ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

Правила успешного OffSec: взаимодействие заказчика с командой атакующих

Цель наступательного кибербеза — это не просто обнаружение уязвимостей и поиск недостатков в системе информационной безопасности. Основная задача offensive security — это повышение уровня защищенности инфраструктуры компании с помощью оценки и совершенствования существующих процессов ИБ.

Чтобы провести Red Team, Purple Team или любой другой вид наступательной кибербезопасности максимально эффективно, важно конструктивное взаимодействие заказчика и команды исполнителей.

ДЛЯ ЭТОГО НА ЭТАПЕ ПЕРЕГОВОРОВ НЕОБХОДИМО:

01 **Четко поставить цели и задачи,** например:

- реализация недопустимых событий: удаление резервных копий, разглашение конфиденциальной информации
- оценка эффективности процессов ИБ

02 **Определить сроки работ:** например, 30 рабочих дней с момента подписания договора.

03 **Определить границы работ,** например:

- внешний периметр компании
- внутренняя корпоративная сеть
- продуктивная инфраструктура
- беспроводные сети

Также необходимо указать, допустимы ли социотехнические проверки.

04 **Обозначить прозрачные условия завершения работ,** например:

- реализация недопустимых событий
- демонстрация доступа к целевому компоненту инфраструктуры
- обнаружение активности атакующих командой защитников

05 **Совместно с исполнителем составить план мероприятия:** определить порядок и длительность этапов.

06 **Выделить компетентных сотрудников для взаимодействия с командой исполнителей:** согласования проверок, обмена информацией о ходе работ и решения других оперативных задач.

07 **Проинформировать исполнителя, как вы планируете использовать результат работ на практике:** это позволит красной команде корректно расставить акценты при проведении работ и подготовке отчета.

Соблюдение этих простых правил позволит обеспечить слаженное, скоординированное и эффективное сотрудничество исполнителя и заказчика для достижения поставленных целей и получения практических результатов.

Если у вас есть вопросы по анализу защищенности и кибербезопасности, напишите нам!

Мы поможем определить ваши цели и подберем наилучшее решение

sec@ussc.ru

sec.ussc.ru