

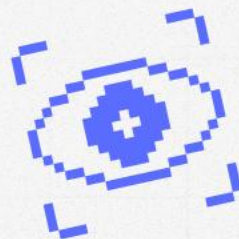
КАК ВЫБРАТЬ СВОЙ ТРЕК ОБУЧЕНИЯ
И НЕ ПОТЕРЯТЬСЯ В ИБ

CyberED

CYBERED В КАРТЕ КОМПЕТЕНЦИЙ



[О СПИКЕРЕ]



CyberED

КУЛАКОВ АЗАМАТ

■ КЛЮЧЕВЫЕ НАВЫКИ:

ВНЕШНИЙ ПЕНТЕСТ

РЕДТИМИНГ

OFFENSIVE SECURITY

OSINT

THREAT INTELLIGENCE

■ ОПЫТ РАБОТЫ:

ГОССЛУБЖБА С 2018 ГОДА - СПЕЦИАЛИСТ ПО
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



CyberED —

CyberED



**НИШЕВАЯ ПЛАТФОРМА
ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ.**

7 лет

обучаем на практике
у лучших экспертов в России

20 +

образовательных
программ по ИБ

5000 +

выпускников

200+

корпоративных клиентов

50+

преподавателей-практиков

80 +

лабораторных стендов

КАРТА НАПРАВЛЕНИЙ

[В КИБЕРБЕЗОПАСНОСТИ]



BLUE TEAM

Защита систем от атак, мониторинг и реагирование на инциденты.

■ Тип мышления:
аналитический, с фокусом на расследование.

■ Верхние роли:

Аналитик SOC

Incident Responder / DFIR

Аналитик киберугроз

Аналитик BPO

INFRA SEC

Обеспечение безопасности IT-инфраструктуры, включая сети, серверы и операционные системы.

■ Тип мышления:
технический, системный.

■ Верхние роли:

Инженер по безопасности инфраструктуры

Сетевой инженер безопасности



Кибербезопасность —
это не набор направлений.

Это цикл защиты, в котором у каждой роли есть своё место и своя функция. Вам важно понять, какие проблемы/боли вам интереснее решать.

APP SEC

Безопасная разработка и тестирование приложений.

■ Тип мышления:
креативный и технический, с акцентом на анализ кода.

■ Верхние роли:

AppSec-инженер

Специалист по анализу кода

Аналитик по безопасности приложений

DevSecOps

RED TEAM

Имитация кибератак для тестирования систем на проникновение и оценки уязвимостей.

■ Тип мышления:
творческий, наступательный.

■ Верхние роли:

Внешний пентест

Red Teaming

Внутренний пентест

Исследование уязвимостей

GRC / ARCH

Проектирование архитектуры безопасности, управление рисками и обеспечение соответствия нормам.

■ Тип мышления:
стратегический, управленческий.

■ Верхние роли:

Управление рисками

Архитектор безопасности

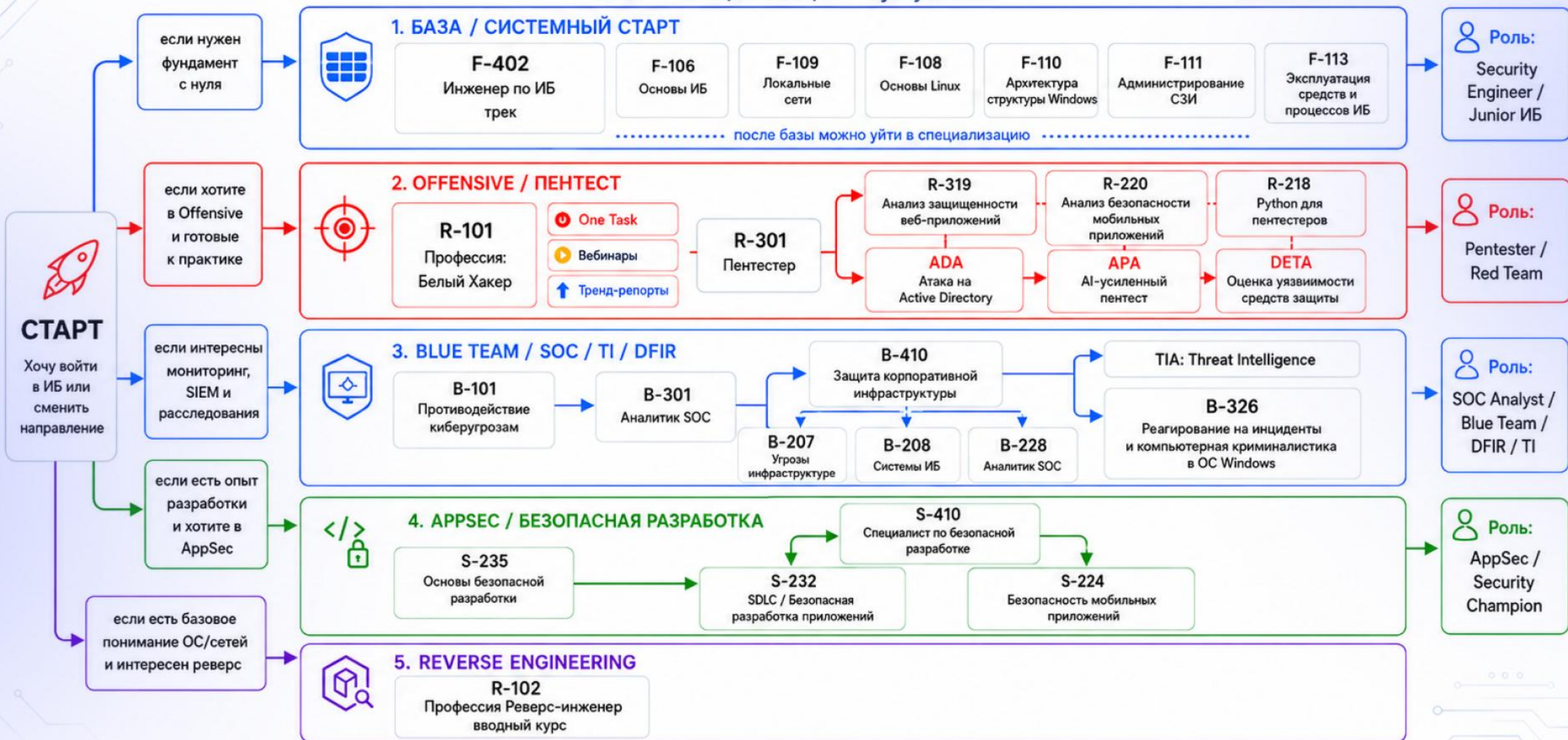
Безопасность поставщиков

Аудитор

КАРТА КУРСОВ

CyberED

База → специализация → углубление



ИЮНЬСКИЕ ЗАПУСКИ

В ИЮНЕ ЗАПУСКАЮТСЯ КУРСЫ И МОДУЛИ ДЛЯ РАЗНЫХ НАПРАВЛЕНИЙ:



OFFENSIVE / RED TEAM

R-301-M10 04 ИЮНЯ

ПРОБРОС СЕТЕВОГО ТРАФИКА

R-301-M7 11 ИЮНЯ

ПОВЫШЕНИЕ ПРИВИЛЕГИЙ В LINUX

R-301-M11 11 ИЮНЯ

АТАКИ НА ЛОКАЛЬНЫЕ СЕТИ

APA 16 ИЮНЯ

AI В ПЕНТЕСТЕ

R-301-M12 18 ИЮНЯ

АТАКИ НА ACTIVE DIRECTORY

ADA 22 ИЮНЯ

АТАКИ НА ACTIVE DIRECTORY

R-301-GM2 11 ИЮНЯ

ПОВЫШЕНИЕ ПРИВИЛЕГИЙ В
ОПЕРАЦИОННЫХ СИСТЕМАХ

R-301-GM3 11 ИЮНЯ

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ
ЛОКАЛЬНЫХ СЕТЕЙ КОМПАНИЙ



BLUE TEAM / SOC

B-301 24 ИЮНЯ

АНАЛИТИК ЦЕНТРА ПРОТИВОДЕЙСТВИЯ
КИБЕРАТАКАМ

B-301-M3 25 ИЮНЯ

ОБНАРУЖЕНИЕ АТАК НА ДОМЕННУЮ
ИНФРАСТРУКТУРУ WINDOWS AD



APPSEC

S-224 19 ИЮНЯ

БЕЗОПАСНОСТЬ ОКРУЖЕНИЯ
ПРИЛОЖЕНИЙ



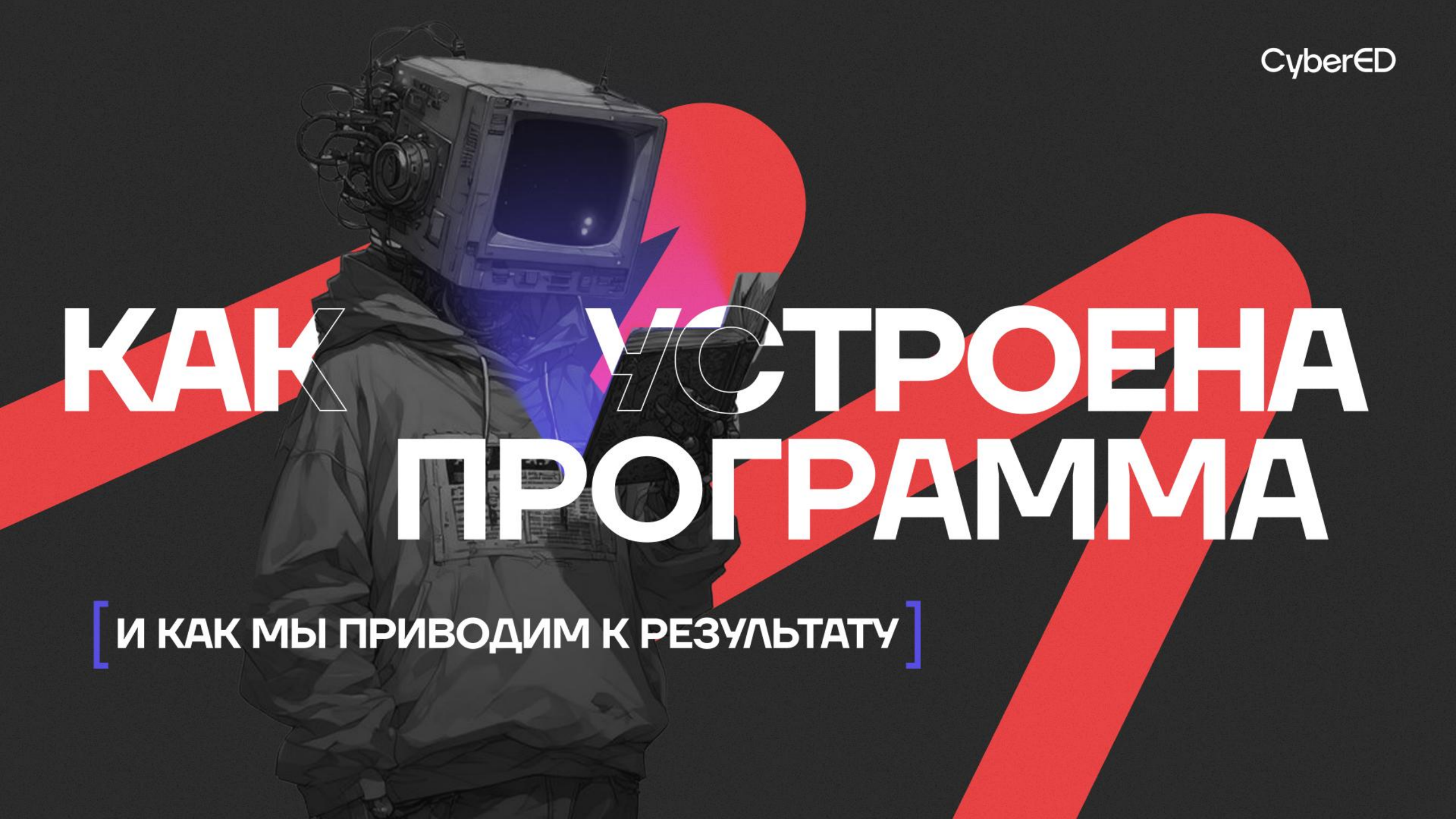
INFRA / BASE

F-110 29 ИЮНЯ

ДОМЕННАЯ СТРУКТУРА
WINDOWS

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ





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

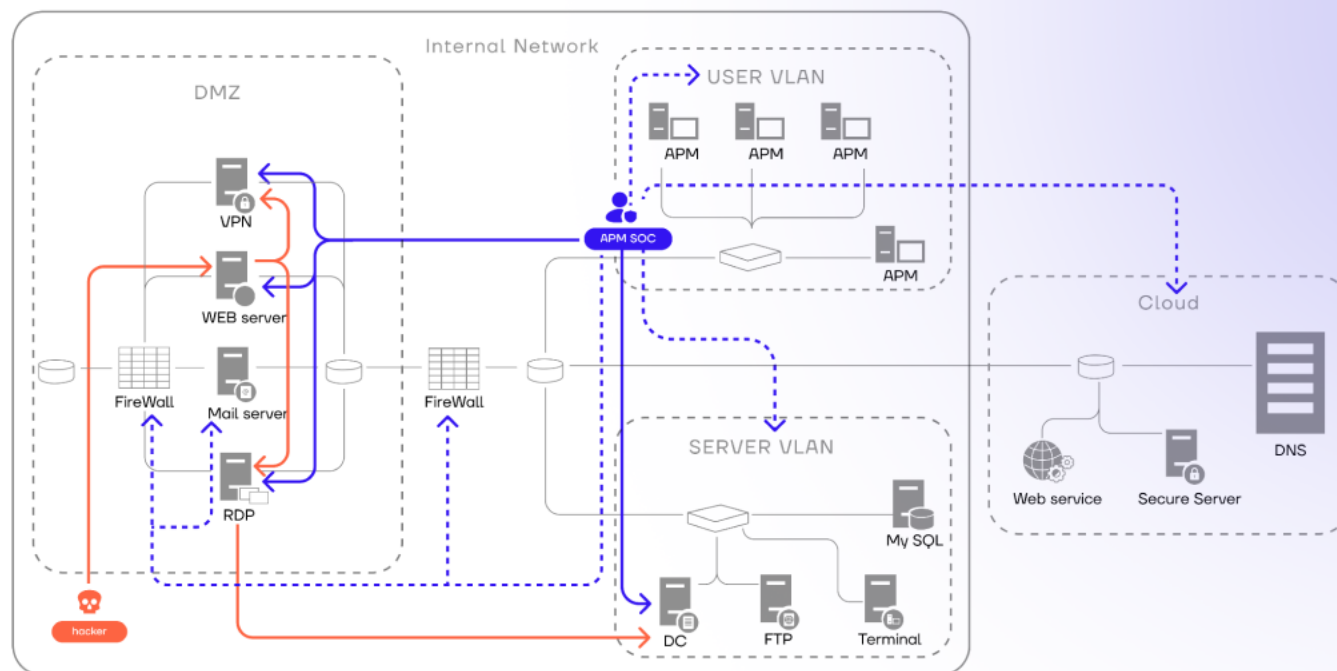
+

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) Соберите информацию о пострадавшем хостине (4) Соберите информацию о личности жертвы (3) Соберите информацию о сети жертвы (3) Соберите информацию об организации-жертве (3) Фишинг (4) Поиск в закрытых источниках (2) Поиск в открытых технических базах данных (1) Поиск	Получить доступ (1) Приобретение инфраструктуры (3) Компрометированные счета (3) Компрометированная инфраструктура (3) Развитие потенциала (4) Создание счетов (3) Получить возможности (7) Возможности сценария (3) Получить информацию (4) Поиск в открытых технических базах данных (1) Поиск	Вставка контента (7) Компрометированный проезд (3) Использование уязвимостей в общедоступных приложениях (3) Внешние удаленные сервисы (3) Дополнительные аппаратные средства (3) Фишинг (4) Размножение с помощью съемных носителей (3) Компрометирование в цепочке поставок (3) Доверительные отношения (3) Действительные учетные записи (4) Сети Wi-Fi	Команда администрирования облака (7) Интерпретатор команд и скриптов (13) Команда управления контейнерами (3) Развернуть контейнер (3) Команда администрирования ESX (3) Эксплуатация для исполнения клиентскими операциями (3) Ввод входных данных (3) Межпроцессная коммуникация (3) Нативный API (3) Исполнение удаленного грубопровода (3) Запланированная	Манипулирование учетной записью (7) Вакансии в BITS (3) Выполнение автозапуска при загрузке или входе в систему (14) Сценарии инициализации загрузки или входа в систему (3) Интеграция облачных приложений (3) Компрометировать двоичный файл программного обеспечения хоста (3) Создать аккаунт (3) Создание или изменение системного процесса (3) Создание или изменение политики домена или арендатора (2) Выполнение, инициированное событием (13) Побег к хосту	Механизм контроля за повышением уровня насилия (3) Манипулирование токенами доступа (1) Манипулирование учетной записью (7) Выполнение автозапуска при загрузке или входе в систему (14) Сценарии инициализации загрузки или входа в систему (3) Оценки деобфускация/декодирования файлов или информации (3) Развернуть контейнер (3) Прямой доступ к тому (3) Изменение политики домена или арендатора (2) Ограничения исполнения (2) Использование	Механизм контроля за повышением уровня насилия (3) Манипулирование токенами доступа (1) Вакансии в BITS (3) Создание образа на хосте (3) Отложенное исполнение (3) Деобфускация/декодирование файлов или информации (3) Развернуть контейнер (3) Прямой доступ к тому (3) Изменение политики домена или арендатора (2) Ограничения исполнения (2) Использование	Противник посредник (4) Грубая сила (4) Учетные данные из хранилища паролей (4) Эксплуатация для получения доступа к учетным данным (3) Принудительная аутентификация (3) Подделка веб-учетных данных (2) Захват ввода (4) Изменение процесса аутентификации (3) Перевод многофакторной аутентификации (3) Генерация запроса на многофакторную аутентификацию (3) Обнаружение	Обнаружение учетных записей (4) Обнаружение информации в браузере (3) Обнаружение облачной инфраструктуры (3) Панель управления облачными сервисами (3) Обнаружение облачных сервисов (3) Обнаружение объектов в облачном хранилище (3) Обход отладчика (3) Обнаружение	Использование удаленных сервисов (3) Внутренний фишинг (3) Боковая передача инструмента (3) Пережатие удаленной службы (2) Удаленные сервисы (3) Размножение с помощью съемных носителей (3) Инструменты развертывания программного обеспечения (3) Загрязнение общего контента (3) Использовать альтернативные материалы аутентификации (4) Обнаружение

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

The screenshot shows the CyberED web application interface. On the left is a sidebar menu with categories like 'Принципы действия', 'Инструменты', 'Последовательность шагов', 'Пример', 'Дополнительные материалы', and specific tasks like 'T-R049 - Техника обхода динамического анализа антивируса' and 'T-R050 - Техника обхода AMSI'. The main content area displays a task titled 'Средняя задача' (Medium task) with a description in Russian about process injection techniques. It includes a code block with a netcat listener and a command to execute a process. Below the code, there's a section for 'Дополнительные материалы' (Additional materials) with links to Process Injection Mitre&Attack, a report on Windows Threads, and a guide on detecting Process Injection. At the bottom, there are buttons for 'Средняя задача' and 'Сложная задача' (Complex task).

■ 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

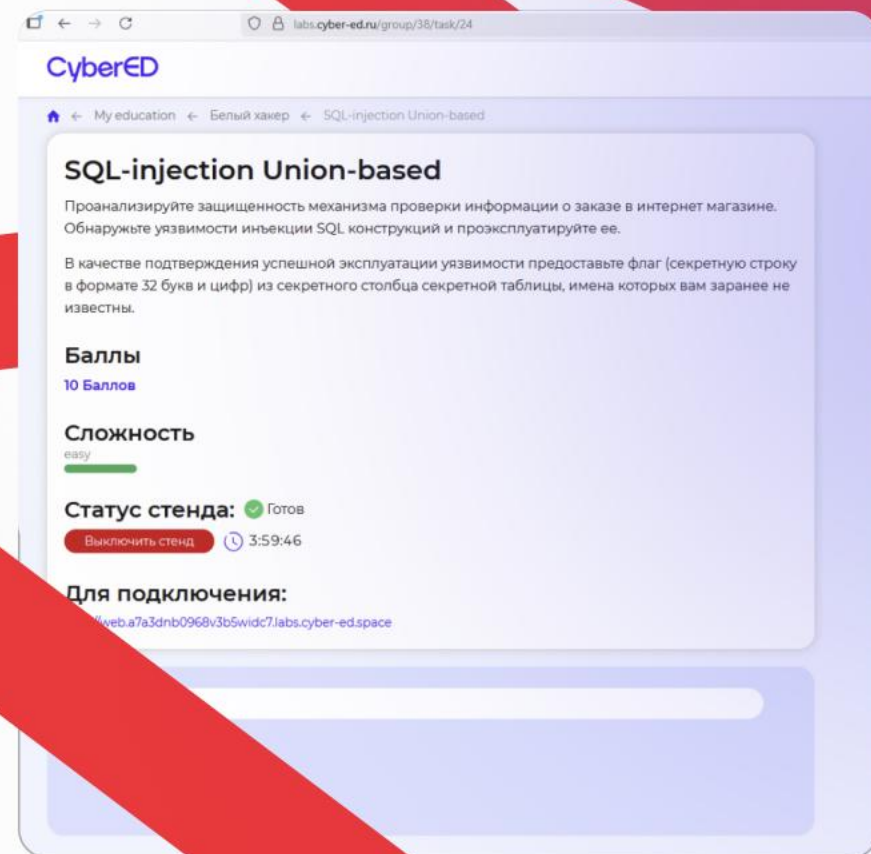
ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ ⚡



Ты **не** «решаешь тест»



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



ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



СНАЧАЛА

Ты знаешь, какую
технику применять

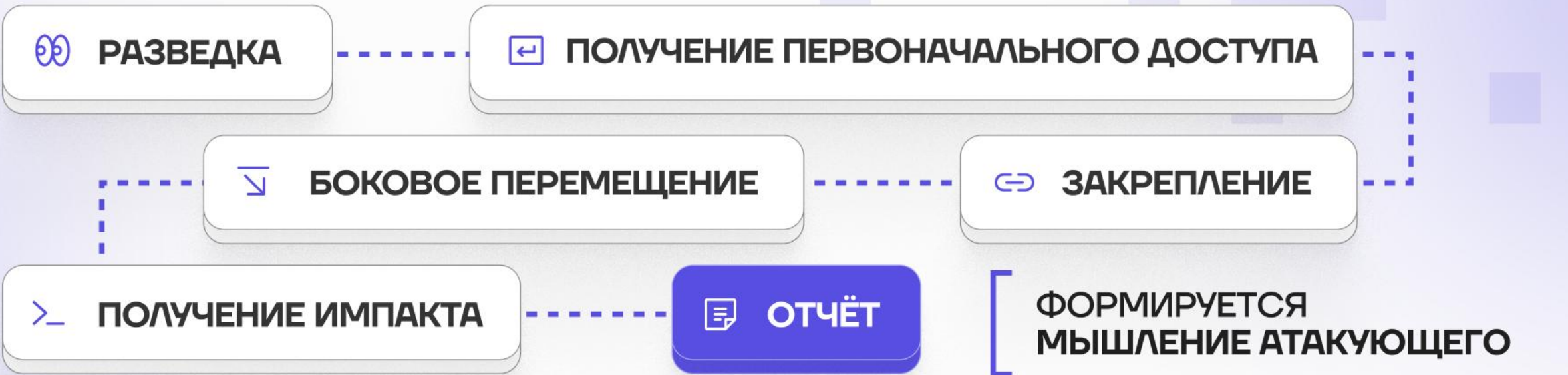


ПОТОМ

Тебе дают инфраструктуру
→ Сам разбирайся

Не изолированные упражнения, а **связанный процесс**

ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



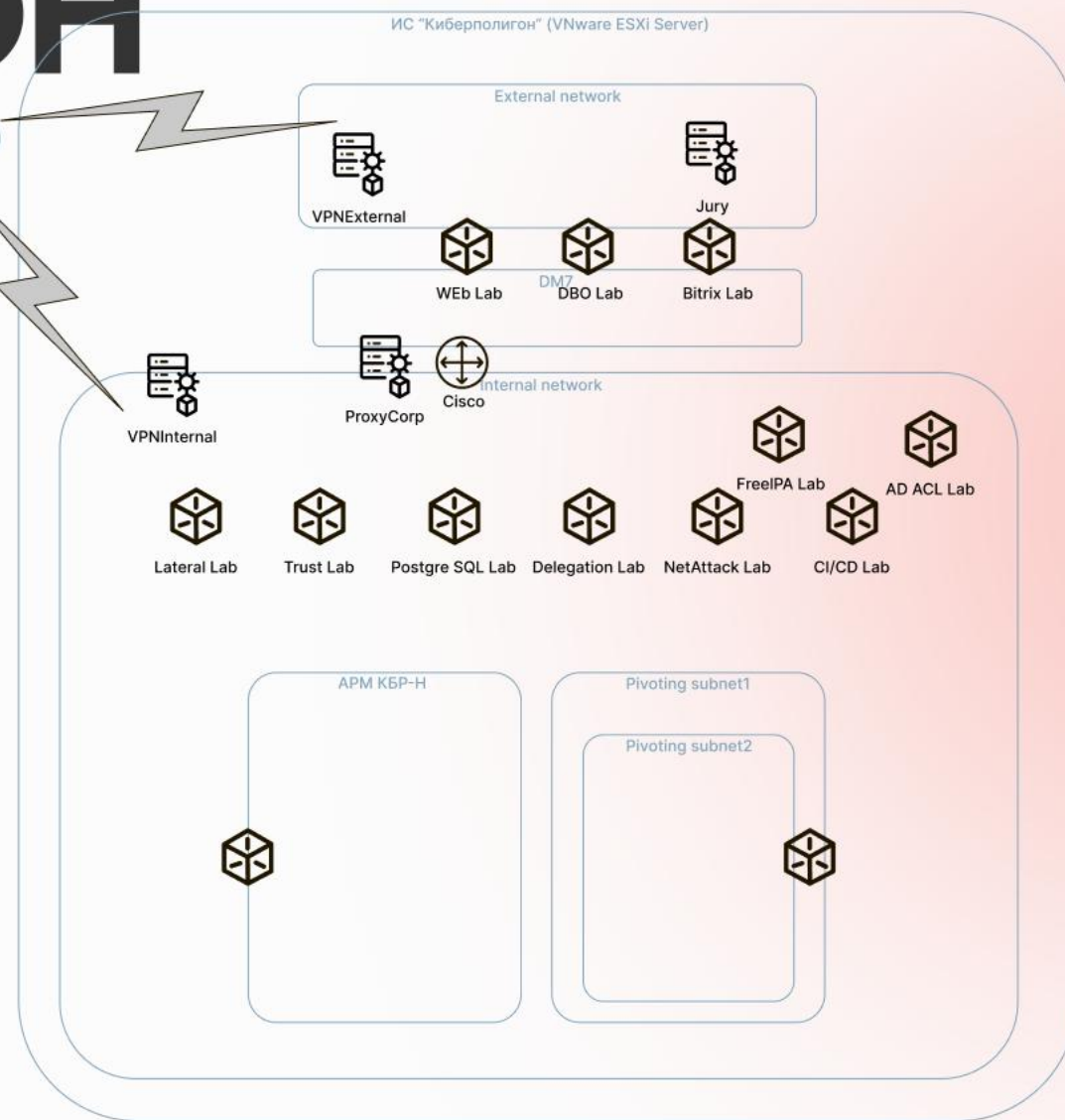
КИБЕРПОЛИГОН

*** CyberED

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

Максимально близко к работе:

« **ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ** »



КИБЕРПОЛИГОН

*** CyberED

6

Цепочек

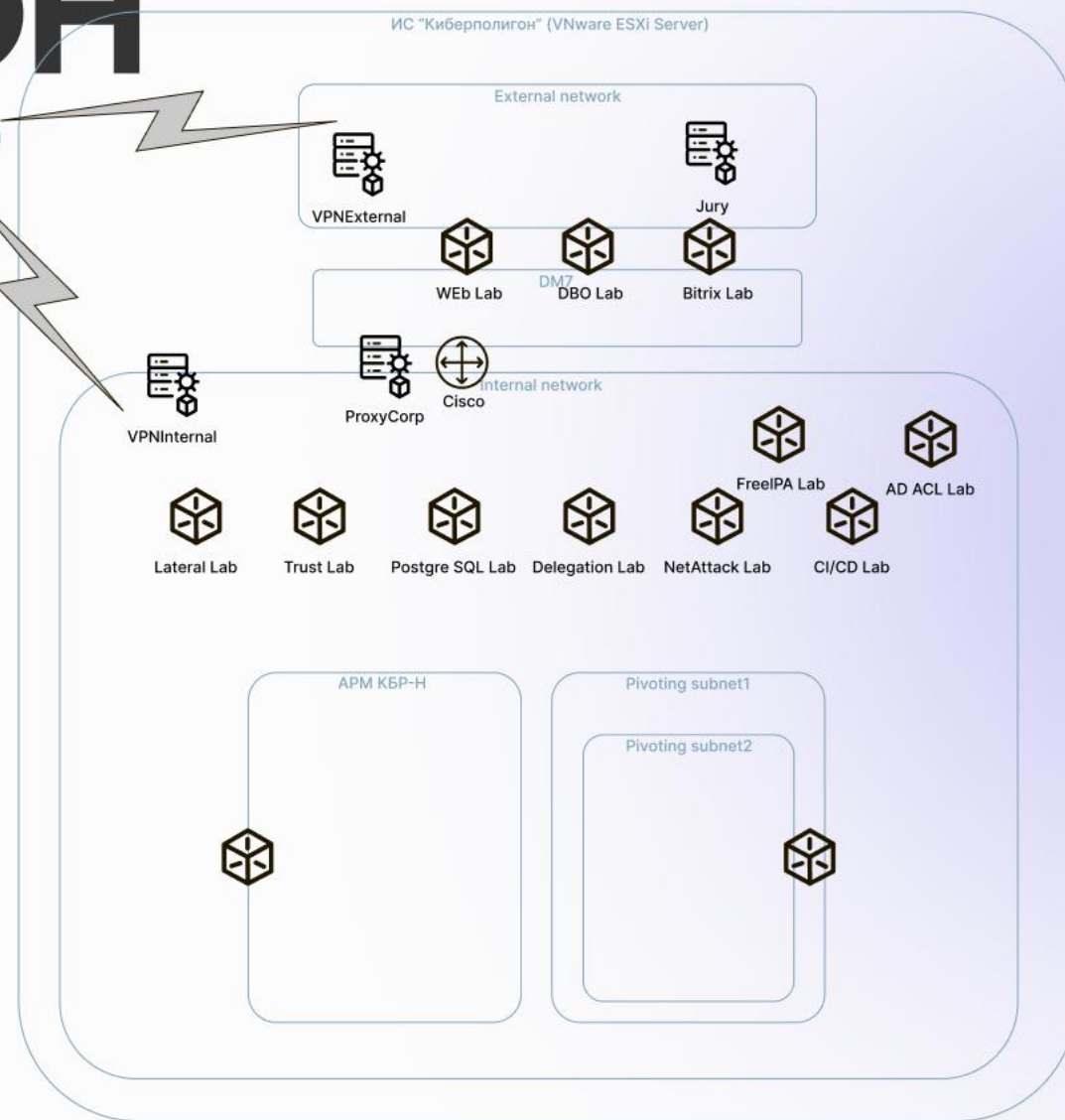
18

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 - M0A

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

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

R301 - M0A

Форензика

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

R301 - M0A

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



Red



Blue



AppSec



Fundamentals

Модуль: Не выбрано ▾

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс

R301 - M0A

Техника обнаружения аномальных активностей в
логировании сетевых устройств и рабочих станций через
активные соединения

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

R301 - M0A

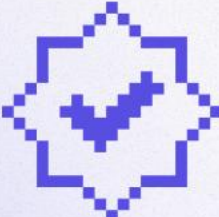
Форензика

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

R301 - M0A

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**

СПЕЦИАЛЬНОЕ ПРЕДЛОЖЕНИЕ



ОСТАВЛЯЙ ЗАЯВКУ!

Атаки на Active Directory
22 июня

за ~~65 900 рублей~~ + 10% скидка
для тех, кто посетил вебинар

ИТОГО: 59 900 рублей

для участников
вебинара

AI-усиленный пентест
16 июня

за ~~60 000 рублей~~

ИТОГО: 45 000 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%

для участников
вебинара



УСПЕЙ ДО КОНЦА НЕДЕЛИ КУПИТЬ ПО ЦЕНЕ МАЯ!