

Вводный вебинар — AI-челлендж

Как использовать AI-агентов в пентесте и баг-баунти

10 сентября · четверг

19:30 МСК

≈ 60 минут



// whoami

Максим

- В свободное время — ресерч по информационной безопасности, самый разный
- Последнее время — мобильные платформы, в первую очередь Android
- Результаты ресерча сразу проверяю на практике — в баг-баунти
- С командой несколько раз участвовал в кибербитвах Standoff
- Профильные сертификаты по внутреннему и вебу
- Веду свой Telegram-канал — t.me/h3ckb0t

Mobile · Android

Bug Bounty

Standoff

// план вебинара

Что нас ждёт сегодня

01 Где взять доступ к моделям

02 Offensive-задачи для LLM

03 Шаблоны контекста

04 Помимо «find all vulns»

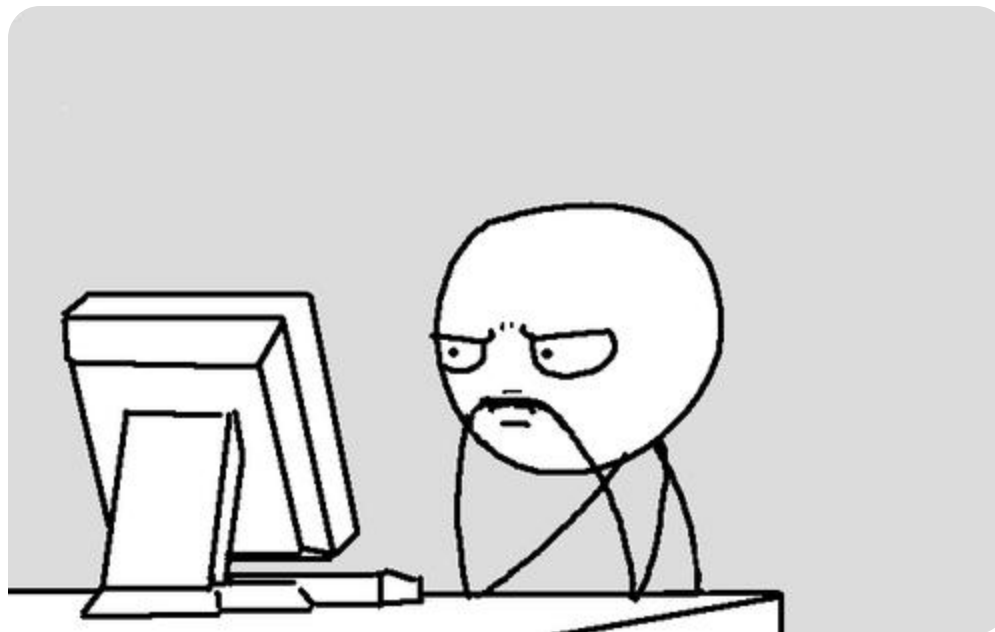
05 Скиллы: что, как и зачем

06 Стенд AI-челленджа

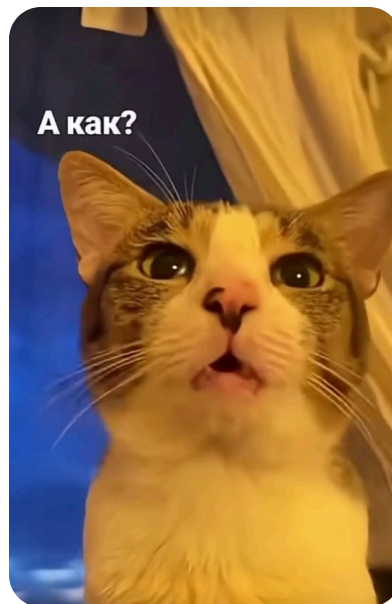
Подписка или развернуть локально?



А где их **применять**?



Заставляем модель делать ТО, ЧТО НУЖНО НАМ



ИИ — мультипликатор навыков,
а не замена им



// для участников челленджа

Твоя неделя на стенде

КАК ПОДКЛЮЧИТЬСЯ

- 01 Регистрируешься на **standoff365**
- 02 Заходишь на стенд челленджа
- 03 Скачиваешь VPN и подключаешься
- 04 Запускаешь агента с дефолтным промптом

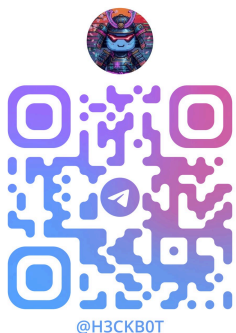
КАК ВЫЖАТЬ МАКСИМУМ

- 05 Решай параллельно — руками и агентами
- 06 Настрой конфигурацию
- 07 Перепроверяй находки
- 08 Через неделю в это же время — разбор

// финал

Увидимся на разборе через неделю

Готов ответить на ваши вопросы прямо
сейчас.



Мой Telegram-канал

@h3ckb0t · t.me/h3ckb0t

