

AI-ХАКЕРЫ

НА ЧТО НА САМОМ ДЕЛЕ СПОСОБЫ ИИ-
ХАКЕРЫ НА СЕГОДНЯШНИЙ ДЕНЬ

А. Ахмедходжаев
C7 CYBERSECURITY

Akhmedkhodjaev

Aziz

Основатель и Руководитель
C7 Cybersecurity
C7 Academy

Со-основатель
Tenax Security Group
Card Reviews
и другие.



AI-ХАКЕРЫ

А. Ахмедходжаев
C7 CYBERSECURITY



XBOW 🏆 @Xbow · 17 дек. 2024 г.



While developing XBOW over the past three months, we played around with using it for bug bounties and ended up at #11 in the US on HackerOne:

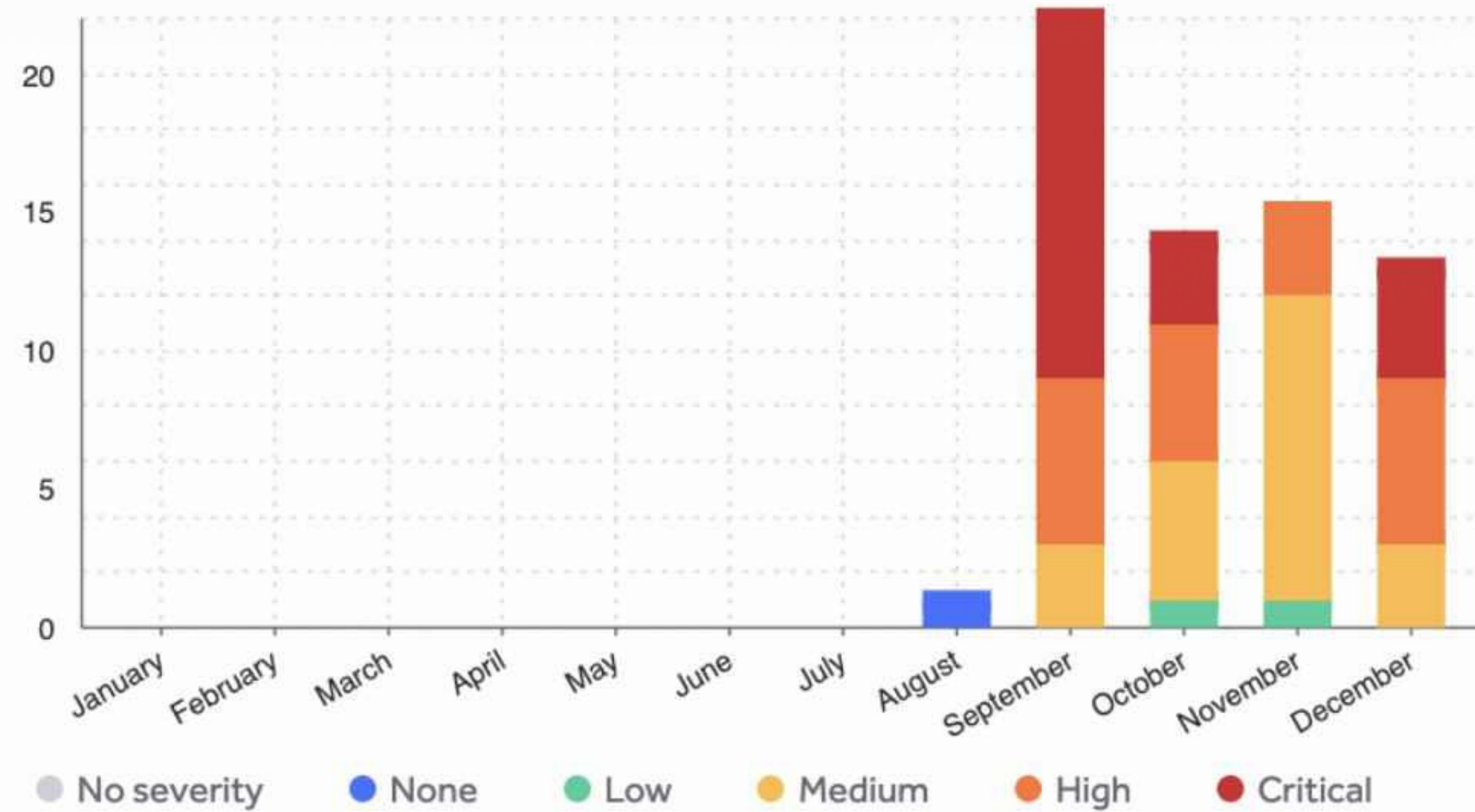
			Reputation	Signal ⓘ	Impact ⓘ
1.		ace_mccloud	1593	7.00	26.67
10.		7urb0	545	7.00	25.88
11.		xbow	481	7.00	29.00



XBOW 🟢 @Xbow · 17 дек. 2024 г.



65 reports were submitted since September, including 20 critical findings



Country

Based on reputation gain.

United States of America (US) ▾

			Reputation
▲ 1.		xbow	1638
▲ 2.		n3rdnymph	1493
▼ 3.		r3aper__	1032
▲ 4.		arw9234	815



XBOW (xbow)

<https://www.xbow.com>

☆ Follow

Joined August 2024



Stats

90 Days ▾

6.63

36th

Hacktivity ?

The Walt Disney Company

0 Bug reported by [xbow](#) was resolved 16 hrs ago

VF Corporation - VDP

0 Bug reported by [xbow](#) was resolved 17 hrs ago

IBM

0 Bug reported by [xbow](#) was resolved 18 hrs ago

KHealth

1 Bug reported by [xbow](#) was resolved 2 days ago

Databricks

2 Bug reported by [xbow](#) was resolved 6 days ago

[See all of xbow's Hacktivity →](#)

C7

ARTIFICIAL INTELLIGENCE | 9 MIN READ

AI vs Human: CTF results show AI agents can rival top hackers

Learn how companies test, train, and benchmarking cybersecurity AI agents with customized CTF competitions.



b3rt0ll0, Apr 16 2025

8 ИИ-АГЕНТОВ

VS

403 ХАКЕРОВ

РЕЗУЛЬТАТЫ

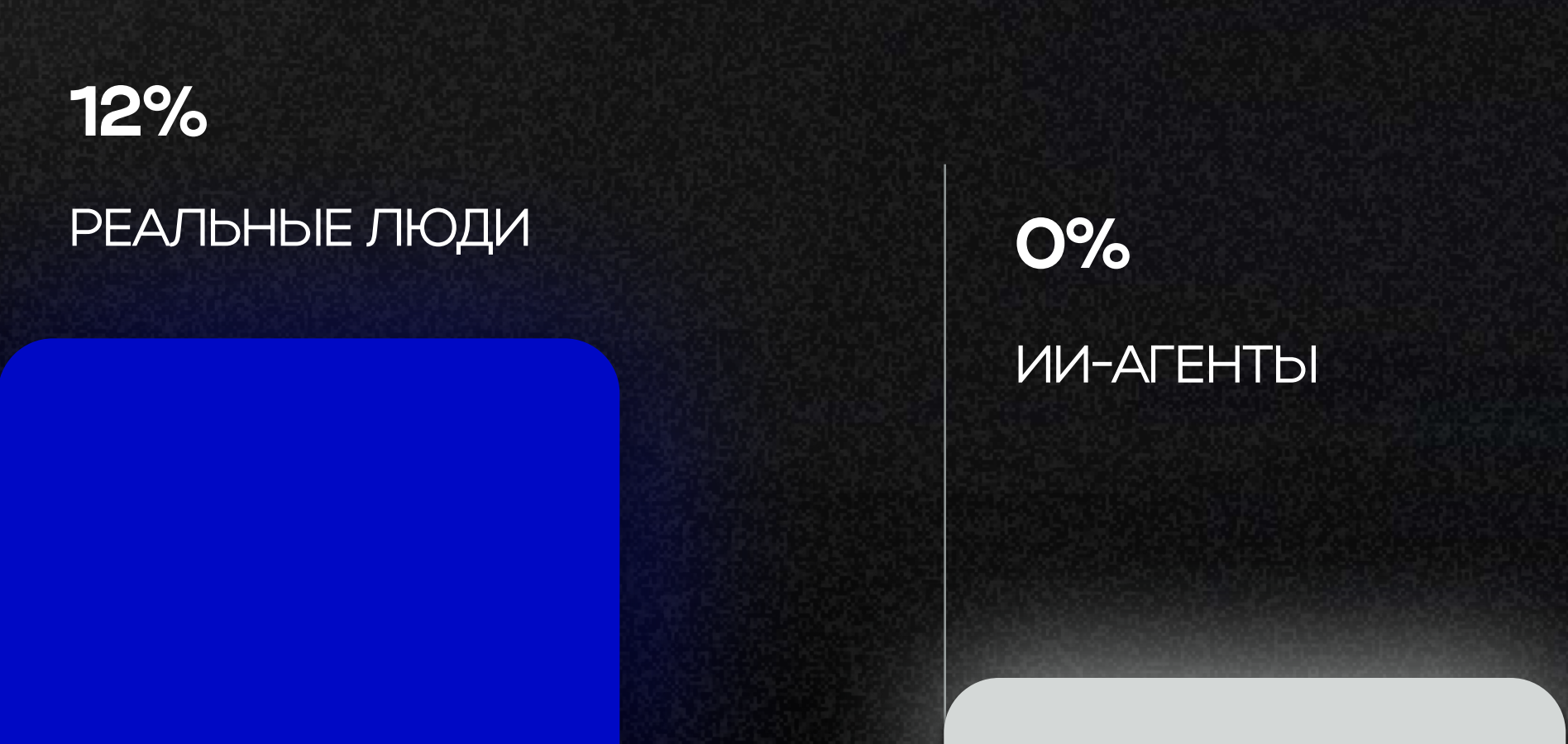
55%

РЕАЛЬНЫЕ ЛЮДИ

95%

ИИ-АГЕНТЫ

РЕЗУЛЬТАТЫ



ЗАМЕНИТ ЛИ ИИ ПЕНТЕСТЕРОВ?

СМОЖЕТ ЛИ ИИ ЗАМЕНИТЬ РАЗРАБОТЧИКОВ?

НЕТ

ПОЧЕМУ?

ИССЛЕДОВАНИЯ



$$\frac{(y \notin \Gamma) \quad \Gamma \vdash \langle \Delta; L \rangle \rightarrow_p \langle \Delta_L; L' \rangle : T_L \quad \langle \Delta; y \rangle \rightarrow_p \langle \Delta_L; \text{property}[L'] \rangle : [T_L] \langle \rangle \vdash \langle \Delta_L; N[L/y] \rangle \rightarrow_p \langle \Delta_N; e^+ \rangle : T^+}{\langle \Delta; \text{if-has } L \ p : T_x \text{ bind-as } x \text{ in } M \text{ else } N \rangle \rightarrow_p \langle \Delta_N; e^+ \rangle : T^+}$$

$$\frac{\Gamma \vdash \langle \Delta_L; N \rangle \rightarrow_p \langle \Delta_N; e_2^+ \rangle : T^+ \quad (p_1 \neq p \wedge \dots \wedge p_n \neq p) \quad \langle \Delta; L \rangle \rightarrow_p \langle \Delta_L; e_1^+ \rangle : [T] \langle p_1 \hookrightarrow e_1[P_1], \dots, p_n \hookrightarrow e_n[P_n] \rangle}{\langle \Delta; \text{if-has } L \ p : T_x \text{ bind-as } x \text{ in } M \text{ else } N \rangle \rightarrow_p \langle \Delta_N; e_2^+ \rangle : T^+} \text{ R-If-Has-2}$$

$$\frac{\Gamma \vdash \langle \Delta_L; N \rangle \rightarrow_p \langle \Delta_N; e_2^+ \rangle : T^+ \quad (P \neq T_x) \quad \Gamma \vdash \langle \Delta; L \rangle \rightarrow_p \langle \Delta_L; e_1^+ \rangle : [T] \langle \dots, p \hookrightarrow e[P], \dots \rangle}{\langle \Delta; \text{if-has } L \ p : T_x \text{ bind-as } x \text{ in } M \text{ else } N \rangle \rightarrow_p \langle \Delta_N; e_2^+ \rangle : T^+} \text{ R-If-Has-3}$$

$$\frac{\Gamma \vdash \langle \Delta_L; e \rangle \rightarrow_p \langle \Delta_L; e \rangle : P \quad \Gamma \vdash \langle \Delta; L \rangle \rightarrow_p \langle \Delta_L; e_1^+ \rangle : [T] \langle \dots, p \hookrightarrow e[P], \dots \rangle \quad x : P, \langle \Delta_L; x \rangle \rightarrow_p \langle \Delta_L; e \rangle : P \vdash \langle \Delta_L; M \rangle \rightarrow_p \langle \Delta_M; e_2^+ \rangle : T^+}{\langle \Delta; \text{if-has } L \ p : P \text{ bind-as } x \text{ in } M \text{ else } N \rangle \rightarrow_p \langle \Delta_M; e_2^+ \rangle : T^+} \text{ R-If-Has-4}$$

ФОРМАЛЬНЫЕ ЯЗЫКИ

1.6 Substitution

$$\begin{aligned}
 (\lambda y . y x)[x := x y] &\equiv \lambda z . ((z x)[x := x y]), \\
 &\equiv \lambda z . ((z[x := x y])(x[x := x y])), \\
 &\equiv \lambda z . z(x y).
 \end{aligned}$$

$$\begin{aligned}
 (2) \quad (\lambda x . y x)[x := x y] &\equiv \lambda z . ((y z)[x := x y]), \\
 &\equiv \lambda z . ((y[x := x y])(z[x := x y])), \\
 &\equiv \lambda z . y z,
 \end{aligned}$$

$$\text{Note:} \quad =_{\alpha} \lambda x . y x \text{ (cf. Remark 1.6.3 (2)).}$$

$$\begin{aligned}
 (3) \quad (\lambda x y . z z x)[z := y] &\equiv \lambda u . ((\lambda y . z z u)[z := y]), \\
 &\equiv \lambda u . \lambda v . ((z z u)[z := y]),
 \end{aligned}$$

:

ЛИДЕРЫ РЫНКА ИИ- ПЕНТЕСТИНГА



GECKO
SECURITY
(УС, ВЕЛИКО-
БРИТАНИЯ)

RIDGEBOT
(США/КИТАЙ)

HADRIAN
(НИДЕРЛАНДЫ)

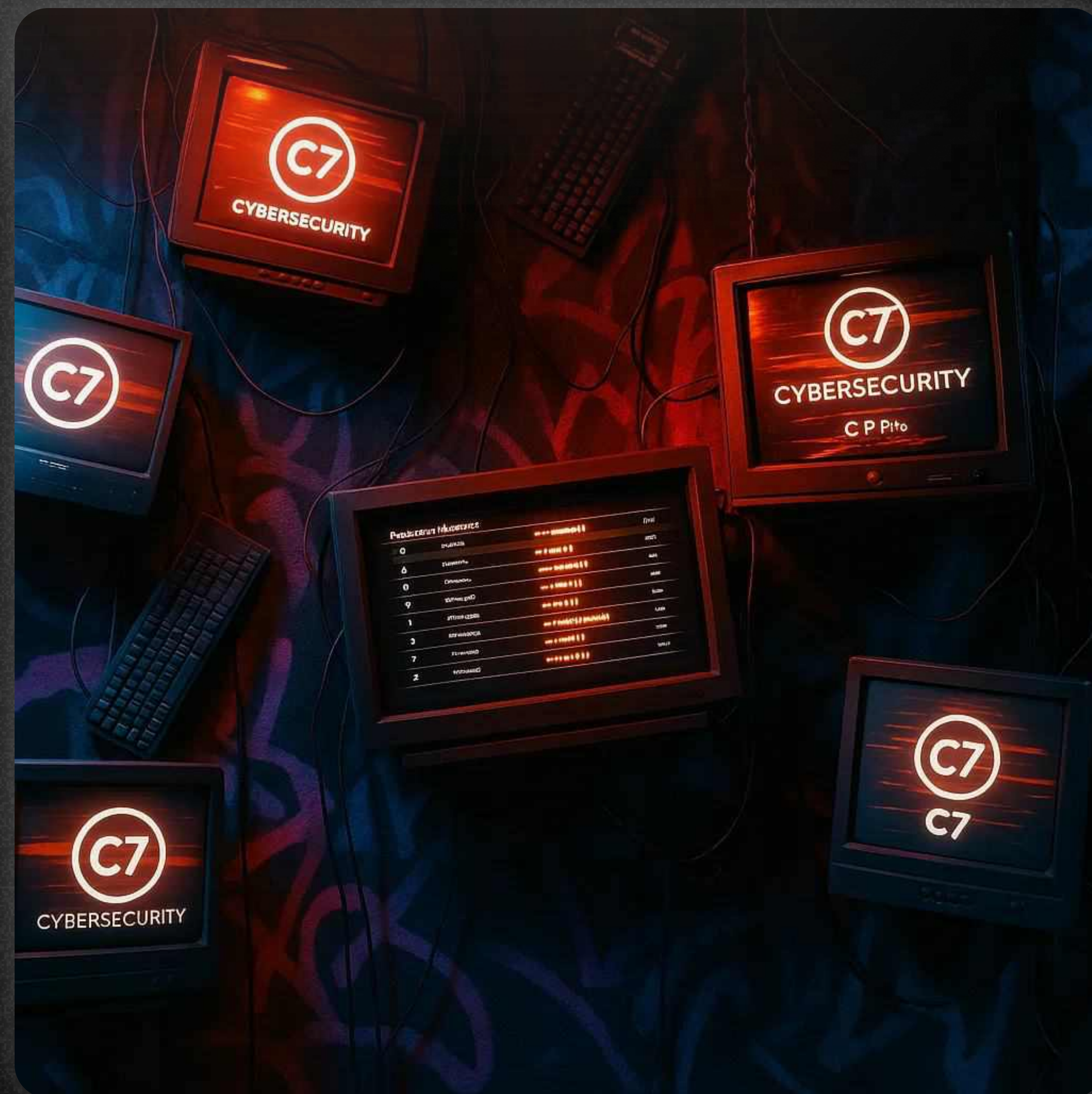
XBOW (США)

СРАВНИТЕЛЬНАЯ ТАБЛИЦА РЕШЕНИЙ

РЕШЕНИЕ	ФУНКЦИОНАЛЬНОСТЬ	АВТОМАТИЗАЦИЯ	АВТОНОМНОСТЬ	ТЕХНОЛОГИИ	ОГРАНИЧЕНИЯ
XBOW (США)	ВЕБ-ПЕНТЕСТ	ПОЛНЫЙ ЦИКЛ	ПОЛНОСТЬЮ АВТОНОМНЫЙ	LLM (БОЛЬШАЯ ЯМ) + СОБСТВЕННЫЙ АГЕНТНЫЙ ДВИЖОК; ОПЫТ GITHUB COPILOT	УЗКАЯ ОБЛАСТЬ
GECKO (UK)	APPSEC-ПОМОЩНИК	ГЛУБОКАЯ ИНТЕГРАЦИЯ	ЧАСТИЧНО АВТОНОМНЫЙ	LLM + СТАТИЧЕСКИЙ АНАЛИЗ КОДА	ФОКУС НА ВЕБ- ПРИЛОЖЕНИЯХ
HADRIAN (NL)	ВНЕШНИЙ ПЕНТЕСТ	АВТО-СКАН И ОЦЕНКА ПРИОРИТЕТОВ	ЧАСТИЧНО АВТОНОМНЫЙ	AI-АГЕНТ С ИНСТРУМЕНТАМИ РАЗВЕДКИ	AI-АГЕНТ С ИНСТРУМЕНТАМИ РАЗВЕДКИ
RIDGEBOT (US/CN)	СЕТЕВОЙ ПЕНТЕСТ	ПОЛНАЯ АВТОМАТИЗАЦИЯ	ПОЛНАЯ АВТОНОМНОСТЬ	DUAL AI: RIDGEBRAIN (TENSORFLOW DL ДЛЯ АТАК) + RIDGEGEN	БОЛЬШЕ ПОКРЫВАЕТ ИЗВЕСТНЫЕ УЯЗВИМОСТИ

АНАЛИЗ РЕШЕНИЙ: ЧТО КОНКРЕТНО МОЖЕТ ИИ В ХАКИНГЕ?

ПРОЦЕСС ХАКИНГА







СКАНИРОВАНИЕ И РАЗВЕДКА

ВЫПОЛНЯЕТ РУТИННУЮ
РАБОТУ ПО
СКАНИРОВАНИЮ ВСЕГО
ПЕРИМЕТРА

МОЖЕТ ВЫПОЛНИТЬ
УМНОЕ СКАНИРОВАНИЕ
ДЛЯ УМЕНЬШЕНИЯ ШУМА
И УБРАТЬ FALSE
POSITIVES (ИДЕАЛЬНО
ПОДХОДИТ ДЛЯ
ПОСЛЕДНЕГО)

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ – СОВМЕСТНАЯ РАБОТА

ПОИСК
ЭКСПЛОЙТОВ

ГЕНЕРАЦИЯ
АТАК

НАПИСАНИЕ
ЭКСПЛОЙТА

ОГРАНИЧЕНИЯ

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

ИДЕАЛЬНО СПРАВЛЯЕТСЯ:
ПОИСК CVE И УЯЗВИМОСТЕЙ
КОНКРЕТНОЙ ТЕХНОЛОГИИ
ВО ВСЕХ ИСТОЧНИКАХ;
ДАЖЕ АДАПТАЦИЯ
ЭКСПРОИТА ПОД
КОНКРЕТНЫЙ EDGE КЕЙС;

МОЖЕТ СГЕНЕРИРОВАТЬ
МНОГО PAYLOADS (ЛЕГЧЕ,
ЧЕМ ЧЕЛОВЕКУ),
ВКЛЮЧАЯ СЛОЖНЫЕ
PAYLOADS (ПРИМЕР —
УЯЗВИМОСТЬ С JENKINS);

ТРУДНО ПИШЕТ
СЛОЖНЫЕ ЭКСПЛОИТЫ
ВНЕ ВЕБА, КОТОРЫЕ
СВЯЗАННЫ С
ИСПОЛНЕНИЕМ В ОС;
МНОГО ГАЛЛЮЦИНИРУЕТ

ПОСТ-ЭКСПЛУАТАЦИЯ – ПРОДВИЖЕНИЕ ВНУТРИ И ЗАКРЕПЛЕНИЕ

ПОВЫШЕНИЕ
ПРИВИЛЕГИЙ

БОКОВОЕ
ДВИЖЕНИЕ

ЗАКРЕПЛЕНИЕ

РИСКИ

ПОСТ-ЭКСПЛУАТАЦИЯ – ПРОДВИЖЕНИЕ ВНУТРИ И ЗАКРЕПЛЕНИЕ

ПРИ НАСТОЯЩЕМ RED TEAMING ДОЛЖЕН ВСЕ КОМАНДЫ ИСПОЛНЯТЬ ТОЛЬКО СПЕЦИАЛИСТ; НИ В КОЕМ СЛУЧАЕ НЕЛЬЗЯ ДОПУСТИТЬ НЕЖЕЛАТЕЛЬНУЮ ДАЖЕ КОПЕЙКУ ШУМА, ПОЭТОМУ ХАКЕРЫ МОГУТ НАХОДИТЬСЯ В СЕТИ ДАЖЕ ГОД

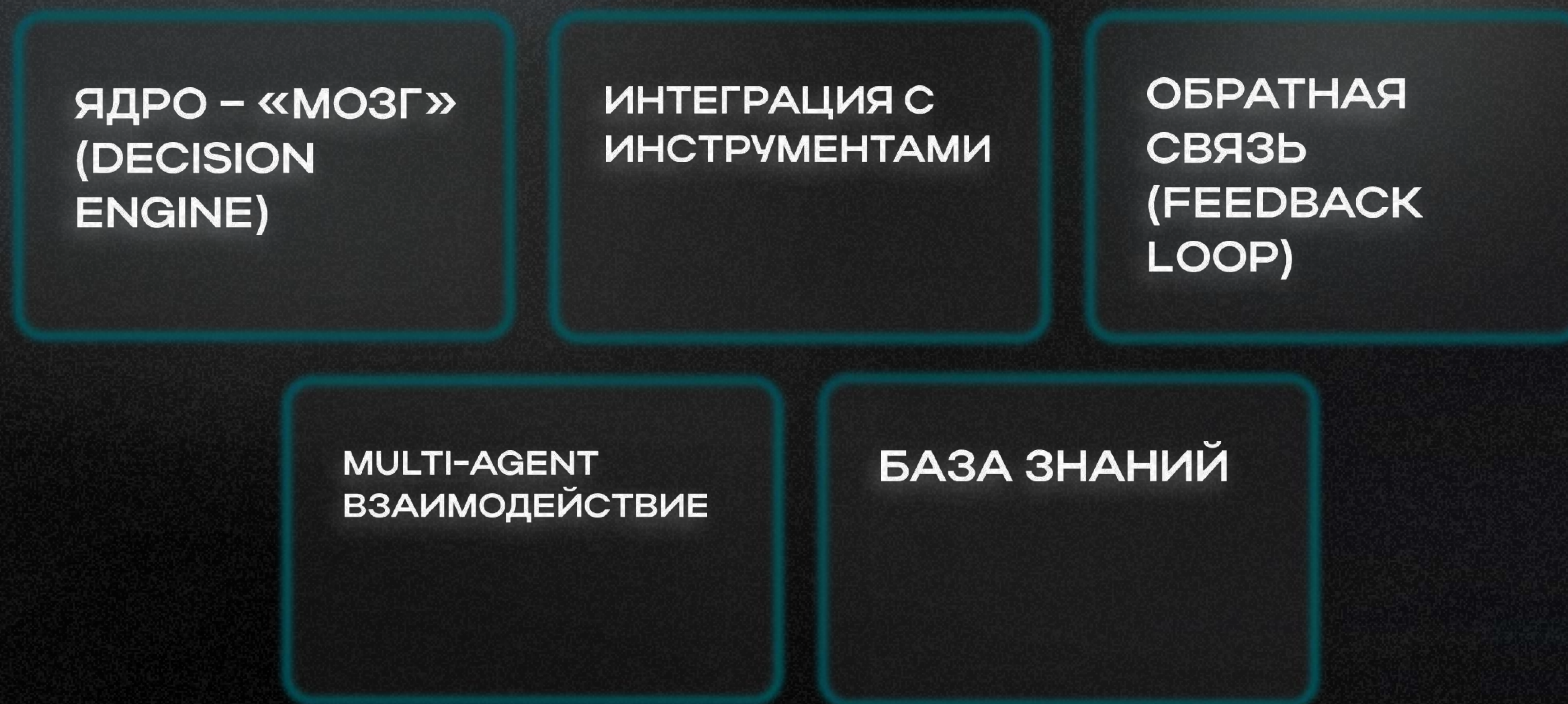
ПРИ ПЕНТЕСТЕ ОДНАКО (КОГДА ШУМ РАЗРЕШЕН) ХОРОШО СПРАВЛЯЕТСЯ С ЛОКАЛЬНЫМ ENUMERATION, ТАК КАК ЭТО РАЗВЕДКА ИЗНУТРИ

RENTERA И АНАЛОГИЧНЫЕ РЕШЕНИЯ БЕЗ ИИ УЖЕ ПРОВОДЯТ АВТОМАТИЗИРОВАННЫЕ ПРОВЕРКИ LATERAL MOVEMENT ПО ИЗВЕСТНЫМ СЦЕНАРИЯМ. С ПРИМЕНЕНИЕМ ИИ ЭТА АКТИВНОСТЬ СТАНОВИТСЯ ГИБЧЕ: АГЕНТ САМ РЕШАЕТ, КУДА ПОЙТИ ДАЛЬШЕ, И КАКИЕ ИНСТРУМЕНТЫ ПРИМЕНИТЬ, ПРАКТИЧЕСКИ КАК ОПЫТНЫЙ ЗЛОУМЫШЛЕННИК

ОТЧЕТНОСТЬ

ИДЕАЛЬНАЯ ЗАДАЧА ДЛЯ ИИ

КАК РАБОТАЮТ ИИ-АГЕНТЫ ДЛЯ ПЕНТЕСТА (ОБЩАЯ АРХИТЕКТУРА)



ОГРАНИЧЕНИЯ И ВЫЗОВЫ ИИ-ПЕНТЕСТИНГА

ТВОРЧЕСКИЕ
АТАКИ

КОНТЕКСТ
И СРЕДА

ЛОЖНЫЕ
СРАБАТЫВАНИЯ

ОБНОВЛЁННОСТЬ
ЗНАНИЙ

ЭТИЧНОСТЬ
И КОНТРОЛЬ

QnA?