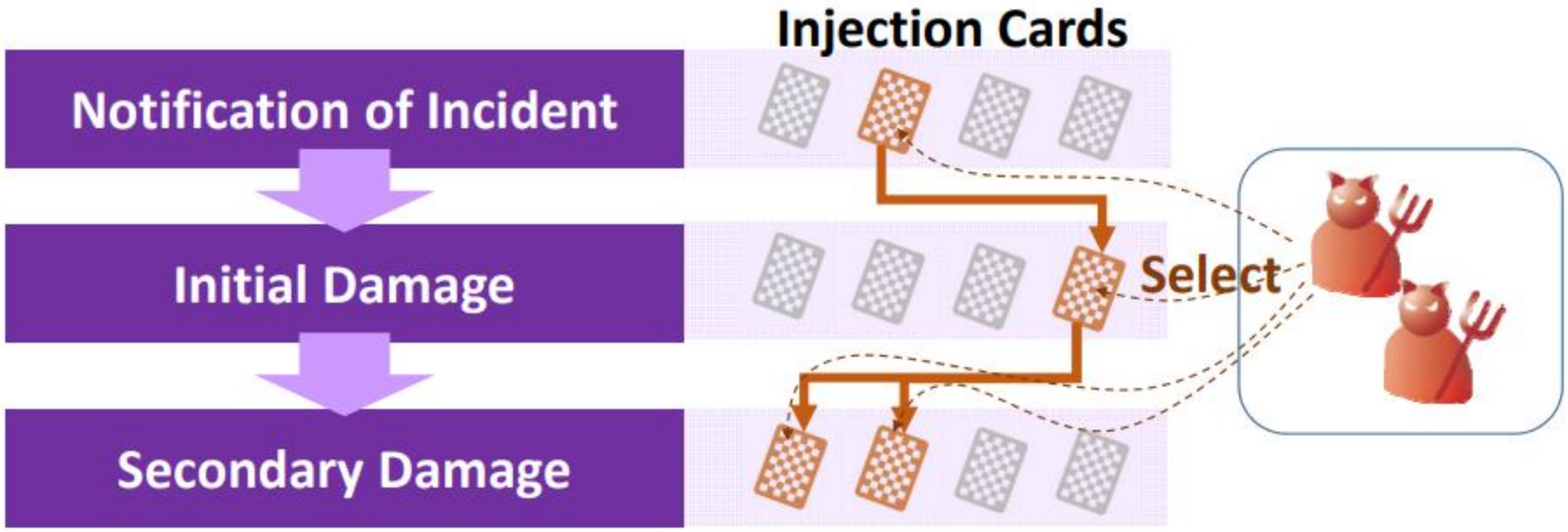
Вариант 1. Непосредственное общение и обмен опытом Red Team и Blue Team



https://www.first.org/resources/papers/conf2019/Blue-team-vs.-Red-team-Tabletop-Exercise-to-Train-the-Process-of-Attack-Investigation.pdf

Tabletop Exercises

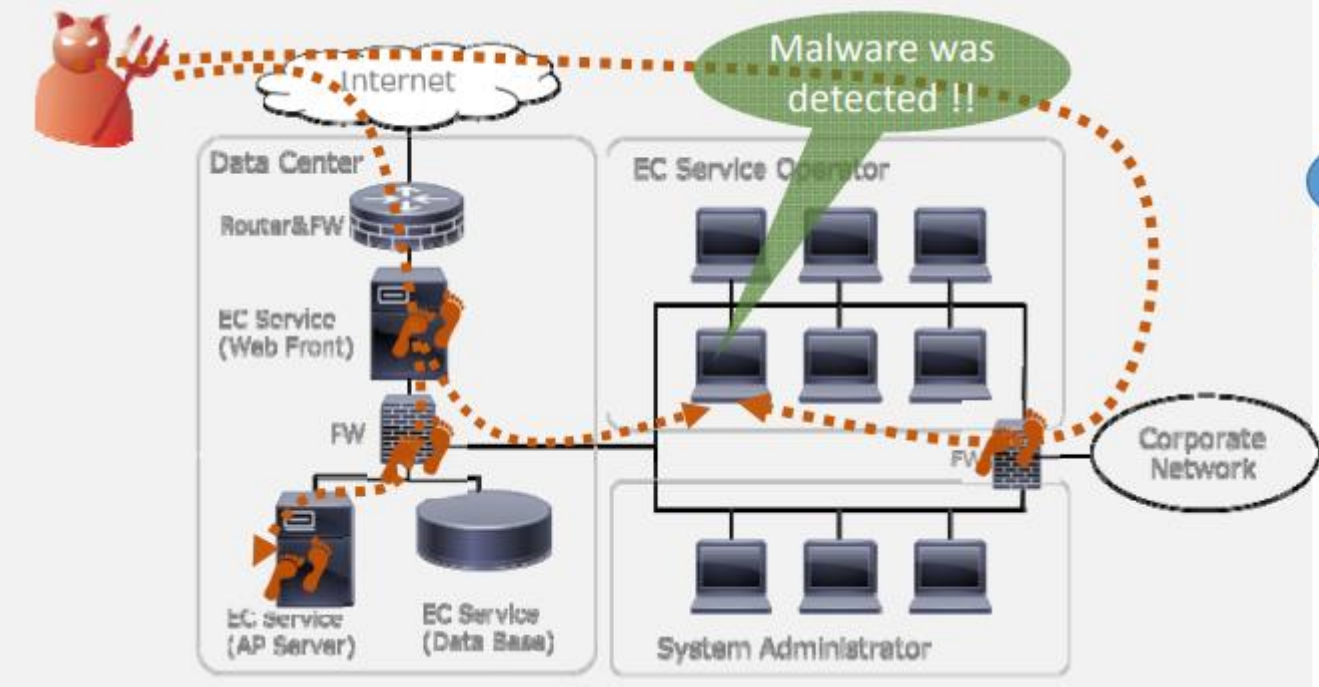
Вариант 2. Формирование случайных сценариев

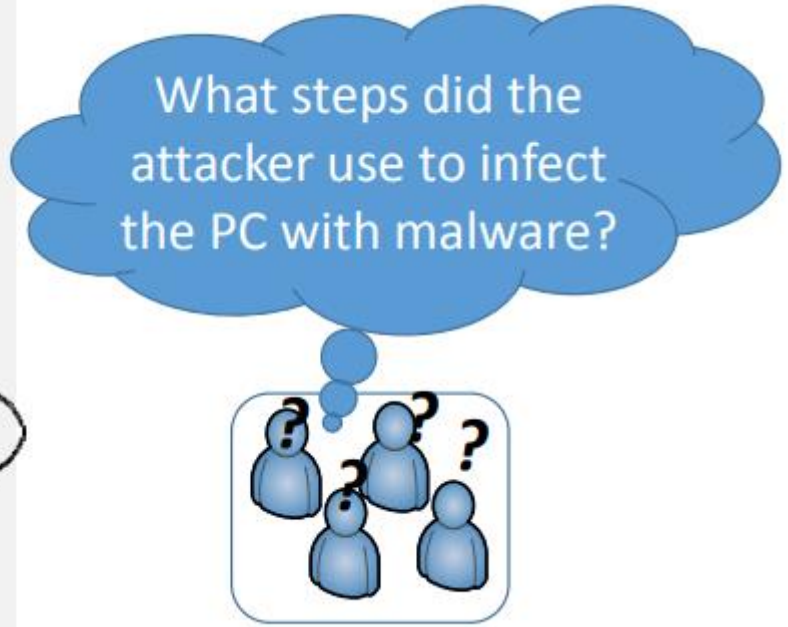


https://www.first.org/resources/papers/conf2019/Blue-team-vs.-Red-team-Tabletop-Exercise-to-Train-the-Process-of-Attack-Investigation.pdf

Tabletop Exercises

Вариант 3. Задачи на форензику и анализ логов





https://www.first.org/resources/papers/conf2019/Blue-team-vs.-Red-team-Tabletop-Exercise-to-Train-the-Process-of-Attack-Investigation.pdf

Пентесты vs Red Team Exercises

Red Team Exercises vs Пентесты:

- Большая область и глубина тестирования*
- Достижение цели наиболее эффективными методами
- Длительность тестирования
- Закрепление в системах
- Сложные параллельные атаки, запутывание следов
- Противодействие
- Стоимость

* - обычно

Red Team Exercises.

Выявляемые проблемы:

- Недостаточность области покрытия или детализации логов
- Нерабочие правила (некорректные изменения)
- Коммуникация между подразделениями
- Нарушение процесса обработки во внерабочее время
- Компетенции специалистов SOC, пропуск True Positive
- Подверженность атакам самой SOC-инфраструктуры

ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ

СПАСИБО ЗА ВНИМАНИЕ

Вопросы?