Реагирование на киберинциденты - с чего начать, чтобы не "утонуть в море событий" и к чему быть готовым при автоматизации реагирования

- Проблематика
  - Человеческие ресурсы
    - Злоумышленники vs Защитники
    - Мотивация
    - Финансовый вопрос
    - Про электровеники и выгорание
  - Процессные вопросы
    - Сложность процессного подхода
      - Бумажная безопасность vs Практическая безопасность
      - Процессы разные нужны, процессы разные важны
  - Разнообразие и количество компьютерных атак
    - Новые угрозы каждый день
    - Автоматизация вредоносного ПО
    - Киберинформационная усталость
- Подходы к решению
  - Реактивный или превентивный подход
  - Секрет про процессы от Капитана "Очевидность"
    - Необходимость формализации или кто знает, как работает Волшебный рубильник
    - Мукулатурный подход
  - Итерационность в процессном подходе
    - Про уровень ИБ-зрелости
    - Немного про модели угроз и нарушителя
      - OSINT и источники угроз
      - Кто знает о моей инфраструктуре и причем здесь Соглашение о неразглашении
    - Управление активами или нужно ли уподобляться бухгалтерам
    - Стоит ли говорить с бизнесом про риски?
    - Управление уязвимостями
      - Обновление и виртуальный патчинг
  - Ранжирование инцидентов в процессе реагирования и вопросы автоматизации реагирования
    - Вопросы автоматизации реагирования применительно к внутренним и внешним инцидентам
    - Так ли страшны превенты
    - Экспертиза от вендоров ИБ решений
      - TI
      - Правила детектирования и сигнатуры
      - Трендовые уязвимости
    - Security Awareness