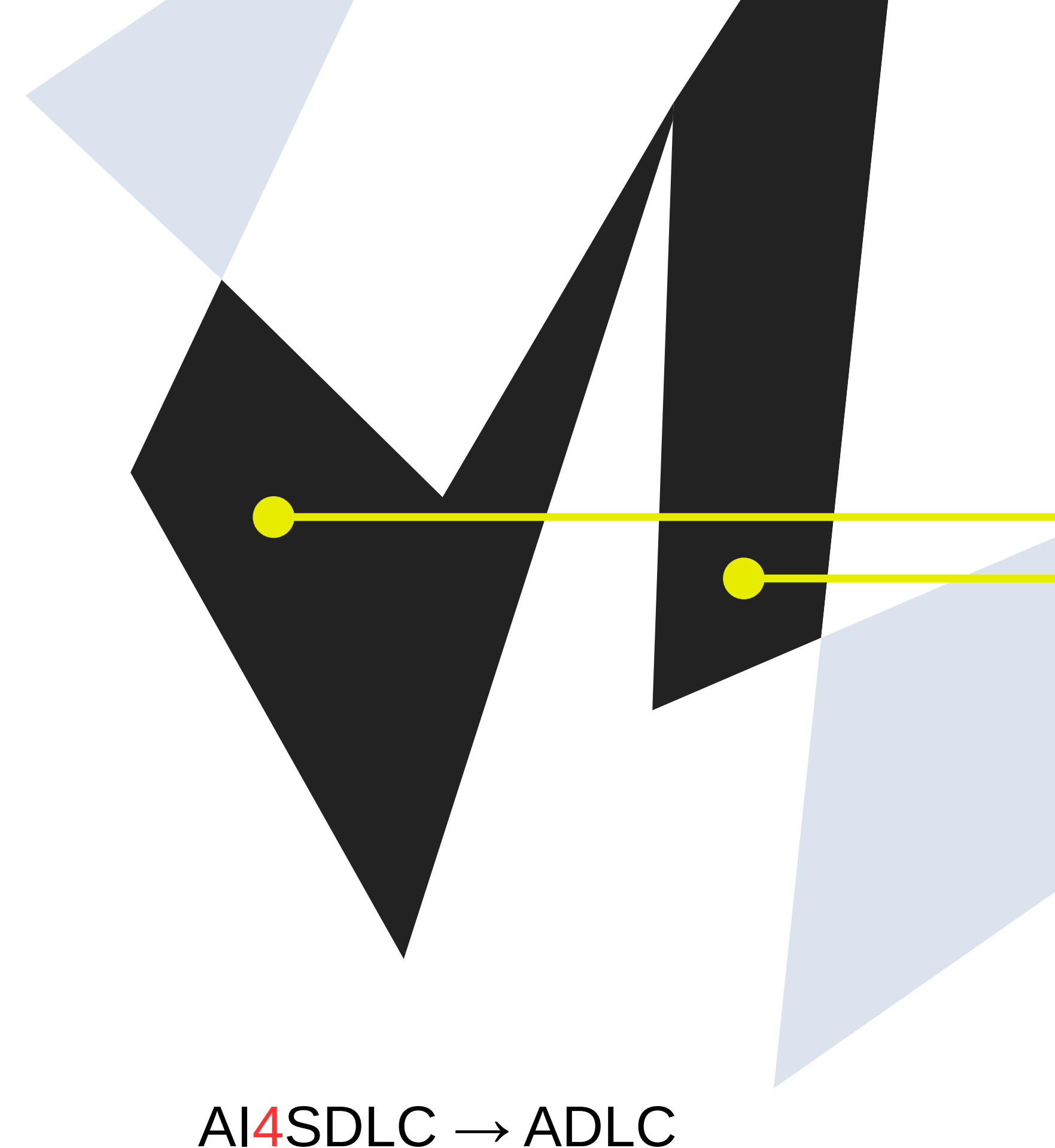




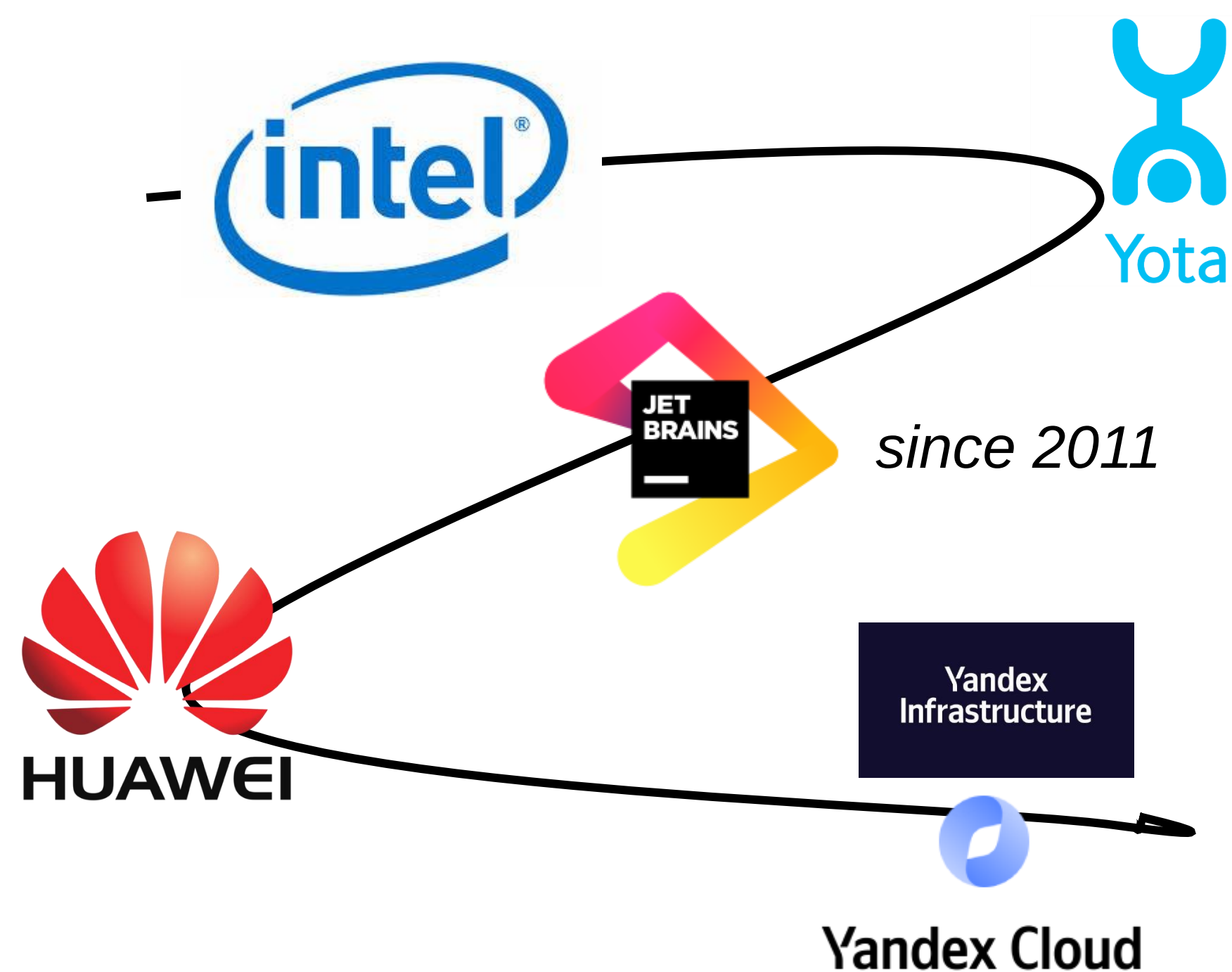
Когда код пишут не только люди

Как меняется разработка в эпоху
Agentic Development Lifecycle

Дмитрий Иванов, @korifey_ad
SourceCraft, Yandex Cloud



Дмитрий Иванов



Руководитель платформы
SourceCraft, Yandex Cloud



Дмитрий Иванов

Опыт в создании инструментов
разработки: 15 лет

Релевантных эпохе: **0** лет

Руководитель платформы
SourceCraft, **Y**andex Cloud



Коротко о том, что я
делаю

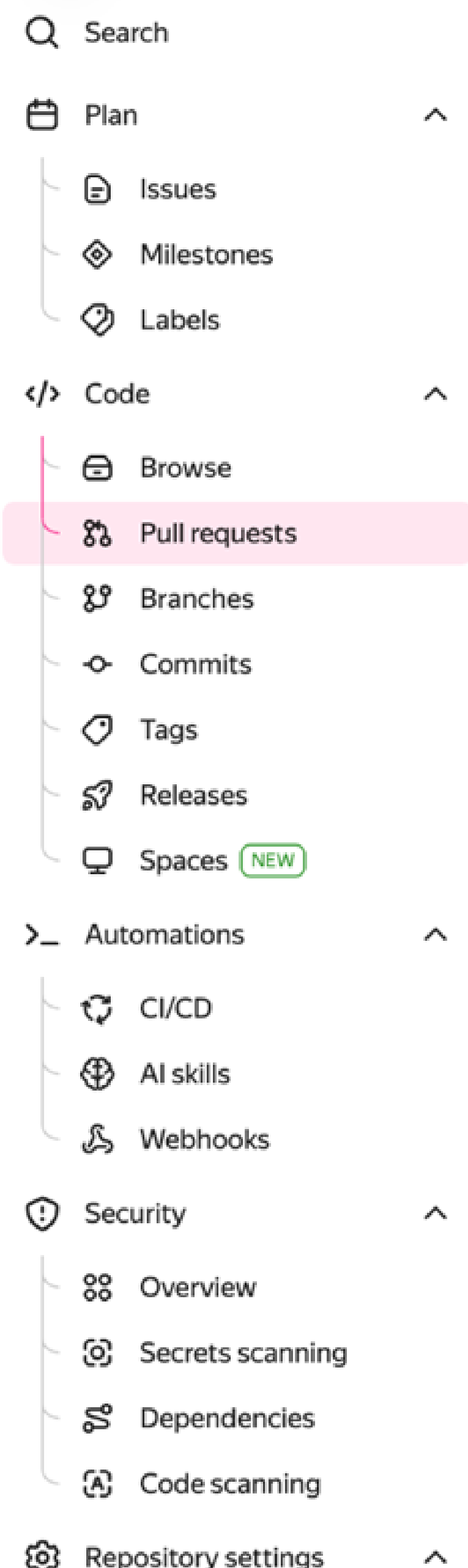


Платформа для разработчиков SourceCraft.dev

- AI-native платформа для разработки
- Глубоко интегрирована с Yandex Cloud
- Сразу создавалась под AI SDLC



Но ключевое отличие в том, что мы начали создавать эту платформу уже в эпоху ИИ: **без ограничений, связанных с legacy**, которые могли бы нас сдерживать, и с **мощной поддержкой широко используемого Облака от Яндекса**.



Created: 23 Jul 2026 • Updated: 23 Jul 2026 • 4

Stepan merged 4 commits from [feature/axidex/uploader-sync](#) into [main](#)

🔔 Overview 📄 Files changed 6 🔗 Commits 4 +88 -15

✔ Pull request successfully merged and closed

The source branch was automatically deleted after the merge.

 All required checks have passed
4 Success

Description

What's done:

- Added DAST
- Removed SA

Linked Issues

 Add issue

Activity

↶ ↷ B I U S M H ∨ ≡ ∨ 🔗 📄 ✂️ 🧩 </> ∨ f(x) ∨ 🖼️ 📎 📊 📋 ... ⚙️

Add your markup here

☐ Change request

Draft 7 Comment

Выглядит как обычная платформа для разработки

Author

 Stepan

Reviewers

✔ All approvals received

 Andrey Kuleshov

 Auto assign

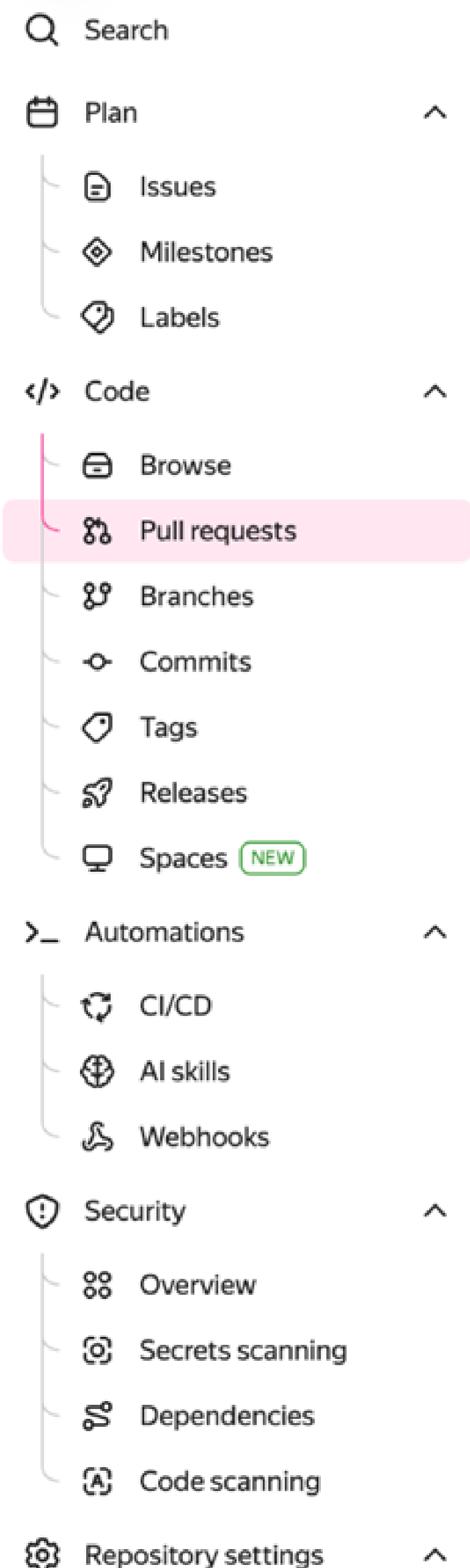
Code review rules

✔ All passed

Details

Labels

+ Add label



Created: 23 Jul 2026 • Updated: 23 Jul 2026 • 4

Stepan merged 4 commits from [feature/axidex/uploader-sync](#) into [main](#)

🔔 Overview 📁 Files changed 6 ➡ Commits 4 +88 -15

✔ Pull request successfully merged and closed

The source branch was automatically deleted after the merge.

 All required checks have passed
4 Success

Description

 Generate with AI PRO

What's done:

- Added DAST
- Removed SA

Linked Issues

 Add issue

Activity

↶ ↷ B I U S M H ∨ ≡ ∨ 🔗 📄 ✂ 🔗 </> ∨ f(x) ∨ 🖼️ 📎 📊 ✅ ... ⚙️

Add your markup here

☐ Change request

[Draft](#) [Comment](#)

Author



Stepan

Reviewers

✔ All approvals received

 Andrey Kuleshov

 Auto assign

Code review rules

✔ All passed

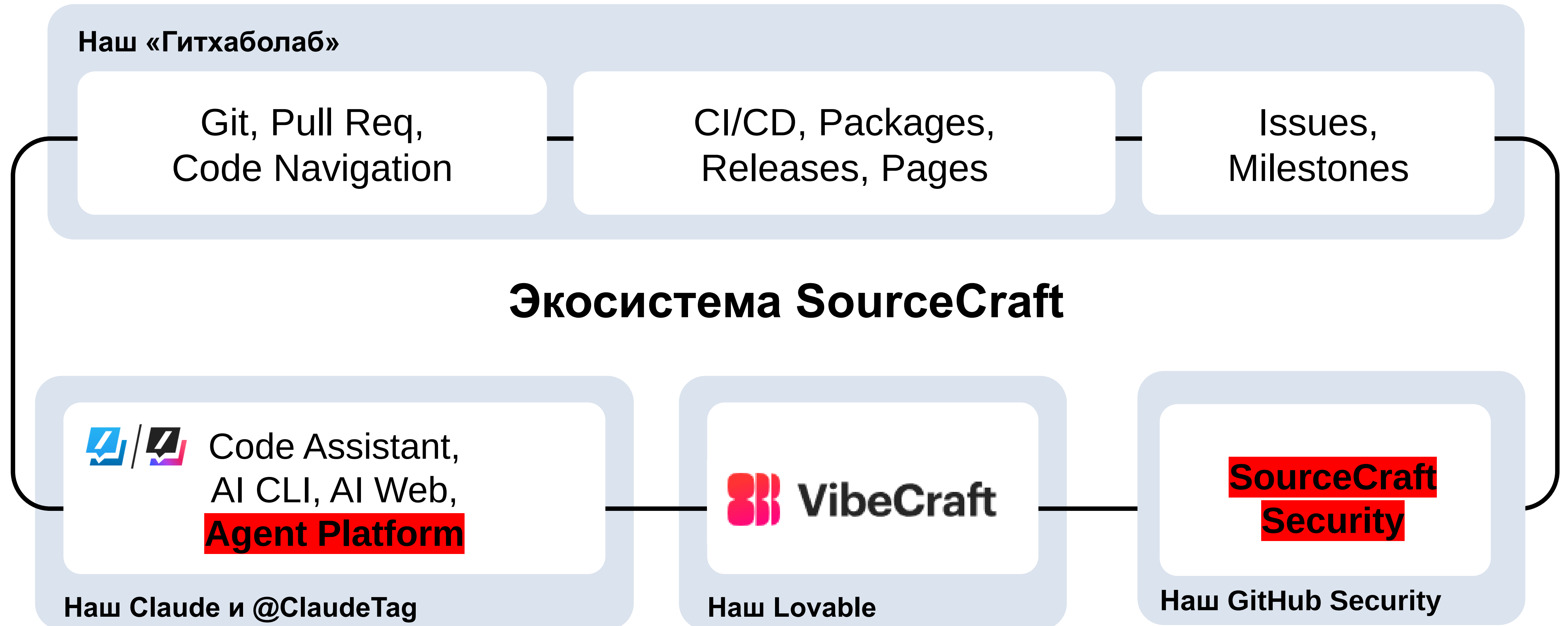
 Details 

Labels

+ Add label

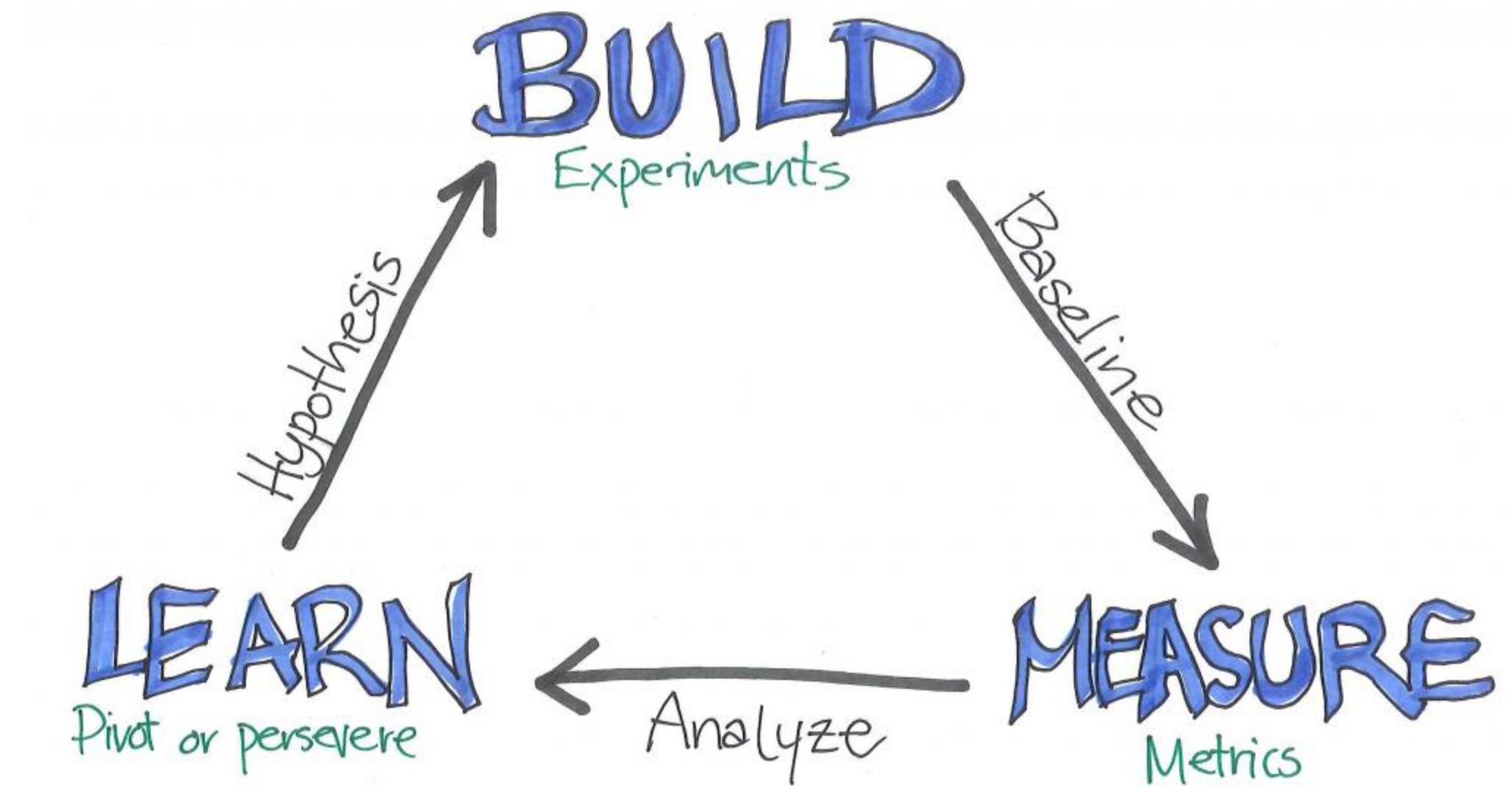
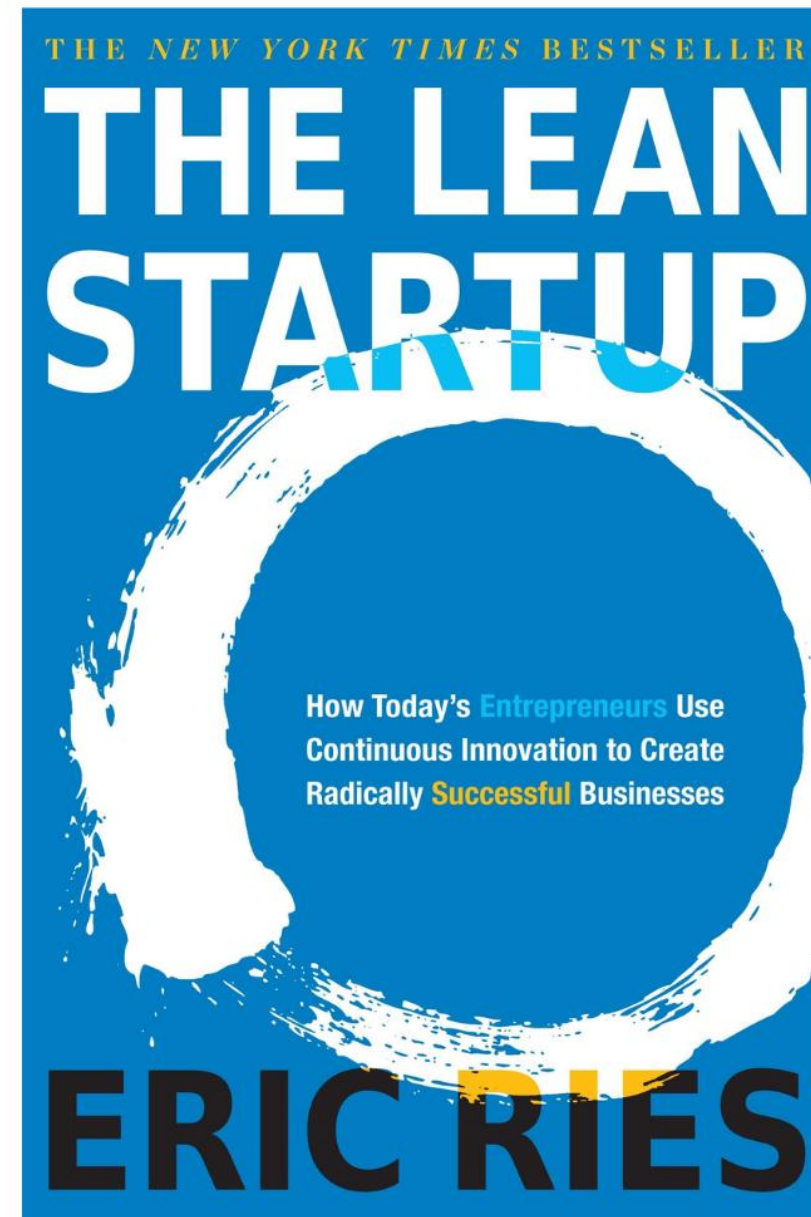
Но если
присмотреться,
повсюду AI-
native
функциональность

Состояние на сегодня



Эволюция AI-средств разработки





Все хотят получить
кратное ускорение
цикла разработки



Как было

К середине 2026-го года ИТ-специалисты уже привыкли воспринимать AI-агентов как персональных помощников или копилотов. Хорошо подходит метафора **экзоскелета**, который усиливает/ускоряет твои текущие задачи по разработке, тестирование, девопсу, мониторингу.

Типичные инструменты: Claude Coude, Cursor, SourceCraft Code Assistant, SourceCraft CLI



На что тратили время в Microsoft в 2019

Activity Category	All	
	100% (N=5928)	
	pct	min
Development-Heavy Activities		
Coding (reading or writing code and tests)	15%	84
Bugfixing (debugging or fixing bugs)	14%	74
Testing (running tests, performance/smoke testing)	8%	41
Specification (working on/with requirements)	4%	20
Reviewing code	5%	25
Documentation	2%	9
Collaboration-Heavy Activities		
Meetings (planned and unplanned)	15%	85
Email	10%	53
Interruptions (impromptu sync-up meetings)	4%	24
Helping (helping, managing or mentoring people)	5%	26
Networking (maintaining relationships)	2%	10
Other Activities		
Learning (honing skills, continuous learning, trainings)	3%	17
Administrative tasks	2%	12
Breaks (bio break, lunch break)	8%	44
Various (e.g. traveling, planning, infrastructure set-up)	3%	21
Total	9.08 hours	

Что делаем в Яндексе

На что разработчики тратят время

45%

Работа с кодом

20%

Поиск информации

10%

SRE и дежурства

20%

Оверхед (встречи, рутина)

5%

Ревью кода

Повысить продуктивность разработки+

Наши приоритеты

- **Работа с кодом**
Рост throughput на 30%+
- **Е2Е сценарии написания и модификации приложений**
Железные роли и профессии (Dev/QA/Analysts/SRE)
- **Поиск информации**
Сокращение времени в Ask / Exploration сценариях минимум в 2 раза

Workflow программиста сегодня

Создание задачи



PM/TL/PO создаёт
таск в трекере

Кодирование и коммит



Открываем IDE и
начинаем
кодировать,
загружаем код на
гит-хостинг

Ревью кода



Владелец фичи /
техлид /
ответственные люди
смотрят на
платформе

Проверки и мердж



Мердж-чеки,
такие как
компиляция,
тесты, секьюрити
проходят; можно
мержить

Workflow программиста сегодня

CI & Build



Собираются артефакты, выкладываются пакеты

Тестирование



Раскатываем на стейджинг, проверяем e2e тестами, нагрузочными тестами, тестами на проникновение

Деплой в продакшен



С помощью CD системы раскатываем в прод

Мониторинг и логгинг



Получаем данные системы, если есть проблемы - фиксируем



SOURCECRAFT

SourceCraft CodeAssistant CLI | powered by OpenCode

```
Выполни задачу из тикета #3  
Build Default SourceCraft
```

tab agents ctrl+p commands



Обзор

Изменённые файлы 1

Изменения 1

AI-задачи

+2 -1

8

System.out.println("Hello World!");

8

var password = "iddqd"

9

System.out.println(password);

9

10

}

10

11

}

Пароль в открытом виде в коде — утечка секрета. Используйте переменные окружения или конфигурационные файлы:

```
var password = System.getenv("APP_PASSWORD");
```

Создано с помощью ИИ. Пожалуйста, проверьте важную информацию и используйте критическое мышление.

SourceCraft Review Bot

24 сент. 2026, 08:12

src / main / java / com / mycompany / app / App.java

@@ -5,6 +5,7 @@

5 5 */

6 6 public class App {

7 7 public static void main(String[] args) {

8 System.out.println("Hello World!");

8 var password = "iddqd"

9 System.out.println(password);

9 10 }

10 11 }

Пропущена точка с запятой после присваивания. Код не скомпилируется. Добавьте ; в конце строки:

```
var password = "iddqd";
```

Создано с помощью ИИ. Пожалуйста, проверьте важную информацию и используйте критическое мышление.

Чат Code Assistant

+ ↻ ✕

Вот итоги:

Краткий обзор изменений

Единственный изменённый файл —
src/main/java/com/mycompany/app/App.java :

Замечания

1. Синтаксическая ошибка (блокирующая): в строке var password = "iddqd" пропущена точка с запятой (;). Код не скомпилируется — сборка проекта упадёт.

2. Хранение секрета в коде: пароль захардкожен прямо в исходниках. Это анти-паттерн безопасности — секреты нельзя хранить в репозитории (даже в тестовом коде), их следует выносить в переменные окружения или секретные хранилища.

3. Название PR: заголовок «idd» и ветка pwd не отражают суть изменений — рекомендуется давать осмысленные названия.

Также я запустил автоматическое AI-ревью — его комментарии появятся в PR, как только фоновый процесс завершится. Могу дополнительно посмотреть результат, когда он будет готов.

08:12

template-java-with-maven !2

Планируйте, создавайте и тестируйте что угодно

↑

Code review — ревью кода с AI

Первый подход

Запустили нейроревью

Adoption 17% Требуется повышение качества и аналитика

Фокусировка

Выбор проблемы для фокусировки

Фокусируемся на категории Бизнес-логики

Тип проблемы	Доля, %	Время на починку, мин.
Minor	~30	38
Business logic	~25	55
Refactoring	~20	63

К чему пришли

На фикс тратится гораздо больше времени, чем на поиск проблем в ревью

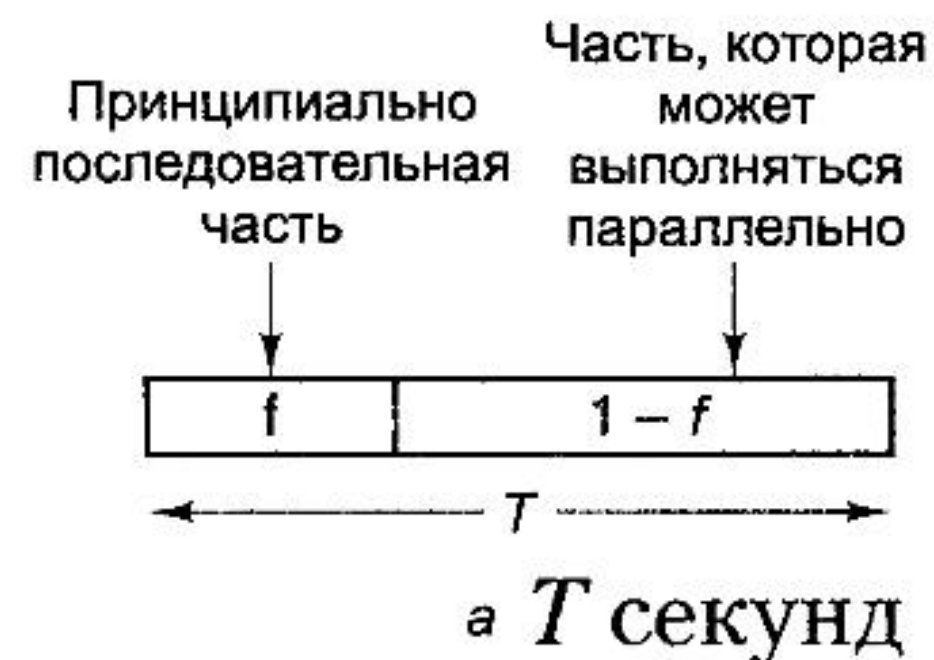
Нейроревью пивотится в генерацию саджестов кода

55 мин.
На фикс

6 мин.
На поиск проблем

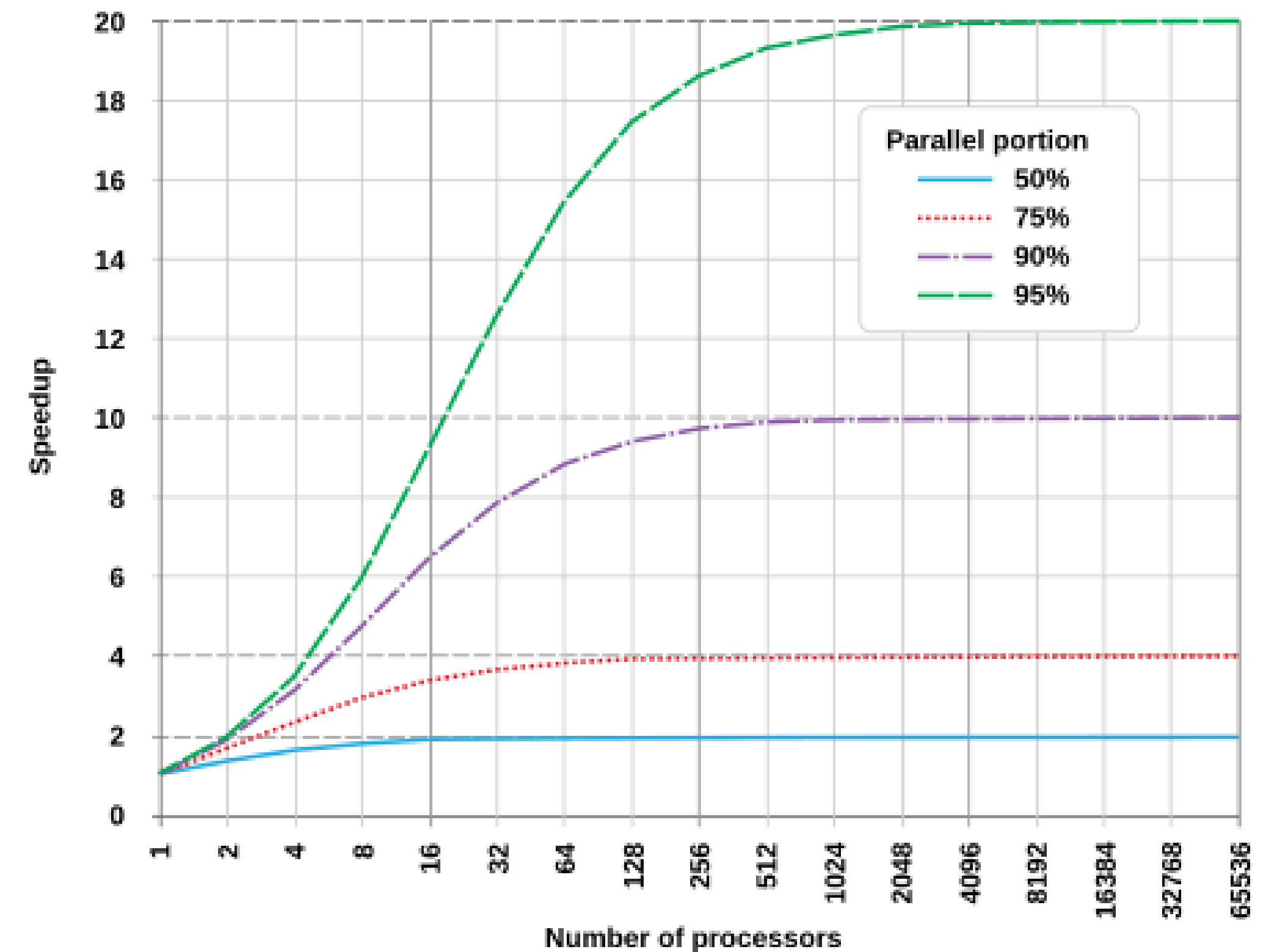
Закон Амдала

$$fT + (1 - f)T/n.$$



$$\text{Ускорение} = \frac{n}{1 + (n - 1)f}.$$

Amdahl's Law



Как будет

Новый паттерн использования агентов – создание и управление агентской командой прямо на платформе для разработки. В такой ситуации ИТ-специалисты команды выполняют роль технически грамотных менеджеров ИИ-агентов и отвечает за их набор, настройку, постановку и корректировку задач, наблюдение за показателями эффективности.

Референсы: Claude Tag, GitLab Duo Agentic Platform, GitHub Agentic Workflows, Multica, Roomote



Вектор мирового рынка

Агенты выполняют работу — человек контролирует риски и исключения

Компания	Ключевой тезис
Anthropic Claude Tag	Любой участник канала может отметить @Claude и делегировать ему задачи
GitLab Duo Agent Platform	Встраивает множество интеллектуальных агентов на всех этапах жизненного цикла разработки ПО
Roomote (ex Roo Code)	Облачный ИИ-агент: запускает среду разработки, проверяет свою работу, проводит ревью и возвращает пулл-реквесты (PR)

Фокус

Управляемая
автономность
и промышленная
эксплуатация **ADLC**

Чего хотят бизнес-заказчики?

Нужна инфраструктура, в которой агенты работают надёжно, безопасно и измеримо

На самом деле все хотят лучше-быстрее-дешевле

Управляемое внедрение ИИ

Полный контроль над моделями, лимитами, логам.

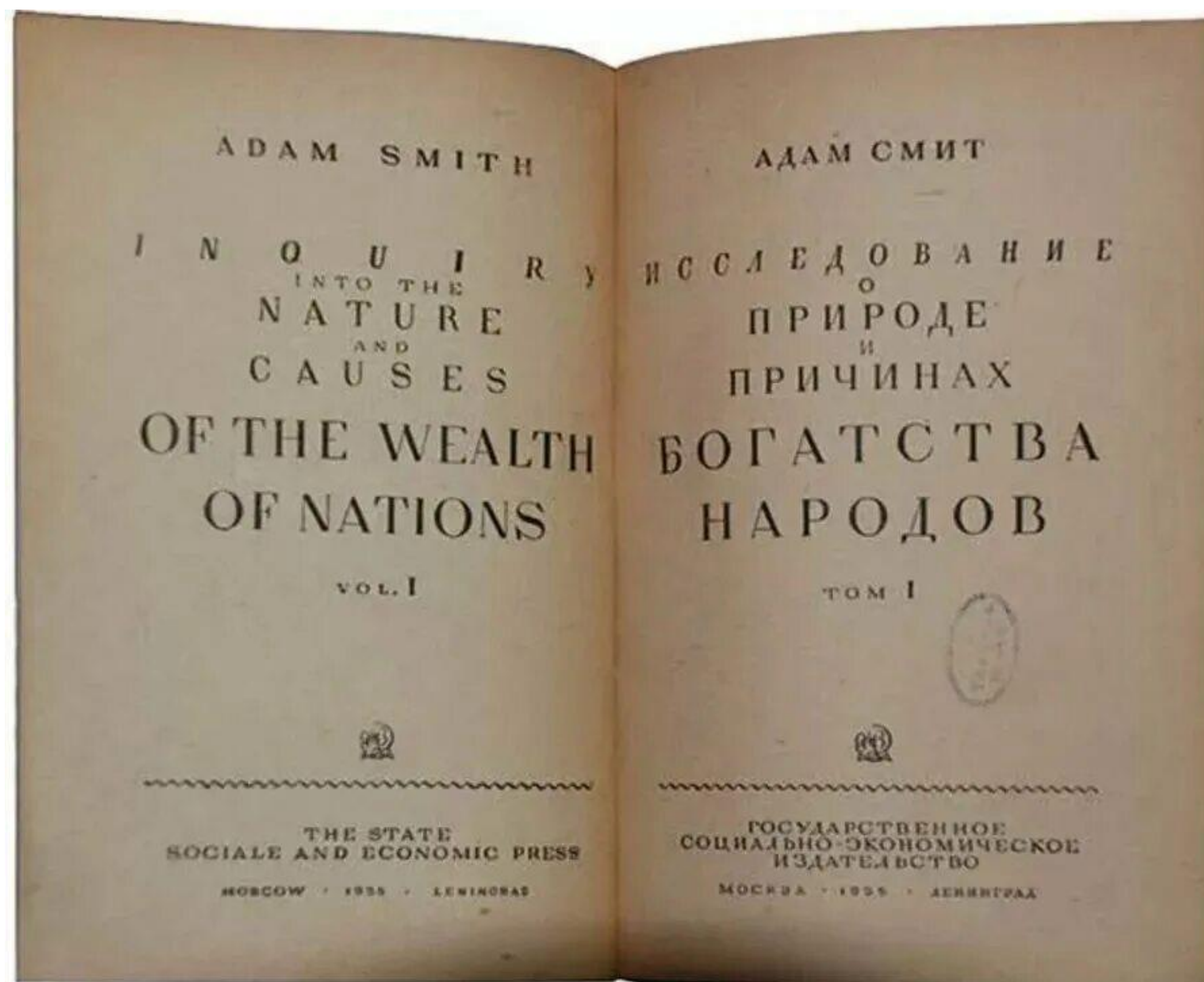
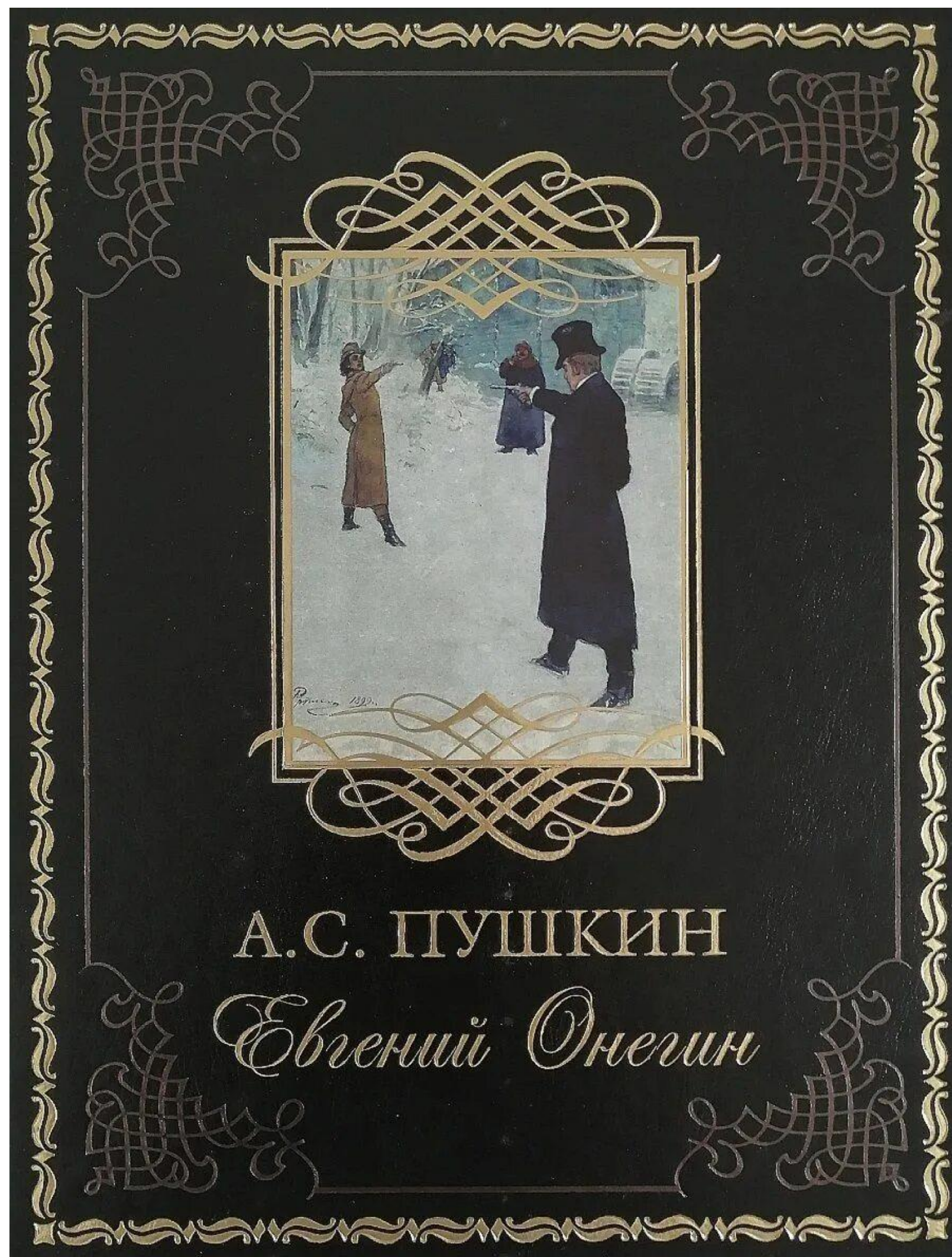
Видеть все метрики: adoption, экономическую целесообразность

Единая база знаний агентов

Доступ сотрудников из разных команд к каталогу MCP, правилам, навыкам, промптам, RAG. AI OS компании

Фабрика по созданию ПО

Замена типовых, простых и умеренно сложных операций безопасными агентами





- Один ремесленник производит 20 булавок в день
- Производство булавки можно разбить на 18 операций
- **Сколько** булавок в день произведут 18 ремесленников, если каждый будет заниматься только одной операцией?

48000 булавок



МЫ ОТКРЫТЫ

QA

Product
manager

Project
manager

HR

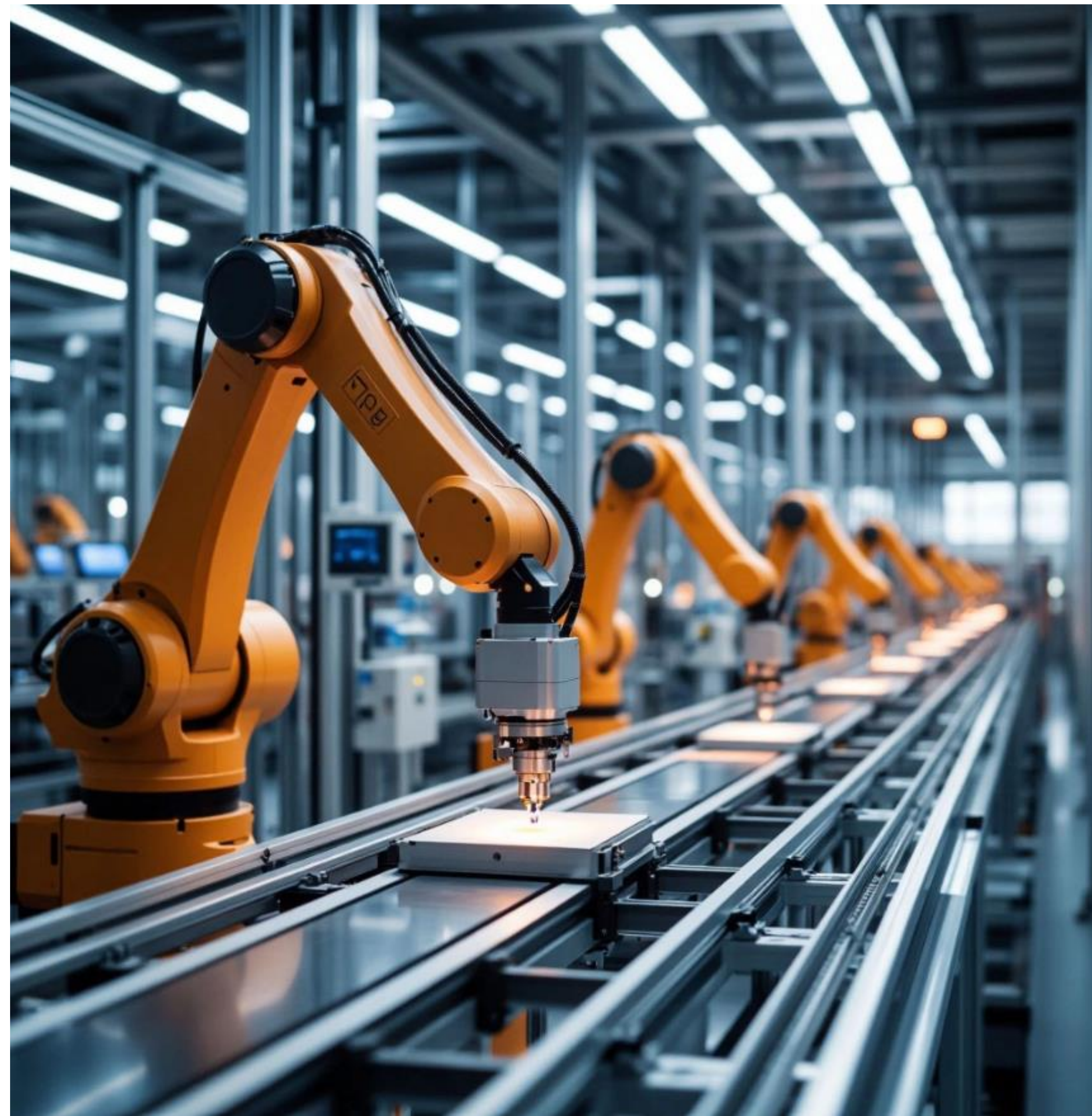
SRE

AppSec

Marketing

CTO
Developer

CEO
Sales



Механики и водители?

Платформенные и продуктовые команды



Обратно на земя



Какие проблемы решаем?

Если посмотреть на то, что команды разработки в российских компаниях делают «под себя», становятся понятны общие потребности.

Некоторые команды делают простые «решатели», позволяющие назначить тикет на работа. Под это стартует виртуальная машина, там разворачивается Claude Code / OpenCode, который пытается one-shot решить задачу и выдать изменения в исходном коде.

Похожие **one-shot кастомные решатели на виртуальных машинах и CLI агентах** делают для ревью кода, тестирования, проверки соответствия СИБ требований и многого другого.

Другие команды делают кастомных агентов, которые **берут задачи и отвечают прямо в командных мессенджерах**.

Есть общий список осознанных и неосознанных потребностей клиентов, которые мы агрегируем в понятие «**ИИ-сотрудник**».

Что предлагаем?

1. Подготовленная **инфраструктура** запуска от Яндекса с мониторингами, надёжностью и Hybrid mode (хватает мощностей – Onprem, нет - Cloud)
2. **Безопасность**. Агенты запускаются с настроенными правами роботов (сервисных аккаунтов), а не токенами запустивших пользователей.
3. Удобный **кабинет создания и управления** командой агентов. Есть встроенные агенты, а пользователь может легко настроить своего агента.
4. Управление доступом агентов к моделям, токен-квотами подписками (**Governance**)
5. **Наблюдаемость**. Лог задач агентов, графики эффективности, ROI от использования
6. **Обучаемость**. Агенты становятся лучше в процессе использования, накапливают знания в проекте и орг-и.
7. **Интерактивное** взаимодействие с любой **поверхности**. Задачу можно поставить, уточнить и увидеть ответы в Tg, Y-messenger, веб-чате платформ разработки SourceCraft, GitLab

Платформа для совместной разработки ИИ-агентов и специалистов

ИИ-команда SourceCraft

Встроенные агенты

Агент	Функция
 ИИ-разработчик	Пишет код по задаче, делает ревью
 ИИ-безопасник	Ищет и исправляет уязвимости всех видов

ИИ-команда — это:

- управляемость
- безопасность
- наблюдаемость
- непрерывное улучшение
- ваша база знаний (код, документация и правила)
- прозрачная тарификация

Что должно получиться в итоге?

Агент по ощущениям должен быть как живой человек.

Ты можешь ставить ему задачу в мессенжере, трекере, где угодно. Он доуточняет, делает, выдаёт артефакт. Ты можешь микроменеджить, вмешиваться в процесс.

Может срабатывать по триггеру так же как ты реагируешь на нотификации.



Платформа для совместной разработки ИИ-агентов и специалистов

ИИ-команда SourceCraft

Встроенные агенты

Агент	Функция
 ИИ-разработчик	Пишет код по задаче, делает ревью
 ИИ-безопасник	Ищет и исправляет уязвимости всех видов

ИИ-команда — это:

- управляемость
- безопасность
- наблюдаемость
- непрерывное улучшение
- ваша база знаний (код, документация и правила)
- прозрачная тарификация



collab-whiteboard

Приватный репозиторий

🏠

🔍 Поиск

📅 Планирование

📁 Задачи

🎯 Цели

🏷️ Метки

📄 Код

📖 Обзор

🔗 Предложения изменений

🌿 Ветки

🔄 Изменения

🏷️ Теги

📢 Релизы

💻 Рабочие пространства

🔧 Автоматизации

🔄 CI/CD

📚 AI-навыки

🌟 AI-задачи NEW

🔗 Вебхуки

🕒 Расписания NEW

👤 Люди и роботы

📄 AI-коллеги NEW

🏠

eugenemt9

/

collab-whiteboard

/

AI-коллеги

+

Новый AI-коллега

🗪 Карточки

📋 Список

AI-коллеги

Beta

✕

Познакомьтесь с AI-коллегами

AI-коллеги — автономные агенты, которые работают вместе с вашей командой. Назначайте их исполнителями задач или призывайте в комментариях к задачам и предложениям изменений. Они напишут код, создадут предложения изменений и доработают решение с учётом обратной связи.

[Подробнее об AI-коллегах](#)



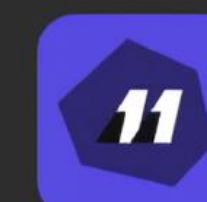


Добавьте AI-коллегу в репозиторий

Настройте под стек и процессы вашего репозитория

+ Создать

🔗 Подключить



✓ Активный

SourceCraft Auditor

@ src-auditor • 🧠 Системный

AI-коллега для аудита безопасности проекта.

⚙️ Настроить



✓ Активный

SourceCraft AppSec

@ src-appsec • 🧠 Системный

AI-коллега для поиска и исправления уязвимостей.

⚙️ Настроить



✓ Активный

SourceCraft

@ src • 🧠 Системный

Универсальный AI-коллега для работы над проектом.

⚙️ Настроить

Что такое свой ИИ-коллега

Идентити



@src, @T800,
@robocorp

Как у реального человека, можно подключать в организации, тэгать, назначать задачи, давать подписку

Конфиг



Репозитории-
плагины в
формате Codex:
Skills, Rudes,
Mcp, Hooks

Среда



Настроенный
DevContainer

Ничем не
отличается от
реальной среды
разработчика

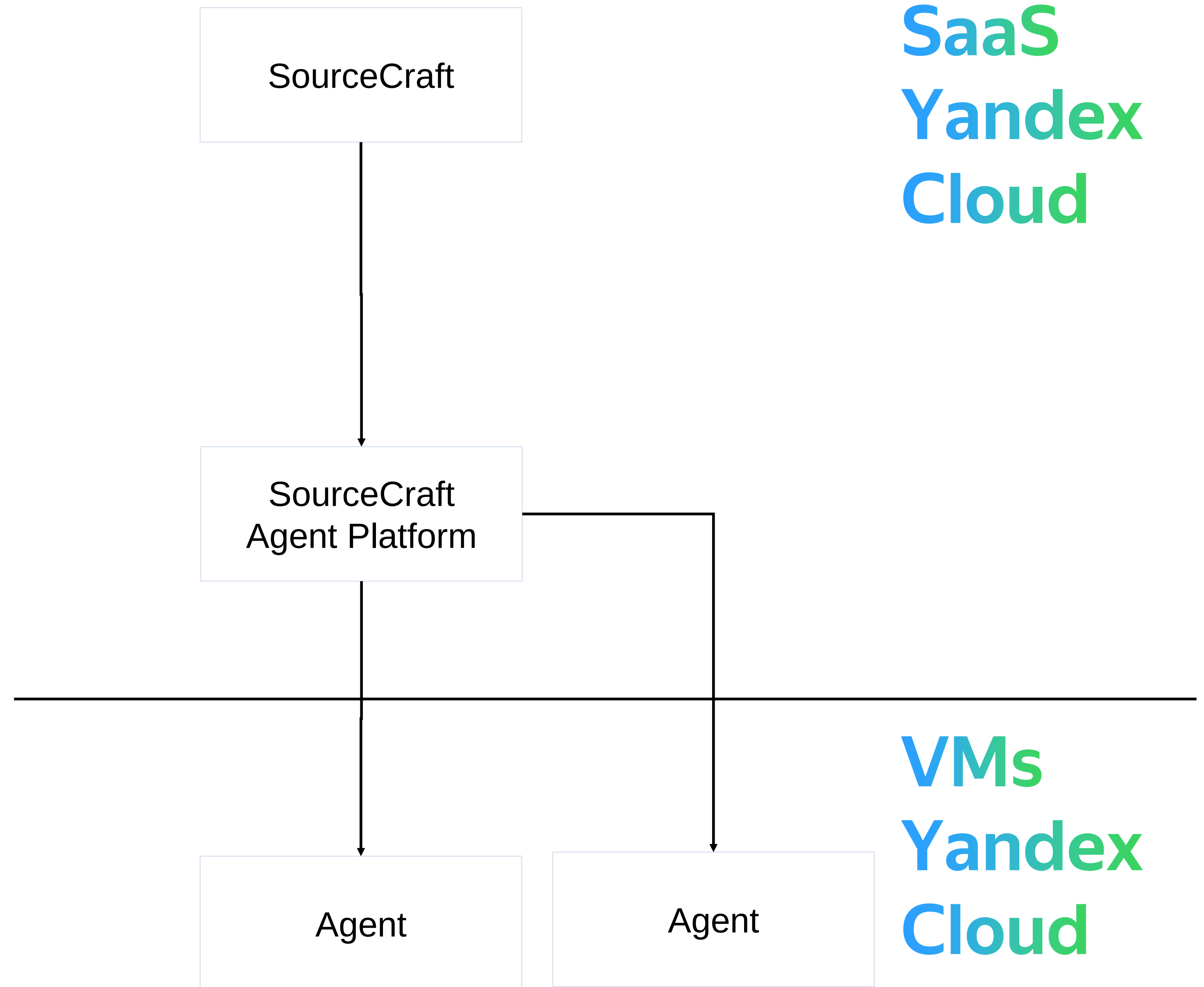
Интеграции



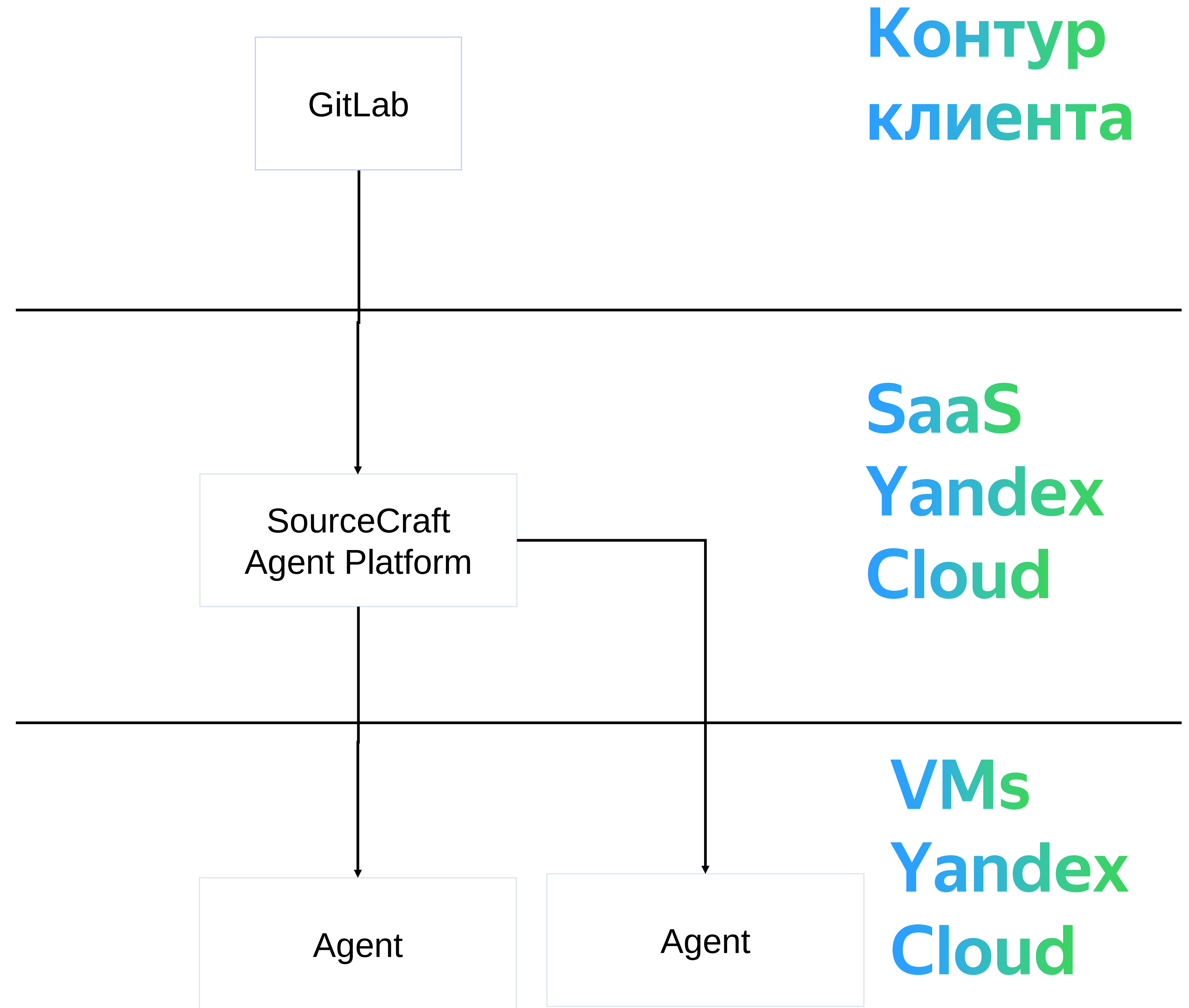
С ботом
телеграм,
гитлабом или
любой другой
информационной
системой

Пример развёртывания

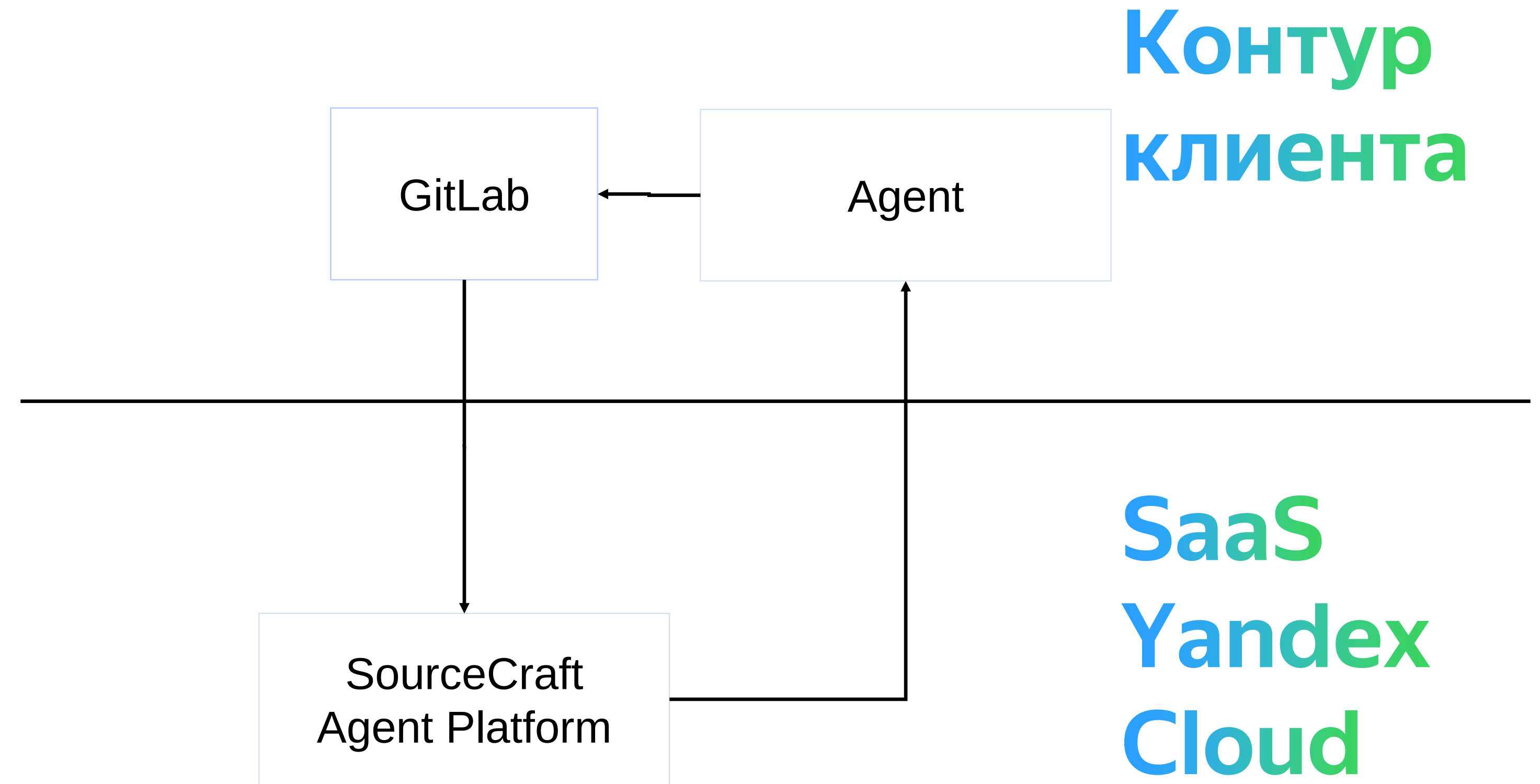
«Пробуем на
SourceCraft»



Пример развёртывания «Все в Облаке»

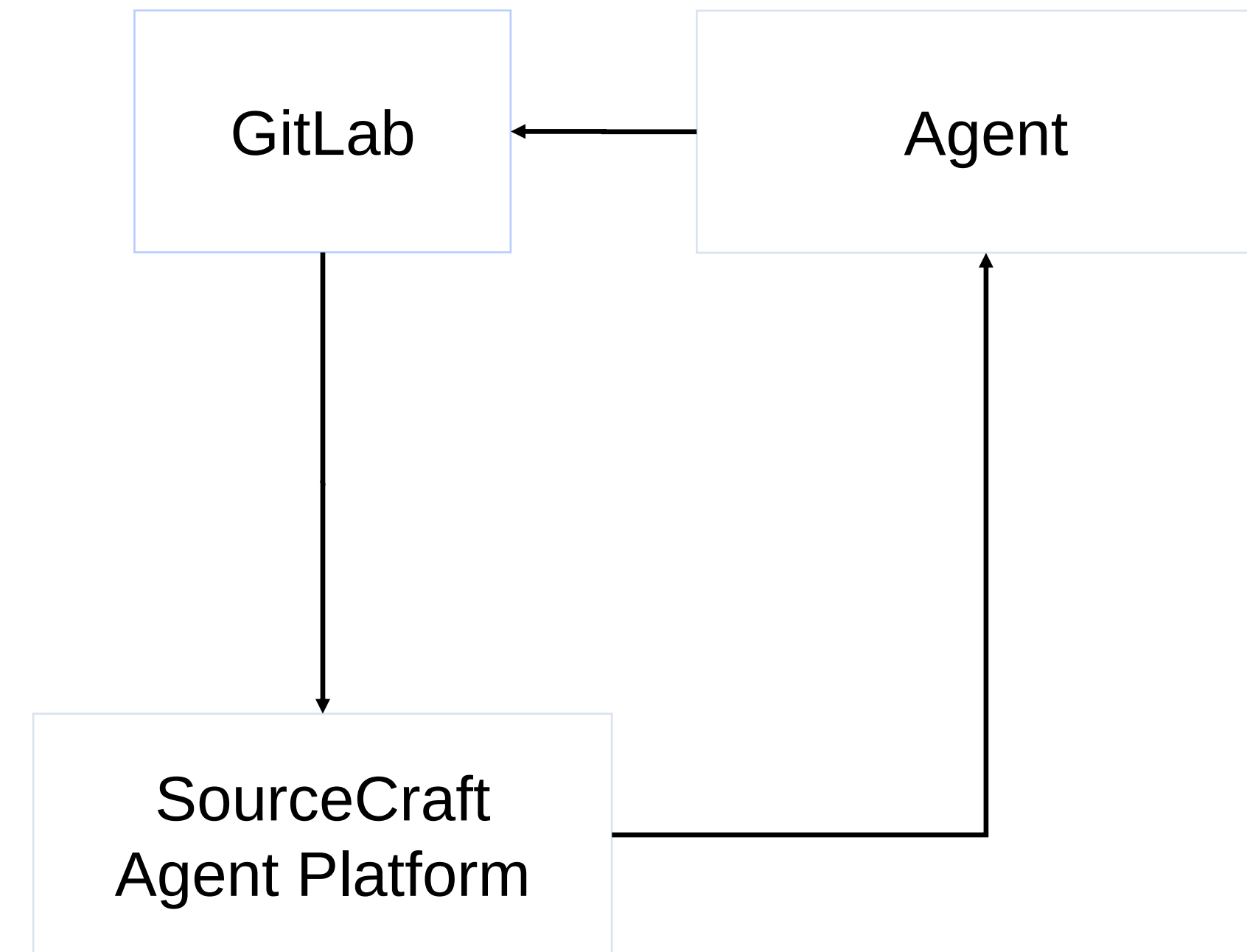


Пример развёртывания «Агенты в контуре»



Пример развёртывания

«Все онпрем»



Контур
клиента

Конец 2026



Search or go to...

0

0

0



src / Example / Work items

example#1

All items

+ Add view

↺

State

is

Open

1 item

Bulk edit

FizzBuzz

src/example#1 · created 7 mi

FizzBuzz

Open

Issue created 7 minutes ago by siniavskijand

Нужно написать решение каноничной задачи FizzBuzz

👍 0

👎 0

😊

Add design

Create merge request

Assignee

None - assign yourself

Edit

Labels

None

Edit

Milestone

None

Edit

Dates

Start: None

Due: None

Edit

Time tracking

Add an estimate or time spent.

+

1 Participant



Child items 0

No child items are currently assigned. Use child items to break down work into smaller parts.

Linked items 0

Link items together to show that they're related.



GitLab

horns-and-hoofs / gitlab-integration / AI-задачи

Статус: Все

Номер

AI-задачи

Нет AI-задач

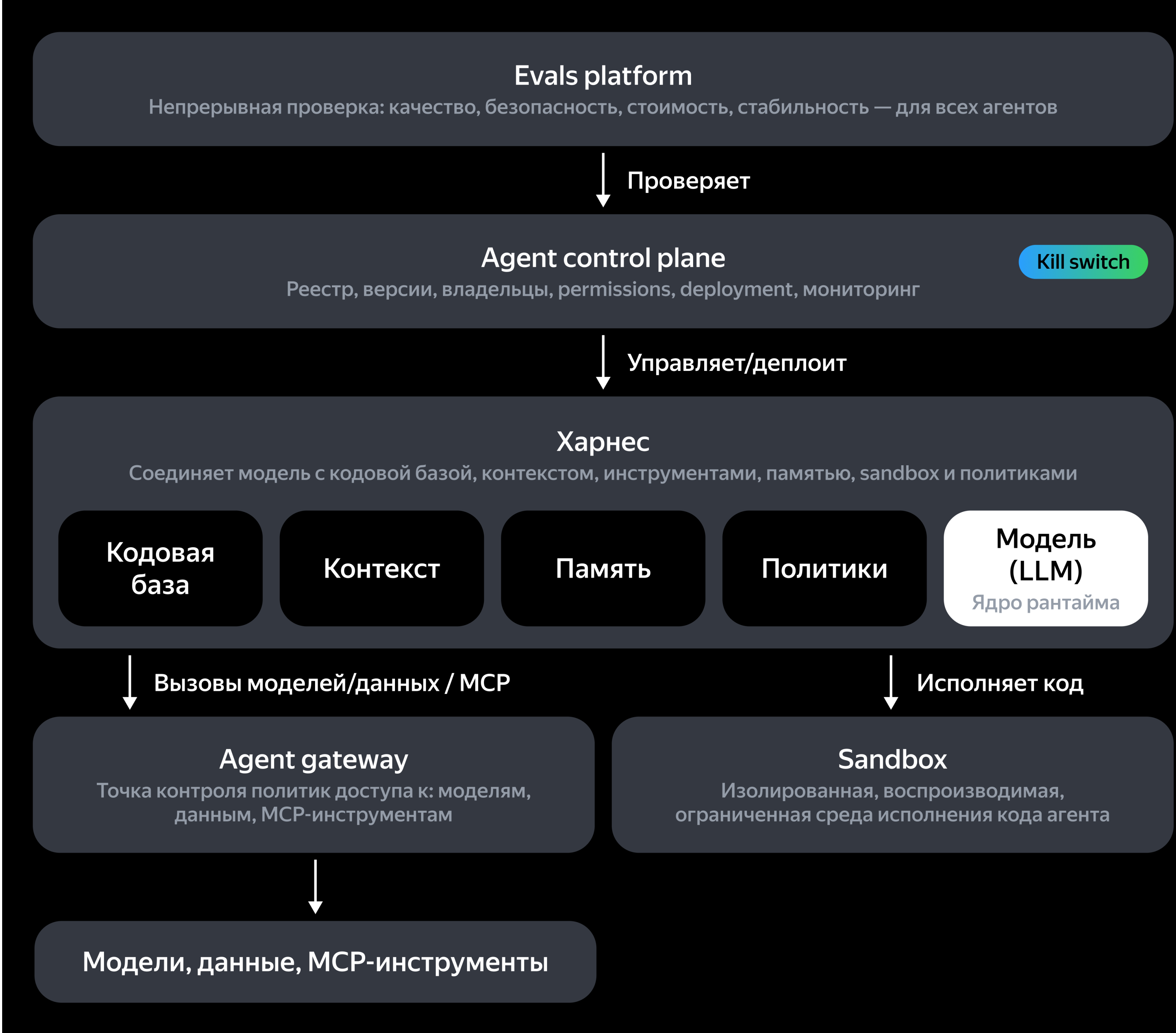
Здесь появятся AI-задачи



А что с безопасностью?



Архитектура агентской платформы

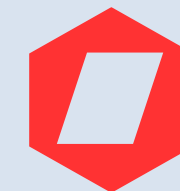


Неудобные вопросы #1

Есть ли LLM файрвол?
Что маскируется из
коробки, какие
метрики качества?



Как вы боретесь с
prompt injection?
Логируется?
Блокируется?



Как реализован
Agent Gateway?
Какой контроль вызова
инструментов?

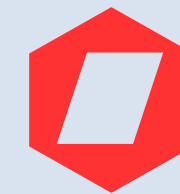


Неудобные вопросы #2

Какая технология
Sandbox?
Ограничения
на сеть и файловую
систему?



Есть ли аудит трейсов
агента?



Как убедиться, что
создаваемый код
безопасный?



Три всадника AppSec Апокалипсиса

SAST

SCA

Secret
Scan

SD

sourcecraft-security-den

Публичный репозиторий

Поиск

Планирование

Код

Автоматизации

Люди и роботы

AI-коллеги NEW

Участники и роли

Безопасность

Обзор

Сканирование секретов

Зависимости

Анализ кода

Динамическое тестирование

Агент безопасности

Настройки репозитория

Поиск

Планирование

Код

Автоматизации

Люди и роботы

AI-коллеги NEW

Участники и роли

Безопасность

Обзор

Сканирование секретов

Зависимости

Анализ кода

Динамическое тестирование

Агент безопасности

Настройки репозитория

axidex / sourcecraft-security-demo / Безопасность / Зависимости

Зависимости

Уязвимости 21Пакеты 76Карта зависимостей

Статус = ОткрытСканер = trivyВведите текст для поиска или выберите фильтры

21 предупреждение

CVE-2026-56854

#224 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-39828

#212 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-39829

#213 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-39830

#214 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-39831

#215 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-39832

#216 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-39835

#219 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-42508

#220 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-46595

#221 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-46597

#222 • Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

CVE-2026-56852

Зависимости / #208 Подтверждено

golang.org/x/crypto/ssh/agent: SSH client panic due to...

Последнее обнаружение: 03 сент. 2026 • Trivy • golang.org/x/crypto@v0.35.0

Переоткрыть

Начать исправление

Начать разбор

Исправить с AI

Обзор

AI-задачи 0

CVE-2025-47913

SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.

Дополнительная информация

Ссылки 2

https://avd.aquasec.com/nvd/cve-2025-47913

https://nvd.nist.gov/vuln/detail/cve-2025-47913

Активность

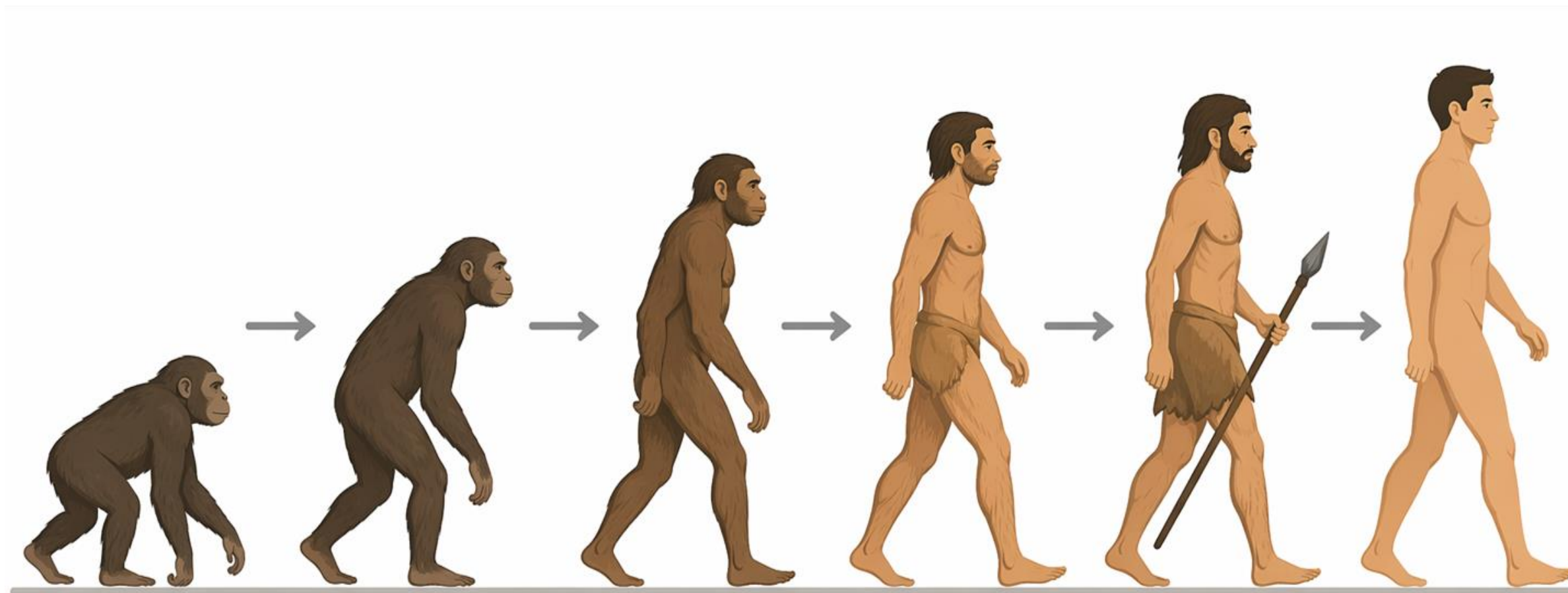
03 сент. 2026

Дмитрий Иванов подтвердил предупреждение • 03 сент. 2026, 19:16 • Открыт >> Подтверждено

Дмитрий Иванов повторно открыл предупреждение • 03 сент. 2026, 19:10 • Исправляется >> Открыт

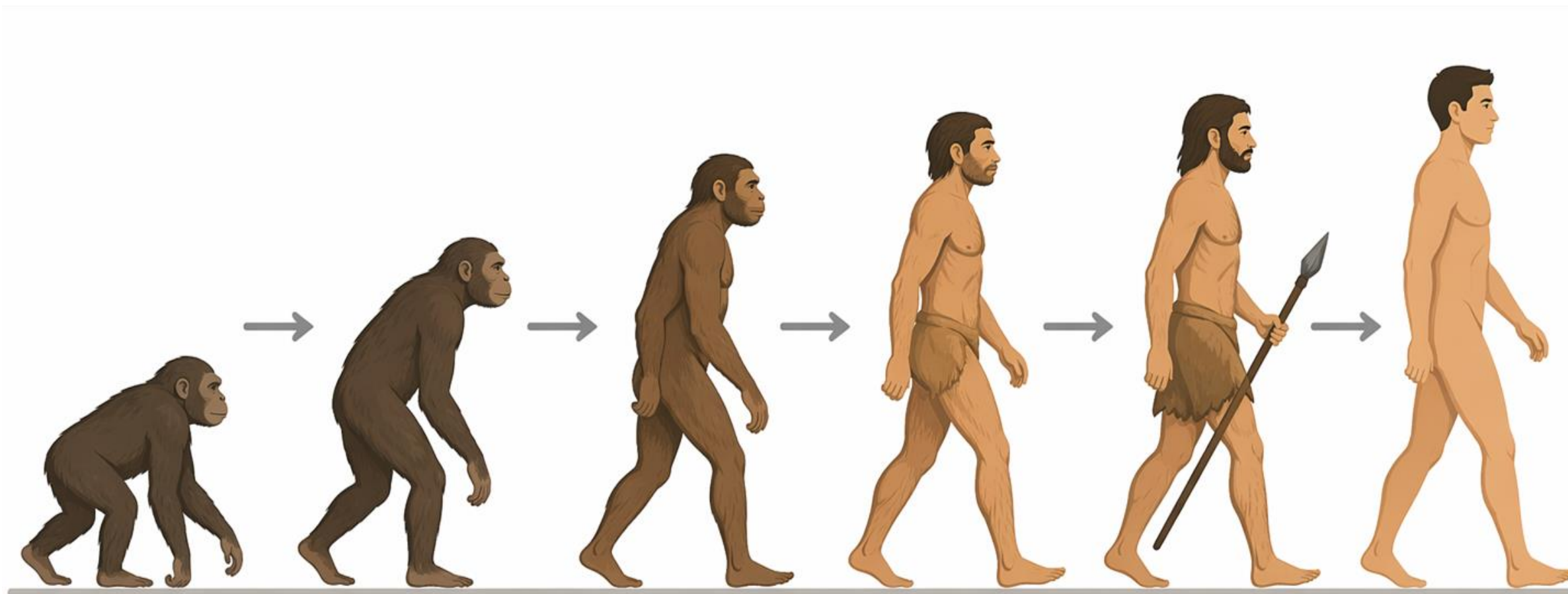
Дмитрий Иванов подготавливает исправление • 03 сент. 2026, 19:10 • Подтверждено >> Исправляется

Мне нравится
эта эволюция!



2023: LLM assists static
analysis (particular rule,
FP/non-FP?)

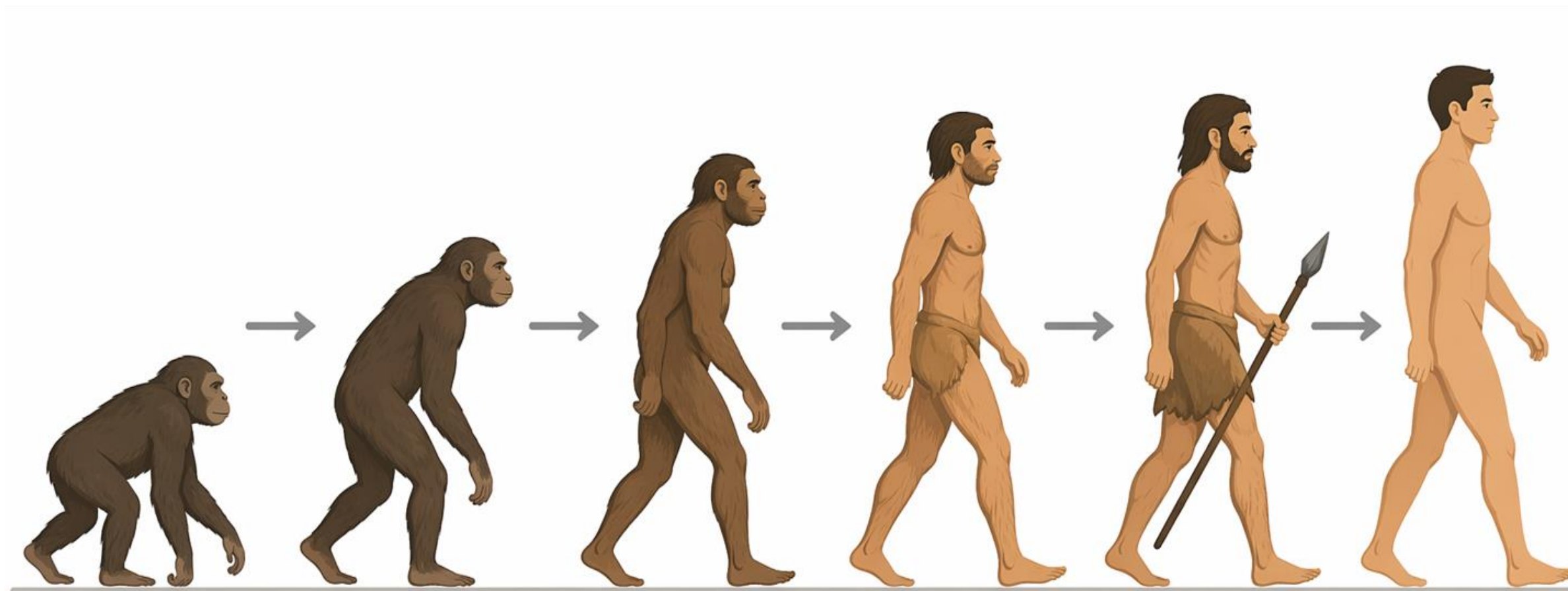
Мне нравится
эта эволюция!



2023: LLM assists static
analysis (particular rule,
FP/non-FP?)

2025: LLM performs structured
program-analysis reasoning
(reachability, criticality,
constraints)

Мне нравится
эта эволюция!

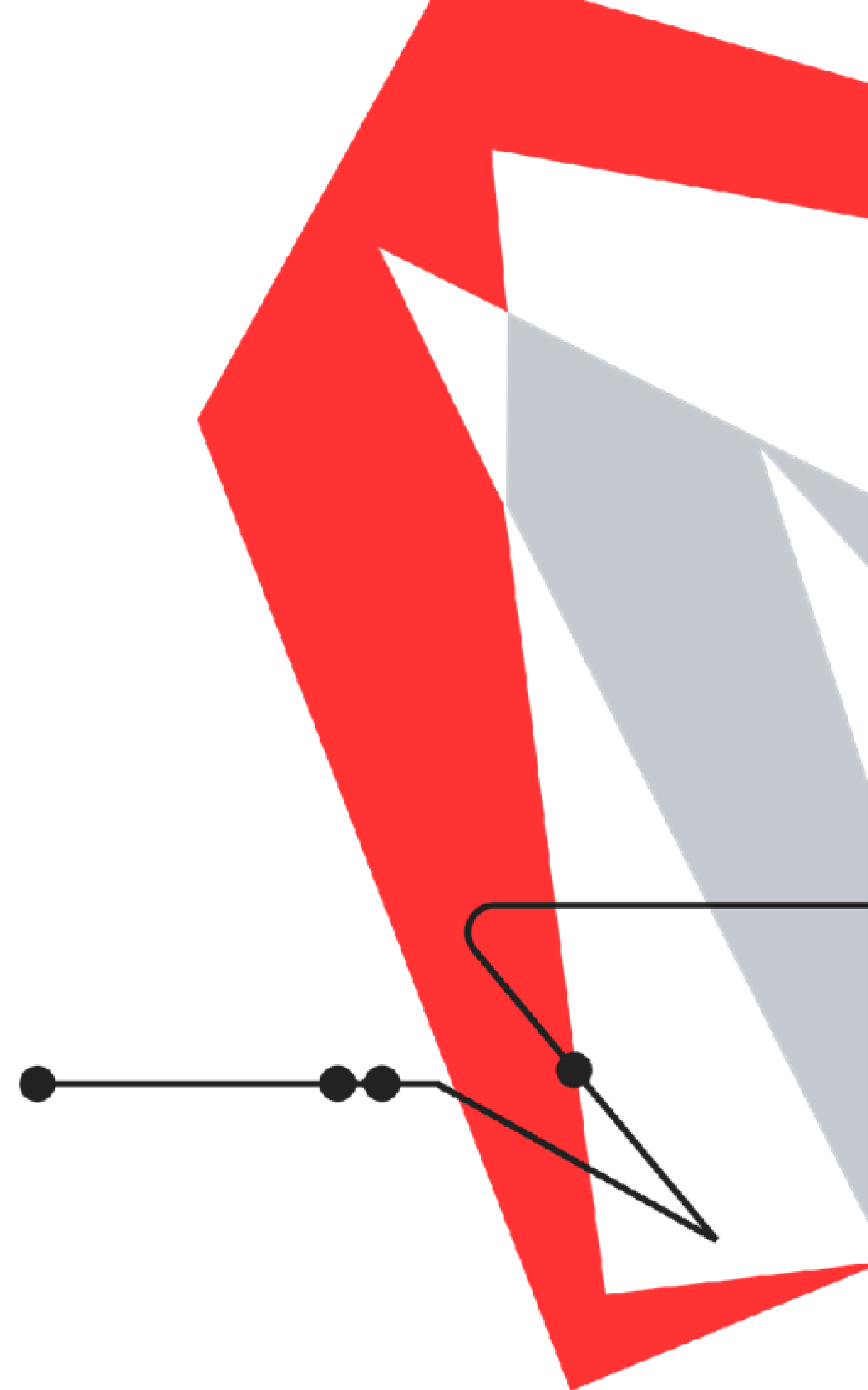


2023: LLM assists static
analysis (particular rule,
FP/non-FP?)

2025: LLM performs structured
program-analysis reasoning
(reachability, criticality,
constraints)

2026: LLM orchestrates formal
analysis instead of being
trusted as the oracle (LLMs
construct analysis; formal tools
verify)

Двухфазный поиск уязвимостей от CloudFlare



JUNE 18, 2026

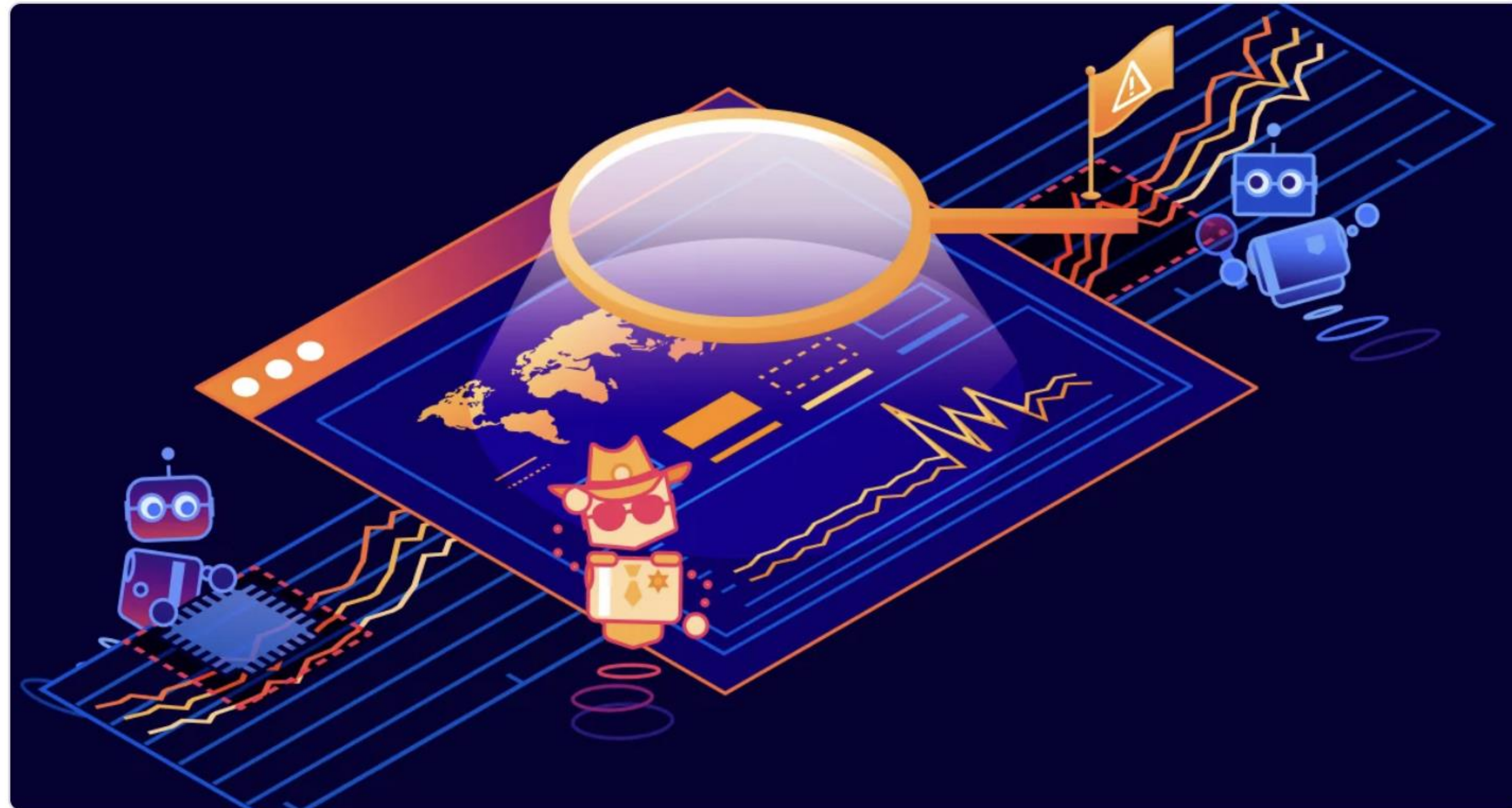
Build your own vulnerability harness



Dan Jones, Alexandra Godoi, and Grant Bourzikas

🕒 21 MINUTE READ

🔗 COPY URL



<https://blog.cloudflare.com/build-your-own-vulnerability-harness/>

Подход простой!

- Несколько запусков в виде непрерывного producer-consumer **цикла**
- Три агента, которые **проверяют** друг друга, голосуют и ранжируют результаты
- **Динамическое моделирование угроз** — агенты строят threat model на основе репозитория, а не получают его заранее



SD

sourcecraft-security-demo

Публичный репозиторий



</> Код

Обзор

Предложения изменений

Ветки

Изменения

Теги

Релизы

Рабочие пространства

> Автоматизации

CI/CD

AI-навыки

AI-задачи NEW

Вебхуки

Люди и роботы

AI-коллеги NEW

Участники и роли

Безопасность

Обзор

Сканирование секретов

Зависимости

Анализ кода

Динамическое тестирование

Агент безопасности

Настройки репозитория

Общее

Секреты



Предупреждения динамического тестирования

Важность

Статус = Открыт

Введите текст для поиска или выберите фильтры

Элементы не найдены

Попробуйте изменить или сбросить фильтры



Внедрение ИИ-аудитора СИБ

Проблема: долгий аудит

Решение: ИИ-аудитор
безопасности SourceCraft

Результаты: сроки — короче,
затраты — ниже. Число найденных
багов сопоставимо с аудитом
подрядчика

1 баг

новый, 9 багов
подтверждены

На 98%

сократили расход
бюджета на аудит

~1–2 часа

занимает полный аудит

Спасибо за внимание!



Дмитрий Иванов
Руководитель SourceCraft
@korifey_ad
korifey@yandex-team.ru

