

Анализ защищенности ИТ-инфраструктуры предприятий



Теория и практика
реализации



Услуги – анализ ИС

Поможем оценить реальный уровень защищенности ваших информационных систем и соблюсти требования регуляторов

Security Assessment



Анализ
защищенности



Red Teaming



AS IS – TO BE



SSDLS



Тестирование
на проникновение



Реагирование
на инциденты



Социотехническое
тестирование

Compliance



Безопасность КИИ



Защита
персональных
данных



Защита ГИС



Кейс «На последней минуте»

Вид деятельности: ИТ-компания

Задачи заказчика:

Крупной ИТ-компании РФ, вышедшей на международный рынок, потребовалось провести внешнее тестирование, анализ защищенности Wi-Fi, социальную инженерию.

Необходимо подготовить отчетную документацию с перечнем рекомендаций и предложений по повышению уровня обеспечения ИБ.

Решение:

Pentest



Кейс «Полный доступ»

Вид деятельности: фармацевтика

Задачи заказчика:

Фармацевтическая компания запросила проверить ИС и WEB ресурсы на предмет уязвимостей, ошибок конфигурации и недостатков механизмов защиты ресурсов информационной инфраструктуры Заказчика после проведенной атаки злоумышленниками.

Необходимо провести анализ внешнего периметра, внутреннего периметра и фишинг атаку.

Решение:

Pentest с противодействием



AS IS – TO BE

Комплексный аудит ИТ/ИБ-инфраструктуры (As Is) и разработкой целевого состояния (To Be)

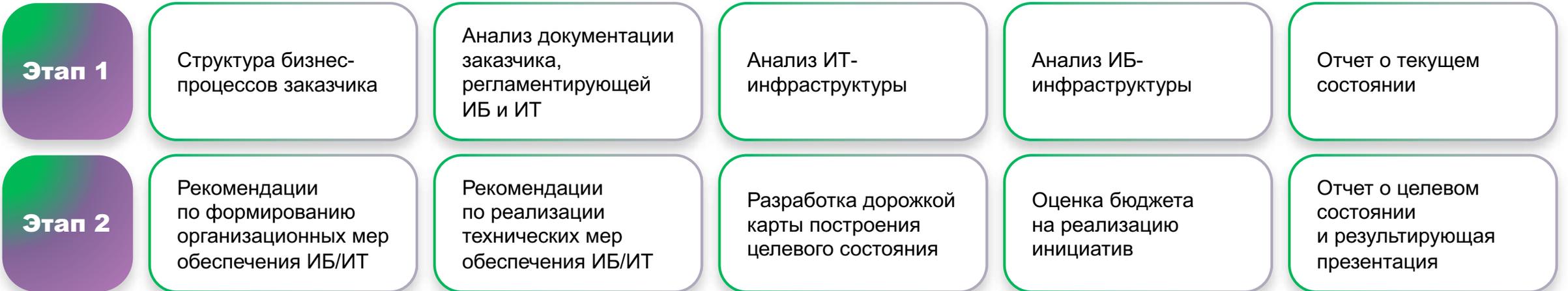
Цели

Целью аудита является определение текущего уровня зрелости ИТ/ИБ-инфраструктуры с дальнейшим формированием перечня инициатив по трансформации ИТ/ИБ заказчика

Результат

- Отчет о текущем состоянии
- Отчет о целевом состоянии
- Презентация: ключевые результаты, дорожные карты построения ИТ/ИБ, перечни и паспорта инициатив

Этапы проекта



Тестирование на проникновение

Поиск критических уязвимостей и оценка возможности злоумышленника продвижения в глубь инфраструктуры

Цели

Определить, может ли текущий уровень защищенности выдержать попытку вторжения потенциального злоумышленника

Выявить критичные уязвимости в инфраструктуре и определить, насколько «глубоко» злоумышленник может проникнуть в системы. Проверить соответствие стандартам безопасности, требующих регулярного анализа защищенности

Результат

Демонстрация возможности фактического проникновения и получения контроля над системой или получения доступа к критической информации

Отчет с описанием выявленных уязвимостей, причастных к векторам атак и рекомендациями по повышению уровня защищенности

Объекты тестирования

Внешний периметр

Внутренний периметр

Мобильные приложения

Сети Wi-Fi

Сотрудники

Бизнес приложения (ERP, CRM)

ДБО



Кейс «Можно попробовать»

Вид деятельности: **Металлургическое производство**

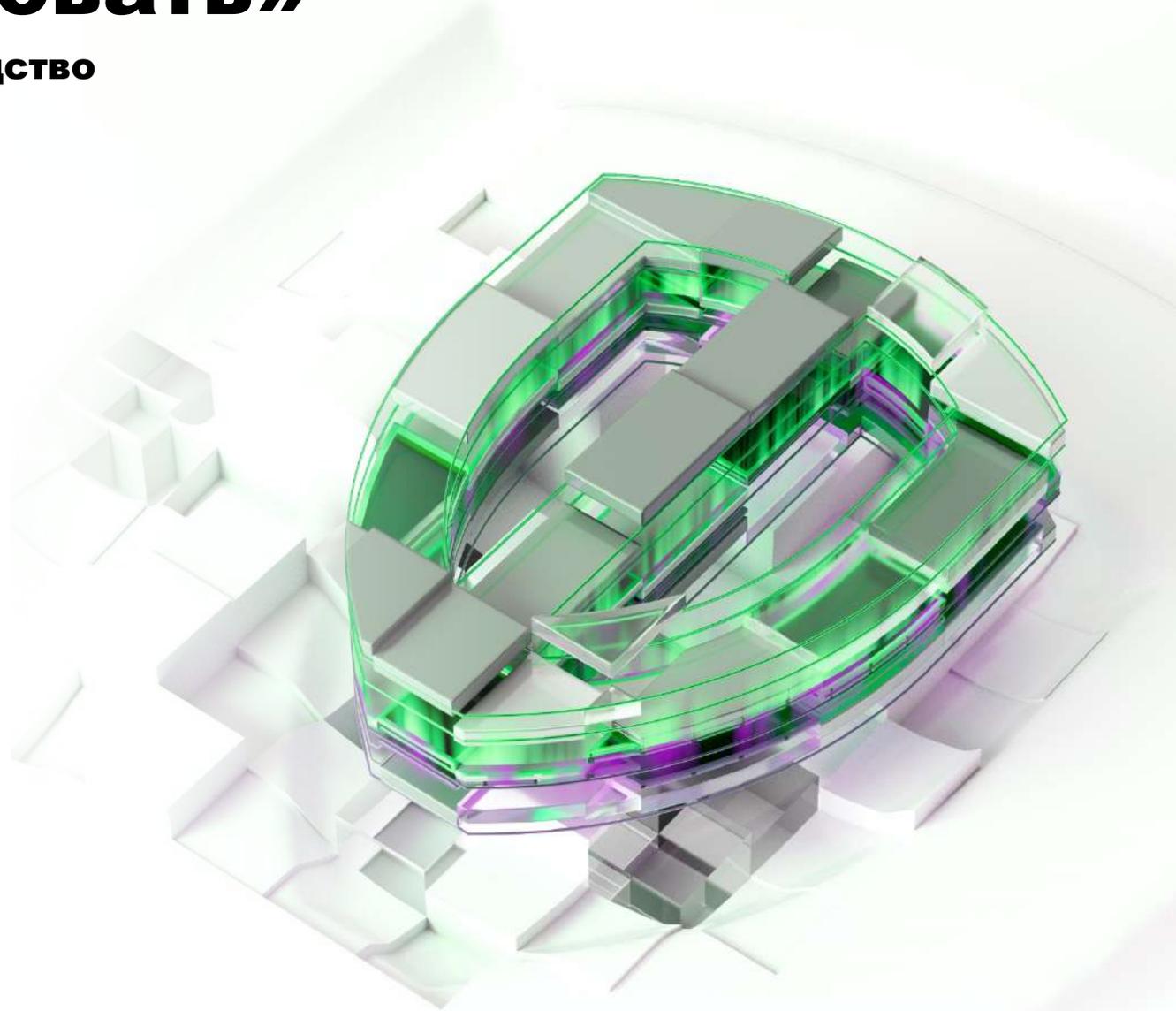
Задачи заказчика:

Металлургическая компания заинтересовалась проведением внешнего тестирования IT инфраструктуры с целью проверки защищенности периметра.

Необходимо подготовить рекомендации по устранению выявленных уязвимостей, исправлению ошибок конфигурации или принятию компенсационных мер защиты.

Решение:

Pentest



Технологии включают бизнес

Александр Шапов

Менеджер по внедрению
цифровых решений