

DAILY BRIEF · WHAT AI ENGINEERS ARE BUILDING

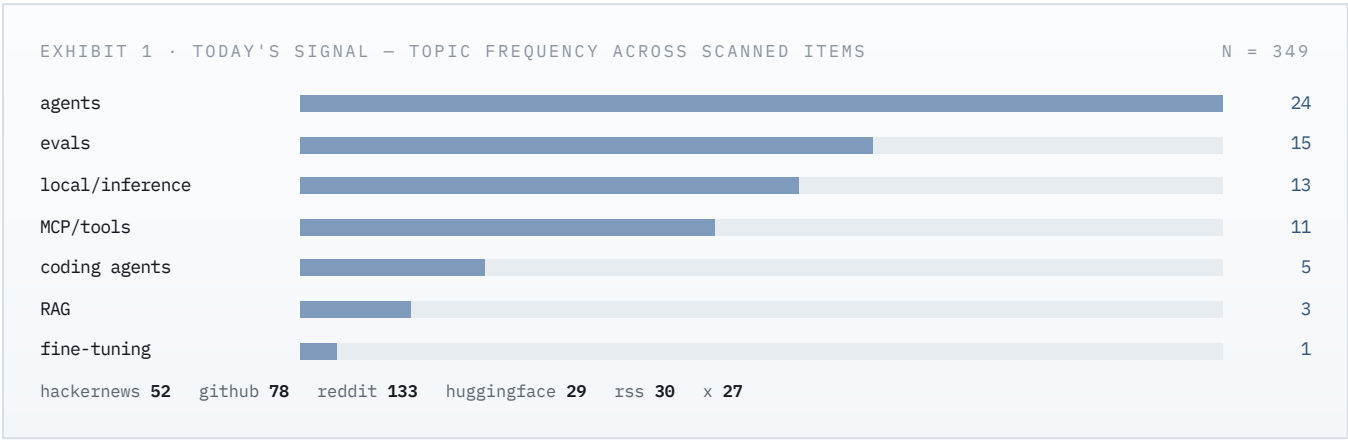
Today in AI engineering

2026-07-25

Developers are building and sharing open-source tools for AI agent development, deployment, and evaluation

3 deep dives 2 builder stories 10 quick hits 349 items scanned

- ai agents
- open-source tools
- machine learning
- software development
- evaluation frameworks



DEEP DIVES

eli-labz/Agent-Execution-Partnership

github

Eli Labz built an open-source control plane for AI agents, ensuring every action is authorized, observable, and verifiable. The project aims to provide a secure and reliable way to deploy AI agents. The control plane is designed to work with various AI frameworks and provides features like role-based access control and auditing.

Why it matters. This project addresses the need for secure and reliable AI agent deployment, which is critical for widespread adoption. It provides a flexible and scalable solution for managing AI agents.

TRY THIS

Explore the Agent-Execution-Partnership repository and try deploying an AI agent using the control plane

<https://github.com/eli-labz/Agent-Execution-Partnership>

- ai agents
- control plane
- security

baidu/Unlimited-OCR

huggingface

Baidu released an open-source OCR model, Unlimited-OCR, which can recognize text in images. The model is trained on a large dataset and achieves state-of-the-art results. It can be used for various applications, such as document scanning and text recognition.

Why it matters. This model has the potential to revolutionize text recognition and document scanning, making it easier to digitize and process large amounts of text data.

TRY THIS

Try using the Unlimited-OCR model for text recognition in your own projects

<https://huggingface.co/baidu/Unlimited-OCR>

ocr

text recognition

computer vision

krishagarwal314/autodev-studio

github

Krish Agarwal built an open-source autonomous multi-agent SDLC harness, Autodev Studio. The harness allows users to describe a feature in plain English and AI agents will scope, code, test, review, and open a PR. It provides a unique approach to software development, leveraging AI agents to automate the development process.

Why it matters. This project has the potential to significantly improve software development efficiency and quality, by leveraging AI agents to automate repetitive tasks.

TRY THIS

Explore the Autodev Studio repository and try using the harness for your own software development projects

<https://github.com/krishagarwal314/autodev-studio>

ai agents

software development

autonomous systems

WHAT PEOPLE ACTUALLY BUILT

I built an open-source multi-agent SDLC harness that beats a cold Claude Code run on large repos

reddit

The author built an open-source multi-agent SDLC harness that can beat a cold Claude Code run on large repositories. The harness uses AI agents to learn the repository and improve the development process.

How it works. The harness works by using AI agents to analyze the repository and identify areas for improvement. The agents then work together to scope, code, test, and review the changes, resulting in a more efficient and effective development process.

STEAL THIS

The author's approach to using AI agents for software development can be applied to other projects, improving efficiency and quality

https://www.reddit.com/r/LLMDevs/comments/1v5byy0/i_built_an_opensource_multiagent_sdlc_harness/

Show HN: PocketLens – free, self-hosted Mint alternative via Plaid

hackernews

The author built PocketLens, a free and self-hosted alternative to Mint, using Plaid for automatic bank sync. The application provides a secure and private way to manage personal finances.

How it works. PocketLens uses Plaid to connect to the user's bank account and sync their financial data. The application then provides a user-friendly interface to manage and track expenses, budgets, and financial goals.

STEAL THIS

The author's approach to building a self-hosted financial management application can be applied to other projects, emphasizing security and privacy

<https://github.com/PocketLens/pocketlens-app>

QUICK HITS

Show HN: Twigg – open-source big-tech-like version control and software forge HACKERNEWS

Twigg is an open-source version control and software forge that provides a similar developer experience to Google/Meta/Phabricator
<https://github.com/twigg-vc/monorepo>

poolside/Laguna-S-2.1 HUGGINGFACE

Laguna-S-2.1 is a trending model on HuggingFace, with 613 likes and 28,992 downloads
<https://huggingface.co/poolside/Laguna-S-2.1>

drpwchen/textbook-to-note GITHUB

Textbook-to-note is an open-source tool that turns PDF textbooks into an AI-searchable knowledge base and structured, fully-cited notes
<https://github.com/drpwchen/textbook-to-note>

sudoingX/dgx-spark-laguna GITHUB

Dgx-spark-laguna is a working stack for serving Poolside Laguna S 2.1 on the NVIDIA DGX Spark, with crash-safe configs and benchmarks
<https://github.com/sudoingX/dgx-spark-laguna>

Prism-Shadow/penguin-harness GITHUB

Penguin-harness is an open-source automated agent builder that lives on the desktop, providing a self-improving harness
<https://github.com/Prism-Shadow/penguin-harness>

Octen-Team/search-eval GITHUB

Search-eval is a re-runnable web-search evaluation framework with in-house benchmarks and open-benchmark scoring
<https://github.com/Octen-Team/search-eval>

RimZ is a realtime dashboard and control room for harnessing agentic coding GITHUB

RimZ provides a unique approach to agentic coding, leveraging a realtime dashboard and control room
<https://github.com/rimio-ai/rimz>

AxisAgentic: An Extensible Runtime and Trajectory-Collection Framework for Long-Horizon Agents GITHUB

AxisAgentic provides a framework for long-horizon agents, enabling extensible runtime and trajectory-collection
<https://github.com/XYZ-AI-Lab/AxisAgentic>

Turo – An Aggressive Token-Saving Proxy for CLI AI Agents HACKERNEWS

Turo is an open-source proxy for CLI AI agents, providing aggressive token-saving capabilities
<https://github.com/kdeps/turo>

AgentWatch – Local MCP proxy that catches agents leaking your data HACKERNEWS

AgentWatch is an open-source local MCP proxy that detects and prevents AI agents from leaking user data
<https://github.com/dhanraj176/agentwatch>

