

# БОЛЬШОЙ РАЗБОР ONE TASK

КАК РЕШАТЬ СТФ-ЗАДАЧИ БЫСТРЕЕ,  
ГЛУБЖЕ И КАЧЕСТВЕННЕЕ

[ О СПИКЕРЕ ]

# НИКИТА КОЛОМИЕЦ



Текущая должность и место работы:

**Старший эксперт по анализу  
защищенности СберТех**



# ЧТО БУДЕТ НА ВЕБИНАРЕ

А)

ЧТО ТАКОЕ ONE TASK

Б)

ПОЧЕМУ CTF ПОЛЕЗЕН БЕЛОМУ  
ХАКЕРУ

В)

КАК ЭКСПЕРТ ПОДХОДИТ  
К ЗАДАЧЕ

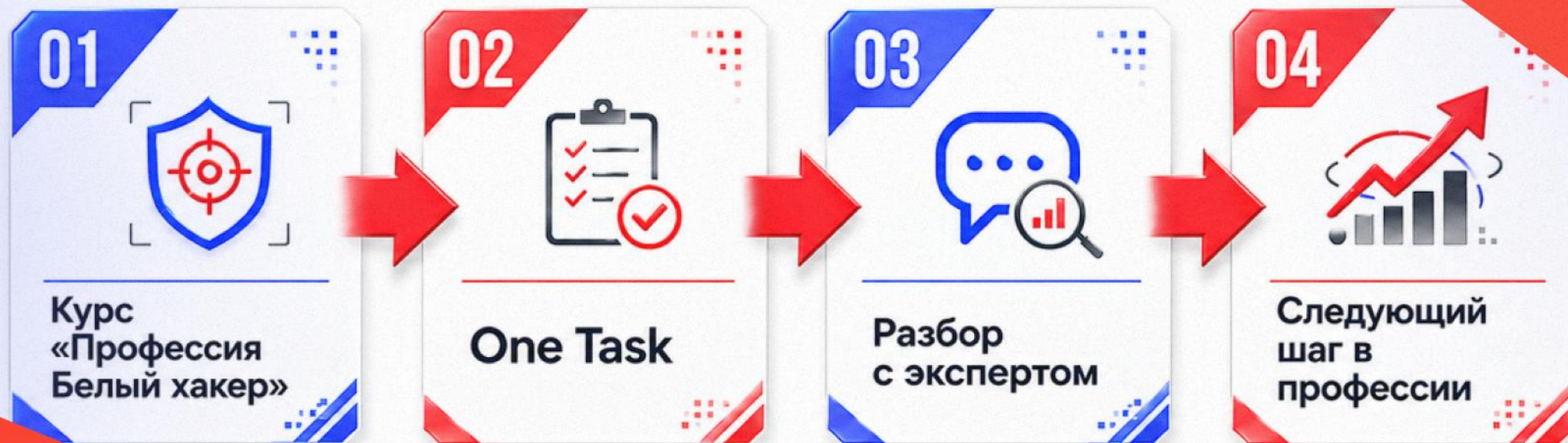
В)

РАЗБОР 3 ТАСКОВ ОТ УСЛОВИЯ  
ДО ФЛАГА



# CYBERED, КУРС “ПРОФЕССИЯ БЕЛЫЙ ХАКЕР И ПРОЕКТ ONE TASK

[ ОТ ТЕОРИИ К РЕГУЛЯРНОЙ ПРАКТИКЕ ]



# ЧТО ТАКОЕ ONE TASK?

Одна CTF-задача каждую неделю

1. Самостоятельное решение

2. Накопились 3 задачи

3. Проходит большой разбор с экспертом



[ Почему CTF — это не просто игра ]

# CTF ТРЕНИРУЕТ МЫШЛЕНИЕ АТАКУЮЩЕГО



анализ вводных



поиск зацепок



проверка гипотез



работа с инструментами



внимание к деталям



умение не застревать



[ Что CTF даёт профессии ]

CyberED

# ЧТО ПЕРЕНОСИТСЯ В РАБОТУ БЕЛОГО ХАКЕРА

## CTF развивает:



разведку



анализ артефактов



поиск слабого места

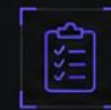


эксплуатацию



работу с неизвестностью

## В профессии нужно добирать:



методологию



отчётность



контекст инфраструктуры



коммуникацию



ответственность

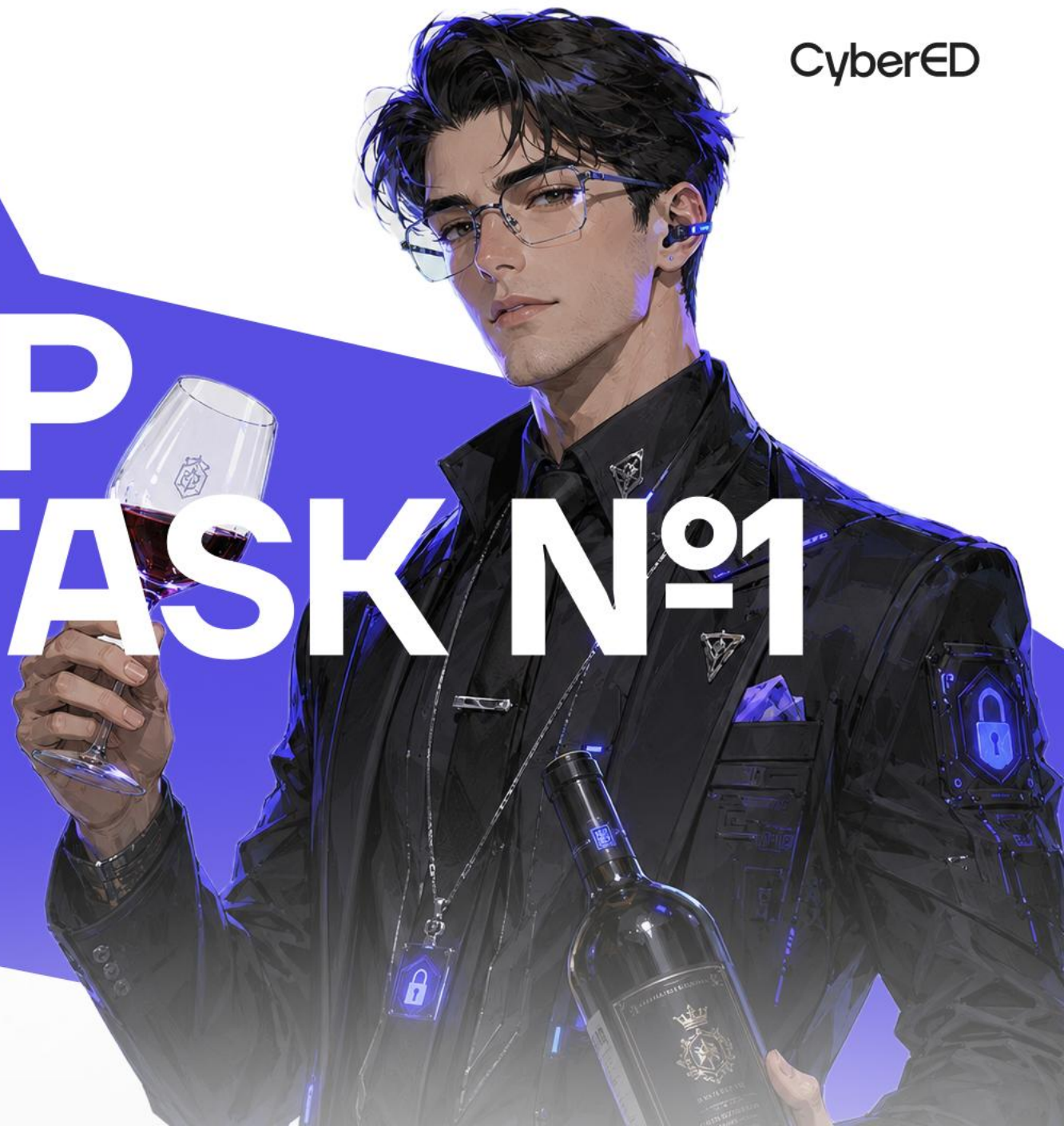


# МЕТОДИКА РЕШЕНИЯ CTF-ЗАДАЧ

- 01 ПРОЧИТАТЬ УСЛОВИЕ И ВЫДЕЛИТЬ ЗАЦЕПКИ.
- 02 ОПРЕДЕЛИТЬ КАТЕГОРИЮ ЗАДАЧИ И ВОЗМОЖНЫЕ КЛАССЫ УЯЗВИМОСТЕЙ.
- 03 СОБРАТЬ МАКСИМУМ ИНФОРМАЦИИ ИЗ ДОСТУПНЫХ АРТЕФАКТОВ.
- 04 СФОРМИРОВАТЬ ПЕРВЫЕ ГИПОТЕЗЫ.
- 05 ПРОВЕРИТЬ БЫСТРЫЕ И ДЕШЕВЫЕ ГИПОТЕЗЫ.
- 06 ЗАФИКСИРОВАТЬ, ЧТО НЕ СРАБОТАЛО.
- 07 УГЛУБИТЬСЯ В САМЫЙ ВЕРОЯТНЫЙ ПУТЬ.
- 08 ПОЛУЧИТЬ РЕЗУЛЬТАТ И ПРОВЕРИТЬ ЕГО.
- 09 СФОРМУЛИРОВАТЬ УНИВЕРСАЛЬНЫЙ ВЫВОД: ЧЕМУ ЭТА ЗАДАЧА УЧИТ И КАК ЭТО СВЯЗАНО С ПРОФЕССИЕЙ.

# РАЗБОР ONE TASK №1

[ЭЛИТНЫЙ СОМЕЛЬЕ]



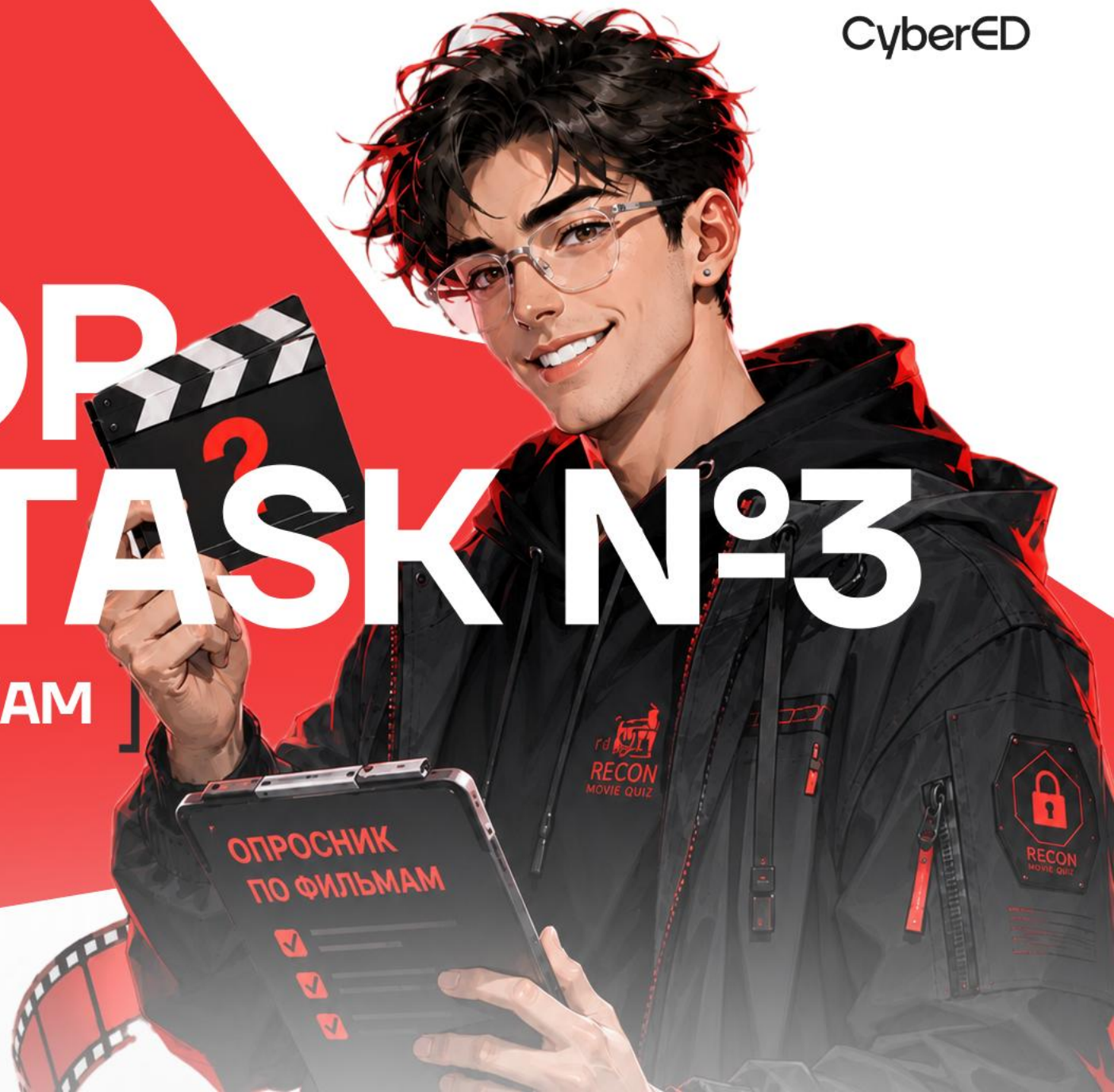
# РАЗБОР ONE TASK №2

[ ШАУРМИЧНАЯ "У ДЖАМШУТА" ]



# РАЗБОР ONE TASK №3

[ОПРОСНИК ПО ФИЛЬМАМ]





**ЗАДАВАЙТЕ  
ВОПРОСЫ  
И ПРЕДЛАГАЙТЕ ОБСУДИТЬ КЕЙСЫ**

# БАТТЛ-КАРТА

САМОСТОЯТЕЛЬНО **vs** С ЭКСПЕРТОМ



Самостоятельно / write-up:

- непонятно, с чего начать
- много ложных гипотез
- легко скопировать, но не понять
- нет обратной связи

x

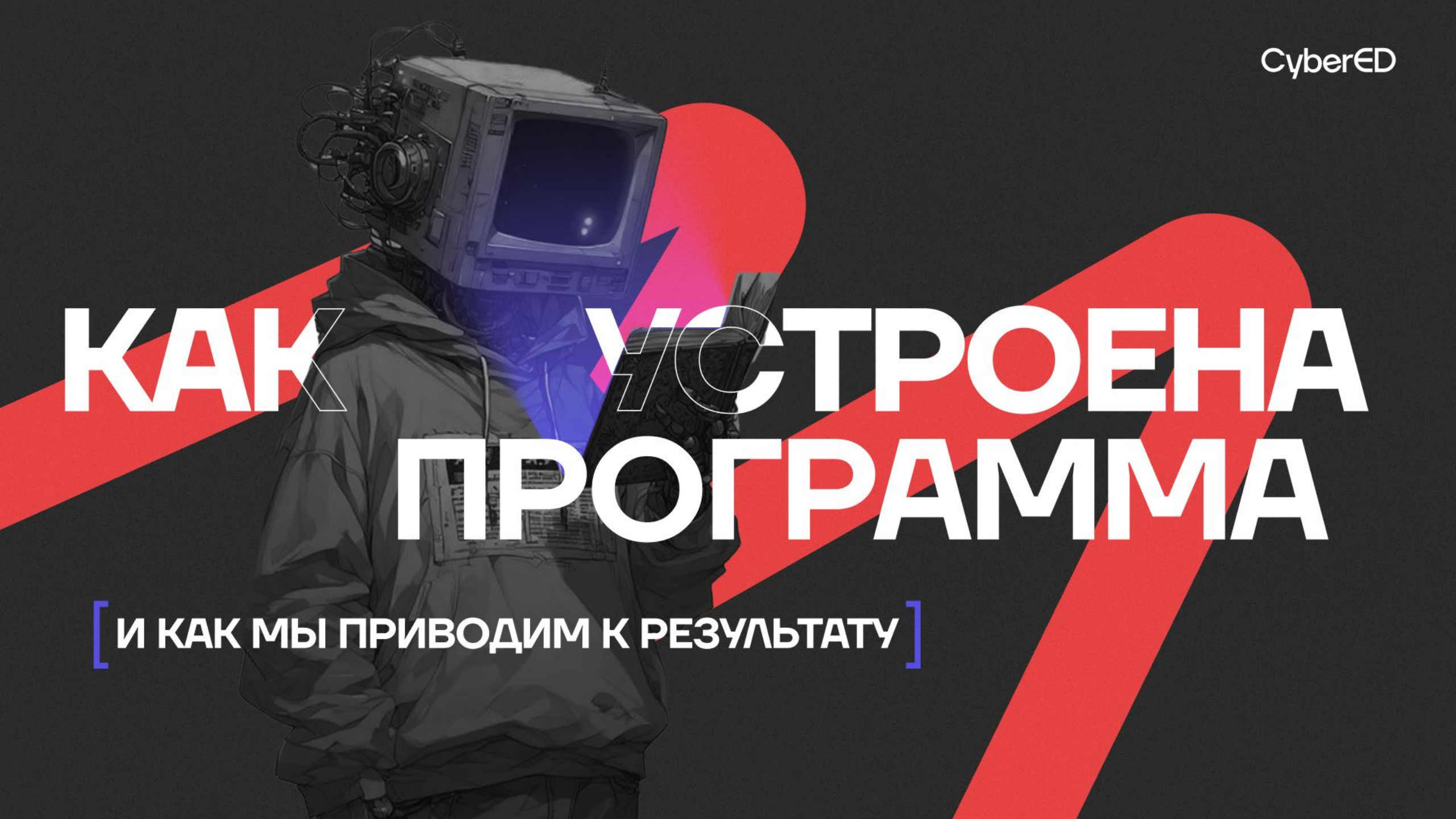


С экспертом CyberED:

- понятная методика
- объяснение логики
- разбор тупиков
- перенос навыка на новые задачи

**VS**





# КАК УСТРОЕНА ПРОГРАММА

[ И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ ]

## Этап 1. Разведка

Модуль 1. Исследование целей тестирования (Reconnaissance)

+

Модуль 2. Получение первичного доступа через атаки на аутентификацию (Authentication)

+

Модуль 3. Получение первичного доступа через атаки на веб-приложения

+

Модуль 4. Получение первичного доступа через атаки социальной инженерии

+

## Этап 2. Получение первоначального доступа

Модуль 5. Эксплуатации известных уязвимостей

+

## Этап 3. Повышение привилегий/закрепление

Модуль 6. Повышение привилегий в Linux

+

Модуль 7. Повышение привилегий в контейнерных средах

+

Модуль 8. Повышение привилегий в Windows

+

## Этап 4. Боковое перемещение в сети

Модуль 9. Проброс сетевого трафика (Pivoting)

+

Модуль 10. Проведение атак на локальные сети

+

Модуль 11. Проведение атак на Active Directory

+

## Этап 5. Получение импакта

Модуль 12. Написание отчета

+

Дополнительный модуль. Оценка устойчивости средств защиты

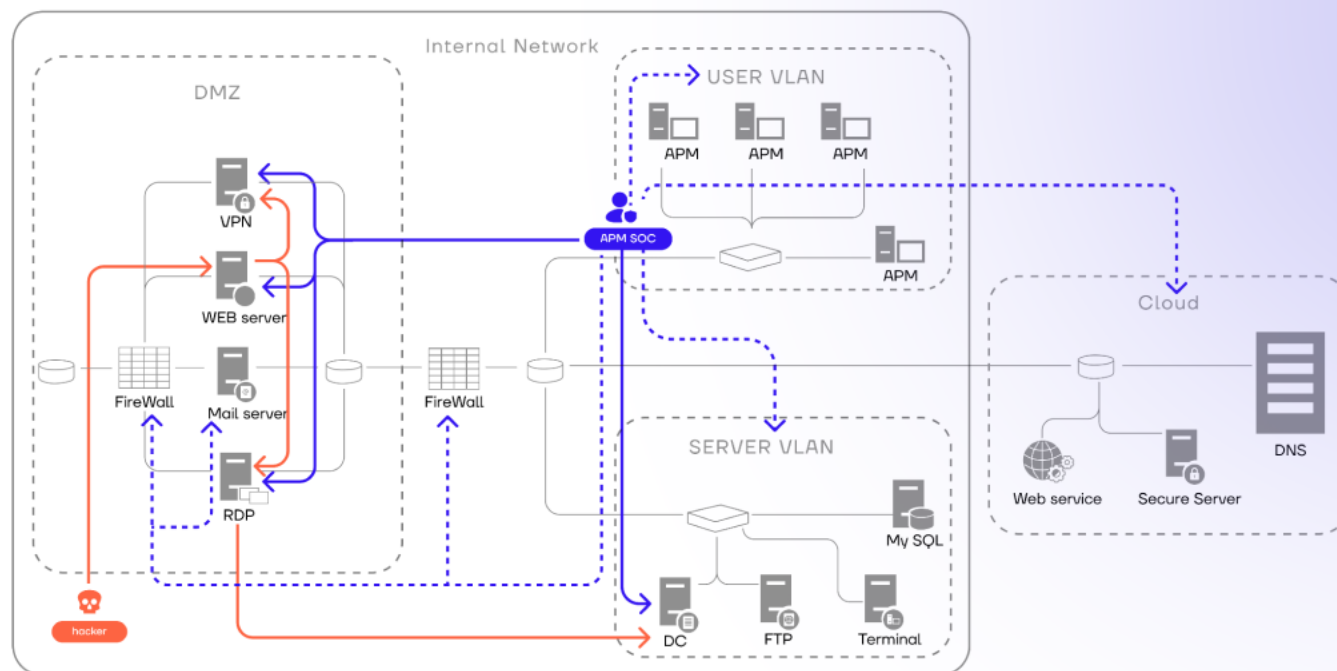
+

Встречи с экспертами по развитию своего профессионального трека: 5 встреч, 20 ак.ч.

CyberED

# ТЕМЫ МОДУЛЕЙ

**ЭТО ГОТОВЫЙ ПЛАН ВЫПОЛНЕНИЯ  
ВСЕЙ ЦЕПОЧКИ АТАКИ В КОМПАНИЯХ**



[ КАК МЫ ДОВОДИМ ТЕМУ ]

# ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

Формат: асинхрон + live разбор



## ПРОХОДИШЬ ТЕОРИЮ САМ

+ разбираешь с наставником



## ВСТРЕЧА С ЭКСПЕРТОМ

- + ответы на вопросы по практике
- + углубление
- + дополнительные техники

Формат помогает понять материал и сформировать навык, а **не** просто посмотреть материал.

ЭТО **НЕ**

«ПОСМОТРЕЛ И ПОШЁЛ ДАЛЬШЕ»

ЭТО

«РАЗОБРАЛ, ДОКРУТИЛ, ПОНЯЛ, ГДЕ **ОШИБСЯ**»

[ КАК МЫ ДОВОДИМ ТЕМУ ]

# ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

КАЖДАЯ ТЕХНИКА

= ОТДЕЛЬНЫЙ СКИЛЛ

= ОТДЕЛЬНАЯ ПРАКТИКА

- 1–2 задачи на ⚠️ каждую технику
- от 1 до 3 уровня сложности
- 3й уровень - на 🏠 киберполигоне

Не «один раз попробовал»

→ а закрепление через повторение

- 120+ техник (скиллов) для пентеста из MITRE ATT&CK и от архитекторов программы

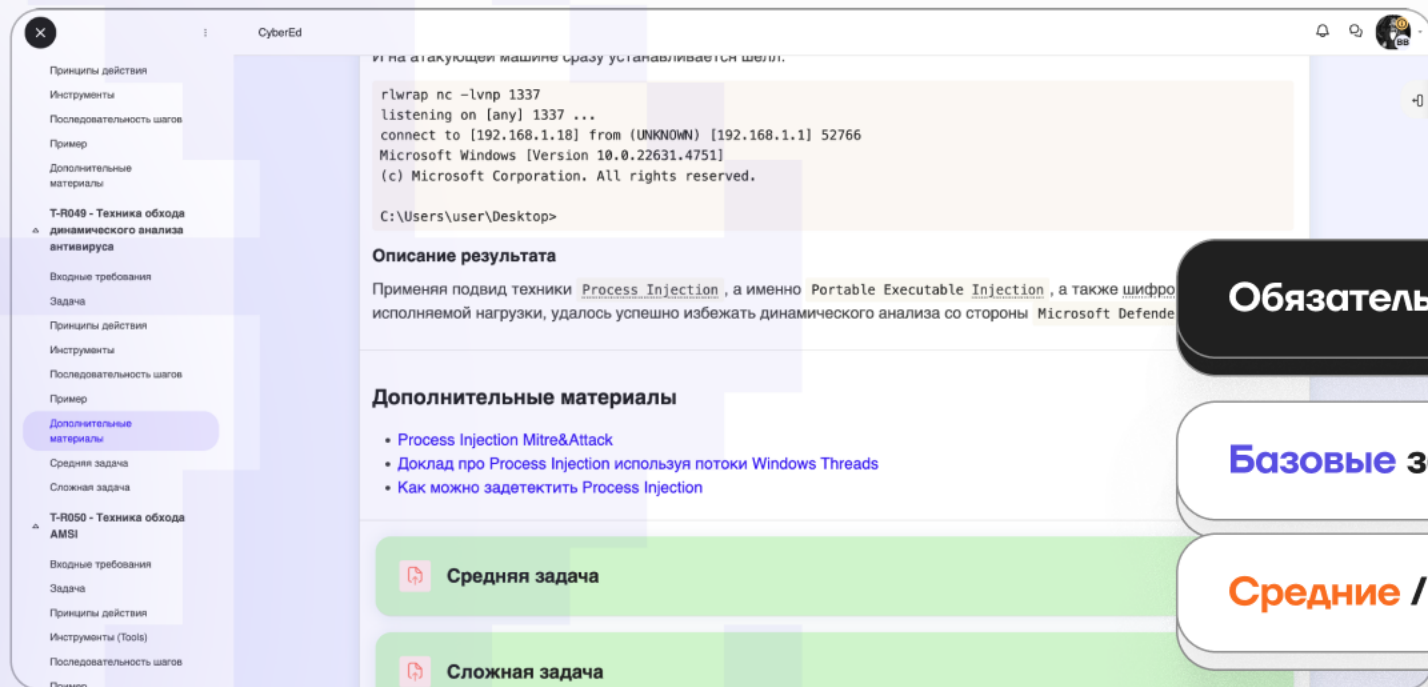
| MITRE ATT&CK                                                                              |                                   |                                                       |                                                    |                                                                 |                                                              |                                                    |                                                     |                                           |                                                     |  |
|-------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------|-------------------------------------------|-----------------------------------------------------|--|
| Матрицы Тактика Методы Защитные сооружения CTI Ресурсы Благотворители Способствовать Блог |                                   |                                                       |                                                    |                                                                 |                                                              |                                                    |                                                     |                                           |                                                     |  |
| Поиск Q                                                                                   |                                   |                                                       |                                                    |                                                                 |                                                              |                                                    |                                                     |                                           |                                                     |  |
| Разведка                                                                                  | Разработка ресурсов               | Первоначальный доступ                                 | Исполнение                                         | Упорство                                                        | Повышение привилегий                                         | Оборонительное уклонение                           | Доступ по учетным данным                            | Открытие                                  | Боковое движение                                    |  |
| 11 техник                                                                                 | 8 техник                          | 11 техник                                             | 17 техник                                          | 23 техники                                                      | 14 техник                                                    | 47 методов                                         | 17 техник                                           | 34 техники                                | 9 техник                                            |  |
| Активное сканирование (1)                                                                 | Получить доступ                   | Вставка контента                                      | Команда администрирования облака                   | Манипулирование учетной записью (7)                             | Механизм контроля за повышением уровня насилия (5)           | Механизм контроля за повышением уровня насилия (5) | Противник посредник (4)                             | Обнаружение учетных записей (4)           | Использование удаленных сервисов                    |  |
| Соберите информацию о пострадавшем хозяине (4)                                            | Приобретение инфраструктуры (8)   | Компромисс проеда                                     | Интерпретатор команд и скриптов (18)               | Вакансии в BITS                                                 | Манипулирование токенами доступа (5)                         | Манипулирование токенами доступа (5)               | Грубая сила (4)                                     | Обнаружение информации в браузере         | Внутренний фишинг                                   |  |
| Соберите информацию о личности жертвы (3)                                                 | Компромиссные счета (3)           | Использование уязвимостей в общедоступных приложениях | Команда управления контейнерами                    | Выполнение автозапуска при загрузке или входе в систему (14)    | Манипулирование учетной записью (7)                          | Вакансии в BITS                                    | Учетные данные из хранилища паролей (6)             | Обнаружение облачной инфраструктуры       | Боковая передача инструмента                        |  |
| Соберите информацию о сети жертвы (8)                                                     | Компромиссная инфраструктура (5)  | Внешние удаленные сервисы                             | Развернуть контейнер                               | Сценарии инициализации загрузки или входа в систему (5)         | Выполнение автозапуска при загрузке или входе в систему (14) | Создание образа на хосте                           | Эксплуатация для получения доступа к учетным данным | Панель управления облачными сервисами     | Перехват сеанса удаленной службы (2)                |  |
| Соберите информацию об организационных жертвах (4)                                        | Развитие потенциала (4)           | Дополнительные аппаратные средства                    | Команда администрирования ESX                      | Интеграция облачных приложений                                  | Сценарии инициализации загрузки или входа в систему (5)      | Отложенное исполнение                              | Подделка веб-учетных данных (2)                     | Обнаружение облачных сервисов             | Размножение с помощью съемных носителей             |  |
| Соберите информацию об организационных жертвах (4)                                        | Создание счетов (3)               | Фидбинг (4)                                           | Эксплуатация для исполнения клиентскими операциями | Компрометировать доверенный файл программного обеспечения хоста | Создание или изменение системного процесса (5)               | Деобфускация/декодирование файлов или информации   | Захват ввода (4)                                    | Обнаружение объектов в облачном хранилище | Инструменты развертывания программного обеспечения  |  |
| Фидбинг информации (4)                                                                    | Получить возможности (7)          | Размножение с помощью съемных носителей               | Ввод входных данных                                | Создать аккаунт (3)                                             | Создание или изменение системного процесса (5)               | Развернуть контейнер                               | Изменение процесса аутентификации (5)               | Обнаружение контента и ресурсов           | Загрязнение общего контента                         |  |
| Поиск в закрытых источниках (2)                                                           | Возможности сцен (4)              | Компромисс в цепочке поставок (3)                     | Межпроцессная коммуникация (3)                     | Создание или изменение системного процесса (5)                  | Изменение политики домена или арендатора (2)                 | Прямой доступ к тому                               | Перевод многофакторной аутентификации (5)           | Обход отладчика                           | Используйте альтернативные материалы аутентификации |  |
| Поиск в открытых технических базах данных (5)                                             | Действительные учетные записи (4) | Доверительные отношения                               | Нативный API                                       | Выполнение, инициированное событием (18)                        | Побег к хосту                                                | Изменение политики электронной почты               | Генерация запроса на аутентификацию                 | Обнаружение                               |                                                     |  |
| Поиск                                                                                     | Сети Wi-Fi                        | Запланированная                                       |                                                    |                                                                 |                                                              |                                                    |                                                     |                                           |                                                     |  |

Матрица ATT&CK – всемирно признанная карта действий хакеров, основанная на реальных атаках.

[ КАК МЫ ДОВОДИМ ТЕМУ ]

# ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

ПРОГРАММУ МОЖНО ОСВАИВАТЬ  
ДО УРОВНЯ **СЛОЖНОСТИ**,  
→ КОТОРЫЙ ПОТЯНЕШЬ



■ Встроенная система давления на результат → Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

# ИНДИВИДУАЛЬНЫЙ СТЕНД ПОД КАЖДОГО

КАЖДОМУ СТУДЕНТУ ПОДНИМАЕТСЯ  
→ СВОЯ ИНФРАСТРУКТУРА

01 

Ты не зависишь от других

02 

Никто не «сломал всё за тебя»

03 

Можно спокойно копать и ошибаться

04 

Доступ 24/7 к машинам



# ПРАКТИКА, БЛИЗКАЯ К BUG BOUNTY / РЕАЛЬНОЙ РАБОТЕ

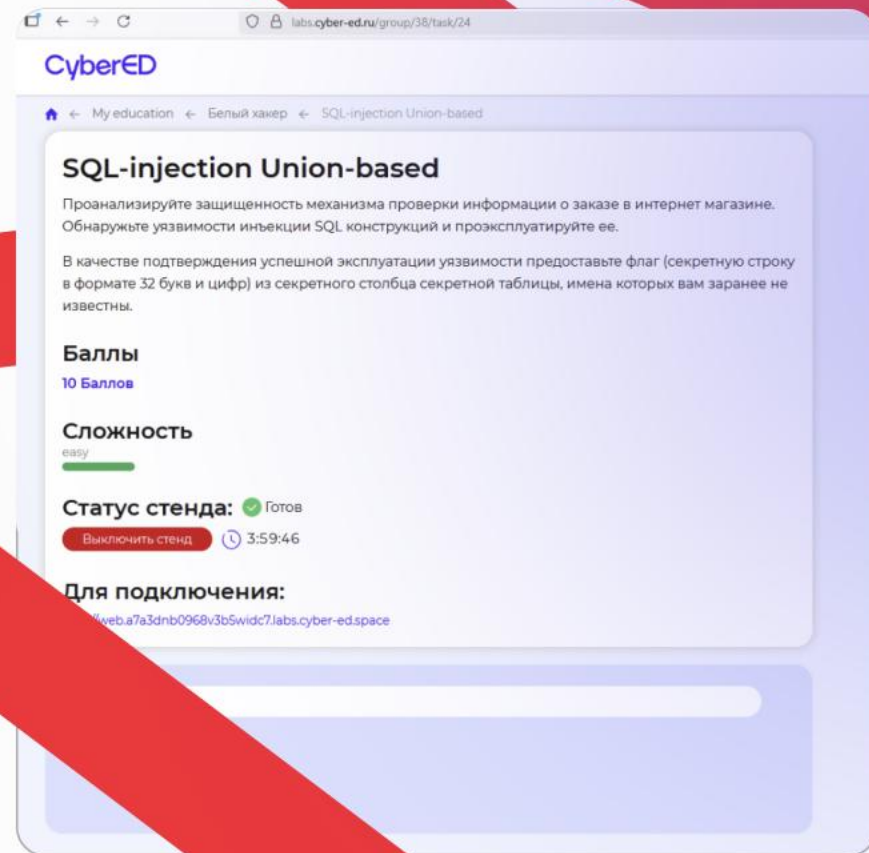
ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ ⚡



Ты **не** «решаешь тест»



Ты работаешь в инфраструктуре  
и получаешь **результат** ⚡ (флаг)



# ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



## СНАЧАЛА

Ты знаешь, какую  
технику применять



## ПОТОМ

Тебе дают инфраструктуру  
→ Сам разбирайся

Не изолированные упражнения, а **связанный процесс**

# ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



РАЗВЕДКА



ПОЛУЧЕНИЕ ПЕРВОНАЧАЛЬНОГО ДОСТУПА



БОКОВОЕ ПЕРЕМЕЩЕНИЕ



ЗАКРЕПЛЕНИЕ



ПОЛУЧЕНИЕ ИМПАКТА



ОТЧЁТ

ФОРМИРУЕТСЯ  
МЫШЛЕНИЕ АТАКУЮЩЕГО

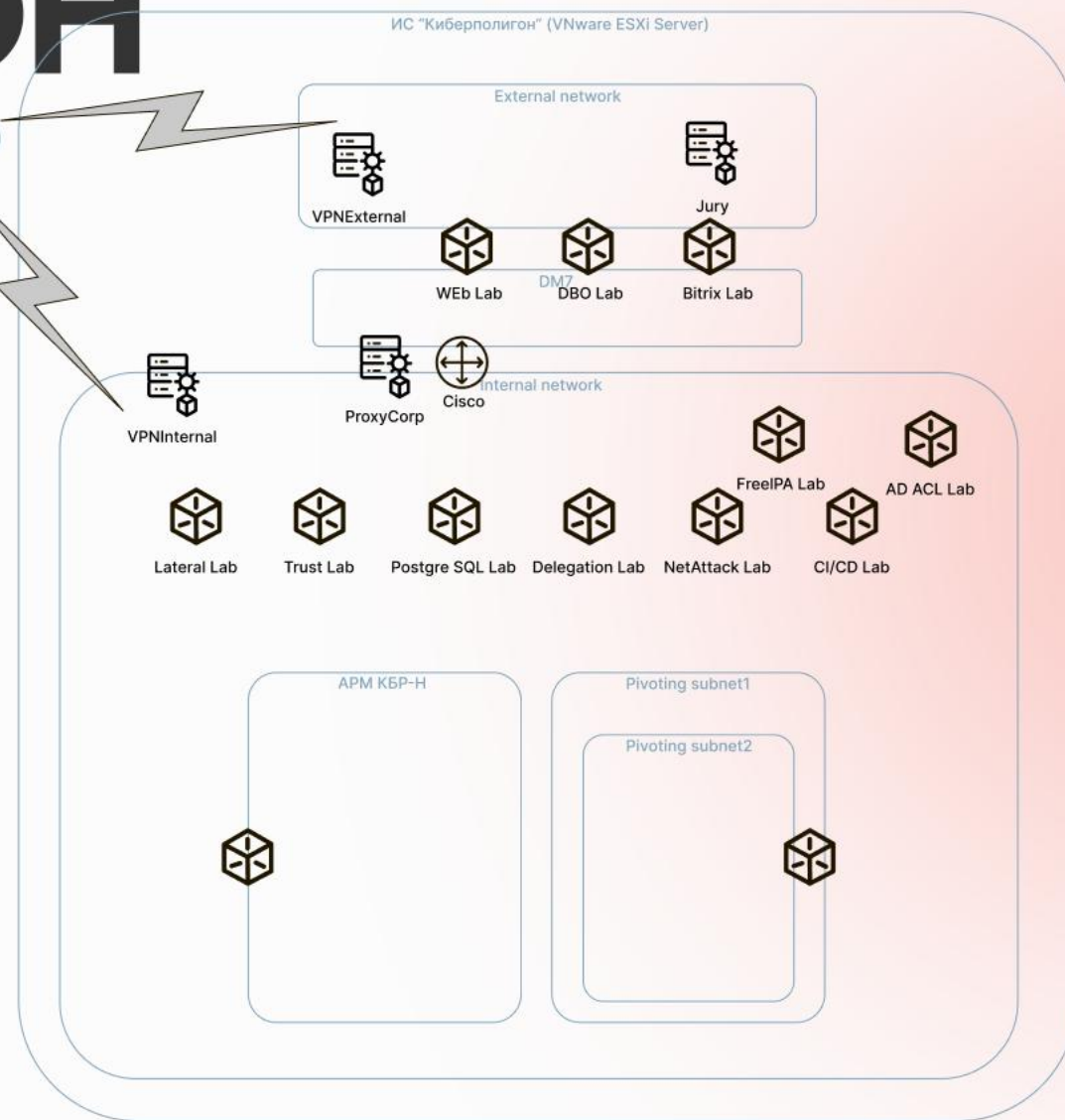
# КИБЕРПОЛИГОН

\*\*\* CyberED

- ▶ Имитация инфраструктуры компании
- ▶ Цепочки атак
- ▶ Нет подсказок, **нет** «правильного пути»

Максимально близко к работе:

« **ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ** »



# КИБЕРПОЛИГОН

## \*\*\* CyberED

6

Цепочек

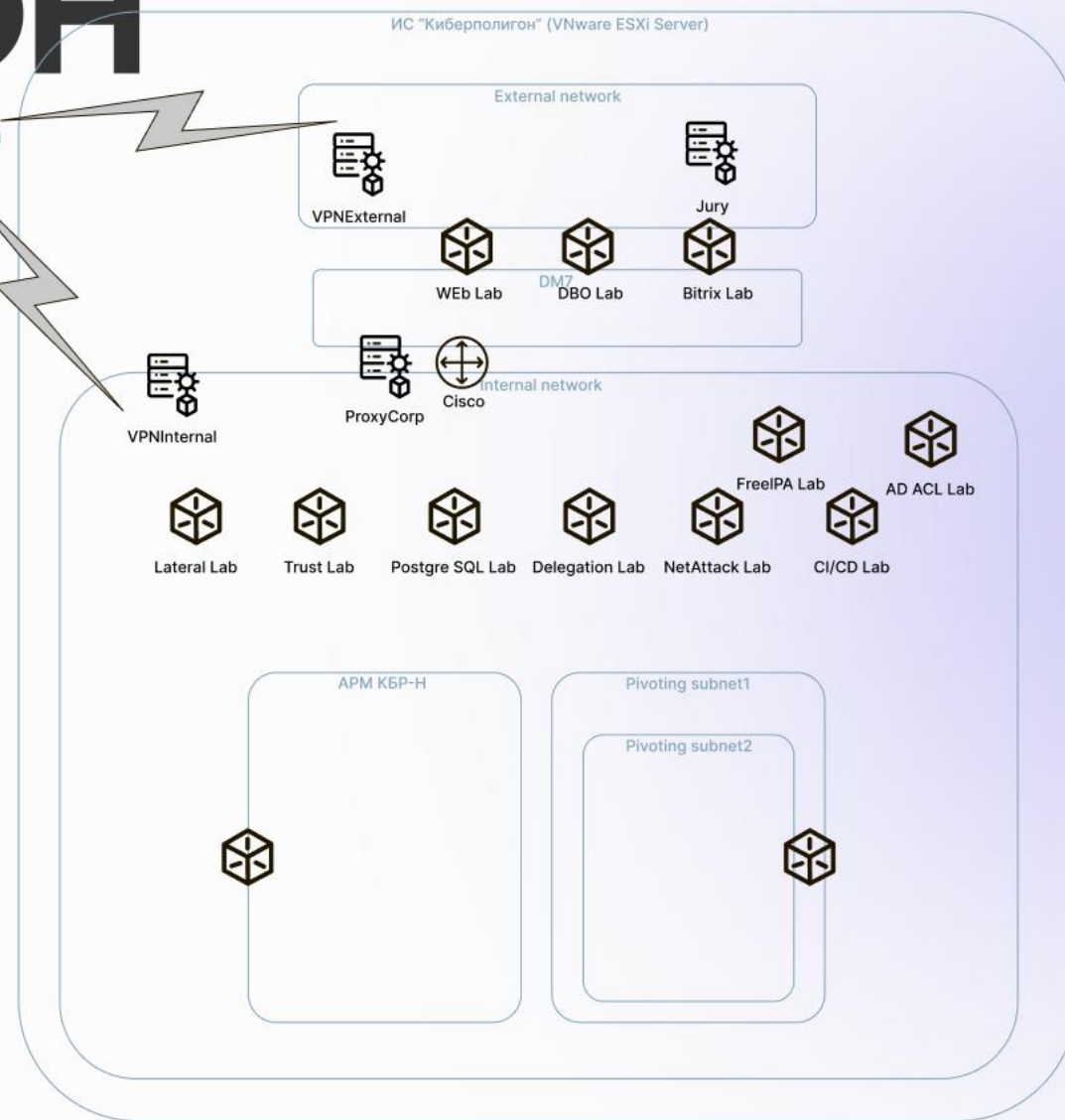
18

Задач

## ЗАДАЧИ

- ▶ атаки на операционные системы (Windows, Linux),
- ▶ веб
- ▶ сетевые атаки.

- + Нарбатываете насмотренность по сценариям атак
- + Сталкиваетесь с вариативностью уязвимостей



# УКАЖЕТЕ В РЕЗЮМЕ КОНКРЕТНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

 **Не так:** умею применять BurpSuite - X

 **А так:** нашел уязвимость path traversal в таком-то сервисе, используя инструмент BurpSuite, эксплуатировал данную уязвимость и получил учетные данные для последующей компрометации инфраструктуры Заказчика - Y.

 **Не так:** умение работать в среде Active Directory - X

 **А так:** реализовал цепочку атаки до компрометации AD и захвата инфраструктуры с помощью обнаруженной уязвимости в центре сертификации - Y.

## ПРИМЕР 1

 **Не так:** умею сканировать порты и подбирать пароли.

 **Так:** обнаружил открытый порт 3389 на непубличном хосте, осуществил подбор пароля для учётной записи локального администратора через RDP, получил shell и развернул прокси для дальнейшего движения по внутренней сети Заказчика.

## ПРИМЕР 2

 **Не так:** знаю Docker и Kubernetes.

 **Так:** через уязвимость в конфигурации GitLab CI (незащищенные переменные окружения) получил токен доступа к приватному registry, внедрил вредоносный образ, извлёк секреты production-окружения и достиг компрометации оркестратора кластера.

## Карта компетенций

🔗 Поделиться

Аналитик Центра противодействия кибератакам

Аналитик SOC. Демо-курс 29 / 100

Обнаружение агрессивного на стадии  
работы с периметром 9 / 80

Пентестер (Penetration Testing Specialist)

Цели исследования 0 / 0

Атаки в локальных сетях 0 / 0

Получение первичного доступа через  
механизм аутентификации 0 / 0

## Общие показатели по направлениям



35%

Red



66%

Blue



24%

AppSec



24%

Fundamentals

Модуль: Не выбрано ▾

☐ Скрыть неосвоенные

Аналитик SOC. Демо-курс

R301 - MOA

Техника обнаружения аномальных активностей в  
локальных сетях и работе рабочих станций через

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - MOA

Форензика

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - MOA

Аудит безопасности

Базовый 3/3 Средний 3/3 Продвинутый 3/3

# КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

## КАЖДАЯ ЗАДАЧА → ЗАКРЫВАЕТ НАВЫК

УРОВЕНЬ: **БАЗОВЫЙ** / **СРЕДНИЙ** / **СЛОЖНЫЙ**

■ Видно, что ты  
реально умеешь

■ Не «написал в CV»  
а подтвердил

## Карта компетенций

🔗 Поделиться

Аналитик Центра противодействия кибератакам

Аналитик SOC. Демо-курс 29 / 100

Обнаружение агрессивного на стадии  
работы с периметром 9 / 80

Пентестер (Penetration Testing Specialist)

Цели исследования 0 / 0

Атаки в локальных сетях 0 / 0

Получение первичного доступа через  
механизм аутентификации 0 / 0

## Общие показатели по направлениям



35%

Red



66%

Blue



24%

AppSec



24%

Fundamentals

Модуль: Не выбрано ▾

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс

R301 - MOA

Техника обнаружения аномальных активностей в  
локальных сетях с помощью рабочих станций через

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - MOA

Форензика

Базовый 3/3 Средний 3/3 Продвинутый 3/3

R301 - MOA

Аудит безопасности

Базовый 3/3 Средний 3/3 Продвинутый 3/3

# КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

■ Это уже не обучение,  
это **переход к найму**

ДАВАЙТЕ РАЗБЕРЕМ  
ВАШИ   
ВОПРОСЫ



# СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ



для участников  
вебинара

**Атаки на Active  
Directory**

за ~~65 900~~ рублей

**+ 10% скидка**

для тех, кто посетил вебинар

**ИТОГО: 59 900 рублей**

для участников  
вебинара

**Пентестер + AI-усиленный пентест**  
синхронный

или

**Пентестер + Атаки на Active Directory**  
синхронный

**за 165 000 рублей**

Скидка 25%

для участников  
вебинара

**Пентестер + AI-усиленный пентест**  
асинхронный

или

**Пентестер + Атаки на Active Directory**  
асинхронный

**за 111 000 рублей**

Скидка 25%

**ОСТАВЛЯЙ ЗАЯВКУ!**



**УСПЕЙ КУПИТЬ ПО ВЫГОДНОЙ ЦЕНЕ ДО КОНЦА МАЯ!**