Практические замечания по организации удаленного доступа к ИТ-сервисам компании. Подходы к оценке, детектированию и реагированию на внешние киберугрозы

- Окружение
  - Злоумышленники vs Защитники
    - Компетенции
    - Использование искуственного интеллекта
    - Мотивация
    - Финансовый аспект
      - Обеспечение ИБ
      - Провайдеры ВПО и сервисов
  - Ландшафт, тренды киберугроз и противодействия им.
    - Полиморфные вирусы, бесфайловые атаки и т.п.
    - Скорость эксплуатации уязвимостей
    - Автоматизация
  - О стереотипах, шаблонах мышления
    - Публичные кейсы и их влияние
    - СЗИ
    - Немного о вендорах СЗИ и провайдерах MSSP
- Проблематика
  - Мониторинг и реагирование 24x7
  - Количество внешних, доступных из вне ИТ-сервисов
    - Каждый внешний сервис - потенциальная угроза безопасности и точка входа для злоумышленника
  - Кто враг и каковы его компетенции?
    - Атаки на цепочки поставок или разговор про доверие
  - Удаленная работа
    - Используемое оборудование, ПО, каналы связи
  - Регуляторка
    - Кто, кому и что должен?
  - Время на операционные задачи
    - ИТ+ИБ или ИТ. ИБ
    - Бумажная и практическая безопасность
  - Квалификация сотрудников ИБ
  - Кибергигиена
- Подходы к решению
  - Реагировать или недопускать - несколько слов про превентивность
  - Про визуализацию
    - Вектора атак
    - Слабые места
  - Критичные активы и системы, трендовые уязвимости
  - Управление временем доступности ИТ-сервисов
  - Управление используемым оборудованием и ПО
  - Принцип необходимости и достаточности
  - VPN и возможна ли жизнь без него?
  - Гранулированный доступ из вне
  - Волшебный рубильник
  - Security Awarness
  - Автоматизация детектирования и реагирования
  - А может, все-таки, попросить о помощи?
  - Про вероятность и управляемость