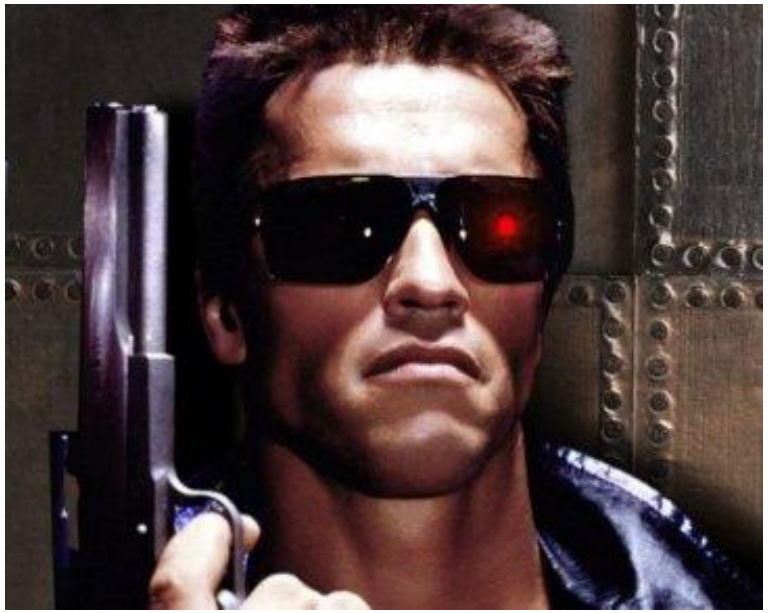
Ждать нельзя защитить

Евгений Акимов, директор по кибербезопасности

КАЛАШНИКОВ
КОНЦЕРН

Почему SOC?

- **Security operation center**
  - Получить бизнес-результат
  - Не уходить в флейм SOC ли это
  или недоSOC или переSOC
- **Цель**
  - Радикальное сокращение потерь от киберинцидентов
- **Задачи**
  - Обнаружение инцидентов
  - Реагирование (локализация и устранение последствий)
  - Улучшение
- **Дополнительно**
  - Быстрая готовность к новым атакам



Время - самый ценный ресурс

- **Сколько можно строить SOC?**
  - ФГУП ххххх России 2 года согласовывала штатку под SOC
  - Внедрение SIEM
    - Проверка технологий
      - Пилотирование решений

      2-6 МЕСЯЦЕВ
    - Выделение бюджета
      - По разному

      + 6 МЕСЯЦЕВ (НА СЛЕДУЮЩИЙ ГОД)
    - Выбор поставщика
      - Конкурс

      + 1-3 МЕСЯЦА
    - Реализация
      - Проект внедрения

      + 3-9 МЕСЯЦЕВ

    Итого: 12-24 месяца

- **Время реагирования на новую атаку**
  - Внедрение нового СрЗИ
  - Примерно столько же – 1-2 года

КЛИЕНТ
РАЗВИТИЕ
УВАЖЕНИЕ
ПРОФЕССИОНАЛИЗМ

WannaCry – 12/05/2017

- **Использованная уязвимость – утечка базы имплантов спецслужб**
  - Закладка в ПО
  - The ShadowsBrokers
- **Появление WannaCry**
  - Вирус-шифровальщик
  - Предположительно разработан в КНДР
  - Самораспространие во внутренней сети
- **Последствия**
  - 126 742 USD – выкуп за расшифрование
  - Основные потери - простои в работе на 1 млрд. USD
- **Пострадали**
  - Железные дороги в Германии
  - Медицинский центр в Великобритании
  - МВД России
  - Автопроизводитель во Франции и многие другие

Мужики пошли выбирать оружие…

- **«Волшебные» таблетки**
  - Резервное копирование
  - Антивирусы
  - Распространение обновлений
  - Межсетевые экраны
  - «Песочницы»
  - Системы обнаружения атак
  - Тесты на проникновение
  - …..

X.Petya – 27/06/2017

- **Использованная уязвимость и схема работы – аналогична WannaCry**
  - Вирус-шифровальщик
  - Уязвимость, закрытая MS несколько месяцев назад
  - Разработчик?
  - Самораспространение во внутренней сети
- **Последствия**
  - Bitcoin-кошелек для выкупа заблокирован
  - Многодневные простои бизнес-процессов
- **Пострадали**
  - Россия
    - Роснефть, Инвитро, Керамма-Маракци, Мегафон…
  - Украина
    - Запорожьеоблэнерго, Аэропорт Харькова, ЧАЭС, Днепроэнерго, Ощадбанк, УкрТелеКом, Киевстар, Новая Почта…
  - Десятки других организаций в других странах

Мониторинг и реагирование на инциденты

- **Мониторинг**
  - Внешний
    - Быстро (~1 месяца)
    - Актуализация правил корреляций под новые атаки
    - Не дорого!

  SIEM+ около 70 млн.руб. (С) Привет Алексею Лукацкому!☺
  ФОТ около 30 млн.руб. в год.

  Аренда 15-30 млн.руб. в год на ту же ИТ-инфраструктуру

- **Реагирование**
  - Внутреннее
    - Быстро (формирование команды ~2-3 месяца)
    - Оперативно и эффективно
    - Не дорого!

    ФОТ около 3-5 млн.руб. в год

КЛИЕНТ
РАЗВИТИЕ
УВАЖЕНИЕ
ПРОФЕССИОНАЛИЗМ

Пилот внешнего SOC

- **Цели**
  - Оценка качества работы
  - Доработка требований к подрядчику
  - Получение аргументов для защиты проекта – обнаружение и реагирование на инциденты
- **Результаты**
  - Много false positive
  - Мало пересечений в срабатываниях
  - Инцидентов не так много, как предполагали☺

КЛИЕНТ
РАЗВИТИЕ
УВАЖЕНИЕ
ПРОФЕССИОНАЛИЗМ

Ждать нельзя. Защитить

Евгений Акимов, директор по кибербезопасности

КАЛАШНИКОВ
КОНЦЕРН