

CyberED

[ПРОФЕССИЯ ПЕНТЕСТЕР]

КОНСУЛЬТАЦИЯ ПО КУРСУ



ПЛАН ВСТРЕЧИ

- 01 Познакомимся со мной, с CyberEd, с Вами
- 02 Какое место занимает Специалист по тестированию на проникновение среди других специальностей ИБ
- 03 Суть работы и ключевые задачи
- 04 Требования работодателей и рынка
- 06 Как устроена программа и почему именно так
- 07 Как мы обучаем специалистов по пентесту

[О СПИКЕРЕ]

КИРИЛЛ НИКОЛАЕВ

- Опыт работы в сфере информационной безопасности – 10+ лет.

Сертификаты:

- Certified Ethical Hacker (CEH)
- Offensive security certified professional (OSCP)
- x86 Assembly Language and Shellcoding on Linux (SLAE)
- Offensive security certified expert (OSCE)
- Offensive security web expert (OSWE)
- Certified Red Team Professional (CRTP)
- Certified Red Team Operator (CRTO)
- Certified Network Pentester (CNPen)
- Hands-on Web Exploitation (HOWE)
- Certified Red Team Expert (CRTE)



ДАВАЙТЕ ПОЗНАКОМИМСЯ

А)

ОТМЕТЬТЕ, КТО ВЫ
И ОТКУДА ПРИШЛИ:

- 01 Новичок: без ИТ / ИБ бэкграунда
- 02 Новичок с ИТ-бэкграундом
- 03 Работаю в ИТ
- 04 Работаю в ИБ

Б)

КАКИЕ У ВАС ЦЕЛИ
НА ВСТРЕЧУ?



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.

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

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

GRC / ARCH

Проектирование архитектуры безопасности, управление рисками и обеспечение соответствия нормам.

■ Тип мышления:
стратегический, управленческий.

■ Верхние роли:

Управление рисками

Архитектор безопасности

Безопасность поставщиков

Аудитор



[СПЕЦИАЛИСТ]

ПО ТЕСТИРОВАНИЮ
НА ПРОНИКНОВЕНИЕ

ПЕНТЕСТЕР



Для чего нужно проводить аудит безопасности в компаниях?



Почему важно проводить пентесты регулярно?



Почему это востребовано?

НАПРАВЛЕНИЯ В ПЕНТЕСТЕ

- Внешнее тестирование (тестирование черным ящиком)
- Аудит приложений (тестирование белым ящиком)
- Аудит мобильных приложений
- Внутреннее тестирование (без противодействия)
- Внутреннее тестирование (с противодействием)
- Фишинг / соц. инженерия
- WI-FI
- Red Team



На курсе мы изучаем:
внешний и внутренний пентест.



Направлений в пентесте много, но фундамент профессии
— это пентест инфраструктуры компании.

КЛЮЧЕВАЯ ЗАДАЧА ОТВЕТИТЬ НА ВОПРОСЫ

01 ?

Насколько компания защищена от внешних угроз

02 ?

Насколько компания защищена от внутренних угроз

03 ?

Насколько компания готова к атакам с точки зрения персонала по ИБ и разработанной внутренней документации (при проведении Red Team)

Пентестер отвечает на главный вопрос бизнеса:
насколько компания реально устойчива к
внешним, внутренним и целевым атакам.

ИДЕАЛЬНЫЙ РЕЗУЛЬТАТ

РАБОТЫ ПЕНТЕСТЕРА

ПОКАЗАТЬ, СМОЖЕТ ЛИ **ЗЛОУМЫШЛЕННИК ДОБРАТЬСЯ** ДО КРИТИЧНЫХ АКТИВОВ КОМПАНИИ И ГДЕ ЗАЩИТА НЕ СРАБОТАЕТ.

[КАК?]

Получить доступа к критическим данным компании
(решение недопустимых событий)

Составить карту покрытия в инфраструктуре по уязвимостям

Получить доступ внутрь инфраструктуры из внешнего контура (при проведении Red Team)



Выполнить работу при отсутствии инцидентов на стороне SOC - остаться незамеченным.

ИИ-АГЕНТЫ В ПЕНТЕСТЕ:

КЕЙС FIREFOX

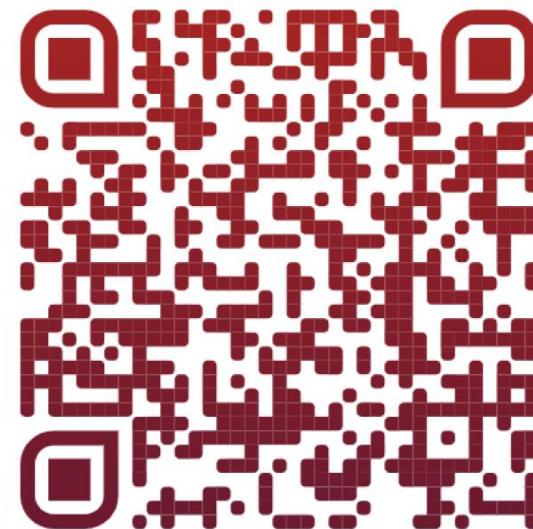
MOZILLA ВСТРОИЛА ИИ-АГЕНТОВ В КОНВЕЙЕР РАЗРАБОТКИ. ТЕПЕРЬ ЭТО НЕ ЭКСПЕРИМЕНТ, А ЧАСТЬ CI-СИСТЕМЫ ДЛЯ ПРОВЕРКИ НОВЫХ ПАТЧЕЙ.

[РЕЗУЛЬТАТ (АПРЕЛЬ 2026)]

423 бага исправлено в апреле 2026 (в 20 раз выше нормы).

271 из них нашла нейросеть Claude Mythos.

180 критических ошибок (sec-high), включая 15-летнюю и 20-летнюю уязвимости.



СХОЖИЕ ДОЛЖНОСТИ,

—> КОТОРЫЕ ПОМОГАЮТ ПЕРЕЙТИ **В ПЕНТЕСТ**

- Системный администратор (Linux/Windows)
- Специалист техподдержки (IT Support / Help Desk)
- SOC-аналитик (Tier 1 / Junior)
- Аналитик уязвимостей (Vulnerability Assessment Analyst)
- Разработчик (Web / Backend)
- DevOps / Cloud-инженер

ПЕН
ТЕСТЕР



Но студентами курса становятся и те, кто не имеет опыт работы в ИТ; важно соответствовать базовым требованиям входа на курс.

ТРЕБОВАНИЯ

Опыт работы: 1-3 года

[АНАЛИЗ ВАКАНСИЙ] РАБОТОДАТЕЛЕЙ

➤ Что предстоит:

- + Проведение мероприятий по анализу защищенности **внутренней инфраструктуры заказчика**
- + Проведение мероприятий по анализу защищенности **внешнего периметра** инфраструктуры заказчика
- + Проведение мероприятий по анализу защищенности **мобильных приложений**
- + Оценка уровня защищенности **информационных систем**
- + **Разработка сценариев** для проведения проверок сотрудников заказчика на предмет устойчивости к атакам методами социальной инженерии
- + **Подготовка отчета** по результатам проведенных мероприятий по анализу защищенности инфраструктуры
- + **Формирование рекомендаций** по повышению уровня защищенности инфраструктуры заказчика

Что необходимо:

- + Знание основных методик по анализу защищенности и тестированию на проникновение
- + Уверенные знания и навыки по анализу защищенности web-приложений, OWASP Top-10
- + Уверенные знания и навыки по анализу защищенности Active Directory, FreeIPA
- + Умение работы с инструментами для проведения анализа защищенности
- + Умение работы с инструментами для проведения фишинговых атак
- + Владение языками программирования (Python, Go, Java, PHP и др.)
- + Знание организационных и технических способов и методов защиты информации
- + Знание сетевых технологий и принципов организации локально-вычислительных сетей
- + Знание английского языка (на уровне, достаточном для свободного чтения технической литературы)

[АНАЛИЗ ВАКАНСИЙ]

CyberED



Rutube

Пентестер инфраструктуры



Опыт работы: 1–3 года

Обязанности:

- Проведение регулярного анализа инфраструктуры для выявления уязвимостей в сетевых компонентах, операционных системах и прикладных сервисах методами black box, grey box, white box;
- Проведение комплексного тестирования на проникновение и имитация действий реального противника (Red Teaming) для проверки эффективности мер защиты и работы SOC;
- Проведение тестирования беспроводных сетей;
- Проведение социотехнического тестирования, включая фишинг-атаки и проверку уровня осведомленности сотрудников о правилах безопасности;
- Подготовка рекомендаций по устранению выявленных уязвимостей и улучшению общей безопасности.

Требования:

- Опыт работы от 1 года в роли **пентестера**;
- Понимание сетевых протоколов: стек TCP/IP, HTTP/S, DNS, DHCP, SMB, RPC, RDP;
- Понимание архитектуры современных ОС и корпоративных сред: Windows и Linux/Unix систем, Active Directory;
- Понимание механизмов аутентификации и авторизации: Kerberos, NTLM, LDAP, а также модели разграничения прав (DACL, ACE, GPO);
- Понимание техник перемещения внутри сети: Методы Lateral Movement, использование Pivot-хостов и обход сегментации;
- Знание BASH, *Python* или любого другого средства скриптовой автоматизации для решения прикладных задач.

[АНАЛИЗ ВАКАНСИЙ]



Сберкорус

Пентестер/Инженер по тестированию защищенности



Опыт работы: 1–3 года

Чем предстоит заниматься:

Основной задачей будет анализ возможности эксплуатации уязвимостей, в частности:

- Выявление уязвимостей и мисконфигураций в информационных системах, веб-приложениях, системном и прикладном ПО
- Проведение проверок применимости уязвимостей, выявленных различными СЗИ
- Оценка (триаж) уязвимостей
- Определение методов и приоритетов устранения уязвимостей
- Формирование аналитических отчетов об уязвимостях
- Инициирование работ по устранению уязвимостей

Ты идеальный для нас кандидат, если у тебя есть:

- Знание базовых мер обеспечения информационной безопасности
- Знание основных типов атак, способов эксплуатации уязвимостей и противодействия им
- Знание стандарта оценки уязвимостей CVSS
- Понимание архитектуры сети и сетевых технологий
- Способность к аналитической работе с данными и внимательность к деталям

Будет большим плюсом:

- Участие в CTF-соревнованиях
- Опыт поиска уязвимостей в качестве внешнего или внутреннего **пентестера** / Red Team / багхантера
- Навыки работы с OWASP ZAP, Burp, Nuclei, Acunetix
- Профильные сертификаты: CEH (Certified Ethical Hacker) и OSCP (Offensive Security Certified Professional)

[АНАЛИЗ ВАКАНСИЙ]



Faberlic

RedTeam специалист



Опыт работы: 1-3 года

Чем предстоит заниматься:

1. Проводить оценку наших текущих правил детектирования в SIEM на предмет функционала их обнаружения.
2. Общаться с командой Аналитиков SOC в рамках разработки/улучшения детектирующей логики.
3. Проводить киберучения с использованием платформы BAS и фреймворков тестирования на проникновение.
4. Исследовать новые техники атак и совместно с командой SOC-аналитиков работать над устранением пробелов в детектировании.
5. Регулярно проводить воркшопы Аналитикам SOC для обмена опытом.
6. Подготовка квартального отчета руководству по текущему уровню зрелости сценариев обнаружения и roadmap по их улучшению.

Чем для нас важно:

1. Опыт работы в роли Инфраструктурного **пентестера** или RedTeam специалиста не менее 1 года
2. Опыт работы с BAS-платформами и создания кастомных сценариев эмуляции техник по MITRE ATT&CK
3. Опыт работы с Linux на уровне администратора
4. Понимание ключевых техник атак на инфраструктуру Windows и Active Directory и умеешь их воспроизводить на практике
5. Имеешь опыт применения популярных фреймворков тестирования на проникновение (например, Cobalt Strike, Metasploit, Empire, netexec и др)
6. Готовность активно развиваться в направлении RedTeam, работать в команде.

Что будет преимуществом:

1. Обладаешь опытом разработки правил детектирования в SIEM(мы используем ELK)
2. Имеешь опыт работ в задачах по управлению уязвимостями

ПРИМЕРЫ СТАЖИРОВОК

Кого мы ищем?

- Начинающих или имеющих опыт специалистов по тестированию на проникновение и анализу защищенности веб-приложений!
- Заинтересованных и уже прошедших заметный путь в этой дисциплине, изучающих направление, участвующих в CTF, практикующих новичков.

Как будет проходить отбор?

- Вы решаете предложенные задачи и пишете по ним отчет
- После того, как Вы отправили нам отчет и свое резюме, мы его изучаем и выносим решение по отбору
- Кандидаты, отправившие самые качественные отчеты и решившие наибольшее число задач, будут приглашены на знакомство и мини-собеседование с тим лидами
- По результатам знакомств будет вынесено итоговое решение по приглашению кандидатов на стажировку

Что ждет стажеров?

- Знакомство с командой Singleton и ее подходами и практиками.
- 1.5 месяца обучения с еженедельными лекциями от участников команды.
- Доступ к рабочим задачам по поиску уязвимостей.
- Работа с наставниками.
- Минимальная оплата труда с занятостью 20 часов в неделю.

По окончании 3-х месяцев, основываясь на том, как специалист показал себя в этот период, будет принято решение о приглашении его в команду в качестве мл. специалиста.

КЛЮЧЕВЫЕ ВЫВОДЫ [ИЗ АНАЛИЗА ВАКАНСИЙ]

ОС и сети:

- + Уверенное знание и администрирование Windows / Linux (особенно **Astra, Kali, Parrot**)
- + Сетевые технологии:
- + Глубокое понимание протоколов **TCP/IP, HTTP/S, DNS, SMB, LDAP**
- + Принципов построения **корпоративных сетей** и **Active Directory**.

Безопасность приложений и инфраструктуры:

- + **Веб-уязвимости**: знание OWASP Top 10 на уровне ручного поиска и эксплуатации
- + **Active Directory (AD)**: понимание атак на AD Обход защиты: опыт обхода WAF, EDR, AV и методов защит.

Программирование и автоматизация (скриптинг):

- + **Python, Bash, PowerShell** - обязательный минимум
- + Желательно также знание **JavaScript, PHP, Go, C/C++**

Зачем?

- написание собственных эксплойтов (PoC),
- доработка чужого кода
- автоматизация рутинных задач.

Инструменты и методологии

► Базовый набор:

- + **Nmap** - сканирование портов и сетей
- + **Burp Suite** - анализ веб-трафика, атаки на веб-приложения (желательно знание Pro-версии)
- + **Metasploit** - фреймворк для эксплуатации
- + **SQLmap** - автоматизация SQL-инъекций
- + **Wireshark / tcpdump** - анализ трафика

КЛЮЧЕВЫЕ ВЫВОДЫ [ИЗ АНАЛИЗА ВАКАНСИЙ]

Методологии и стандарты:

- + OWASP
- + MITRE ATT&C;CK
- + PTES / OSSTMM (стандарты проведения тестирований)

Документирование и коммуникация

- + Написание отчетов:
- + Умение описать найденную уязвимость простым языком, дать четкие рекомендации по исправлению и оценить риск.

ОПЫТ, КОТОРЫЙ ВЫДЕЛИТ ВАС:

- | | |
|---------------|--|
| + CTF: | участие в соревнованиях по кибербезопасности . |
| + Bug Bounty: | наличие найденных уязвимостей в реальных программах . |
| + GitHub: | наличие собственных скриптов или форков известных утилит . |

Сертификаты

(будут плюсом для джуниора и стандартом для мидла):

- eJPT (eLearnSecurity Junior Penetration Tester)
- OSCP (Offensive Security Certified Professional)
- CEH (Certified Ethical Hacker)
! Популярный сертификат для HR-фильтров.

Эту сертификацию можно получить в CyberED

КАК ОБЫЧНО ПРОИСХОДИТ НАЙМ

[СПЕЦИАЛИСТОВ ПО ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ]

- | | | |
|-----------|------------------------------|--|
| 01 | Скрининг (HR): | Проверка на адекватность и наличие базы (техническое образование или профильные курсы) |
| 02 | Техническое интервью: | <ul style="list-style-type: none">— Глубокий опрос по знаниям инструментов, как находить уязвимости,— Могут попросить рассказать примеры проведения пентеста из собственного опыта,— Знания сетей и операционных сетей, умение обходить СЗИ,— Написание собственных инструментов и эксплойтов |
| 03 | Практическое задание: | Решить CTF-задание или более реальный кейс (опционально) |
| 04 | Общение с CISO | (если устраиваетесь в крупную компанию) |

ПОЧЕМУ ДЖУНЫ ПРОВАЛИВАЮТСЯ [НА ОТБОРЕ В ПЕНТЕСТЕ]

-  Слабая фундаментальная база (сети, протоколы, базовые принципы ИБ)
-  Недостаток практических навыков (Linux/CLI, работа с инструментами, поиск уязвимостей)
-  Нет подтвержденной практики

Например:

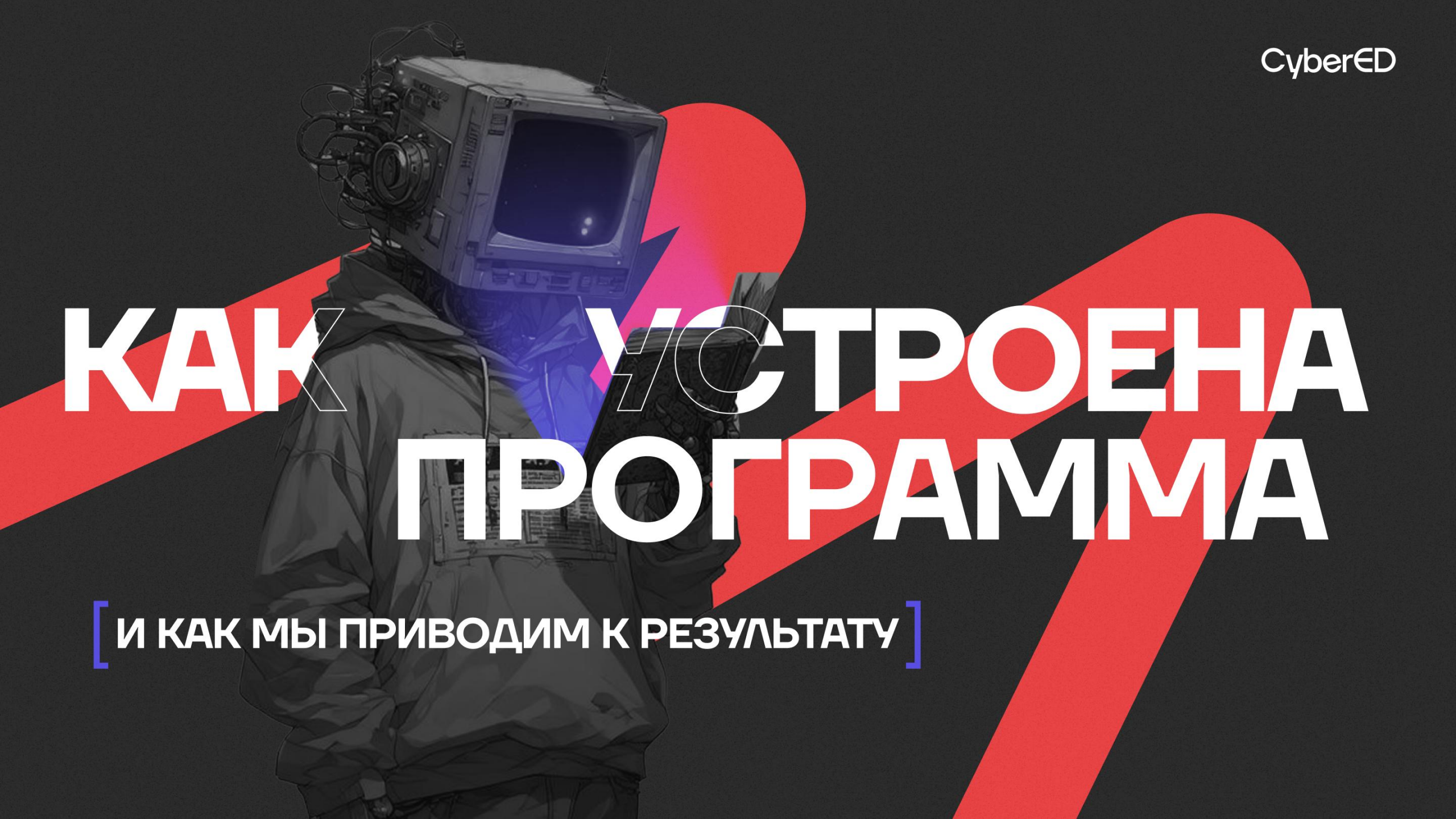
- + Решение CTF
- + Прохождение курсов
- + Кейсы в портфолио



На собеседовании нужно показать: база + логика + практика



Работодатели часто жалуются, что новички **не могут** объяснить, почему инструмент работает принцип работы инструмента и какие уязвимости проверяет данный инструмент на уровне работы протоколов



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

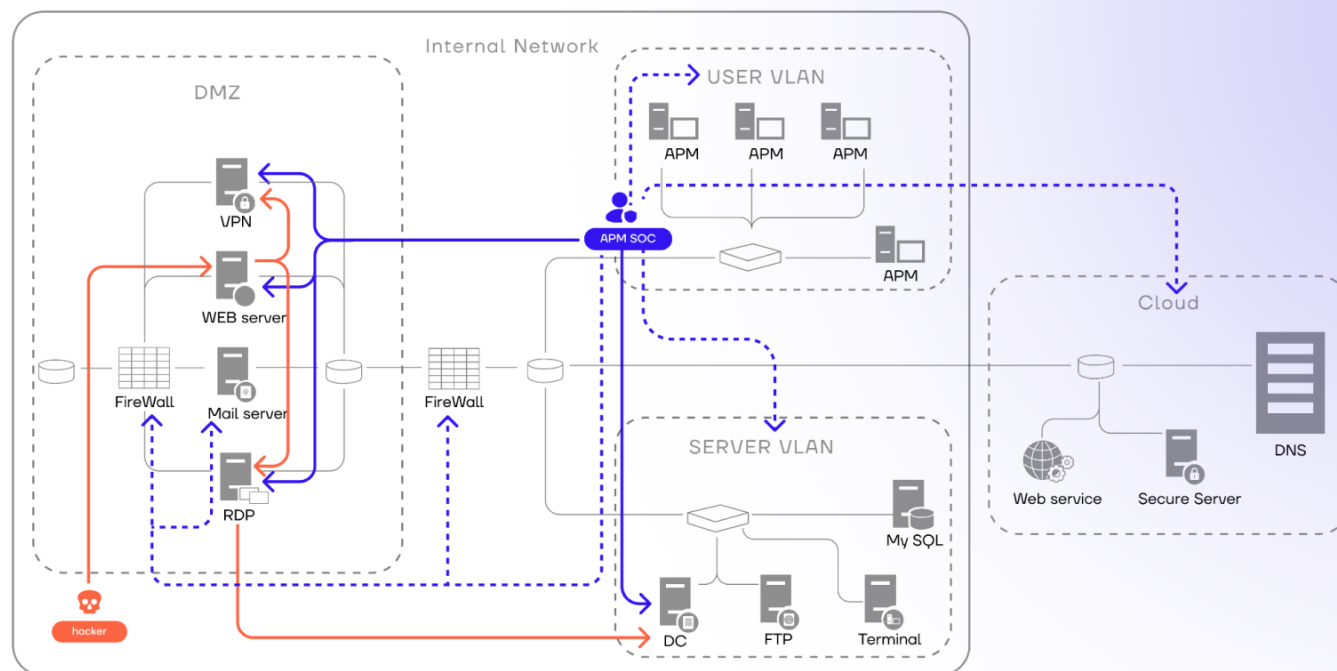
+

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

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

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

Не «один раз попробовал»
→ а закрепление через повторение

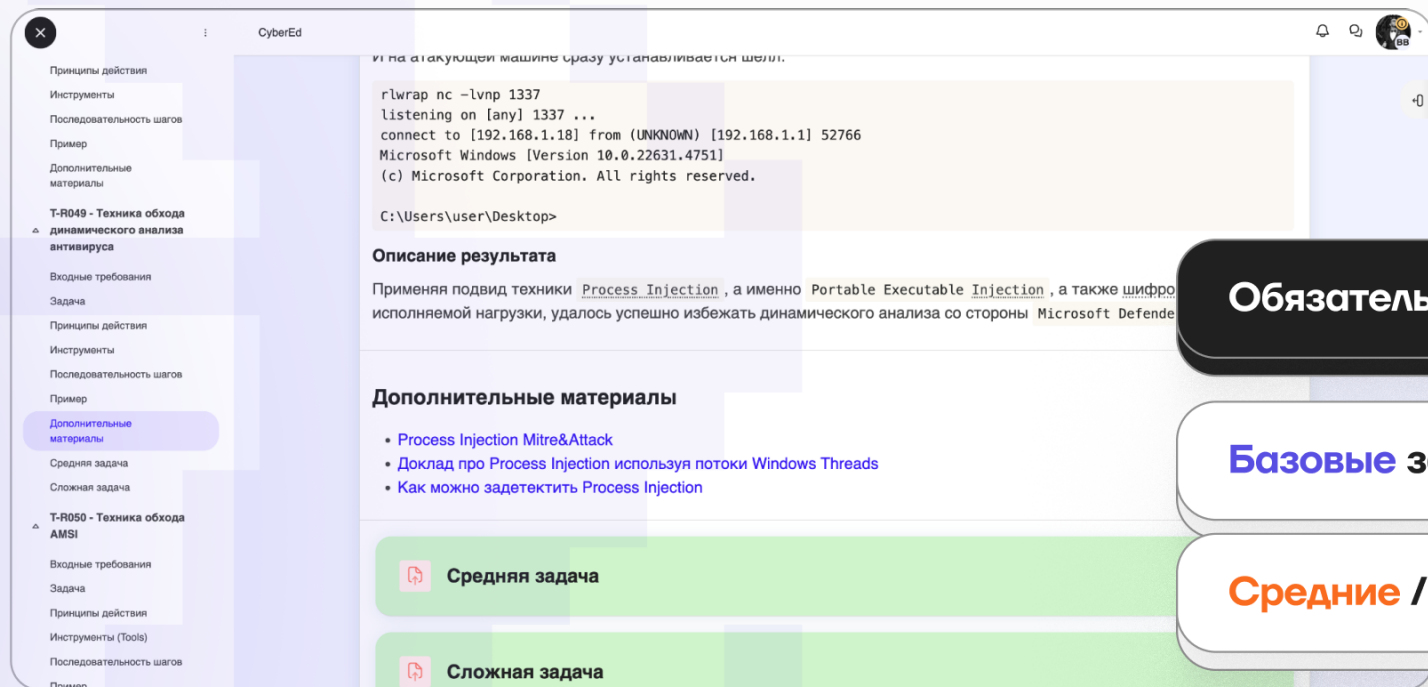
MITRE ATT&CK									
Матрицы Тактика Методы Защитные сооружения СТИ Ресурсы Благотворители Способствовать Блог									
Поиск									
Разведка	Разработка ресурсов	Первоначальный доступ	Исполнение	Упорство	Повышение привилегий	Оборонительное уклонение	Доступ по учетным данным	Открытие	Боковое движение
11 техник	8 техник	11 техник	17 техник	23 техники	14 техник	47 методов	17 техник	34 техники	9 техник
Активное сканирование (3) Соберите информацию о пострадавшем хозяине (4) Соберите информацию о личности жертвы (3) Соберите информацию о сети жертв (3) Соберите информацию об организации-жертве (4) Фининг информации (4) Поиск в закрытых источниках (2) Поиск в открытых технических базах данных (5) Поиск	Получить доступ Приобретение инфраструктуры (8) Компромишенные счета (3) Компромишенная инфраструктура (8) Развитие потенциала (4) Создание счетов (3) Получить возможности (7) Возможности сценария (8) Поиск в открытых технических базах данных (5) Поиск	Вставка контента Компромисс проезда Использование уязвимостей в общедоступных приложениях Внешние удаленные сервисы Дополнительные аппаратные средства Фининг (4) Размножение с помощью съемных носителей Компромисс в цепочке поставок (3) Доверительные отношения Действительные учетные записи (4) Сети Wi-Fi	Команда администрирования облака Интерпретатор команд и скриптов (13) Команда управления контейнерами Развернуть контейнер Команда администрирования ESX Эксплуатация для исполнения клиентскими операциями Ввод входных данных Межпроцессная коммуникация (3) Нативный API Исполнение отравленного трубопровода Запланированная	Манипулирование учетной записью (7) Вакансии в BITS Выполнение автозапуска при загрузке или входе в систему (14) Сценарии инициализации загрузки или входа в систему (5) Интеграция облачных приложений Компрометировать двоящий файл программного обеспечения хоста Создать аккаунт (3) Создание или изменение системного процесса (3) Выполнение, инициализированное событием (18) Побег к хосту	Механизм контроля за повышением уровня насилия (6) Манипулирование токенами доступа (5) Манипулирование учетной записью (7) Выполнение автозапуска при загрузке или входе в систему (14) Сценарии инициализации загрузки или входа в систему (5) Создание или изменение системного процесса (3) Изменение политики домена или арендатора (2) Изменение политики электронной почты Ограничения исполнения (2) Использование	Механизм контроля за повышением уровня насилия (6) Манипулирование токенами доступа (5) Вакансии в BITS Создание образа на хосте Обход отладчика Отложенное исполнение Десобфускация/декодирование файлов или информации Развернуть контейнер Прямой доступ к тому Изменение политики домена или арендатора (2) Подделка электронной почты Ограничения исполнения (2) Использование	Противник посередине (4) Грубая сила (4) Учетные данные из хранилищ паролей (6) Эксплуатация для получения доступа к учетным данным Принудительная аутентификация Подделка веб-учетных данных (2) Захват ввода (4) Изменение процесса аутентификации (3) Перехват многофакторной аутентификации Генерация запроса на многофакторную аутентификацию Обнаружение	Обнаружение учетных записей (4) Обнаружение информации в браузере Обнаружение облачной инфраструктуры Панель управления облачными сервисами Обнаружение облачных сервисов Обнаружение объектов в облачном хранилище Обнаружение контейнеров и ресурсов Обход отладчика Обнаружение	Использование удаленных сервисов Внутренний фининг Боковая передача удаленной информации Перехват сеанса удаленной службы (2) Удаленные сервисы (6) Размножение с помощью съемных носителей Инструменты развертывания программного обеспечения Заграждение общего контента Используйте 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



■ 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

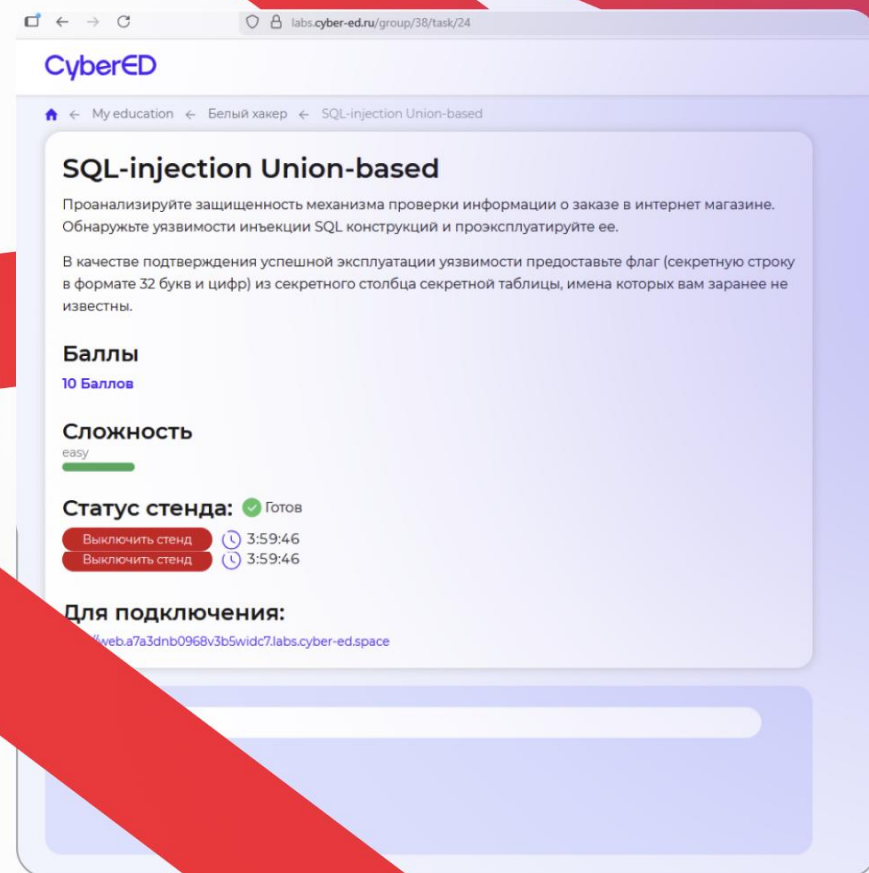
ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ ⚡



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

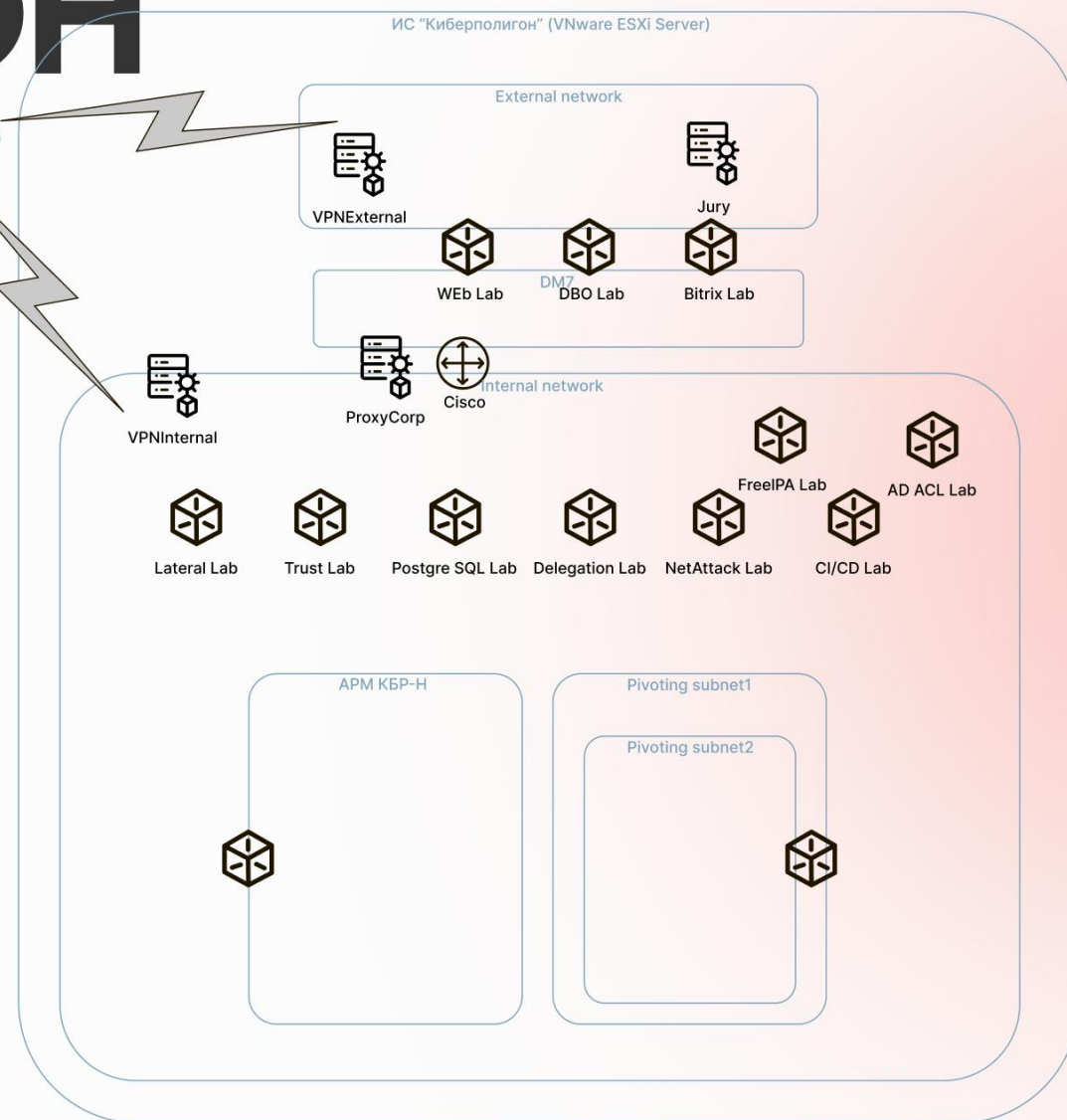
КИБЕРПОЛИГОН

*** CyberED

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

Максимально близко к работе:

« **ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ** »



КИБЕРПОЛИГОН

||** CyberED

30

Сценариев

30

Виртуальных
машин

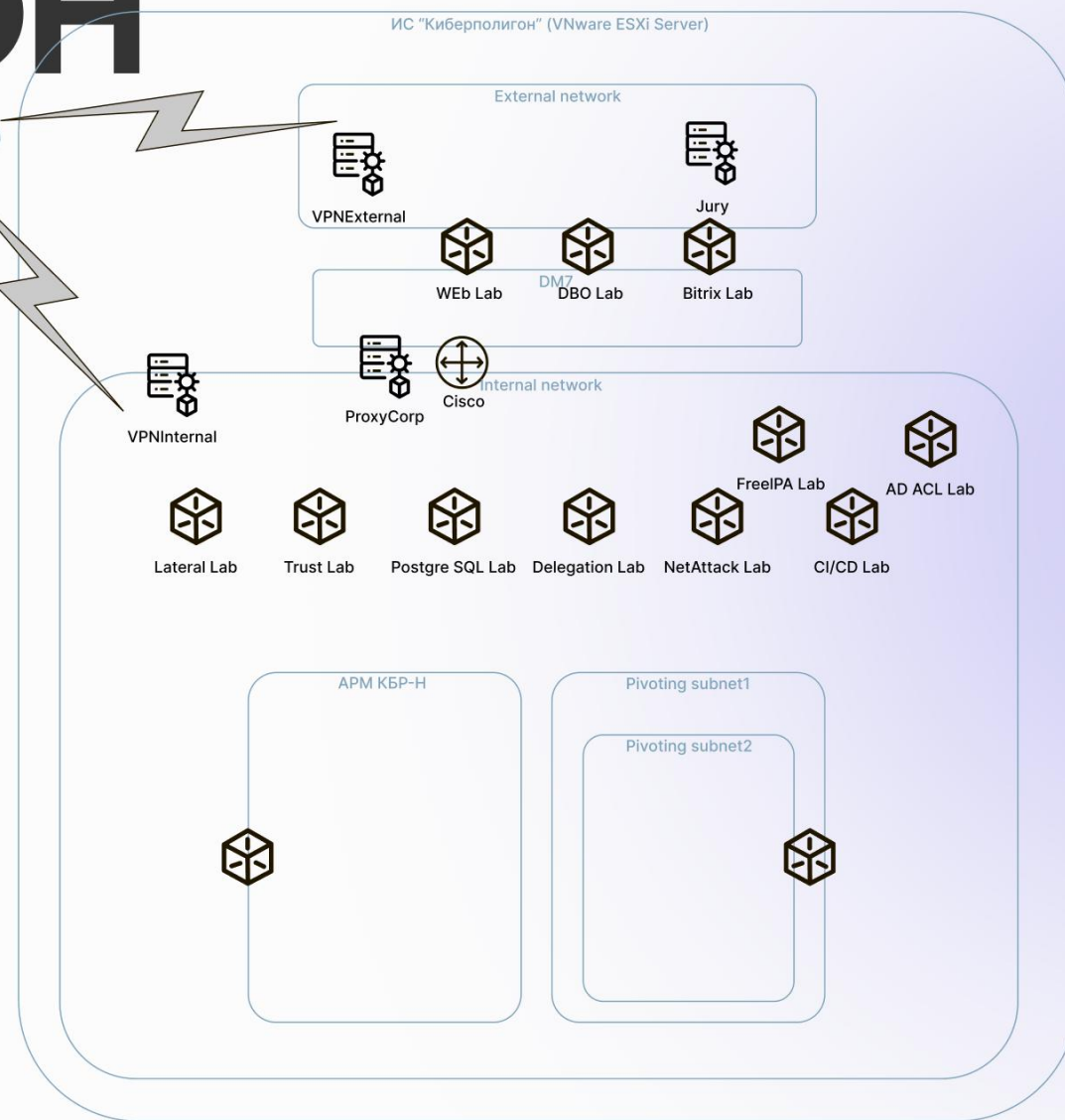
60+

Тасок,
в каждой из которых может быть
несколько уязвимостей.

ЗАДАЧИ

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

- + 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

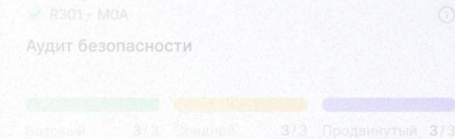
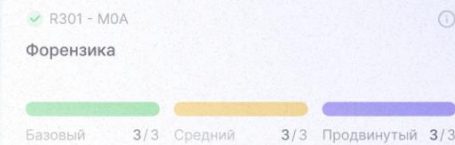
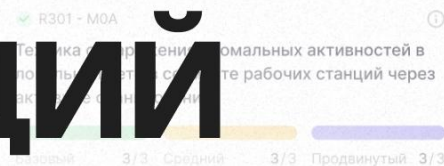
Общие показатели по направлениям



Модуль: Не выбрано ▾

🔍 Скрыть неосвоенные

Аналитик SOC. Демо-курс



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) 0 / 0

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
локальной сети с помощью 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

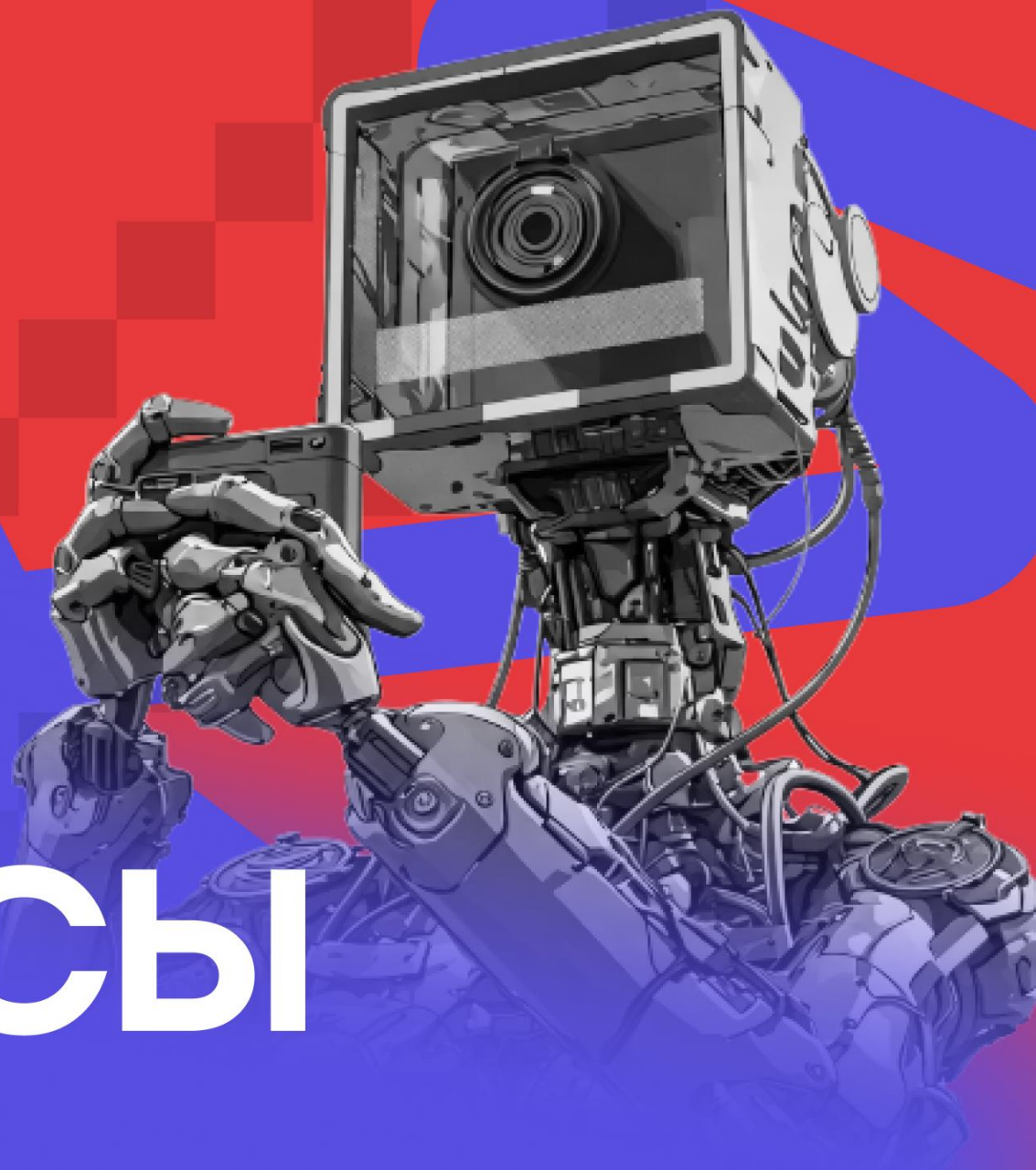
Базовый 3/3 Средний 3/3 Продвинутый 3/3

КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

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

ДАВАЙТЕ РАЗБЕРЕМ
ВАШИ 
ВОПРОСЫ



ПОВЫШЕНИЕ ЦЕНЫ С 1 ИЮЛЯ! ОСТАВЛЯЙ ЗАЯВКУ!



ИИ в пентесте от Похек



Участие в кибериспытаниях



DETA / Авторский курс Егора Зайцева «Обход антивирусов»



1 любой мини-курс из платных программ на выбор



программа «Bug Bounty Hunter» совместно со Standoff 365