

Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

“Trong gian khổ mới thấy được người anh hùng.”

— Tục ngữ Việt Nam

Phẩm chất thật sự của con người chỉ được bộc lộ khi đối mặt với nghịch cảnh và thử thách lớn.

TIN TỨC NỔI BẬT

1

Tình hình các Agent Framework: Lựa chọn Runtime phù hợp cho triển khai AI doanh nghiệp

State of Agent Frameworks: Choosing the Right Runtime for Enterprise AI Execution

Medium

[Đọc bài viết →](#)

Bài viết "Trạng thái của các Framework Truyền thông: Chọn Thời gian Chạy phù hợp cho Thực thi AI Doanh nghiệp" cung cấp cái nhìn tổng quan về trạng thái hiện tại của các framework truyền thông trong bối cảnh thực thi AI doanh nghiệp. Các framework truyền thông là các nền tảng phần mềm cho phép các tổ chức xây dựng, triển khai và quản lý các tác nhân được hỗ trợ bởi AI có thể tương tác với người dùng và các hệ thống khác. Bài viết nhấn mạnh tầm quan trọng của việc chọn thời gian chạy phù hợp cho thực thi AI doanh nghiệp, vì nó có thể ảnh hưởng đáng kể đến hiệu suất, khả năng mở rộng và khả năng bảo trì của các tác nhân được hỗ trợ bởi AI. Nó thảo luận về các framework truyền thông khác nhau, bao gồm Rasa, Dialogflow và Botpress, cũng như các điểm mạnh và điểm yếu tương ứng của chúng. Bài viết cũng đề cập đến các yếu tố quan trọng khi chọn một framework truyền thông, chẳng hạn như dễ sử dụng, tùy chọn tùy chỉnh và tích hợp với các hệ thống hiện có. Nó nhấn mạnh nhu cầu về một framework có thể xử lý các cuộc trò chuyện phức tạp, cung cấp thông tin trực tiếp và hỗ trợ nhiều kênh truyền thông. Cuối cùng, bài viết nhằm giúp các tổ chức đưa ra quyết định sáng suốt khi chọn một framework truyền thông cho nhu cầu thực thi AI doanh nghiệp của họ.

2

Xây dựng Workflow dùng Agent với Cortex AI và Managed MCP Servers

Snowflake đã giới thiệu một khả năng mới cho phép người dùng xây dựng các quy trình làm việc được hỗ trợ bởi các tác nhân sử dụng Cortex AI và Máy chủ MCP được Quản lý. Sự tích hợp này cho phép các nhà phát triển tạo ra các quy trình làm việc tùy chỉnh tận dụng sức mạnh của Cortex AI, một nền tảng AI dựa trên đám mây, và Máy chủ MCP được Quản lý, một dịch vụ được quản lý để chạy và mở rộng các ứng dụng được chứa. Với sự tích hợp này, người dùng có thể xây dựng và triển khai các quy trình làm việc tự động hóa các nhiệm vụ phức tạp, chẳng hạn như xử lý dữ liệu, đào tạo mô hình học máy, và nhiều hơn nữa. Các quy trình làm việc có thể được kích hoạt bởi các sự kiện khác nhau, bao gồm cả đầu vào của người dùng, cuộc gọi API, hoặc các nhiệm vụ được lên lịch. Việc sử dụng Máy chủ MCP được Quản lý cung cấp một môi trường có thể mở rộng và bảo mật để chạy các ứng dụng được chứa, trong khi Cortex AI cung cấp các khả năng AI cần thiết để tự động hóa các nhiệm vụ phức tạp. Sự tích hợp này cho phép các nhà phát triển tập trung vào việc xây dựng các quy trình làm việc tùy chỉnh mà không cần phải lo lắng về cơ sở hạ tầng cơ bản, giúp dễ dàng tự động hóa các quy trình kinh doanh và cải thiện hiệu quả.

AWS mã nguồn mở MCP Server cho Bedrock AgentCore để tinh gọn phát triển AI Agent

3

AWS Open-Sources an MCP Server for Bedrock AgentCore to Streamline AI Agent Development

MarkTechPost

[Đọc bài viết →](#)

Amazon Web Services (AWS) đã thực hiện một bước tiến quan trọng trong lĩnh vực phát triển trí tuệ nhân tạo (AI) bằng cách mở mã nguồn một máy chủ MCP (Nền tảng Đa đám mây) cho Bedrock AgentCore. Động thái này nhằm mục đích đơn giản hóa việc phát triển các tác nhân AI bằng cách cung cấp một nền tảng tiêu chuẩn hóa và có thể mở rộng để xây dựng và triển khai các tác nhân AI. Máy chủ MCP được thiết kế để hoạt động mượt mà với Bedrock AgentCore, một framework để xây dựng các tác nhân AI có thể hoạt động trên nhiều nền tảng đám mây. Bằng cách mở mã nguồn máy chủ MCP, AWS đang cho phép các nhà phát triển xây dựng và triển khai các tác nhân AI một cách hiệu quả hơn, mà không bị ràng buộc vào một nhà cung cấp đám mây cụ thể. Động thái này dự kiến sẽ đẩy nhanh sự phát triển của các tác nhân AI và ứng dụng, cho phép các nhà phát triển tập trung

vào việc xây dựng các giải pháp sáng tạo thay vì lo lắng về cơ sở hạ tầng cơ bản. Việc mở mã nguồn máy chủ MCP cũng thúc đẩy sự hợp tác và tham gia của cộng đồng, điều này có thể dẫn đến sự đổi mới và tiến bộ hơn nữa trong lĩnh vực phát triển AI.

4

Hành trình giữ các cơ quan sống bên ngoài cơ thể

The quest to keep organs alive outside the body

MIT Tech Review

[Đọc bài viết →](#)

Các nhà nghiên cứu đang làm việc để phát triển các phương pháp bảo tồn các cơ quan ngoài cơ thể, giải quyết tình trạng thiếu hụt cơ quan hiến tặng do thời gian tồn tại hạn chế của chúng. Hiện tại, các cơ quan chỉ có thể tồn tại trong vài giờ khi được lưu trữ trên đá. Để vượt qua điều này, các nhà khoa học đang khám phá các kỹ thuật khác nhau, bao gồm làm mát siêu tốc, đông lạnh và truyền dưỡng chất cho các cơ quan. Một đột phá gần đây liên quan đến việc làm mát siêu tốc thận lợn xuống -4°C và bảo tồn chúng trong vài ngày, với việc tái cấy ghép thành công vào lợn. Các nhà nghiên cứu khác đang tập trung vào bảo tồn lạnh, bao gồm làm mát nhanh đến trạng thái giống như thủy tinh, và đã bảo tồn thành công trứng, tinh trùng và phôi. Tuy nhiên, bảo tồn lạnh các cơ quan người để cấy ghép vẫn còn là một thách thức. Ngoài ra, các nhà khoa học đang phát triển các thiết bị truyền máy để duy trì các cơ quan, chẳng hạn như gan và thận, trong tối đa 24 giờ, và đang thích nghi giao thức này cho các cơ quan khác, bao gồm cả mắt và tử cung. Những tiến bộ này nhằm tạo ra các ngân hàng cơ quan có thể lưu trữ các cơ quan trong thời gian dài, cho phép phù hợp và vận chuyển các cơ quan đến người nhận tốt hơn.

5

Nghiên cứu của VentureBeat: Quản trị AI Agent doanh nghiệp còn chưa theo kịp

VentureBeat Research: Where enterprise AI agent governance hasn't caught up

VentureBeat

[Đọc bài viết →](#)

Một nghiên cứu gần đây của VentureBeat Research đã phát hiện ra rằng nhiều doanh nghiệp đã triển khai các tác nhân AI mà không có các biện pháp kiểm soát đầy đủ để quản lý chúng. Đây là một quyết định có chủ ý, với 57-68% công ty dự định chuyển đổi nhà cung cấp hoặc thêm các nhà cung cấp mới trong vòng 12 tháng để bắt kịp với các tiêu chuẩn của riêng họ. Nghiên cứu đã đo lường năm lớp kiểm

soát chính: danh tính, đánh giá, đo lường chi phí, lớp ngữ cảnh và điều phối. Hầu hết các "tác nhân" được triển khai là các rô-bốt trò chuyện, nhưng chỉ 10% công ty chạy các tác nhân đa bước thực sự, đòi hỏi phải có tất cả năm biện pháp kiểm soát này. Nghiên cứu nhấn mạnh một số mối quan ngại, bao gồm sự thiếu tin tưởng vào đánh giá AI, với hai phần ba công ty cho phép các tác nhân đẩy thay đổi mã mà không cần xem xét của con người. Nó cũng phát hiện ra rằng các công ty cho phép các tác nhân chia sẻ thông tin đăng nhập có nhiều khả năng gặp sự cố bảo mật hơn. Hơn nữa, nhiều công ty không sử dụng phần cứng AI của họ một cách hiệu quả, với hơn 80% những công ty chạy GPU của riêng họ báo cáo mức sử dụng dưới 50%. Nghiên cứu cũng lưu ý rằng các tác nhân thường trả lời một cách tự tin từ dữ liệu không được quản lý, với 57% công ty tìm thấy câu trả lời tự tin nhưng sai lầm do thiếu hoặc không nhất quán ngữ cảnh kinh doanh. Tổng thể, nghiên cứu cho thấy rằng các doanh nghiệp đang gặp khó khăn trong việc theo kịp sự phát triển nhanh chóng của AI và cần có các công cụ quản lý và quản trị tốt hơn, bao gồm cả việc xây dựng các model LLM hiệu quả, quản lý token, và cung cấp API, framework cho các nhà phát triển.

Ba điểm bảo mật doanh nghiệp gặp vấn đề ở quy mô codebase (và tại sao các công cụ hiện tại không bao quát được)

6

Three places enterprise security breaks down at codebase scale (and why your current tools don't cover them)

Sourcegraph Blog

[Đọc bài viết →](#)

Bảo mật doanh nghiệp thường bị tổn thương ở quy mô cơ sở mã do một số vấn đề chính. Một vấn đề lớn là sự cố trong việc khắc phục lỗ hổng. Điều này xảy ra khi phân tích mã được hỗ trợ bởi AI thiếu ngữ cảnh, dẫn đến kết quả không chính xác hoặc không đầy đủ. Hơn nữa, các công cụ phát hiện hiện tại thường có khoảng trống về phạm vi, không thể xác định được lỗ hổng trong một số khu vực của cơ sở mã. Kết quả là, ngay cả khi các bản vá được cố gắng, chúng có thể mất vài tuần để triển khai trên các cơ sở mã lớn, chẳng hạn như những cơ sở có 10.000 kho lưu trữ. Quá trình khắc phục kéo dài này khiến cơ sở mã dễ bị tổn thương bởi các mối đe dọa bảo mật tiềm năng. Tình trạng hiện tại của các công cụ bảo mật doanh nghiệp không được trang bị để xử lý quy mô và độ phức tạp của các cơ sở mã hiện đại, nhấn mạnh nhu cầu về các giải pháp hiệu quả và hiệu suất hơn để giải quyết những vấn đề này.

7

Thứ Sáu, ngày 26 tháng 6 năm 2026: Một ngày của sự chuyển đổi và đổi mới

Friday, June 26, 2026: A Day of Transformation and Renewal

Dev.to AI [Đọc bài viết →](#)

Khi chúng ta tiến gần đến cuối tuần, sự sắp xếp của các thiên thể được dự đoán sẽ mang lại một ngày biến đổi và đổi mới sâu sắc vào thứ Sáu, ngày 26 tháng 6 năm 2026. Theo lá số hàng ngày, Mặt Trăng đang ở giai đoạn giảm dần, tượng trưng cho sự kết thúc của một kỷ nguyên, trong khi Mặt Trời ở cung Cự Giải, nhấn mạnh tầm quan trọng của sự chăm sóc và yêu thương bản thân. Các hành tinh cũng ở một sự sắp xếp độc đáo, với Sao Mộc và Sao Thổ tạo thành một khía cạnh căng thẳng, chỉ ra nhu cầu về sự cân bằng và kỷ luật trong việc theo đuổi sự phát triển. Lá số khuyên các cá nhân nên phản ánh con đường hiện tại của mình, buông bỏ cái cũ và tạo không gian cho cái mới. Nó cũng nhấn mạnh tầm quan trọng của việc tin tưởng vào quá trình, ưu tiên chăm sóc bản thân và duy trì sự cân bằng và kỷ luật. Bằng cách lắng nghe sự hướng dẫn của các thiên thể, các cá nhân có thể điều hướng ngày biến đổi và đổi mới này hướng tới một tương lai tươi sáng và đầy hứa hẹn hơn.

8

Cách chúng tôi Benchmark Deep Agents

How We Benchmark Deep Agents

LangChain Blog [Đọc bài viết →](#)

Phát triển Deep Agents, một bộ khung đại lý không phụ thuộc vào model mã nguồn mở, đặt ra những thách thức đáng kể, đặc biệt là trong việc đánh giá hiệu suất của chúng. Để giải quyết vấn đề này, nhóm đã đổi mới khuôn khổ đánh giá của họ, tập trung vào đánh giá từ đầu đến cuối thay vì các bài kiểm tra nhỏ theo phong cách đơn vị. Sự thay đổi này là cần thiết do sự phức tạp và thời gian thực hiện nhiệm vụ của đại lý ngày càng tăng. Để hỗ trợ đánh giá từ đầu đến đầu, nhóm sử dụng Harbor, một khuôn khổ mã nguồn mở phổ biến để chạy đánh giá đại lý. Khuôn khổ đánh giá hiện bao gồm ba điểm chuẩn, mỗi điểm chuẩn nhằm vào một loại công việc đại lý riêng biệt. Điều này cho phép nhóm đánh giá bộ khung Deep Agents trên nhiều lĩnh vực, cung cấp một hiểu biết toàn diện hơn về khả năng của nó. Bằng cách tạo điểm chuẩn cho các thay đổi, nhóm có thể đưa ra quyết định thông minh và lặp lại với sự tự tin, như được chứng minh bởi sự chuẩn bị của họ cho phiên bản 0.7 của Deep Agents. Khuôn khổ đánh

giá sẽ tiếp tục phát triển và thay đổi, giúp nhóm tinh chỉnh bộ khung và cải thiện hiệu suất của nó.

TIPS & TRICKS CHO DEV

Tự động hóa kiểm thử đơn vị

Vấn đề: Thiếu thời gian và nguồn lực để viết các thử nghiệm đơn vị.

Cách làm: Sử dụng framework như Pytest hoặc Unittest, tích hợp với CI/CD pipeline. Ví dụ: `pytest --cov=src` để chạy thử nghiệm và đo độ bao phủ mã.

Đánh giá: Tăng hiệu suất, giảm thiểu sai sót.

Code Review Tự động

Vấn đề: Quá trình xem xét mã nguồn tốn thời gian và dễ xảy ra sai sót.

Cách làm: Sử dụng công cụ như GitHub Code Review, tích hợp với GitHub Actions. Ví dụ: `github actions` để chạy kiểm tra mã tự động.

Đánh giá: Cải thiện chất lượng mã nguồn, giảm thời gian xem xét.

Kiểm thử UI tự động

Vấn đề: Kiểm thử giao diện người dùng tốn thời gian và dễ bị lỗi.

Cách làm: Sử dụng framework như Selenium, tích hợp với CI/CD pipeline. Ví dụ: `selenium webdriver` để chạy thử nghiệm UI tự động.

Đánh giá: Tăng tốc độ phát triển, giảm thiểu sai sót.

BÀI HỌC AI HÔM NAY CHO DEV

1. Tích hợp AI API vào ứng dụng

2. Tích hợp AI API vào ứng dụng giúp tăng cường khả năng thông minh và tự động hóa, cho phép developer tạo ra các ứng dụng có khả năng học hỏi và thích nghi. Điều này giúp cải thiện trải nghiệm người dùng và tăng hiệu suất công việc.

Developer cần biết cách tích hợp AI API để tận dụng lợi thế của công nghệ này.

3. Ví dụ, một ứng dụng điện thoại có thể sử dụng AI API để nhận dạng giọng nói và thực hiện các tác vụ tương ứng, như đặt lịch hẹn hoặc gửi tin nhắn.

4. Tip hoặc bước tiếp theo: Để bắt đầu tích hợp AI API, developer nên nghiên cứu các thư viện và framework như TensorFlow hoặc PyTorch, và chọn một mô hình AI phù hợp với nhu cầu của ứng dụng.

Luôn đi đầu trong thế giới AI! · Stay ahead in AI!

Nguồn: Google News · Groq AI