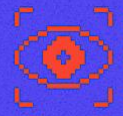
CyberED

КАК СТАТЬ БЕЛЫМ ХАКЕРОМ В 2026 ГОДУ И НЕ ВЫГОРЕТЬ

ЯРОСЛАВ ШМЕЛЕВ



[СПИКЕР]

ЯРОСЛАВ ШМЕЛЕВ

- Старший вирусный аналитик в Kaspersky Lab
- Ключевые навыки:

  ИССЛЕДОВАНИЕ УГРОЗ, ВИРУСНАЯ АНАЛИТИКА, ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ, КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА, АДМИНИСТРИРОВАНИЕ LINUX
- Участие в профильных соревнованиях и награды:

  2024: SOC FORUM (СРЕДИ АТАКУЮЩИХ В РОЛИ КАПИТАНА КОМАНДЫ) - 1 МЕСТО

  2022: THE STANDOFF 2022 (В СОСТАВЕ КОМАНДЫ INVULS) - 3 МЕСТО

  2021: THE STANDOFF 365 (BETA ЗАПУСК) - 1 МЕСТО

  2018: ВСЕРОССИЙСКАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - 1 МЕСТО

  2016: МЕЖДУНАРОДНАЯ ОЛИМПИАДА «IT-ПЛАНЕТА», НОМИНАЦИЯ «АДМИНИСТРИРОВАНИЕ LINUX» - 1 МЕСТО
- Телеграм

  @HUMMELCHENO



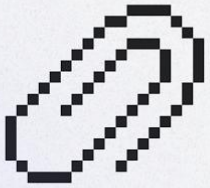
CyberED

О ЧЁМ СЕГОДНЯ

- КТО ТАКИЕ БЕЛЫЕ ХАКЕРЫ И КАКИЕ У НИХ ЕСТЬ НАПРАВЛЕНИЯ РАЗВИТИЯ
- КАК УСТРОЕНА ПРОГРАММА ОБУЧЕНИЯ
- КАК ЭФФЕКТИВНО УЧИТЬСЯ
- РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

CyberED

ПРОФЕССИЯ



БЕЛЫЙ ХАКЕР

01 Легальная и этичная практика по обнаружению и устранению брешей ИБ

02 Разнообразные направления развития

03 Множество интересных задач

04 Дефицит подготовленных специалистов

05 Постоянно меняющаяся и усложняющаяся среда

CyberED

02

ТРЕНДЫ РЫНКА ТРУДА

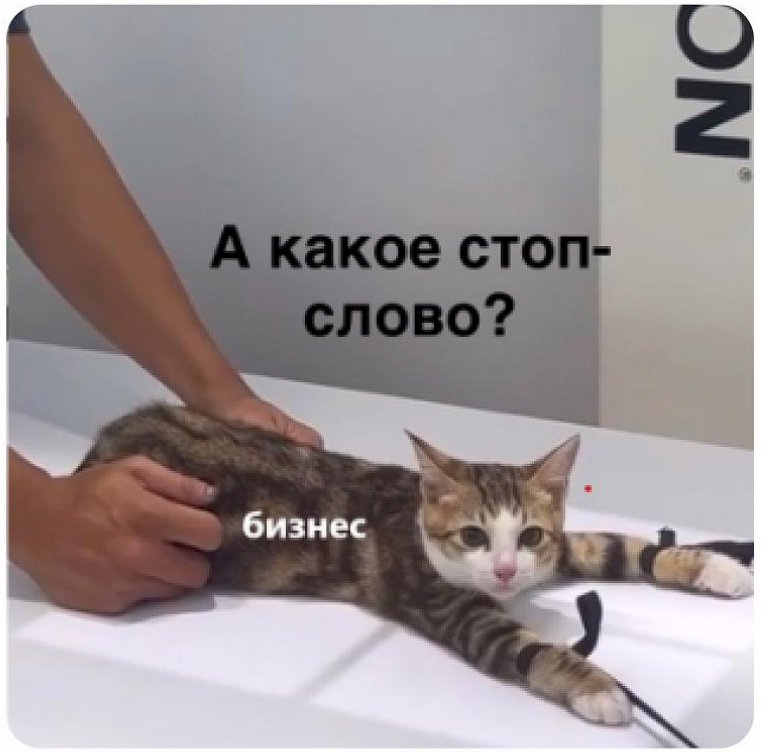
[В ИБ]



CyberED

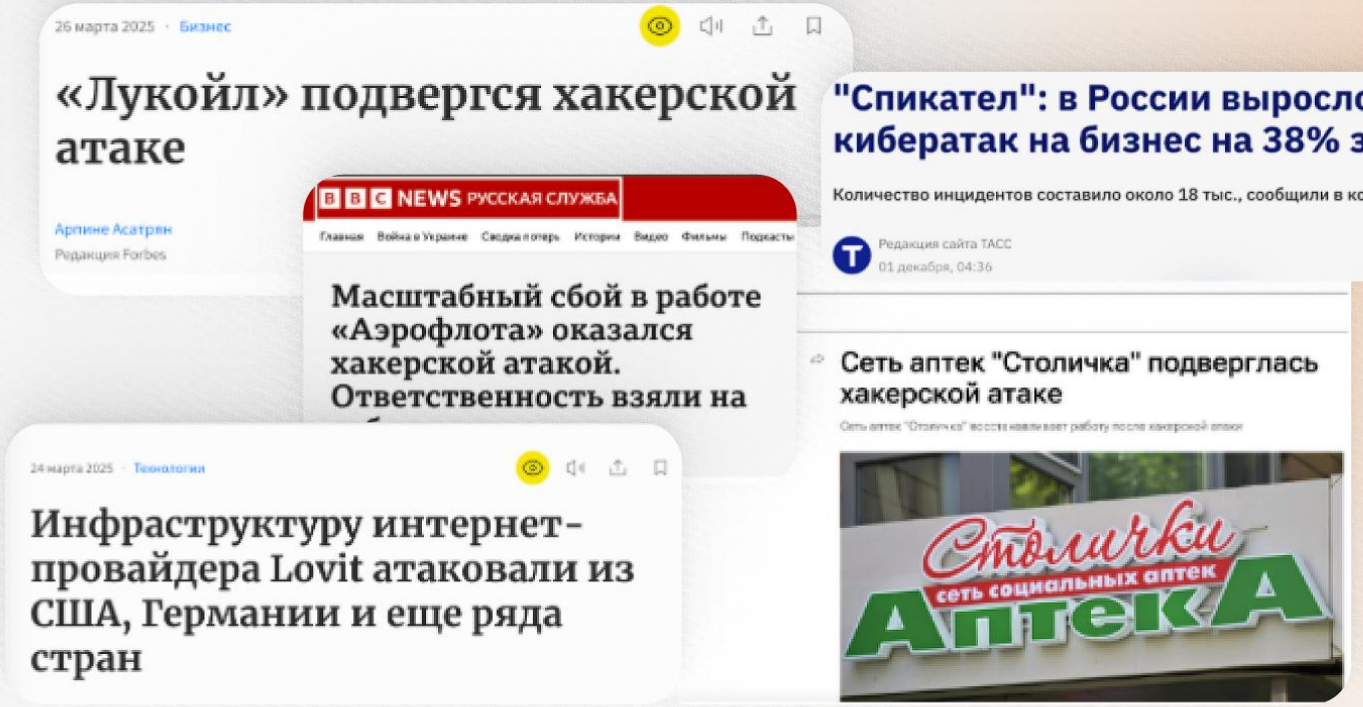
СЕЙЧАС — ЛУЧШЕЕ ВРЕМЯ,

ЧТОБЫ ВОЙТИ В КИБЕРБЕЗОПАСНОСТЬ



[ПРИЧИНА №1]

В РОССИИ ВЫРОСЛО ЧИСЛО КИБЕРАТАК НА БИЗНЕС НА 38% ЗА ГОД



Примеры громких кибератак за 2025

CyberED

СЕЙЧАС — ЛУЧШЕЕ ВРЕМЯ,

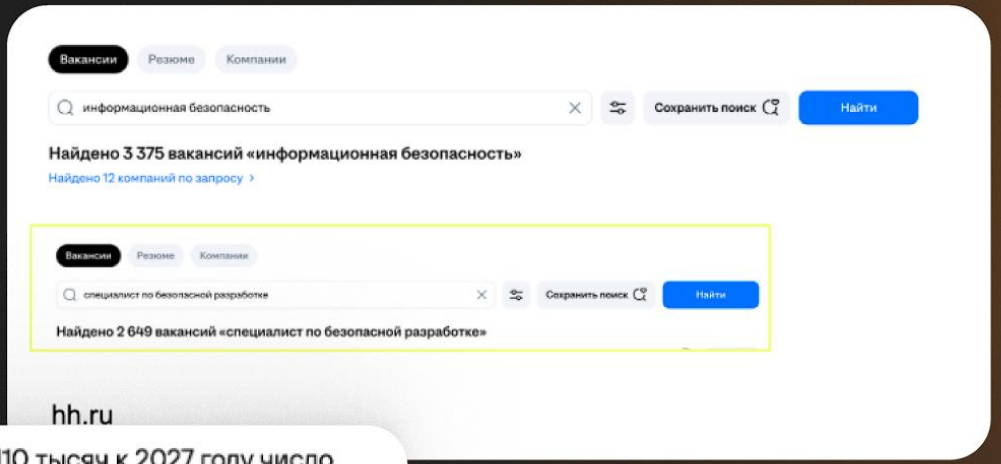
ЧТОБЫ ВОЙТИ В КИБЕРБЕЗОПАСНОСТЬ



[ПРИЧИНА №2]

ДЕФИЦИТ КАДРОВ: К 2027 ГОДУ НА РЫНКЕ БУДЕТ НЕ ХВАТАТЬ ОКОЛО 65 000 СПЕЦИАЛИСТОВ ПО ИБ

Спрос на квалифицированных специалистов **значительно опережает предложение.**



1. **Масштабный рост занятости:** с текущих 110 тысяч к 2027 году число занятых в ИБ может вырасти до 181—196 тыс. человек, число вакансий вырастет в 1,5–1,6 раза. Тем не менее ожидается что дефицит в кадрах сократится до 29-33% от количества занятых (22-25% от потребности рынка в специалистах) с текущих 45% от количества занятых (31% от потребности рынка), но вырастет в абсолютном значении — с текущих 50 тыс. до 52–65 тыс. человек в 2027 году. Таким образом, ситуация «рынка предложения» сохранится в горизонте до 2027 года.

PositiveTechnologies, Рынок труда в информационной безопасности в 2024 -2027 г., 2024 г.

CyberED

СЕЙЧАС — ЛУЧШЕЕ ВРЕМЯ,

ЧТОБЫ ВОЙТИ В КИБЕРБЕЗОПАСНОСТЬ



[ПРИЧИНА №3]

ВЫСОКИЕ ТЕМПЫ РОСТА РЫНКА ИБ: 23% ЕЖЕГОДНО

Это открывает широкие перспективы для карьерного роста как для тех, кто уже развивается в ИБ, так и для новичков, только начинающих свой путь.

> Объем российского рынка информационной безопасности в 2025 году составит 369 млрд рублей. По данным аналитиков ЦСР, в ближайшие три года рынок будет расти в среднем на 23,6% ежегодно. Годовой бюджет одной российской компании на обеспечение информационной безопасности в 2025 году в среднем превысил 294 млн рублей

Forbes,2025

CyberED

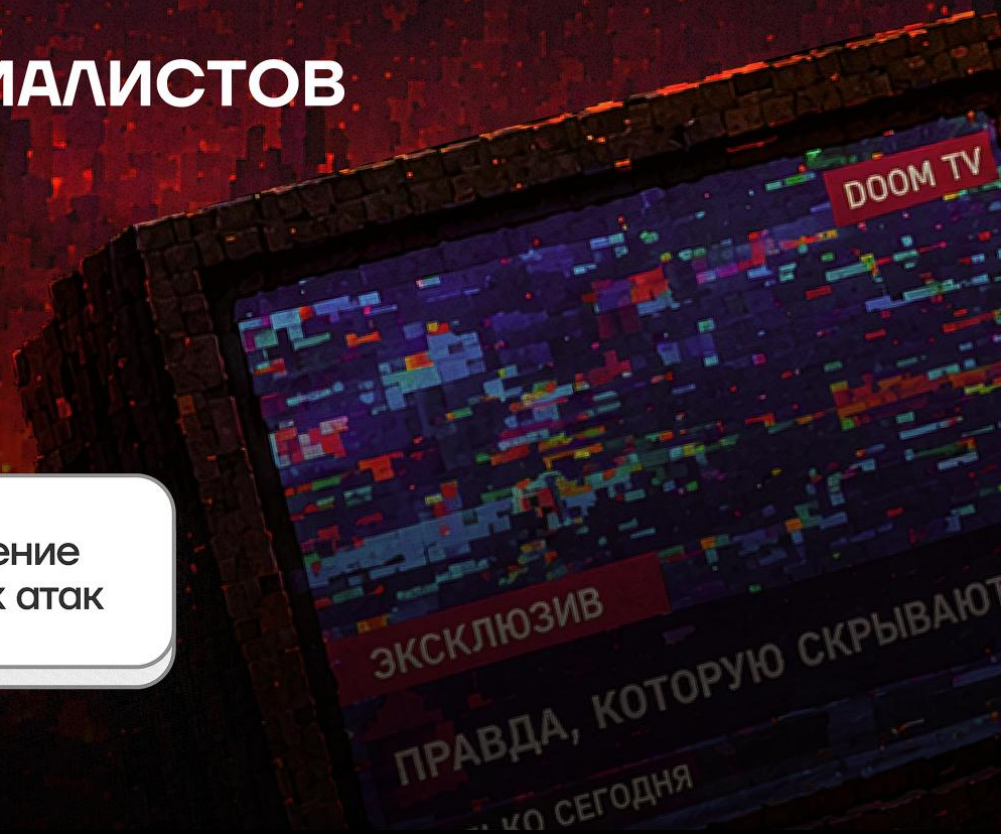
СПРОС НА ПЕНТЕСТЕРОВ УВЕЛИЧИВАЕТСЯ ~ НА 30% В ГОД

30%

ДЕФИЦИТ КВАЛИФИЦИРОВАННЫХ СПЕЦИАЛИСТОВ ДО 100 000 ЧЕЛОВЕК В РОССИИ

ПЕНТЕСТ - ПОСТОЯННОЕ РЕШЕНИЕ НЕСТАНДАРТНЫХ ЗАДАЧ:

- Анализ инфраструктуры
- Поиск уязвимостей
- Построение цепочек атак



НАПРАВЛЕНИЕ: ПЕНТЕСТ



CyberED

КАКИЕ БЫВАЮТ ВИДЫ ПЕНТЕСТЕРОВ

- СПЕЦИАЛИСТ ПО АНАЛИЗУ ЗАЩИЩЕННОСТИ
- СПЕЦИАЛИСТ ПО ВЕБ-ПРИЛОЖЕНИЯМ
- СПЕЦИАЛИСТ ПО СОЦИАЛЬНОЙ ИНЖЕНЕРИИ
- СПЕЦИАЛИСТ ПО ОБЛАКАМ И ИНФРАСТРУКТУРЕ
- СПЕЦИАЛИСТ ПО МОБИЛЬНЫМ ПРИЛОЖЕНИЯМ
- BUG BOUNTY HUNTER

CyberED

[ПЕНТЕСТЕР]

СУТЬ РАБОТЫ И КЛЮЧЕВЫЕ ЗАДАЧИ



ПЕНТЕСТЕР

специалист, который имитирует действия реального злоумышленника, чтобы обнаружить слабые места в системах, сетях, веб-приложениях, облаках или инфраструктуре компании.

ГЛАВНАЯ ЗАДАЧА:

Находить уязвимости и слабые места в системах, моделируя реальные атаки, и демонстрировать, как злоумышленник мог бы их использовать, чтобы компания могла усилить свою защиту.

CyberED

[ПЕНТЕСТЕР]

ЗАРПЛАТА

СТАРТ	ДЖУН+	ЭКСПЕРТ	АРХИТЕКТОР	LEAD/CISO	МЕЖДУНАРОД. УРОВЕНЬ
0–1,5/2 года	2–3 года	3-5 лет	5+лет	5+ лет (управление/стратегия)	
80-150 ТЫС.	**180-250 ТЫС.**	**250-400 ТЫС.**	**350-600 ТЫС.**	**600 ТЫС. -1 МЛН+**	**500 ТЫС -1,2 МЛН**

ВАРИАНТЫ ДОП. ДОХОДА:

01 Bug bounty: от 20–50 тыс. до 1 млн.+ в месяц

02 Фриланс-проекты: 50–300 тыс. за проект

03 Разработка эксплойтов / ресёрч: сильно зависит от уровня, может быть выше средней зарплаты

CyberED

[ПЕНТЕСТЕР]

ОТРАСЛИ, ГДЕ ВОСТРЕБОВАНЫ



ФИНАНСОВЫЙ СЕКТОР



КРУПНЫЙ КОРПОРАТИВНЫЙ СЕКТОР



IT-КОМПАНИИ



КОНСАЛТИНГОВЫЕ И АУДИТОРСКИЕ КОМПАНИИ

CyberED

[ПЕНТЕСТЕР]

ЭТА СПЕЦИАЛЬНОСТЬ ДЛЯ ВАС, ЕСЛИ

- Вам нравится искать слабые места в системах и разбираться, как они устроены
- Вы получаете удовольствие от логических задач, расследований и экспериментов
- Вам интересно анализировать, тестировать, проверять гипотезы, а не просто выполнять инструкции
- Вы готовы постоянно учиться новому, следить за CVE, техниками атак и инструментами
- Вы хотите развиваться в сторону Red Team, Exploit Dev, Bug Bounty или Offensive Research

CyberED

НАПРАВЛЕНИЕ: RED TEAM



CyberED

RED TEAM OPERATORS

СУТЬ РАБОТЫ И КЛЮЧЕВЫЕ ЗАДАЧИ



RED TEAM OPERATORS

Специалист наступательной безопасности, который моделирует действия реального злоумышленника: скрытно проникает в инфраструктуру, двигается по сети, повышает привилегии и достигает целей атаки. Его задача — не просто «взломать», а проверить, насколько компания готова к реальной атаке, и выявить слабые места в процессах, технологиях и реакции защитных команд.

ГЛАВНАЯ ЗАДАЧА:

Не искать уязвимости ради отчёта, а имитировать реального противника: проникнуть, закрепиться, обойти защиту, остаться незамеченным и показать, как далеко может зайти злоумышленник в реальных условиях.

CyberED

КОМБИНАЦИЯ ИНСТРУМЕНТОВ [✓] [ОПРЕДЕЛЯЮЩИХ СПЕЦИАЛИСТА]

01



C2-ФРЕЙМВОРКИ:

Cobalt Strike, Sliver, Havoc, Mythic

02



ИНСТРУМЕНТЫ ПЕРВИЧНОГО ДОСТУПА:

фишинговые платформы,
эксплойт-фреймворки, веб-сканеры

03



ИНСТРУМЕНТЫ ОБХОДА ЗАЩИТ:

кастомные загрузчики, шифровщики
payload'ов

04



ИНСТРУМЕНТЫ LATERAL MOVEMENT:

Impacket, CrackMapExec, WinRM/RDP/
SMB утилиты

05



ИНСТРУМЕНТЫ АТАК НА ACTIVE DIRECTORY:

BloodHound, Rubeus, Mimikatz, Kerbrute

05



ИНСТРУМЕНТЫ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ:

Metasploit, PoC-наборы, кастомные
эксплойты

CyberED

УРОВНИ СПЕЦИАЛИСТОВ

RED TEAM OPERATORS

JUNIOR RED TEAM OPERATOR	Начинающий специалист, который выполняет отдельные этапы операции под руководством	**Основные задачи:** Настройка C2-инфраструктуры, подготовка payload'ов, выполнение простых техник lateral movement, сбор OSINT, участие в фишинговых сценариях.
MIDDLE RED TEAM OPERATOR	Уверенный оператор, способный проводить значительную часть операции самостоятельно	**Основные задачи:** Первичное проникновение, скрытное движение по сети, атаки на AD, обход защит, разработка цепочек атак, поддержка OPSEC
SENIOR RED TEAM OPERATOR	Эксперт, который строит стратегию атаки и моделирует действия APT-уровня	**Основные задачи:** Проектирование операций, сложные многоходовые атаки, кастомизация инструментов, обход EDR, разработка методологий, менторинг

CyberED

[RED TEAM OPERATORS]

ОТРАСЛИ, ГДЕ ВОСТРЕБОВАНЫ



ФИНАНСОВЫЙ СЕКТОР



КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА



IT-КОМПАНИИ



ГОСУДАРСТВЕННЫЙ СЕКТОР И ГОСКОМПАНИИ

CyberED

[RED TEAM OPERATORS]

ЭТА СПЕЦИАЛЬНОСТЬ ДЛЯ ВАС, ЕСЛИ

- Вам нравится думать как злоумышленник и искать нестандартные пути
- Вам интересны скрытные операции, где важны аккуратность, стратегия и OPSEC
- Вам комфортно действовать в условиях неполной информации и самостоятельно строить цепочки атак
- Вам нравится разбираться в сетях, AD, инфраструктуре, уязвимостях и обходе защит
- Вы хотите моделировать реальные угрозы, а не просто проверять чеклист

CyberED

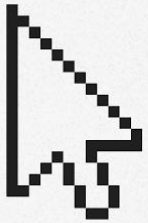
НАПРАВЛЕНИЕ:
BUG BOUNTY



CyberED

[BUG BOUNTY HUNTER]

СУТЬ РАБОТЫ И КЛЮЧЕВЫЕ ЗАДАЧИ



BUG BOUNTY HUNTER

Специалист по поиску уязвимостей в веб-приложениях, сервисах и инфраструктуре компаний, участвующих в публичных или частных программах вознаграждений. Работает как внешний исследователь: самостоятельно выбирает цели в рамках правил программы, ищет ошибки безопасности и отправляет отчёты напрямую заказчику или платформе.

ГЛАВНАЯ ЗАДАЧА:

Находить реальные уязвимости, которые могут привести к компрометации данных или систем, и корректно оформлять отчёты, чтобы компания могла воспроизвести проблему и устранить её. Чем ценнее и опаснее найденная уязвимость — тем выше награда.

КОМБИНАЦИЯ ИНСТРУМЕНТОВ [✓] [ОПРЕДЕЛЯЮЩИХ СПЕЦИАЛИСТА]

01



СКАНЕРЫ И АНАЛИЗАТОРЫ:

Burp Suite, ZAP, Nuclei

02



ИНСТРУМЕНТЫ РАЗВЕДКИ:

Amass, Subfinder, Assetfinder

03



ИНСТРУМЕНТЫ ПОИСКА ПОДДОМЕНОВ:

Sublist3r, DNSx, Knockpy

04



ИНСТРУМЕНТЫ ДЛЯ FUZZING:

FFUF, Dirsearch, Gobuster

05



ИНСТРУМЕНТЫ ПЕРЕХВАТА И МОДИФИКАЦИИ ТРАФИКА:

Burp Suite Proxy, mitmproxy

05



ИНСТРУМЕНТЫ АНАЛИЗА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ:

JADX, MobSF, Frida

CyberED

УРОВНИ СПЕЦИАЛИСТОВ

BUG BOUNTY HUNTER

JUNIOR BUG BOUNTY HUNTER	Начинающий исследователь, изучающий основы веб-безопасности и методологии поиска уязвимостей	**Основные задачи:** Поиск простых уязвимостей (XSS, IDOR), работа с поддоменами, использование готовых инструментов, участие в открытых программах
MIDDLE BUG BOUNTY HUNTER	Уверенный охотник, способный находить уязвимости средней сложности и комбинировать техники	**Основные задачи:** Анализ API, логические уязвимости, обход защит, автоматизация поиска, работа с мобильными приложениями, подготовка качественных отчётов
SENIOR BUG BOUNTY HUNTER	Эксперт, находящий сложные и редкие уязвимости, создающий собственные инструменты и техники	**Основные задачи:** Поиск критичных багов (RCE, auth bypass), исследование бизнес-логики, анализ больших поверхностей атаки, разработка скриптов и автоматизации

CyberED

[BUG BOUNTY HUNTER]

ОТРАСЛИ, ГДЕ ВОСТРЕБОВАНЫ



ФИНАНСОВЫЙ СЕКТОР



ИНТЕРНЕТ-МАГАЗИНЫ И МАРКЕТПЛЕЙСЫ



IT-КОМПАНИИ



ВЕНДОРЫ СРЕДСТВ ЗАЩИТЫ, КОНСАЛТИНГ, ПЕНТЕСТ

CyberED

[BUG BOUNTY HUNTER]

ЭТА СПЕЦИАЛЬНОСТЬ ДЛЯ ВАС, ЕСЛИ

- Вам нравится искать уязвимости и разбираться, как работают веб-сервисы и приложения
- Вы готовы самостоятельно изучать новые техники, инструменты и уязвимости
- Вам подходит формат, где нет начальников, а результат зависит только от вас
- Вы хотите работать с крупнейшими компаниями мира, выбирая цели сами
- Вам комфортно работать в условиях высокой конкуренции и постоянно меняющихся правил

CyberED

ПРОГРАММА: БЕЛЫЙ ХАКЕР



CyberED

CyberED

СТРУКТУРА ОБУЧЕНИЯ НА КУРСЕ



ИЗУЧЕНИЕ ТЕОРИИ

Подробное изложение принципов работы техник пентеста и примеры их применения в различных ситуациях.

CYBERED LABS

Проверка знаний на практике через самостоятельное применение техник на обучающих стендах, развернутых в инфраструктуре CyberEd.

ВОРКШОПЫ

Встречи с экспертами и разбор способов решения актуальных практических задач.

[ИЗУЧЕНИЕ ТЕОРИИ]

CyberED

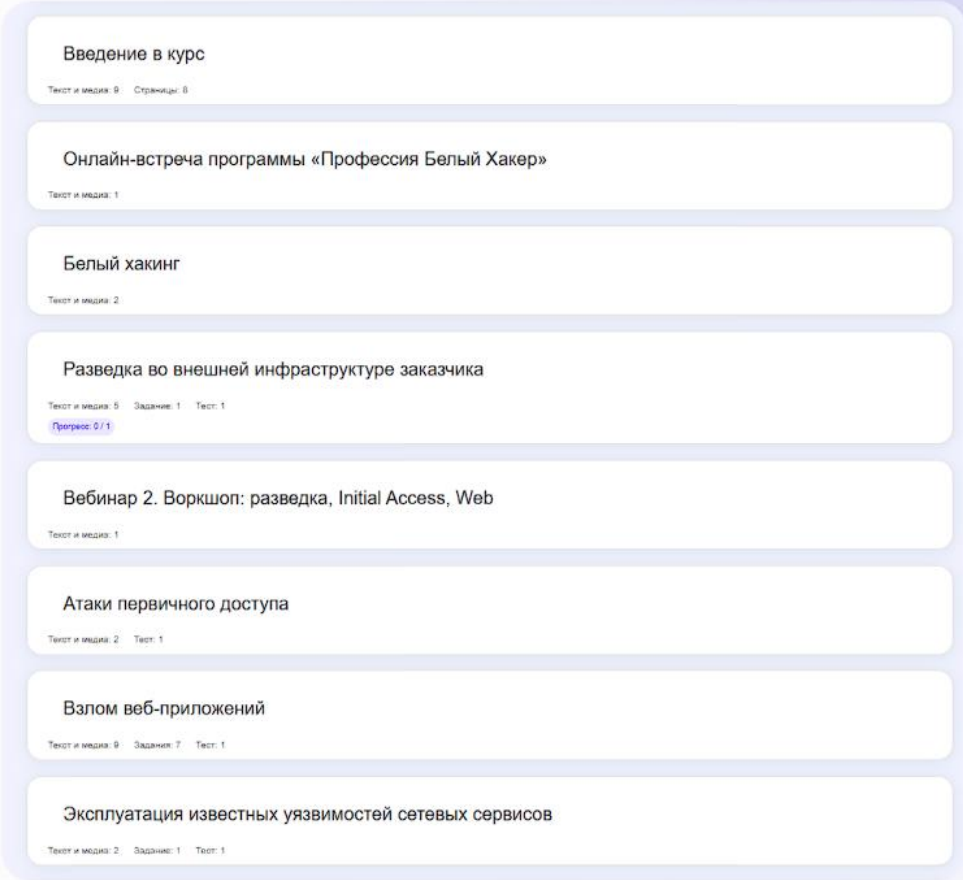
РАБОТА С LMS

ПОДРОБНОЕ ИЗЛОЖЕНИЕ ПРИНЦИПОВ РАБОТЫ ТЕХНИК И ИНСТРУМЕНТОВ

Алгоритм действий по сканированию узлов сети

На примере самого распространенного сканера сети `Nmap` рассмотрим, как можно просканировать произвольное пространство сети:

1. Определить адрес подсети, в которой будет производится поиск узлов. Например, `192.168.88.0/24` .
2. Провести Ping-сканирование сети: `nmap -sn--traceroute <network>` :
   - `-sn` — ping-сканирование. По умолчанию посылаются запрос на ICMP,эхо-запрос и TCP-ACK пакет на порт 80;
   - `--traceroute` — также для того, чтобы проводить трассировку маршрута до каждого найденного узла. Эта опция может помочь в составлении карты подсети.
3. Если есть подозрение, что ICMP-пакеты и TCP-ACK сообщения блокируются сетевым экраном, можно применить другие виды сканирования:
   - `-PS` — TCP-SYN сканирование;
   - `-PU` — UDP сканирование;
   - `-PE; -PP; -PM` — ICMP-сканирование других типов: запрос временной метки (13), информационный запрос (15), запрос адресной маски (17). Многие узлы и брандмауэры могут блокировать исключительно ICMP-пакеты типа echo request, но в спецификации ICMP присутствуют еще несколько типов запросов, позволяющих получить ответ от узлов.

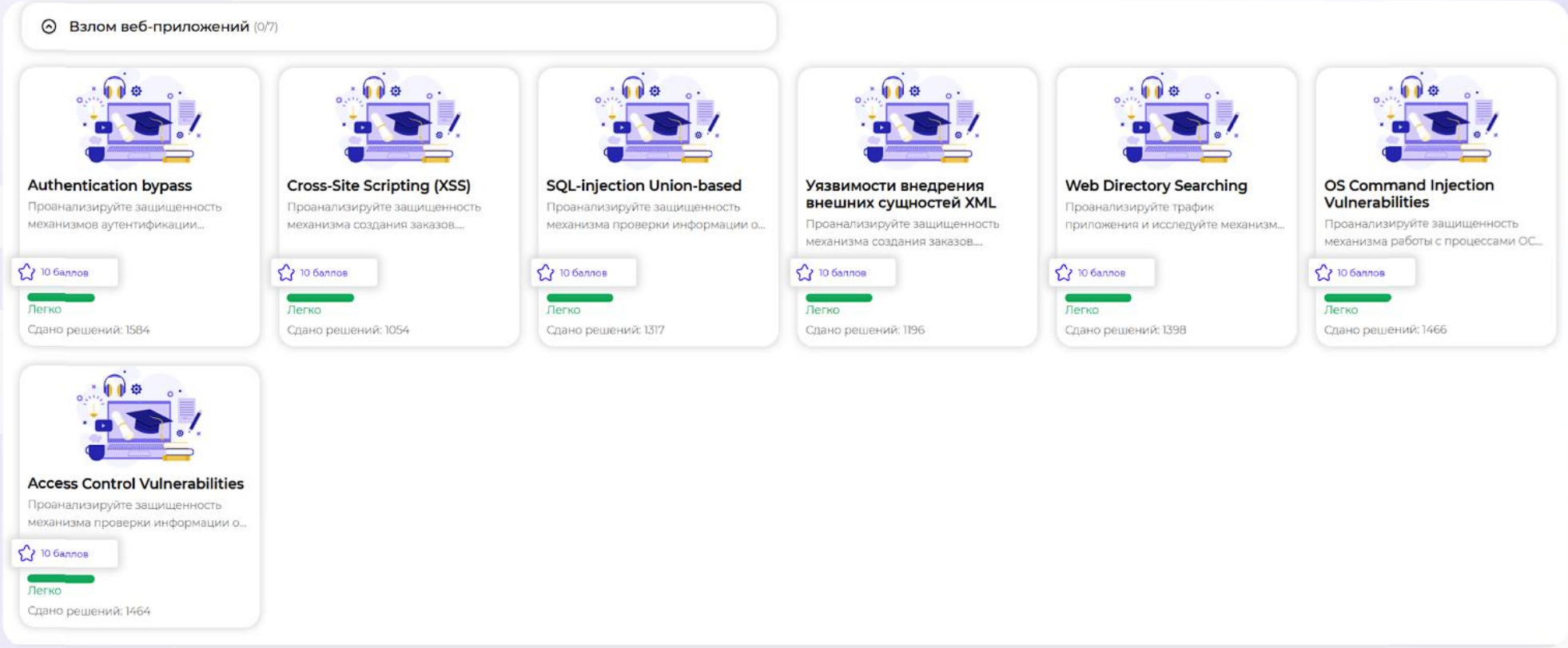


CyberED

[ЖИВАЯ ПРАКТИКА]

ПРАКТИКА НА LABS

ЗАКРЕПЛЕНИЕ ТЕОРИИ
НА МНОЖЕСТВЕ РЕАЛЬНЫХ ПРИМЕРОВ

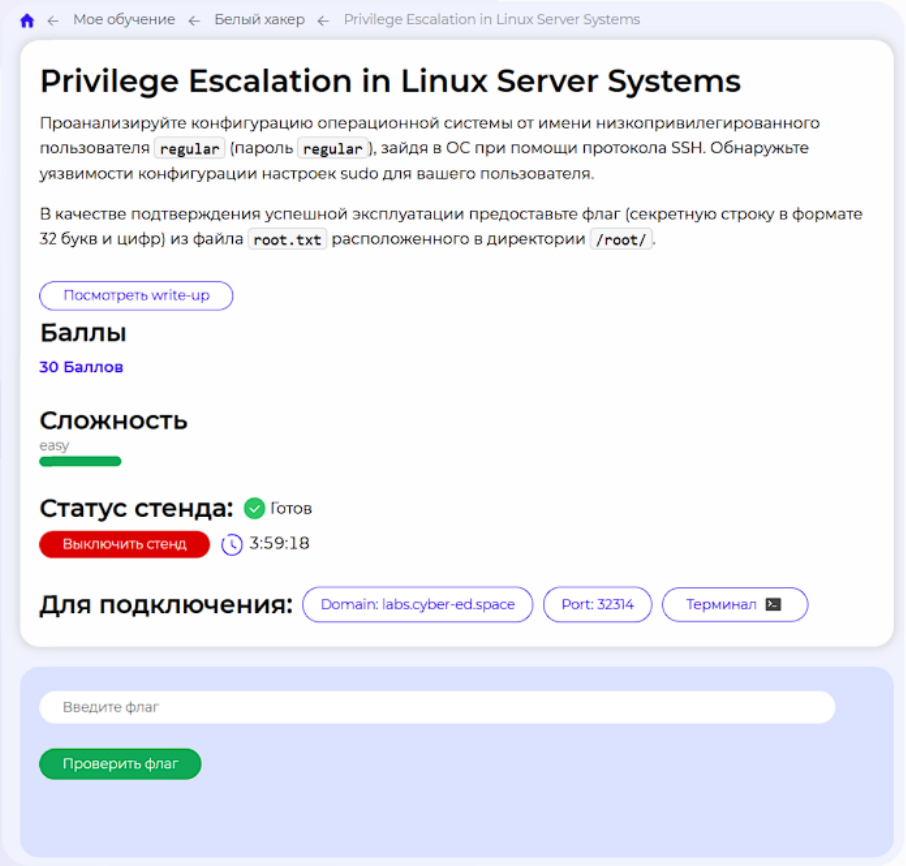


CyberED

[ЖИВАЯ ПРАКТИКА]

ПРАКТИКА НА LABS

ИНДИВИДУАЛЬНЫЕ СТЕНДЫ ДЛЯ УДОБНОЙ РАБОТЫ




```
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-216-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

regular@ssh-8657587b4d-qw766:~$ id -a
uid=999(regular) gid=999(regular) groups=999(regular)
regular@ssh-8657587b4d-qw766:~$
```

[ОПЫТ ЭКСПЕРТОВ]

CyberED

ВОРКШОПЫ

РЕШЕНИЕ АКТУАЛЬНЫХ ЗАДАЧ
ПОД РУКОВОДСТВОМ ЭКСПЕРТОВ-ПРАКТИКОВ

Состоявшиеся встречи
🎯 Встреча «Реальные техники атак хакеров»
⚙️ Воркшоп: разведка, Initial Access, Web
🧿 Встреча: «Фишинг»
🛠️ Встреча «Подготовка окружения пентестера»
🏢 Встреча: «Как получить доменную учётную запись и развернуть атаку внутри сети»
🔓 Вебинар "Компрометация внутренней инфраструктуры без привилегий"
🌆 Запись "Обход сегментации сетей"

CyberED

СТРУКТУРА КУРСА



ПЕРВИЧНЫЙ ДОСТУП

01 Разведка внешнего периметра

02 Атаки на веб-приложения

03 Эксплуатация уязвимостей сетевых сервисов

04 Социальная инженерия

Получение первичного доступа открывает путь для дальнейшего продвижения в инфраструктуре

CyberED

СТРУКТУРА КУРСА



ПРОДВИЖЕНИЕ И ЗАКРЕПЛЕНИЕ

01 Закрепление доступа

02 Повышение привилегий на Linux-хостах

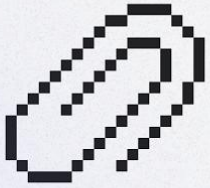
03 Выход за DMZ

04 Проброс трафика

Продвижение по сети позволяет найти вектор для получения полного контроля над инфраструктурой

CyberED

СТРУКТУРА КУРСА



ЗАХВАТ УПРАВЛЕНИЯ

01 Разведка в локальной сети

02 Компрометация Windows-хостов и повышение привилегий

03 Захват управления инфраструктурой сети

04 Противодействие обнаружению и реагированию

Захват управления инфраструктурой позволяет реализовать актуальные для заказчика недопустимые события и успешно выполнить проект

CyberED

СТРУКТУРА КУРСА



ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ

01 Введение в курс

02 Тренд-репорты 2025-2026

03 Встречи с экспертами

04 Развитие хакера

CyberED

CAPTURE THE FLAG



ДЛЯ УЧАСТНИКОВ КУРСА

01 Онлайн-соревнование в формате task-based CTF

02 Категории задач - web, privesc, reverse engineering, forensics

03 Решение практических задач и поиск флагов

04 Отличное начало для пути в практический кибербез

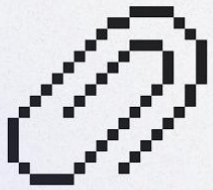
05 Возможность найти наиболее интересное вам направление

06 Задачи для новичков и не только

07 Старт в начале июня

CyberED

ЕЖЕНЕДЕЛЬНЫЕ



ПРАКТИЧЕСКИЕ ЗАДАЧИ

01 Регулярное добавление новых задач

02 Простой и средний уровень сложности

03 Фокус на самостоятельное исследование

04 Работа сразу с несколькими темами курса, все как в реале

05 Разбор решения задач с экспертами

06 Отличный вариант для продолжения после базовой практики курса

07 Первая задача будет опубликована в ближайшее время

ЭФФЕКТИВНОЕ ОБУЧЕНИЕ



CyberED

CyberED

ОСНОВЫ ЭФФЕКТИВНОГО ОБУЧЕНИЯ

- Теория закрепляется только практикой, до 70% времени стоит выделить на неё
- Важно самостоятельно воспроизводить каждую технику
- Поощряйте в себе желание экспериментировать и углубляться в суть
- Возвращайтесь к сложным задачам и повторяйте уже изученное
- Личная база знаний поможет сохранить прогресс

СИСТЕМНОСТЬ В ОБУЧЕНИИ ЭКОНОМИТ ВРЕМЯ И ЛУЧШЕ ФОРМИРУЕТ НАВЫКИ

CyberED

ТРУДНОСТИ НА СТАРТЕ

- Непонимание, с чего начать
- Пробелы в знаниях основ
- Хаотичный подход к обучению
- Фрустрация от высокой сложности
- Тупики при решении задач

СЛОЖНОСТИ НЕИЗБЕЖНЫ, ГЛАВНОЕ – ПРАВИЛЬНЫЙ ПОДХОД

CyberED

ПРЕОДОЛЕНИЕ ТРУДНОСТЕЙ

- Расстановка приоритетов при изучении базовых тем: Linux, сети, программирование
- Выбор специализации: пентест/SOC/AppSec и т.п.
- Структурирование знаний и разработка своей методологии
- Настройка и поддержка рабочего окружения
- Внимательное изучение инструкций к платформе и базовым инструментам

ПРЕОДОЛЕНИЕ ТРУДНОГО НАЧИНАЕТСЯ С ЛЕГКОГО

CyberED

МОТИВАЦИЯ

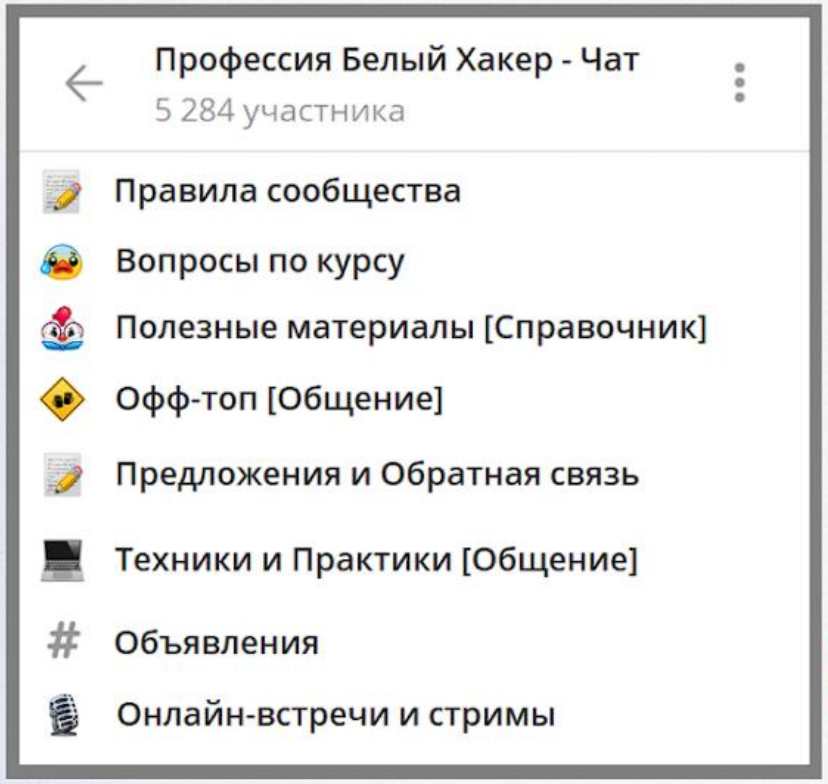
- Фиксация прогресса: райтапы, заметки
- Выбор конкретных небольших целей
- Избегание лишних сравнений с другими людьми
- Участие в CTF и ИБ-челленджах
- Баланс учебы и отдыха

ОСНОВНОЙ КРИТЕРИЙ УСПЕХА - САМОСТОЯТЕЛЬНОЕ РЕШЕНИЕ ЗАДАЧИ

CyberED

РАБОТА С КОМЬЮНИТИ

Форум в Telegram



CyberED

РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

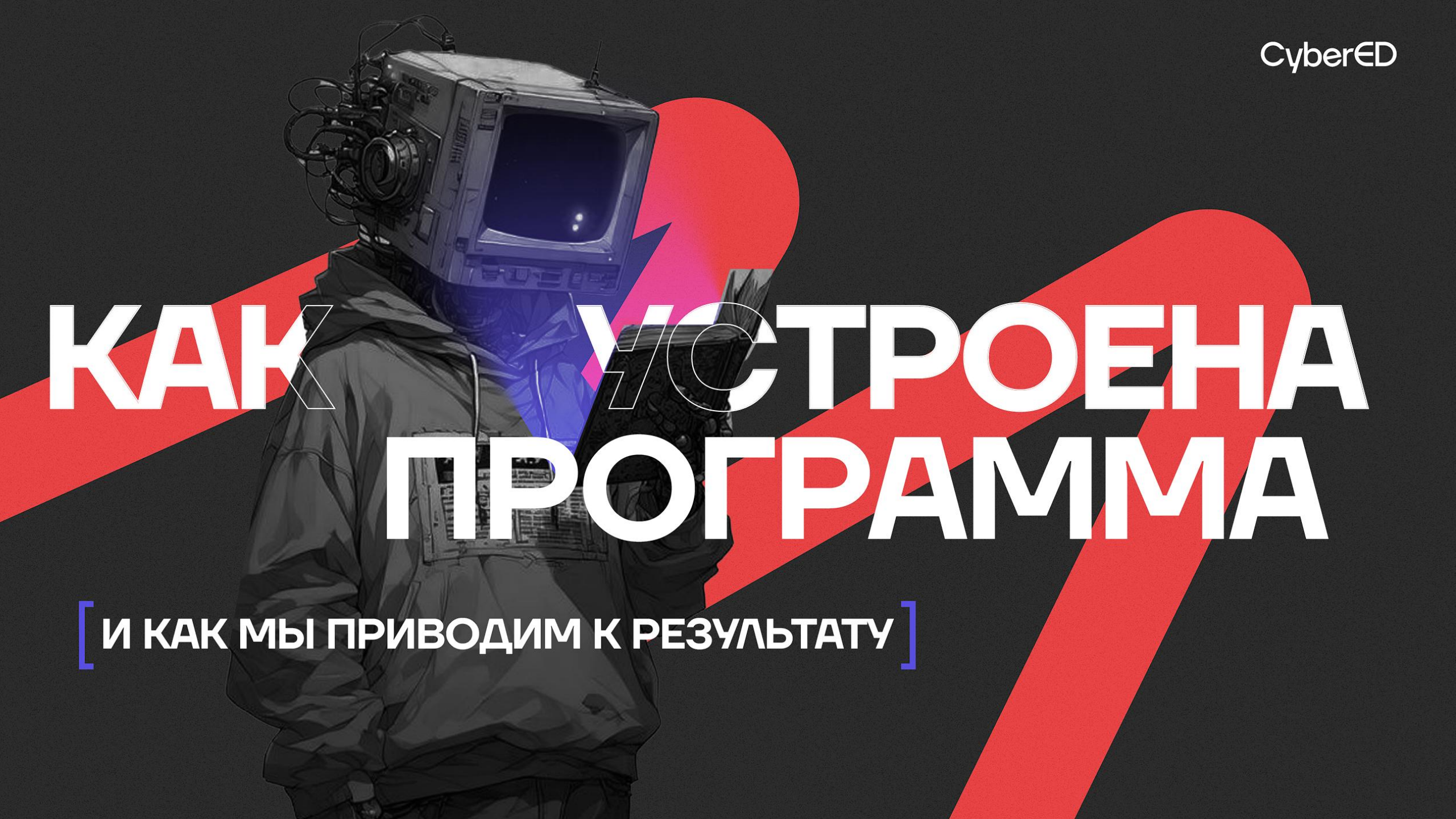
- ПОНИМАНИЕ КЛЮЧЕВЫХ НАПРАВЛЕНИЙ ПЕНТЕСТА
- ПРАКТИЧЕСКИЙ ОПЫТ РЕШЕНИЯ ЗАДАЧ И ПРИМЕНЕНИЯ ИНСТРУМЕНТОВ ПЕНТЕСТЕРА
- ОСНОВЫ МЫШЛЕНИЯ АТАКУЮЩЕГО
- ДОСТУП К ПЕРЕДОВОМУ ОПЫТУ ЭКСПЕРТОВ ЧЕРЕЗ ВОРКШОПЫ И ВЕБИНАРЫ

CyberED

ДАВАЙТЕ РАЗБЕРЕМ ВАШИ ВОПРОСЫ



CyberED



КАК УСТРОЕНА ПРОГРАММА

[И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ]

CyberED

ТЕМЫ МОДУЛЕЙ

ЭТО ГОТОВЫЙ ПЛАН ВЫПОЛНЕНИЯ ВСЕЙ ЦЕПОЧКИ АТАКИ В КОМПАНИЯХ

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

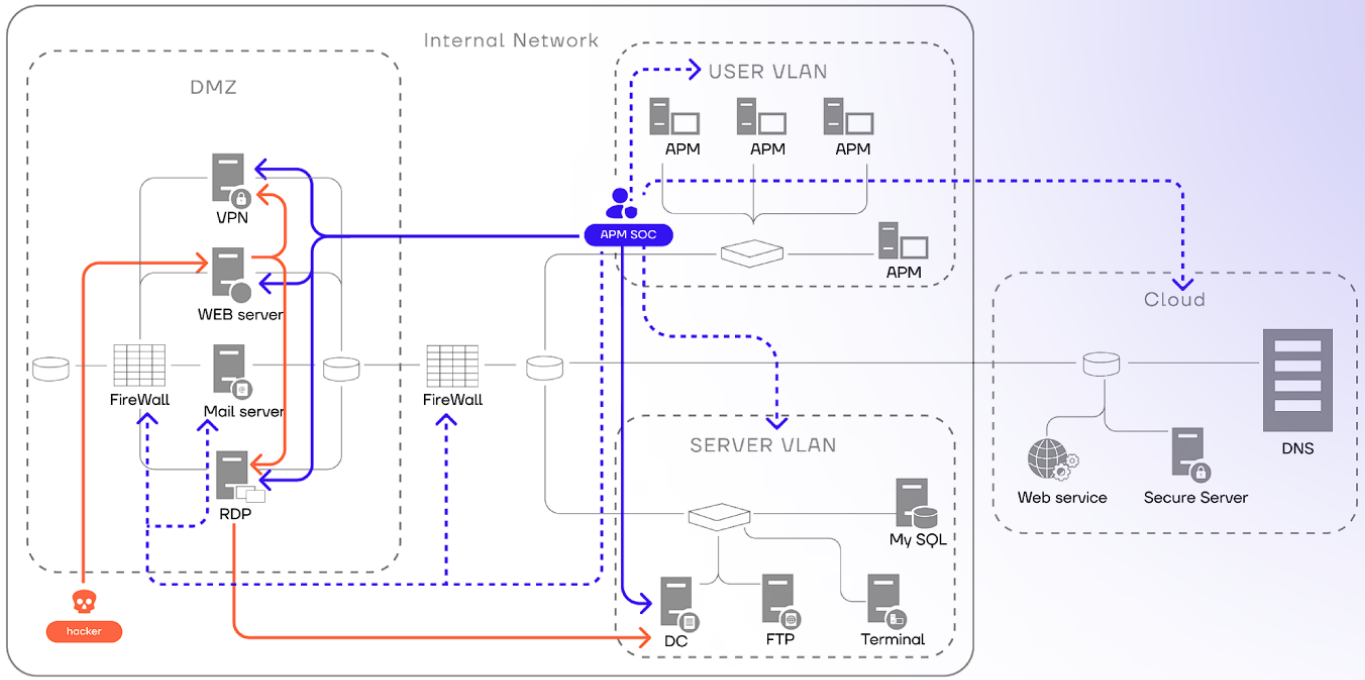
- Модуль 6. Повышение привилегий в Linux
- Модуль 7. Повышение привилегий в контейнерных средах
- Модуль 8. Повышение привилегий в Windows

Этап 4. Боковое перемещение в сети

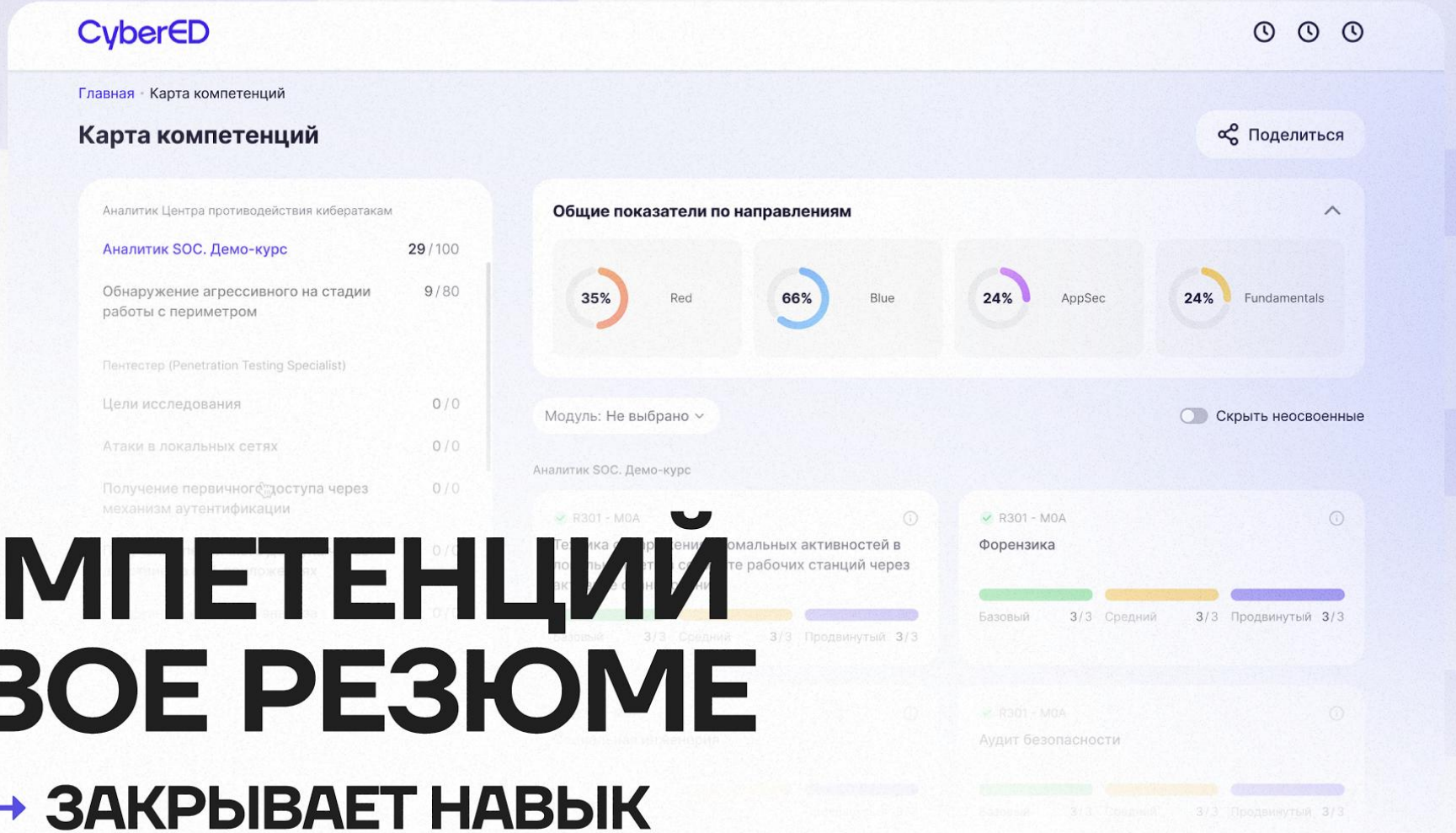
- Модуль 9. Проброс сетевого трафика (Pivoting)
- Модуль 10. Проведение атак на локальные сети
- Модуль 11. Проведение атак на Active Directory

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



КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

КАЖДАЯ ЗАДАЧА → ЗАКРЫВАЕТ НАВЫК

УРОВЕНЬ: БАЗОВЫЙ / СРЕДНИЙ / СЛОЖНЫЙ

- Видно, что ты реально умеешь
- Не «написал в CV» а подтвердил

CyberED

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

CyberED

ПРАКТИКА, БЛИЗКАЯ К BUG BOUNTY / РЕАЛЬНОЙ РАБОТЕ

ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ

Ты **не** «решаешь тест»

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



CyberED

[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»

CyberED

КАК МЫ ДОВОДИМ ТЕМУ

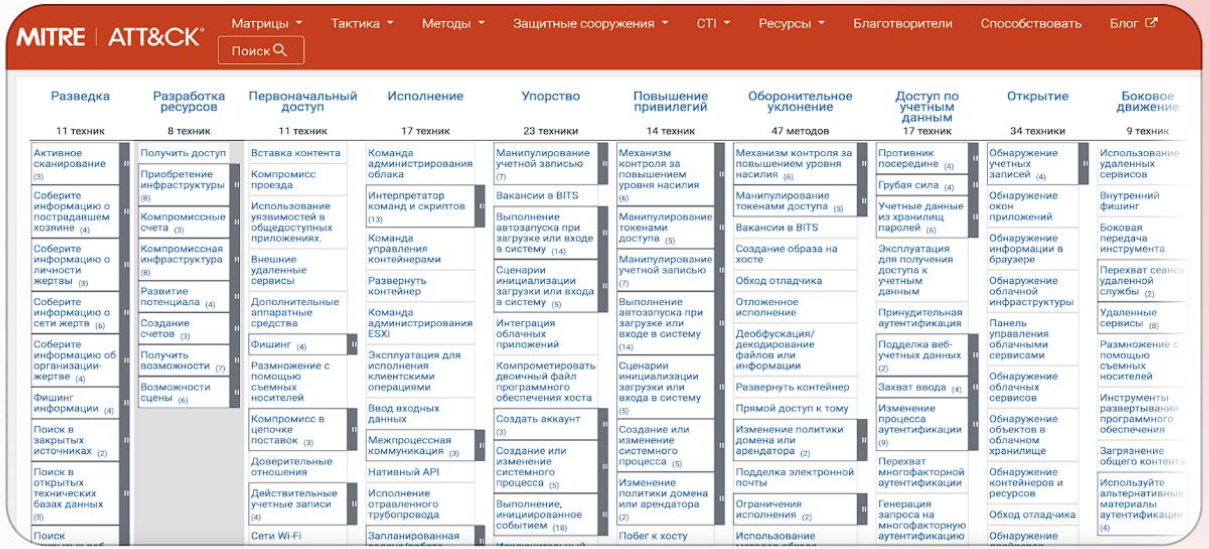
ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

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



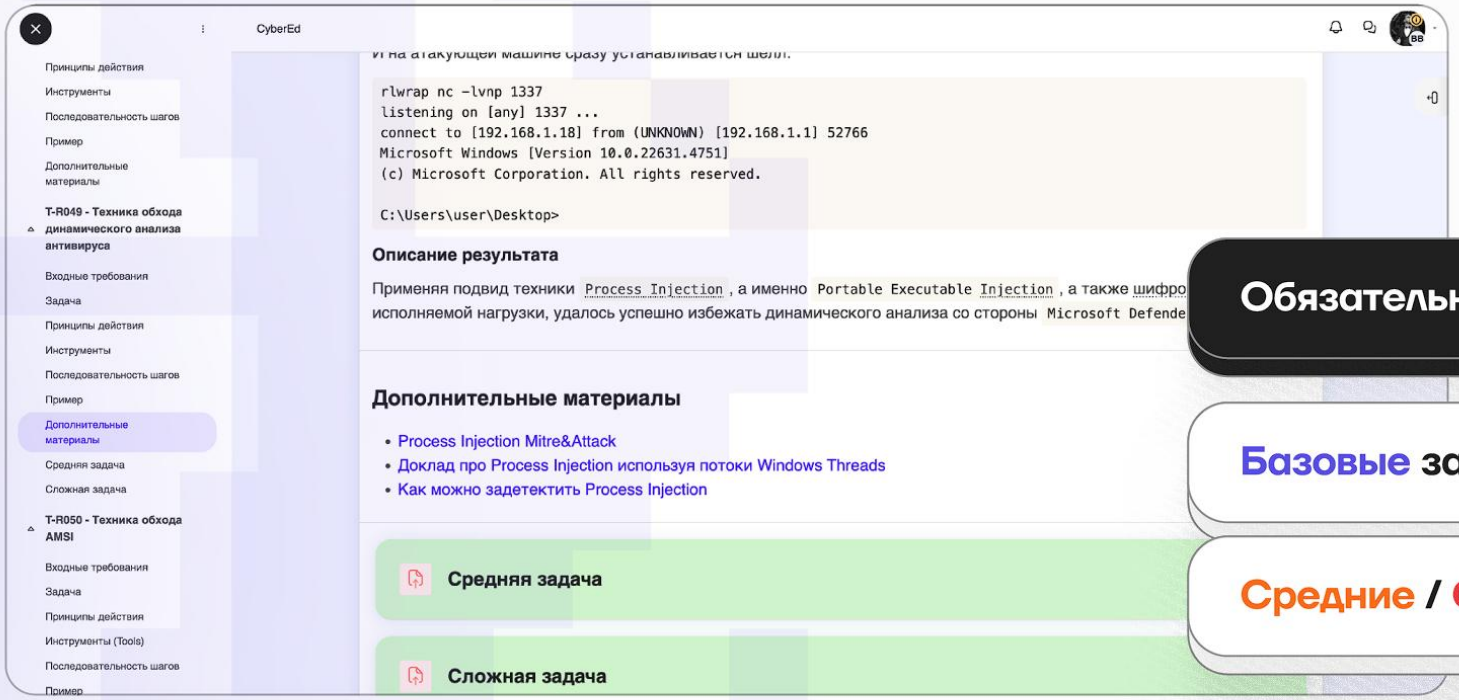
Матрица ATT&CK - всемирно признанная карта действий хакеров, основанная на реальных атаках.

CyberED

[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

CyberED

ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



СНАЧАЛА

Ты знаешь, какую технику применять

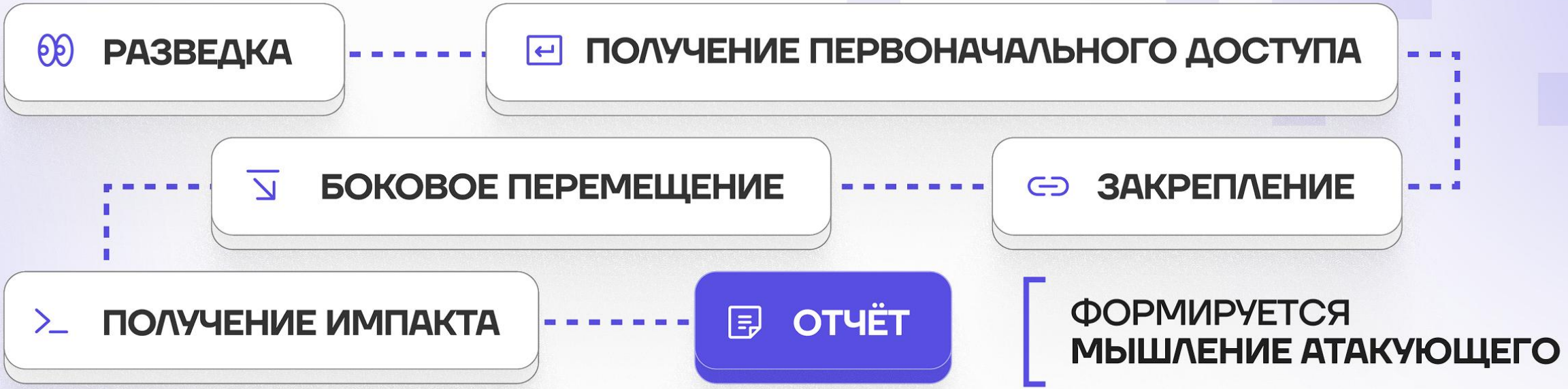
ПОТОМ

Тебе дают инфраструктуру
→ Сам разбирайся

CyberED

Не изолированные упражнения, а **связанный процесс**

ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



ФОРМИРУЕТСЯ
МЫШЛЕНИЕ АТАКУЮЩЕГО

CyberED

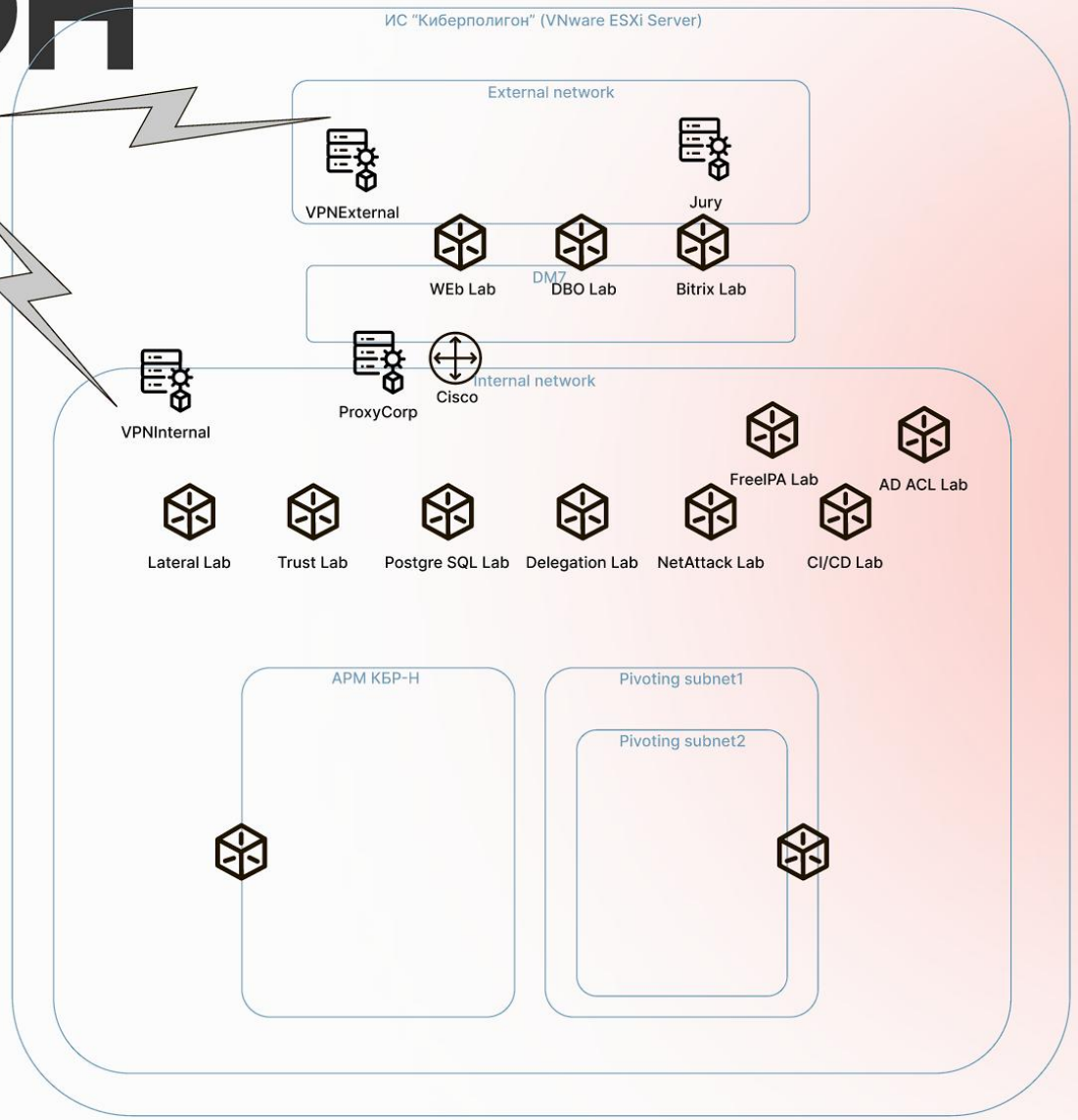
КИБЕРПОЛИГОН

|** CyberED

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

Максимально близко к работе:

« ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ »



CyberED

КИБЕРПОЛИГОН

CyberED

30
Сценариев

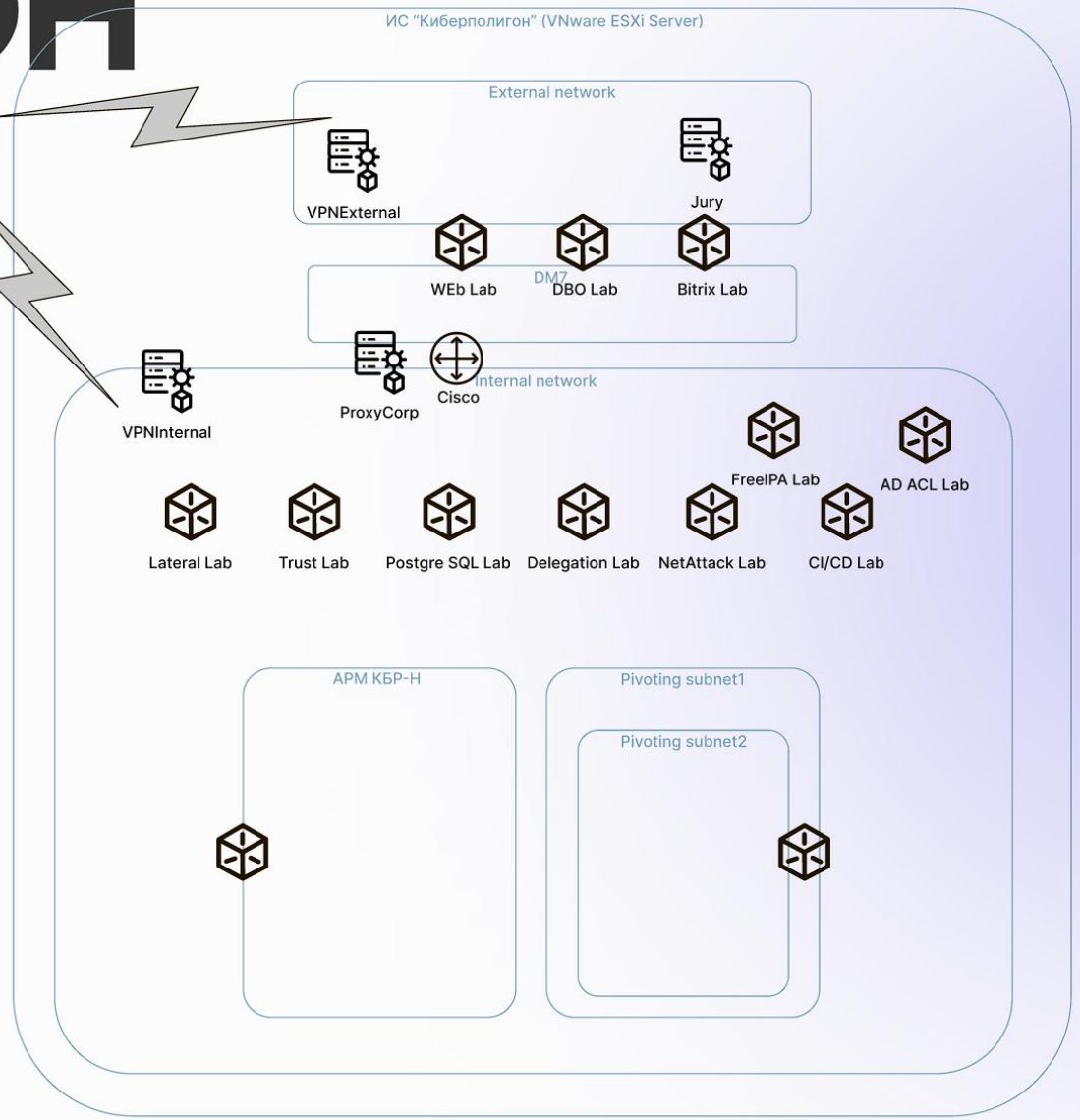
30
Виртуальных машин

60+
Тасок,
в каждой из которых может быть несколько уязвимостей.

ЗАДАЧИ

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

+ Нарабатываете насмотренность по сценариям атак
+ Сталкиваетесь с вариативностью уязвимостей



CyberED

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 инфраструры с помощью обнаруженной уязвимости в центре сертификации - Y.

ПРИМЕР 1

Не так: умею сканировать порты и подбирать пароли.

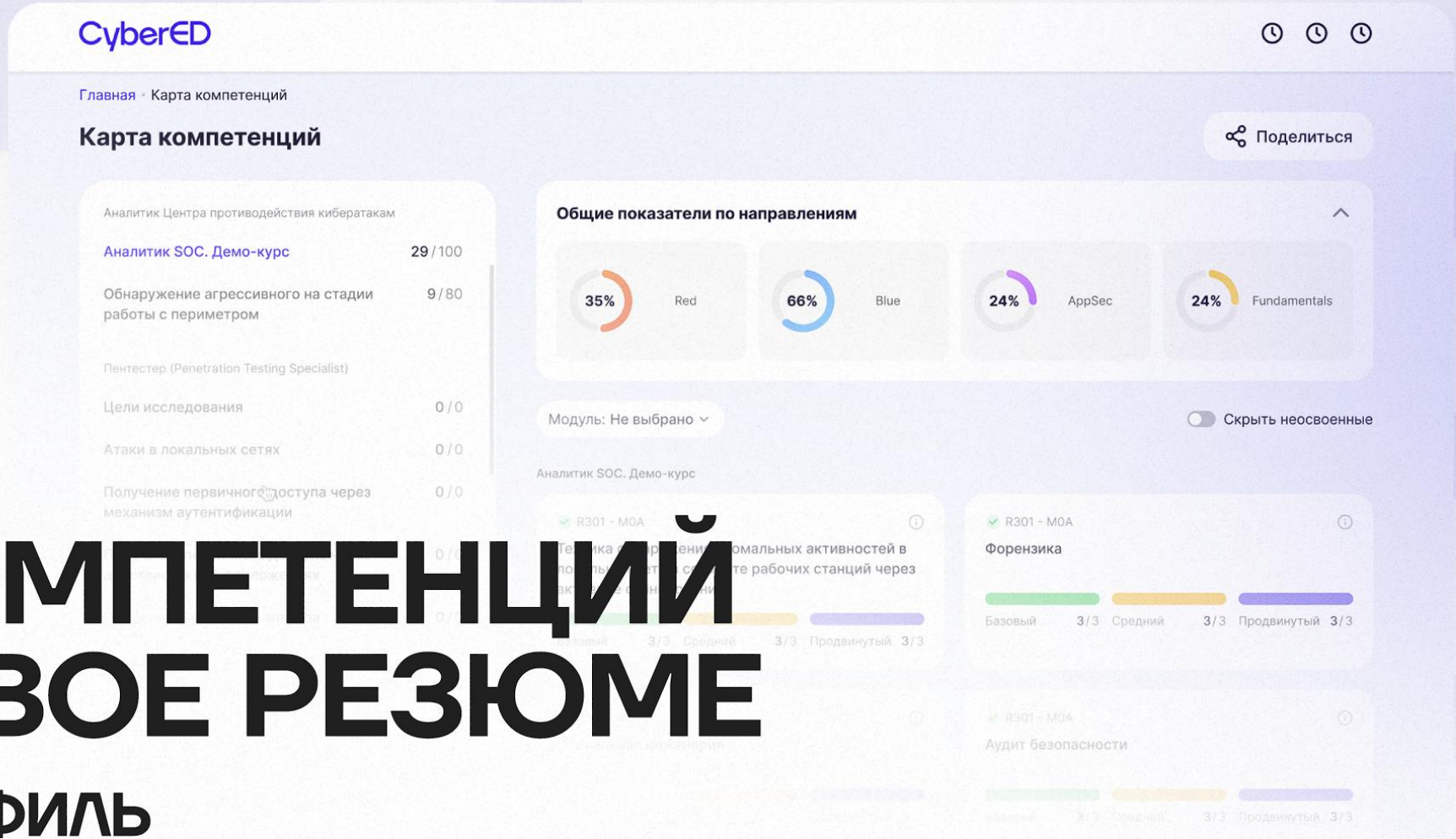
Так: обнаружил открытый порт 3389 на непубличном хосте, осуществил подбор пароля для учётной записи локального администратора через RDP, получил shell и развернул прокси для дальнейшего движения по внутренней сети Заказчика.

ПРИМЕР 2

Не так: знаю Docker и Kubernetes.

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

CyberED



КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

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

CyberED

ДАВАЙТЕ РАЗБЕРЕМ ВАШИ ВОПРОСЫ

