BIS - MT · 28/05/2026

🤖 Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

✨ *"The purpose of life is a life of purpose."*

↪ Mục đích của cuộc sống là một cuộc sống có mục đích.

— Robert Byrne

💡 *Sống có định hướng rõ ràng và theo đuổi điều có ý nghĩa với bản thân là nền tảng của cuộc sống trọn vẹn và hạnh phúc.*

📰 TIN TỨC NỔI BẬT

1

Các nhà nghiên cứu bảo mật phát tín hiệu cảnh báo về lỗ hổng trong mã được tạo bởi AI

🇬🇧 *Security Researchers Sound the Alarm on Vulnerabilities in AI-Generated Code*

📰 Infosecurity Magazine 🔗 Đọc bài viết →

> Các nhà nghiên cứu bảo mật đã bày tỏ mối quan ngại về các điểm yếu bảo mật trong mã được tạo ra bởi AI. Một nghiên cứu gần đây đã nhấn mạnh các rủi ro tiềm ẩn liên quan đến mã được tạo ra bởi trí tuệ nhân tạo (AI) và các thuật toán học máy (ML). Các nhà nghiên cứu đã phát hiện ra rằng mã được tạo ra bởi AI có thể chứa các lỗi bảo mật, chẳng hạn như tràn bộ đệm, lỗ hổng tiêm SQL và các lỗi mã hóa thông thường khác. Các điểm yếu này có thể bị các kẻ tấn công khai thác để truy cập trái phép vào hệ thống hoặc dữ liệu. Nghiên cứu này gợi ý rằng việc sử dụng mã được tạo ra bởi AI trong phát triển phần mềm có thể giới thiệu các rủi ro mới, đặc biệt là trong các ngành công nghiệp nơi bảo mật là quan trọng, chẳng hạn như tài chính và chăm sóc sức khỏe. Các nhà nghiên cứu nhấn mạnh nhu cầu của các nhà phát triển phải xem xét và kiểm tra kỹ lưỡng mã được tạo ra bởi AI trước khi triển khai nó trong môi trường sản xuất. Họ cũng khuyến nghị rằng các nhà phát triển nên sử dụng mã được tạo ra bởi AI kết hợp với sự giám sát và xác thực của con người để giảm thiểu rủi ro của các lỗ hổng bảo mật.

2

AWS mở mã nguồn một máy chủ MCP cho Bedrock AgentCore để tối ưu hóa phát triển AI agent

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

📰 MarkTechPost 🔗 Đọc bài viết →

> Amazon Web Services (AWS) đã mở mã nguồn một máy chủ MCP (Nền tảng Đa đám mây) cho Bedrock AgentCore, một framework được thiết kế để đơn giản hóa việc phát triển đại lý AI. Động thái này nhằm mục đích đơn giản hóa quá trình tạo và triển khai các đại lý AI trên nhiều nền tảng đám mây khác nhau. Máy chủ MCP là một thành phần chính của Bedrock AgentCore, cho phép các nhà phát triển xây dựng, thử nghiệm và triển khai các đại lý AI trên nhiều môi trường đám mây. Bằng cách mở mã nguồn máy chủ MCP, AWS đang cung cấp cho cộng đồng nhà phát triển một nền tảng tiêu chuẩn hóa cho việc phát triển đại lý AI, giảm thiểu sự phức tạp và chi phí liên quan đến việc xây dựng và triển khai các giải pháp AI. Máy chủ MCP mã nguồn mở dự kiến sẽ đẩy nhanh tốc độ phát triển đại lý AI bằng cách cung cấp một nền tảng thống nhất để xây dựng và triển khai các model AI. Động thái này phù hợp với nỗ lực của AWS trong việc thúc đẩy sự đổi mới và áp dụng AI trên nhiều ngành công nghiệp khác nhau. Việc mở mã nguồn máy chủ MCP là một bước quan trọng hướng tới việc dân chủ hóa sự phát triển AI và làm cho nó trở nên dễ tiếp cận hơn với nhiều nhà phát triển.

3 Xây dựng một agent phân tích tài chính thông minh với LangGraph và Strands Agents | Amazon Web Services

🇬🇧 *Build an intelligent financial analysis agent with LangGraph and Strands Agents | Amazon Web Services*

📰 Amazon Web Services (AWS) 🔗 Đọc bài viết →

> Amazon Web Services (AWS) đã công bố một giải pháp mới để xây dựng một tác nhân phân tích tài chính thông minh sử dụng LangGraph và Strands Agents. Tác nhân này được thiết kế để cung cấp các khả năng phân tích tài chính tiên tiến, cho phép người dùng đưa ra quyết định thông minh. LangGraph là một thư viện xử lý ngôn ngữ tự nhiên (NLP) cho phép người dùng phân tích và hiểu dữ liệu tài chính phức tạp, chẳng hạn như báo cáo và tuyên bố tài chính. Nó có thể trích xuất thông tin chính, xác định xu hướng và cung cấp thông tin về hiệu suất tài chính. Strands Agents, mặt khác, là một nền tảng phát triển low-code cho phép người dùng xây dựng, triển khai và quản lý các model AI và học máy tùy chỉnh. Bằng cách tích hợp LangGraph với Strands Agents, người dùng có thể tạo ra một tác nhân phân tích tài chính toàn diện có thể phân tích các tập dữ liệu lớn, xác định mẫu và cung

cấp các khuyến nghị có thể thực hiện được. Giải pháp này dự kiến sẽ mang lại lợi ích cho các tổ chức tài chính, nhà đầu tư và nhà phân tích bằng cách cung cấp một cách chính xác và hiệu quả hơn để phân tích dữ liệu tài chính, cuối cùng dẫn đến việc đưa ra quyết định tốt hơn.

4

sqlite AGENTS.md

🇬🇧 *sqlite AGENTS.md*

📰 Simon Willison 🔗 Đọc bài viết →

SQLite gần đây đã thêm tệp AGENTS.md vào cơ sở mã của mình, trong đó phác thảo các chính sách về việc chấp nhận đóng góp từ các tác nhân tự động. Tệp này tuyên bố rằng SQLite không chấp nhận yêu cầu kéo (pull requests) mà không có thỏa thuận trước và giấy tờ pháp lý kèm theo, nhưng các nhà phát triển con người sẽ xem xét các yêu cầu kéo ý tưởng chứng minh khái niệm rõ ràng và viết tốt. Dự án cũng từ chối mã do tác nhân tạo ra, nhưng sẽ chấp nhận báo cáo lỗi với các trường hợp thử nghiệm có thể tái tạo. Để đáp ứng với sự gia tăng của các báo cáo lỗi được tạo ra bởi AI trên diễn đàn SQLite, các nhà phát triển đã tạo ra một Diễn đàn Lỗi SQLite mới để tách các báo cáo này khỏi các vấn đề khác. Tệp AGENTS.md đã được cập nhật để tăng cường lập trường chống lại mã do tác nhân tạo ra, và các nhà phát triển con người đang tích cực giải quyết các vấn đề trên diễn đàn mới. Cập nhật này nhằm làm rõ các chính sách của SQLite và cải thiện việc quản lý các đóng góp và báo cáo lỗi.

5

Tải xuống: cập nhật về AI và tương lai của IVF

🇬🇧 *The Download: keeping up with AI, and the future of IVF*

📰 MIT Tech Review 🔗 Đọc bài viết →

Trong số này của The Download, một bản tin hàng ngày từ MIT Technology Review, nhấn mạnh những phát triển mới nhất trong công nghệ, đặc biệt là trong lĩnh vực trí tuệ nhân tạo (AI) và thụ tinh trong ống nghiệm (IVF). Bản tin thừa nhận tốc độ phát triển nhanh chóng của AI, điều này có thể khiến người đọc choáng ngợp khi theo dõi. Để giúp người đọc hiểu được tầm quan trọng của những phát triển này, bản tin cung cấp danh sách "10 Điều Quan Trọng Trong AI Hiện Tại" và đề nghị giảm giá 25% cho việc đăng ký để tìm hiểu sâu hơn về AI trong mùa hè này. Trong lĩnh vực IVF, các nhà nghiên cứu đang sử dụng AI để xác định tinh trùng và phôi hứa hẹn, phát triển hệ thống

robot để tự động hóa một phần của quá trình, và khám phá các kỹ thuật chỉnh sửa gene để ngăn chặn các bệnh di truyền. Những công nghệ này nhằm mục đích làm cho IVF hiệu quả và dễ tiếp cận hơn, nhưng cũng đặt ra những câu hỏi khó về giới hạn của y học sinh sản. Bản tin cũng bao gồm các câu chuyện công nghệ khác, bao gồm kế hoạch của NASA cho các nhiệm vụ không có phi hành đoàn đến Mặt Trăng, kế hoạch tiền thưởng của Samsung cho công nhân chip, và việc sử dụng AI ngày càng tăng trong giám sát và ứng dụng quân sự.

6 Các trang web có một cách mới để theo dõi người truy cập: phân tích hoạt động SSD của họ

🇬🇧 *Websites have a new way to spy on visitors: analyzing their SSD activity*

📰 Ars Technica 🔗 Đọc bài viết →

Các trang web đã phát hiện ra một cách mới để theo dõi hoạt động của người truy cập, sử dụng một kỹ thuật gọi là FROST (lấy dấu vân tay từ xa sử dụng thời gian SSD dựa trên OPFS). Phương pháp này cho phép các trang web theo dõi các trang web khác mà người truy cập đang xem và các ứng dụng nào đang mở trên thiết bị của họ. FROST khai thác một kênh phụ, đo lường sự tương tác của các quá trình cạnh tranh cho một tài nguyên, chẳng hạn như ổ đĩa trạng thái rắn (SSD). Bằng cách phân tích thời gian của các hoạt động I/O nhất định, các nhà nghiên cứu đã có thể xác định các trang web đang mở trong các tab khác và các ứng dụng đang mở trên thiết bị. Loại tấn công này không yêu cầu sự tương tác từ người truy cập và có thể được thực hiện chỉ trong trình duyệt sử dụng JavaScript. Kỹ thuật này có những hạn chế, bao gồm nhu cầu về một tệp OPFS lớn và yêu cầu tệp đó phải được lưu trữ trên cùng một SSD với thiết bị của người truy cập. Để ngăn chặn các cuộc tấn công FROST, người dùng có thể đóng các tab không cần thiết và theo dõi việc tạo và kích thước của các tệp OPFS được phân bổ bởi các trang web không xác định. Các nhà sản xuất trình duyệt cũng có thể thực hiện các biện pháp để ngăn chặn loại tấn công này.

7 AI cố gắng chôn vùi chính trị gia này — nhưng bây giờ mọi người đã biết đến anh ấy

🇬🇧 *AI tried to bury this politician — now people have actually heard of him*

📰 The Verge AI 🔗 Đọc bài viết →

Trong một sự kiện bất ngờ, một thành viên hội đồng lập pháp bang New York, Alex Bores, đã trở thành ứng cử viên hàng đầu trong cuộc bầu cử sơ bộ của đảng Dân chủ cho khu vực quốc hội thứ 12, mặc dù bị nhắm mục tiêu bởi một siêu ủy ban vận động hành lang mạnh mẽ được hỗ trợ bởi các giám đốc điều hành của OpenAI, Palantir và a16z. Siêu ủy ban vận động hành lang này, Leading the Future, đã chi khoảng 2,4 triệu đô la cho các quảng cáo tấn công chống lại Bores từ tháng 12 năm 2025, trong một nỗ lực nhằm chấm dứt cuộc chạy đua của ông cho chiếc ghế này. Tuy nhiên, Bores đã quản lý để giành được động lực mà không cần chạy một chiến dịch quảng cáo lớn, và chiến dịch của ông chỉ mới đặt mua quảng cáo đầu tiên ở New York. Người chiến thắng thực sự của cuộc chiến ủy nhiệm này có thể là chính Bores, người đã trở thành biểu tượng cho việc quản lý an toàn AI do những nỗ lực của ông trong việc soạn thảo luật về chủ đề này. Chiến dịch của Bores đã được thúc đẩy bởi một tính năng bìa gần đây trên Tạp chí New York, đã gọi ông là "gương mặt của Manhattan". Kết quả của cuộc bầu cử sơ bộ, dự kiến kết thúc vào tháng 6, sẽ được theo dõi chặt chẽ vì nó có thể có những ý nghĩa quan trọng đối với việc quản lý AI.

8

Bên ngoài động cơ: 10 dự án mã nguồn mở định hình cách trò chơi thực sự được tạo ra

🇬🇧 *Beyond the engine: 10 open source projects shaping how games actually get made*

📰 GitHub Blog 🔗 Đọc bài viết →

GitHub đã nhấn mạnh 10 dự án mã nguồn mở đang định hình quá trình phát triển trò chơi. Những dự án này phục vụ các khía cạnh khác nhau của phát triển trò chơi, bao gồm nghệ thuật, hoạt hình, cấp độ, âm thanh, đối thoại và gỡ lỗi. Trong khi các công cụ trò chơi như Godot, Unity và Unreal cung cấp nền tảng cho phát triển trò chơi, những công cụ mã nguồn mở này giải quyết các quy trình và đường ống thường bị bỏ qua nằm ngoài công cụ. 10 dự án mã nguồn mở này bao gồm Blockbench, một trình chỉnh sửa mô hình 3D cho mô hình poly thấp với kết cấu nghệ thuật pixel, và các công cụ khác cho chỉnh sửa cấp độ, xử lý âm thanh và gỡ lỗi. Những dự án này được tạo ra để giải quyết các điểm đau cụ thể trong phát triển trò chơi, với mục tiêu làm cho phát triển trò chơi trở nên hiệu quả và hợp tác hơn. Bằng cách tận dụng những công cụ mã nguồn mở này, các nhà phát triển trò chơi có thể tối ưu hóa quy trình làm việc của họ, cải thiện năng suất và tạo ra các trò chơi chất lượng cao. Các công cụ này được thiết kế để

> không phụ thuộc vào công cụ, cho phép nhà phát triển tích hợp chúng vào đường ống hiện có của mình, bất kể họ sử dụng công cụ trò chơi nào. Sự chuyển dịch này hướng tới các phương pháp mã nguồn mở và tự động hóa được hỗ trợ bởi AI đang trở nên phổ biến ngày càng tăng trong số các tổ chức trên toàn thế giới, và GitHub đang ở vị trí tiên phong trong phong trào này.

⚡ TIPS & TRICKS CHO DEV

⚡ Sử dụng LangSmith cho AI Observability

Vấn đề: Khó theo dõi hiệu suất của mô hình AI.

Cách làm: Sử dụng LangSmith để theo dõi và phân tích hiệu suất của mô hình. Ví dụ, với lệnh `langsmith monitor --model my_model`, bạn có thể theo dõi hiệu suất của mô hình.

Đánh giá: LangSmith hiệu quả trong việc theo dõi và phân tích hiệu suất của mô hình AI, giúp giảm thiểu thời gian và chi phí.

⚡ Áp dụng Langfuse cho Tracing

Vấn đề: Khó xác định nguyên nhân của lỗi trong mô hình AI.

Cách làm: Sử dụng Langfuse để tạo ra các bản ghi vết của mô hình. Ví dụ, với lệnh `langfuse trace --model my_model`, bạn có thể tạo ra bản ghi vết của mô hình.

Đánh giá: Langfuse giúp xác định nguyên nhân của lỗi trong mô hình AI, giúp cải thiện độ tin cậy và hiệu suất.

⚡ Kiểm soát chi phí với Arize Phoenix

Vấn đề: Chi phí vận hành mô hình AI quá cao.

Cách làm: Sử dụng Arize Phoenix để theo dõi và kiểm soát chi phí. Ví dụ, với lệnh `arize phoenix --model my_model --cost-control`, bạn có thể theo dõi và kiểm soát chi phí của mô hình.

Đánh giá: Arize Phoenix hiệu quả trong việc kiểm soát chi phí vận hành mô hình AI, giúp giảm thiểu chi phí và tối ưu hóa tài nguyên.

📚 BÀI HỌC AI HÔM NAY CHO DEV

1. **Tối ưu chi phí & hiệu năng LLM**

Dev cần biết về tối ưu chi phí và hiệu năng LLM để giảm thiểu chi phí vận hành và nâng cao hiệu suất của ứng dụng AI. Điều này giúp đảm bảo sự ổn định và tiết kiệm tài nguyên khi triển khai mô hình ngôn ngữ lớn.

2. Việc tối ưu hóa chi phí và hiệu năng LLM là quan trọng vì nó ảnh hưởng trực tiếp đến hiệu suất và chi phí của ứng dụng.

3. Ví dụ, sử dụng kỹ thuật fine-tuning và LoRA (Low-Rank Adaptation) có thể giúp giảm thiểu số lượng tham số cần thiết, từ đó giảm chi phí tính toán và tăng hiệu suất.

4. 💡 Tip: Để bắt đầu tối ưu hóa chi phí và hiệu năng LLM, hãy xem xét việc sử dụng các kỹ thuật như quantization, pruning và knowledge distillation để giảm thiểu số lượng tham số và tăng hiệu suất của mô hình.