



Relatório diário de tecnologia

As tendências de tecnologia de hoje

25 de outubro de 2026 (domingo)

Em poucos goles

Hoje, no ecossistema de desenvolvedores, destacam-se os agentes de IA que interagem com o mundo físico (embodied agents) e as estruturas de auditoria que visam as vulnerabilidades de segurança dos grandes modelos de linguagem (LLM). Novas ferramentas no GitHub e Hugging Face focam tanto no gerenciamento de sistemas baseados em hardware quanto em testes de privacidade de modelos distribuídos.

25 em destaque · ~9 min de leitura

10 GitHub
Trending

5 Hacker
News

5 Hugging Face ·
modelos do dia

5 Hugging Face ·
artigos do dia

Dados coletados em 25 de outubro de 2026 às 07:49.

As contagens das fontes e os metadados dos itens deste relatório são fixos no momento da coleta. As páginas de Descoberta podem mostrar valores de fontes ao vivo mais recentes.

Os resumos e as traduções deste relatório são preparados com inteligência artificial. Antes de tomar decisões importantes, recomendamos conferir a fonte pelo link indicado em cada item.

01 cloudflare/security-audit-skill

O security-audit-skill, desenvolvido pela Cloudflare, é um pacote de habilidades baseado em JavaScript que transforma agentes de software em auditores capazes de realizar auditorias de segurança em várias etapas. Esta ferramenta gerencia processos que vão desde a descoberta até a geração de relatórios com descobertas verificáveis de forma independente e legíveis por máquina.

JavaScript · ★ 44.962 · +2.264 hoje <https://github.com/cloudflare/security-audit-skill>

[Relatar um erro](#)

02 NVIDIA/OpenShell

O OpenShell, desenvolvido pela NVIDIA, oferece um ambiente de tempo de execução (runtime) seguro e focado em privacidade para agentes de IA autônomos. Escrita na linguagem Rust, esta ferramenta audita o acesso aos dados limitando as capacidades dos agentes, como a leitura de arquivos ou o uso de APIs (uma ponte digital que permite que dois softwares diferentes se comuniquem), dentro de estruturas de políticas específicas.

Rust · ★ 19.571 · +896 hoje <https://github.com/NVIDIA/OpenShell>

[Relatar um erro](#)

03 aws/agent-toolkit-for-aws

O aws/agent-toolkit-for-aws, oferecido pela Amazon Web Services, inclui ferramentas oficiais, plug-ins e servidores do Protocolo de Contexto de Modelo (MCP) que permitem que agentes de IA desenvolvam, implantem e gerenciem aplicativos na AWS. Este conjunto de ferramentas baseado em Python permite que os agentes de IA trabalhem de forma mais compatível com a infraestrutura da AWS nos processos de desenvolvimento de software.

Python · ★ 3.178 · +13 hoje <https://github.com/aws/agent-toolkit-for-aws>

[Relatar um erro](#)

04 Nutlope/hallmark

O Nutlope/hallmark oferece uma habilidade de design que impede que o conteúdo criado em editores de código com suporte de IA, como Cursor, Claude Code e Codex, pareça ter sido gerado por IA. Esta ferramenta visa tornar os resultados padrão de IA que surgem nos processos de desenvolvimento de software visualmente originais.

CSS · ★ 32.343 · +455 hoje <https://github.com/Nutlope/hallmark>

[Relatar um erro](#)

05 luongnv89/claude-howto

O luongnv89/claude-howto oferece um guia visual e focado em exemplos para o Claude Code, abrangendo desde conceitos básicos até estruturas de agentes avançadas. O objetivo é facilitar os processos de codificação com suporte de IA com modelos de copiar e colar que os usuários podem aplicar diretamente.

Python · ★ 44.665 · +392 hoje <https://github.com/luongnv89/claude-howto>

[Relatar um erro](#)

06 pbakaus/impeccable

O pbakaus/impeccable oferece uma linguagem de design e um sistema de orientação que os agentes de codificação de IA podem usar ao projetar interfaces. Desenvolvida na linguagem Rust, esta ferramenta visa melhorar os designs de front-end gerados por IA por meio de 24 comandos e 62 regras de detecção determinísticas.

Rust · ★ 86.572 · +619 hoje <https://github.com/pbakaus/impeccable>

[Relatar um erro](#)

07 pollen-robotics/microduck

O microduck, desenvolvido pela Pollen Robotics, é um projeto de robô pato bípede de 25 centímetros que funciona com o processador Rockchip RK3566. O software, escrito na linguagem Rust, gerencia quinze servomotores por meio de políticas neurais (neural policies) para executar os processos de movimento e controle do robô.

Rust · ★ 11.089 · +319 hoje <https://github.com/pollen-robotics/microduck>

[Relatar um erro](#)

08 google-gemini/gemini-cli

O gemini-cli, desenvolvido pelo Google, é uma ferramenta de código aberto (cujo código-fonte está disponível para todos) que fornece acesso direto ao modelo de IA Gemini através do terminal. O software permite que os usuários criem prompts de IA de forma rápida e leve no ambiente de linha de comando.

TypeScript · ★ 108.165 · +44 hoje <https://github.com/google-gemini/gemini-cli>

[Relatar um erro](#)

09 jbiaojerry/ebook-treasure-chest

O jbiaojerry/ebook-treasure-chest é um projeto de biblioteca digital que reúne links de download de e-books em várias categorias. O projeto visa fornecer acesso ao conteúdo dentro de aplicativos de leitura populares (帆书, 微信读书, 京东读书, 喜马拉雅).

Python · ★ 22.774 · +227 hoje <https://github.com/jbiaojerry/ebook-treasure-chest>

[Relatar um erro](#)

10 makecindy/cindy

Cindy é um agente de IA de código aberto (cujo código-fonte está aberto para acesso e desenvolvimento por todos), pronto para uso, projetado para realizar trabalhos reais em seus projetos e aplicativos. Ele permite que os usuários gerenciem seus fluxos de trabalho combinando vários modelos e ferramentas em uma única estrutura.

TypeScript · ★ 4.198 · +477 hoje <https://github.com/makecindy/cindy>

[Relatar um erro](#)

01 Local Wikipedia: Wikipedia, but only for things a half hour walk from you

Local Wikipedia é um projeto de enciclopédia que fornece informações sobre locais a uma distância de meia hora de caminhada da localização do usuário. Ele serve como uma versão personalizada em escala local da fonte de informação online Wikipedia.

1.561 pontos · 245 comentários <https://edjefferson.com/localwiki/>

[Relatar um erro](#)

Discussão: news.ycombinator.com/item?id=50202285 (1.561 pontos · 245 comentários)

02 Show HN: Steal My Bitcoin

Steal My Bitcoin é uma plataforma criada para testar como uma vulnerabilidade de execução remota de código (RCE) em PHP, descoberta recentemente, pode ser explorada no mundo real. O desenvolvedor convida os usuários a acessar o sistema para observar os impactos concretos dessa falha de segurança.

440 pontos · 264 comentários <https://stealmybitcoin.com/>

[Relatar um erro](#)

Discussão: news.ycombinator.com/item?id=50224916 (440 pontos · 264 comentários)

03 The Goose Programming Language

The Goose é uma nova linguagem de programação projetada para linguagens de programação de sistemas de baixo nível. Com uma estrutura focada em segurança de memória e desempenho, visa o desenvolvimento de softwares de sistema.

304 pontos · 186 comentários <https://aardappel.github.io/goose/>

[Relatar um erro](#)

Discussão: news.ycombinator.com/item?id=50224100 (304 pontos · 186 comentários)

04 Node2Shell evolves to HTTP2Shell, blast radius affects many HTTP libs and apps

A evolução da vulnerabilidade Node2Shell para HTTP2Shell coloca em risco inúmeras bibliotecas e aplicações HTTP que utilizam o algoritmo de compressão de dados Brotli. Para evitar ser afetado por essa falha, codificada como CVE-2026-111497, é necessário verificar as versões utilizadas e realizar as atualizações.

294 pontos · 140 comentários <https://www.aikido.dev/blog/python-packages-vulnerable-node2shell-brotli-cve-2026-111497>

[Relatar um erro](#)

Discussão: news.ycombinator.com/item?id=50219177 (294 pontos · 140 comentários)

05 I don't understand quantum physics (2018)

Este recurso, preparado pela Universidade de Southampton, aborda os conceitos fundamentais da física quântica e os pontos de difícil compreensão nesta área. Focando na complexidade dos fenômenos físicos, o estudo explica os princípios da mecânica quântica (quantum physics) em um contexto acadêmico.

291 pontos · 235 comentários https://www.southampton.ac.uk/~doug/quantum_physics/index.html

[Relatar um erro](#)

Discussão: news.ycombinator.com/item?id=50219666 (291 pontos · 235 comentários)

01 deepseek-ai/DeepSeek-V4.1-Flash-1017

DeepSeek-V4.1-Flash-1017 é a versão atualizada do modelo DeepSeek-V4.1-Flash, um modelo de inteligência artificial capaz de processar dados visuais e textuais. Ele visa proporcionar eficiência de custo ao reduzir o tempo de processamento e o comprimento da saída, enquanto aumenta seu desempenho em tarefas de raciocínio, codificação e baseadas em agentes.

♥ 2.821 · 73.215 downloads <https://huggingface.co/deepseek-ai/DeepSeek-V4.1-Flash-1017>

[Relatar um erro](#)

02 RecursiveSI/flint

Flint, desenvolvido pela RecursiveSI, é um modelo de geração de texto com estrutura de mistura de especialistas (mixture-of-experts) projetado para agentes de codificação. Com um total de 39,8 bilhões de parâmetros, o modelo foi desenvolvido para analisar bases de código, depurar erros, adicionar funcionalidades e escrever testes.

♥ 782 · 4.795 downloads <https://huggingface.co/RecursiveSI/flint>

[Relatar um erro](#)

03 black-forest-labs/flux-3-image-klein-comfy

flux-3-image-klein-comfy, desenvolvido pela Black Forest Labs, é um modelo de inteligência artificial que permite a conversão de imagem para imagem (image-to-image). O modelo foi projetado para funcionar de forma compatível com ferramentas de fluxo de trabalho baseadas em visual, como o ComfyUI.

♥ 1.512 · 590.742 downloads <https://huggingface.co/black-forest-labs/flux-3-image-klein-comfy>

[Relatar um erro](#)

04 XHToken/Spark-X2.6-4B

Publicado na plataforma Hugging Face, o Spark-X2.6-4B é um modelo de inteligência artificial focado em geração de texto (text-generation). Utilizando a mesma arquitetura da versão anterior, o modelo oferece um aumento de desempenho em áreas como codificação, raciocínio e processamento de conteúdo multilíngue, graças a melhorias no processo pós-treinamento.

♥ 457 · 2.537 downloads <https://huggingface.co/XHToken/Spark-X2.6-4B>

[Relatar um erro](#)

05 Lightricks/LTX-2.5

LTX-2.5, desenvolvido pela Lightricks, é um modelo de imagem para vídeo (image-to-video) que transforma imagens em vídeos animados. Compartilhado na plataforma Hugging Face, este modelo permite que conteúdos visuais sejam animados por meio de inteligência artificial.

♥ 9.200 · 2.087.721 downloads <https://huggingface.co/Lightricks/LTX-2.5>

[Relatar um erro](#)

01 TARSphere: A Robot-Oriented Full-Stack Framework for Long-Horizon Embodied Agents in Evolving Physical and Social Environments

TARSphere é uma estrutura full-stack focada em robótica, desenvolvida para agentes incorporados (embodied agents) de longo prazo que operam sob restrições físicas e sociais. O componente TARSphere-Infra oferece a oportunidade de testar políticas robóticas em simuladores físicos com diálogos restritos e personagens de inteligência artificial incorporados (NPCs).

8 curtidas · 2 comentários <https://huggingface.co/papers/2610.30043>

[Relatar um erro](#)

02 The LLM-Attacker: A Unified Red-Team Framework for Privacy Evaluation of Split and Distributed LLM Systems

O LLM-Attacker, compartilhado pela Hugging Face, é uma estrutura desenvolvida para avaliar vulnerabilidades de privacidade em grandes modelos de linguagem (LLM) fragmentados e distribuídos. Este sistema ajuda os pesquisadores a comparar métodos de ataque e padronizar análises de segurança voltadas para a reconstrução de dados.

9 curtidas · 2 comentários <https://huggingface.co/papers/2610.22722>

[Relatar um erro](#)

03 EvalResearchBench: Can AI Agents Build Their Own Feedback for Recursive Self-Improvement?

EvalResearchBench é um benchmark de pesquisa que examina se os agentes de inteligência artificial conseguem gerar automaticamente o feedback de avaliação necessário para seus processos de autoaperfeiçoamento recursivo (recursive self-improvement). Este estudo apresenta um método que visa reduzir o custo de processos de teste complexos, permitindo que os agentes criem seus próprios designs de avaliação.

18 curtidas · 2 comentários <https://huggingface.co/papers/2610.04184>

[Relatar um erro](#)

04 Diffusion Language Models Change Speed Across Tasks and Languages

Os modelos de linguagem de difusão (diffusion language models) têm a capacidade de gerar múltiplos tokens em uma única passagem direta e decidir quantas passagens realizar durante a geração. As análises mostram que o custo desses modelos varia de acordo com o tipo de tarefa, sendo mais rápidos em operações simples onde o texto de entrada é copiado e mais lentos em tarefas que exigem escrita livre.

9 curtidas · 1 comentário <https://huggingface.co/papers/2610.25835>

[Relatar um erro](#)

05 Different Tasks, Different Timesteps: Temporal Task-Aware Quantization for Diffusion Language Models

O T2Quant, desenvolvido para Diffusion Language Models (DLMs), otimiza esse processo ao detectar que a precisão da quantização varia de acordo com a tarefa e as etapas de tempo. O método oferece uma estrutura de precisão mista ao estimar os níveis de precisão necessários para diferentes tarefas sem a necessidade de rótulos ou métricas.

19 curtidas · 2 comentários <https://huggingface.co/papers/2610.31198>

[Relatar um erro](#)

runtime

O ambiente fundamental necessário para que um software funcione e que opera em segundo plano.

MCP

Um protocolo de conexão que permite que modelos de inteligência artificial se comuniquem de forma padronizada com diferentes fontes de dados e ferramentas.

design skill

Capacidade de edição visual que faz com que os conteúdos gerados por inteligência artificial pareçam mais naturais e feitos por humanos.

deterministic detector rules

Mecanismo de auditoria que permite ao software detectar erros ou características específicas por meio de um conjunto de regras precisas e imutáveis.

frontend

A face de um site ou aplicativo que é vista e com a qual o usuário interage.

neural policies

Regras de tomada de decisão determinadas por redes neurais artificiais para controlar os movimentos do robô.

terminal

Interface que permite dar instruções baseadas em texto ao computador por meio de uma linha de comando.

remote code execution - RCE

Uma vulnerabilidade de segurança grave que permite que um invasor controle remotamente o software em outro computador e execute seu próprio código.

quantum physics

Ramo da física que estuda o comportamento e os níveis de energia das partículas subatômicas.

mixture-of-experts

Uma arquitetura de inteligência artificial na qual pequenos submodelos, cada um especializado em diferentes assuntos, são usados em conjunto para resolver tarefas complexas.

image-to-image

Um processo de inteligência artificial que transforma uma imagem em um estilo ou conteúdo diferente com base nela.

text-generation

A capacidade de gerar textos significativos e coerentes de acordo com os comandos fornecidos.

image-to-video

Tecnologia de inteligência artificial que transforma uma imagem estática em um videoclipe animado.

embodied agents

Sistemas robóticos de inteligência artificial capazes de se mover no mundo físico, perceber o ambiente e reagir de acordo.

full-stack

Uma estrutura holística que abrange tanto a interface visível de um software quanto todos os processos de infraestrutura em segundo plano.

NPCs

Personagens em jogos ou simulações que não são controlados pelo jogador e se movem por meio de inteligência artificial.

trescout.com · O TreScout percorre e resume, e você só precisa ler.