Практические заметки по процессу управления уязвимостями

Проблематика

- Стремительный рост числа выявленных уязвимостей
  - При разработке ПО
    - Акцент на бизнес-ценность при разработке
    - **Отсутствие культуры DevSecOps**
    - Сложности выявления уязвимостей на этапе разработки
      - Инструменты обнаружения — Triage
      - **Зависимости, opensource компоненты и т.п.**
    - **Security by design**
    - **Атаки на цепочки поставок**
  - Из-за геополитической обстановки
    - Недружественные государства и прогосударственные APT — **0-day**
- Triage
  - **Определение трендовых уязвимостей**
  - Определение применимости и актуальности
    - **Наличие рабочего эксплойта**
    - Знание своей ИТ-инфраструктуры
      - **Актуальность данных об активах**
      - **Определение уровня значимости активов**
    - **Актуальная модель угроз и нарушителя**
- Сложности процесса устранения уязвимостей
  - Время на устранение — **Асимметрия ИБ** — Разрушать не строить
  - **Уровень культуры ИБ в ИТ**
  - Уровень коммуникаций между ИБ и ИТ
    - **Ответственность за реализацию**
    - Парадигма о разных целях
- Прочие проблемы
  - **Отсутствие понимания технических деталей эксплуатации уязвимостей со стороны blue team**
  - **Незнание или непонимание техник, тактик и процедур атакующих**

Способы повышения эффективности процесса

- Автоматизация и повышение эффективности процесса управления уязвимостями на всех его этапах
  - Инструменты автоматизации для идентификации и классификации
  - Инструменты автоматизации ИТ
  - Инструменты автоматизации для контроля
- Погружение в технические детали уязвимостей; техники, тактики и процедуры атакующих
  - Обучение по программам Этичный хакинг и т.п.
  - Подписки на чаты, форумы и т.п. ИБ ресурсы
  - Доступ к базам уязвимостей(БДУ ФСТЭК, NVD и т.п.) , MITRE и т.п.
- Митигация рисков эксплуатации
  - Виртуальный патчинг, компенсационные меры
  - Встраивание ИБ в архитектуру ИТ
  - Пентест, CPT, Bug Bounty
- Развитие культуры ИБ
  - Предприятие
    - Осведомленность (не только пользователей, но и ИТ)
      - Корпоративная
      - Персональная
    - Тренинги
    - Инструменты контроля и проверки знаний
  - Поставщики — Требования к ИБ в договоре
- Про ответственность