

// открытый вебинар · 8 сентября · 19:30 мск · 90 минут

Техническое мок-собеседование с пентестером

Как проходят интервью на **junior** и **middle**.

два кандидата · один эксперт · живой разбор



// кто в эфире

Эксперт и два кандидата



// эксперт · интервьюер

Иван Спиридонов

Senior Specialist, Sovcombank Technologies

Pentest · Red Team · Physical Pentest · Standoff DreamTeam
· BSCP · автор t.me/fck_harder



// кандидат · middle

Константин Баженов

Выпускник CyberED · инженер внедрения VM/SIEM,
багхантер

15 лет в ИТ · MaxPatrol SIEM/VM · PT NGFW · призёр CTF:



// кандидат · junior

Станислав Виноградов

Выпускник CyberED · специалист по
информационной безопасности

Готовится к первым собеседованиям в пентесте ·

// на кого и что смотрят

Грейды пентестера

На каждом уровне растут самостоятельность, глубина и ответственность.

// уровень 1

Junior

ЗНАНИЯ	фундамент: сети, веб, Linux/Windows, базовые инструменты
РАБОТА	по инструкции и под ревью, типовые проверки
ОЦЕНИВАЮТ	ход мысли и обучаемость важнее идеальной команды
ПРИМЕР	«объясни, что такое XSS и где его искать»

// уровень 2

Middle

ЗНАНИЯ	AD и внутренний пентест, веб/API, эксплуатация, автоматизация
РАБОТА	самостоятельно, строит цепочки атак, выбирает инструмент
ОЦЕНИВАЮТ	глубину, риск-ориентированность, качество отчёта
ПРИМЕР	«построй цепочку от SSRF до контроллера домена»

// уровень 3

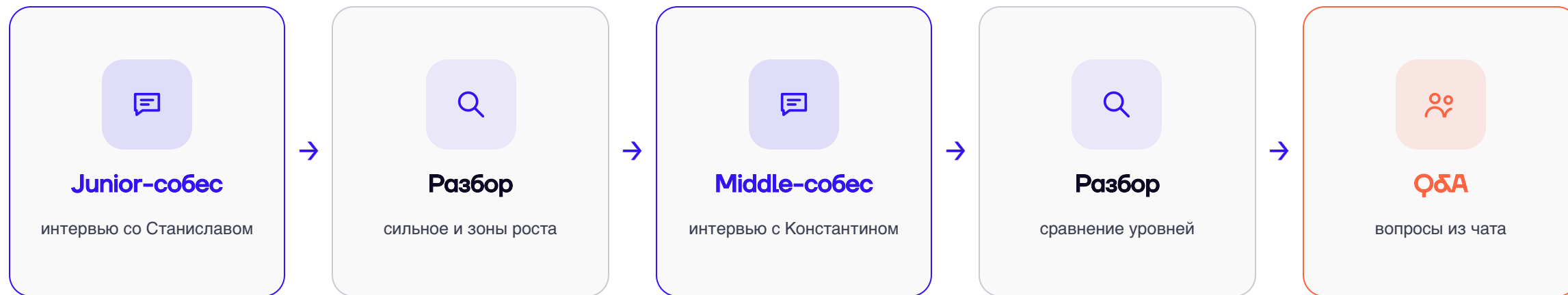
Senior

ЗНАНИЯ	нестандартные векторы, research, методология
РАБОТА	отвечает за результат проекта, менторит команду
ОЦЕНИВАЮТ	коммуникацию с заказчиком и владение процессом
ПРИМЕР	«зашёл в незнакомую инфру без чек-листа — действия?»

// формат эфира

Два ЖИВЫХ собеседования — и разбор

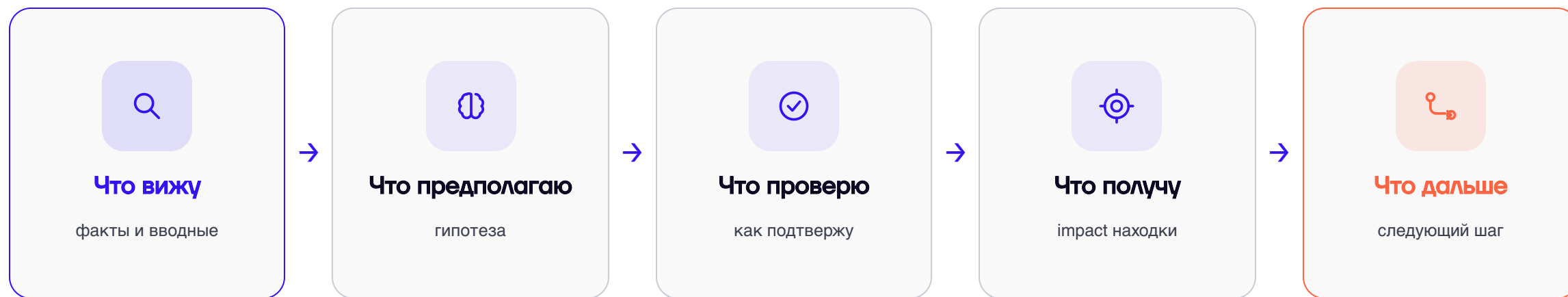
Живая импровизация. После каждого блока — разбор от эксперта.



// оценивают ход мысли, а не зубрёжку

Как построить ответ, даже если не знаешь идеального решения

Точную команду можно забыть — логику рассуждения показать обязательно.



Собеседование Junior

Что ожидают от кандидата на входе в профессию — и какие темы поднимает интервьюер.



// что спрашивают на junior · фундамент

Сети, веб и операционные системы



Сети

Как устроена передача данных и где возникает доверие

- OSI / TCP-IP
- DNS
- HTTP
- cookies / sessions
- REST / SOAP



Веб-основы

Типовые уязвимости веб-приложений и логика их поиска

- OWASP Top-10
- IDOR
- XSS
- SQL Injection
- auth / session



Linux / Windows

Ориентирование в системе и базовое повышение прав

- Linux CLI
- PowerShell
- права и процессы
- службы
- базовый privesc



Инструменты

Чем сканируют, перехватывают трафик и фаззят

- Nmap
- Burp Suite
- Wireshark
- ffuf / wfuzz
- sqlmap

// что спрашивают на junior · подход

Логика тестирования и отчётность



Логика тестирования

Как рассуждает тестировщик, а не набор команд

- reason → гипотеза
- приоритизация
- проверка гипотез
- работа с неизвестным



Отчётность и PoC

Как оформить находку, чтобы её поняли и закрыли

- воспроизводимый PoC
- severity / CVSS
- описание находки
- рекомендации



Методология

По какой структуре идёт проверка

- OWASP WSTG
- чек-листы
- этапы пентеста
- score и правила

// разбор после блока junior

На что смотрит интервьюер

Оценивают не только правильный ответ — важнее ход мысли и умение работать с неизвестным.



Ход мысли

структура рассуждения важнее готового ответа



Уточняющие вопросы

задаёт ли вопросы к условиям задачи



Честность

признаёт границы знаний вместо угадывания



Работа с неизвестным

что делает, когда не знает ответа



Риск-мышление

понимает, что находка даёт атакующему



Конкретика

детали и примеры вместо общих формулировок

Собеседование Middle

Те же темы — но глубже: внутренний пентест,
цепочки атак и самостоятельные решения.



// что спрашивают на middle · глубина

Active Directory, внутренка и web/API



Active Directory

Путь от доменной учётки до контроля над доменом

- enumeration
- Kerberoasting
- AS-REP Roasting
- BloodHound
- ACL / DCSync
- AD CS · delegation



Внутренний пентест

Перемещение и эскалация привилегий внутри сети

- lateral movement
- PsExec / WinRM / WMI
- Responder · NTLM
- Impacket · NetExec
- privilege escalation



Web / API

Глубже базы: логика доступа, доверия и бизнес-правил

- SSRF
- BOLA / IDOR
- Mass Assignment
- CSRF · SameSite
- business logic

// что спрашивают на middle · зрелость

Эксплуатация, автоматизация и оценка риска



Эксплуатация и pivoting

Связывание отдельных багов в рабочую цепочку атаки

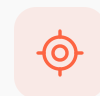
- chaining уязвимостей
- SSRF → internal
- переход web → сеть
- обход allowlist / фильтров



Автоматизация

Свой инструмент под задачу, а не только готовые утилиты

- Python / Bash
- Impacket
- NetExec
- Docker
- свои скрипты и PoC



Оценка риска

Что из найденного действительно опасно для бизнеса

- CVSS
- impact для бизнеса
- приоритизация находок
- что реально эксплуатируемо



Отчётность

Результат, который заказчик сможет воспроизвести и закрыть

- воспроизводимый PoC
- attack chain целиком
- рекомендации по фиксу

// разбор после блока middle

Где планка middle выше

Те же критерии — но глубже: самостоятельность, цепочки и ответственность за результат.



Самостоятельность

ведёт задачу без наводящих вопросов



Цепочки атак

связывает техники в единый сценарий



Impact для бизнеса

не «нашёл баг», а чем это опасно



Выбор инструмента

обосновывает, чем и почему решает



Rules of Engagement

держит в голове ограничения проекта



Альтернативы

не заикливается на одном векторе

// чем отличаются ожидания

Junior → Middle → Senior

Вопросы часто одни и те же — разной остаётся глубина ответа и зона ответственности.

	Junior	Middle	Senior
САМОСТОЯТЕЛЬНОСТЬ	под ревью	ведёт задачу сам	отвечает за проект
ГЛУБИНА	фундамент и типовое	цепочки, AD, эксплуатация	research, нестандартное
КОММУНИКАЦИЯ	проговаривает ход мысли	обосновывает решения	говорит с заказчиком
ОТВЕТСТВЕННОСТЬ	за свой участок	за качество находок	за методологию и команду

↑ Чем выше грейд — тем больше **самостоятельности**, глубины и ответственности за конечный результат.

// работает на любом грейде

Как отвечать на техническом собеседовании



Уточняй условия

Задавай вопросы к вводным — это плюс, а не минус



Проговаривай ход мысли

Вслух: что видишь, что предполагаешь, что проверишь



Обозначай допущения

«Если это так — делаю так; если нет — иначе»



Честно о границах

«Здесь не уверен» лучше, чем уверенная ошибка

// личный план перед собесом

Как готовиться



Повтори фундамент

Сети, веб, ОС, протоколы — база, к которой возвращаются



Практикуйся на стенде

Руками на лабах, а не только в теории



Фиксируй проекты

Что делал и какой результат — это твой рассказ на собеседовании



Тренируй объяснение

Проговаривай решения вслух, как на интервью

// финал эфира

Вопросы из чата и советы напоследок

Разберём ваши вопросы по подготовке к техническому собеседованию
— задавайте в чат.