BIS - MT · 11/05/2026

🤖 Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

✨ *"The best way to predict the future is to invent it."*

↪ Cách tốt nhất để dự đoán tương lai là tạo ra nó.

— Alan Kay

💡 *Đừng chỉ đoán về tương lai — hãy là người chủ động định hình nó thông qua đổi mới, sáng tạo và hành động táo bạo.*

📰 TIN TỨC NỔI BẬT

1

Trí tuệ nhân tạo (AI) có thể thay thế nhà phát triển không? Những điều bạn cần biết - Viện Tiêu chuẩn Quốc gia Mỹ

🇬🇧 *Will AI Replace Developers? What You Need to Know - American National Standards Institute*

📰 ANSI 🔗 Đọc bài viết →

> Viện Tiêu chuẩn Quốc gia Mỹ (ANSI) đã giải quyết các mối quan ngại về việc thay thế các nhà phát triển bằng trí tuệ nhân tạo (AI). Mặc dù AI đã đạt được những tiến bộ đáng kể trong những năm gần đây, nhưng nó không thể thay thế hoàn toàn các nhà phát triển con người. AI có thể tự động hóa các nhiệm vụ lặp đi lặp lại và nhàm chán, giúp các nhà phát triển tập trung vào các nhiệm vụ cấp cao hơn đòi hỏi sự sáng tạo, giải quyết vấn đề và tư duy phản biện. Tuy nhiên, AI cũng có thể tăng cường công việc của các nhà phát triển, giúp họ trở nên hiệu quả và hiệu quả hơn. Các công cụ được hỗ trợ bởi AI có thể hỗ trợ các nhiệm vụ như xem xét mã, gỡ lỗi và kiểm tra, cho phép các nhà phát triển tập trung vào việc viết mã mới và phát triển các giải pháp sáng tạo. ANSI nhấn mạnh rằng mối quan hệ giữa AI và các nhà phát triển là sự hợp tác, không phải là thay thế. Khi AI tiếp tục phát triển, nó có thể thay đổi bản chất công việc của các nhà phát triển, nhưng nó sẽ không loại bỏ hoàn toàn nhu cầu về các nhà phát triển con người. Thay vào đó, AI sẽ cho phép các nhà phát triển làm việc hiệu quả và hiệu quả hơn, thúc đẩy sự đổi mới và tiến bộ trong ngành công nghệ.

2

AI cản trở năng suất của các nhà phát triển phần mềm, mặc dù kỳ vọng nó sẽ tăng hiệu suất

🇬🇧 *AI hampered productivity of software developers, despite expectations it would boost efficiency*

📰 Fortune 🔗 Đọc bài viết →

> Một nghiên cứu gần đây đã phát hiện ra rằng việc sử dụng Trí tuệ Nhân tạo (AI) trong phát triển phần mềm thực sự đã giảm năng suất lao động của các nhà phát triển, trái ngược với những kỳ vọng ban đầu. Mặc dù AI được hứa hẹn sẽ tự động hóa các nhiệm vụ lặp đi lặp lại và tăng cường hiệu quả, công nghệ này đã tạo ra những thách thức và phức tạp mới cho các nhà phát triển. Nghiên cứu cho thấy AI đã giới thiệu thêm khối lượng công việc, tăng nhu cầu bảo trì và xử lý sự cố, và dẫn đến số lượng lỗi cao hơn. Kết quả là, các nhà phát triển đã phải dành nhiều thời gian hơn để giải quyết hậu quả của mã được tạo ra bởi AI, thay vì tập trung vào các nhiệm vụ cấp cao đòi hỏi sự sáng tạo và kỹ năng giải quyết vấn đề. Kết quả không mong đợi này nhấn mạnh nhu cầu cho các nhà phát triển tham gia nhiều hơn vào quá trình phát triển AI và các hệ thống AI được thiết kế với nhu cầu và hạn chế của con người. Phát hiện của nghiên cứu có ý nghĩa quan trọng đối với tương lai của phát triển phần mềm và vai trò của AI trong ngành công nghiệp.

3

Các kỹ sư phần mềm của Google đang chuyển từ viết mã sang đưa ra quyết định

🇬🇧 *Google's software engineers are shifting from coding to calling the shots*

📰 Business Insider 🔗 Đọc bài viết →

> Các kỹ sư phần mềm của Google đang ngày càng đảm nhận các vai trò lãnh đạo trong công ty, rời xa trọng tâm truyền thống là viết mã. Theo báo cáo, những kỹ sư này hiện đang được giao thêm nhiều trách nhiệm, bao gồm giám sát dự án và đưa ra quyết định chiến lược. Sự thay đổi này là một phần trong nỗ lực của Google nhằm trao quyền cho tài năng kỹ thuật của mình và thúc đẩy đổi mới trong tổ chức. Sự di chuyển này được coi là một thay đổi đáng kể so với cấu trúc phân cấp truyền thống của Google, nơi các kỹ sư chủ yếu tập trung vào việc viết mã. Bằng cách trao cho các kỹ sư nhiều vai trò lãnh đạo hơn, Google nhằm tận dụng chuyên môn kỹ thuật của họ và khuyến khích họ đưa ra quyết định kinh doanh. Cách tiếp cận này cũng dự kiến sẽ tạo ra một môi trường hợp tác hơn, nơi các kỹ sư có thể làm việc chặt chẽ với các đội khác để phát triển và triển khai các ý tưởng mới. Sự thay đổi này cũng là sự phản ánh của sự tập trung ngày càng tăng của

Google vào trí tuệ nhân tạo (AI) và học máy (LLM), những lĩnh vực mà chuyên môn kỹ thuật là rất quan trọng. Bằng cách trao quyền cho các kỹ sư phần mềm của mình, Google đang đặt mình vào vị trí dẫn đầu trong những lĩnh vực đang phát triển nhanh chóng này.

4

Tất cả các bản cập nhật mới nhất về trung tâm dữ liệu AI

🇬🇧 *All the latest updates on AI data centers*

📰 The Verge AI 🔗 Đọc bài viết →

Các trung tâm dữ liệu, nền tảng vật lý cho tham vọng AI của các công ty công nghệ, đang gây ra tranh cãi toàn cầu về tác động môi trường và xã hội của chúng. Một cuộc khảo sát mới của Trung tâm Nghiên cứu Pew cho thấy cả đảng Cộng hòa và Dân chủ đều chỉ ra các trung tâm dữ liệu là một lý do chính cho chi phí cao hơn. Tại Mỹ, các dự án trung tâm dữ liệu quy mô lớn đang đối mặt với sự phản đối từ các cộng đồng địa phương, với 47% cử tri ở Georgia phản đối một dự án phát triển trị giá hàng tỷ đô la. Trung tâm dữ liệu hyperscale được lên kế hoạch tại Quận Box Elder, được hỗ trợ bởi nhà đầu tư Shark Tank Kevin O'Leary, dự kiến sẽ sử dụng 9 gigawatt điện, nhiều hơn gấp đôi mức sử dụng điện hiện tại của bang. NAACP đang kiện xAI về dự án trung tâm dữ liệu của Elon Musk ở Tennessee, cáo buộc rằng nó vi phạm Đạo luật Không khí Sạch. Trong khi đó, Lực lượng Vệ binh Cách mạng Hồi giáo Iran đã đe dọa trung tâm dữ liệu Abu Dhabi của OpenAI, cảnh báo về "sự hủy diệt hoàn toàn và tuyệt đối" nếu Mỹ tấn công các nhà máy điện của nước này. Các thượng nghị sĩ Mỹ Elizabeth Warren và Josh Hawley đã kêu gọi Cơ quan Thông tin Năng lượng thu thập và công bố công khai dữ liệu về việc sử dụng năng lượng của các trung tâm dữ liệu. Một trang web theo dõi được huy động từ cộng đồng đang cung cấp cái nhìn tổng quan toàn diện về các dự án trung tâm dữ liệu được đề xuất trên 18 bang.

5

Công cụ AI bị nhiễm độc lộ ra một điểm yếu lớn trong bảo mật agent doanh nghiệp

🇬🇧 *AI tool poisoning exposes a major flaw in enterprise agent security*

📰 VentureBeat 🔗 Đọc bài viết →

Một lỗ hổng lớn trong bảo mật của các đại lý AI doanh nghiệp đã được lộ thông qua một hiện tượng được gọi là nhiễm độc công cụ AI. Điều này xảy ra khi các đại lý AI chọn công cụ từ các sổ đăng ký chung dựa

trên mô tả ngôn ngữ tự nhiên, mà không có sự xác minh của con người đối với những mô tả đó. Kết quả là, nhiều điểm yếu có thể phát sinh tại các giai đoạn khác nhau của chu kỳ sống của một công cụ, bao gồm cả các mối đe dọa tại thời điểm chọn và thời điểm thực thi. Các biện pháp kiểm soát chuỗi cung ứng phần mềm hiện tại, chẳng hạn như ký mã và danh mục vật liệu phần mềm (SBOMs), là không đủ để giải quyết những vấn đề này. Những biện pháp kiểm soát này tập trung vào tính toàn vẹn của các thành phần, nhưng nhiễm độc công cụ AI đòi hỏi tính toàn vẹn về hành vi, đảm bảo rằng một công cụ hành động như mô tả và không thực hiện theo các lệnh từ bên ngoài. Để giải quyết vấn đề này, một proxy xác minh có thể được thực hiện giữa giao thức ngữ cảnh mô hình (MCP) của máy khách và máy chủ. Proxy này thực hiện ba lần xác minh trên mỗi lần gọi: liên kết khám phá, cho phép danh sách điểm cuối và xác thực lược đồ đầu ra. Một thông số kỹ thuật hành vi, chi tiết các điểm cuối bên ngoài của công cụ, đọc và ghi dữ liệu, và các hiệu ứng phụ, cũng được yêu cầu. Việc triển khai giải pháp này đòi hỏi một cách tiếp cận từng bước, bắt đầu với việc cho phép danh sách điểm cuối tại thời điểm triển khai và dần dần thêm các lần xác minh tiên tiến hơn. Cách tiếp cận này đảm bảo rằng đầu tư bảo mật tăng tỷ lệ với rủi ro, và hệ sinh thái trưởng thành theo thời gian, cho phép các nhà phát triển xây dựng các ứng dụng mạnh mẽ và an toàn bằng cách sử dụng các framework và API hiện có, cũng như các mô hình LLM và token.

6

Tại sao luật đảm bảo tuổi tác lại quan trọng đối với các nhà phát triển

🇬🇧 *Why age assurance laws matter for developers*

📰 GitHub Blog 🔗 Đọc bài viết →

Các luật đảm bảo độ tuổi, nhằm bảo vệ trẻ em và thiếu niên trực tuyến, đang được đề xuất bởi các nhà hoạch định chính sách trên toàn thế giới. Những luật này sẽ hạn chế quyền truy cập của trẻ vị thành niên vào một số dịch vụ hoặc nội dung nhất định, hoặc yêu cầu các thiết bị và cửa hàng ứng dụng thu thập thông tin về độ tuổi và chuyển nó đến các ứng dụng và trang web. Mặc dù được thúc đẩy bởi những lo ngại nghiêm trọng, nhưng những đề xuất này có nguy cơ áp đặt các yêu cầu tạp đối với phần mềm mã nguồn mở và dịch vụ cơ sở hạ tầng của nhà phát triển không gây ra cùng mức độ rủi ro cho trẻ vị thành niên như các nền tảng hướng đến người tiêu dùng. Các nhà phát triển nên nhận thức được những luật này và cách thức tương tác với chúng. Các luật này nhằm giải quyết các vấn đề nghiêm trọng như bắt nạt

trực tuyến, tiếp xúc với nội dung bạo lực và quấy rối. Tuy nhiên, nếu không có phạm vi phù hợp, chúng có thể vô tình tạo ra các chướng ngại vật không cần thiết cho các nhà phát triển.

7 Sự hỗn loạn xảy ra khi cuộc tấn công mạng làm gián đoạn nền tảng học tập Canvas giữa kỳ thi cuối

🇬🇧 *Chaos erupts as cyberattack disrupts learning platform Canvas amid finals*

📰 Ars Technica 🔗 Đọc bài viết →

Một cuộc tấn công mạng vào nền tảng học trực tuyến Canvas đã gây ra sự gián đoạn rộng rãi đối với các kỳ thi cuối cấp trên toàn nước Mỹ. Cuộc tấn công, được cho là do nhóm ransomware ShinyHunters thực hiện, đã xảy ra vào thứ Năm khi sinh viên dự kiến sẽ tham gia kỳ thi của họ. Công ty mẹ của Canvas, Instructure, đã tạm thời đưa nền tảng này ngoại tuyến sau khi phát hiện hoạt động không được ủy quyền trong mạng của mình. Công ty đã xác nhận rằng dữ liệu người dùng, bao gồm tên, địa chỉ email và số ID sinh viên, đã bị truy cập trong một sự cố bảo mật dữ liệu trước đó. Một yêu cầu tiền chuộc đã được hiển thị trên trang đăng nhập của Canvas, khiến các trường học và trường đại học phải hoãn hoặc sắp xếp lại các kỳ thi. Đại học Illinois, Đại học Massachusetts Dartmouth và hệ thống Đại học California là những trường bị ảnh hưởng. Instructure đã báo cáo rằng nền tảng đã trở lại trực tuyến vào sáng thứ Sáu.

8 Làm thế nào tôi giảm hóa đơn API của mình một nửa mà không hiểu tôi đang làm gì

🇬🇧 *How I Cut My API Bill in Half Without Understanding What I Was Doing*

📰 Dev.to AI 🔗 Đọc bài viết →

Một nhà phát triển chia sẻ kinh nghiệm của họ trong việc giảm hóa đơn API xuống 50% thông qua một kỹ thuật gọi là bộ nhớ đệm lời nhắc. Ban đầu, họ đã gửi một khối ngữ cảnh 4.000 token với mỗi yêu cầu, với chi phí khoảng 300 đô la mỗi tháng. Khi xem xét lại mã của họ, họ nhận ra rằng hầu hết thông tin được gửi với mỗi yêu cầu vẫn giữ nguyên, chẳng hạn như lời nhắc hệ thống và hướng dẫn phong cách của công ty. Bằng cách xác định và lưu trữ các yếu tố tĩnh này, họ đã đạt được sự giảm chi phí đáng kể. Tuy nhiên, nhà phát triển nhấn mạnh rằng chìa khóa để lưu trữ thành công nằm ở việc hiểu những gì là tĩnh và những gì là động trong yêu cầu. Điều này đòi hỏi sự xem xét

> cẩn thận và mã hóa có chủ đích, chứ không chỉ đơn giản là áp dụng một giải pháp lưu trữ. Bằng cách áp dụng phương pháp này, các nhà phát triển có thể cải thiện sự rõ ràng và khả năng bảo trì của mã, buộc họ phải suy nghĩ một cách nghiêm túc về lời nhắc và hướng dẫn của mình. Nhà phát triển cũng nhấn mạnh lợi ích của việc lưu trữ, bao gồm tiết kiệm chi phí và cải thiện chất lượng mã, và cung cấp một ví dụ về cách thực hiện lưu trữ trong mã của họ bằng cách sử dụng tham số `cache_control`.

⚡ TIPS & TRICKS CHO DEV

⚡ Tối ưu GitHub Copilot

Sử dụng GitHub Copilot để tự động hoàn thành code. Ví dụ: "Implement bubble sort algorithm".

⚡ Tăng hiệu suất ChatGPT

Khai thác ChatGPT để debug code. Ví dụ: "Fix error in này code snippet".

📚 BÀI HỌC AI HÔM NAY CHO DEV

1. **Tối ưu chi phí & hiệu năng LLM**
2. Dev cần biết về tối ưu chi phí và hiệu năng LLM để giảm thiểu chi phí và tăng tốc độ xử lý. Điều này giúp ứng dụng hoạt động hiệu quả hơn và tiết kiệm tài nguyên.
3. Ví dụ: Sử dụng mô hình LLM nhỏ hơn để giảm chi phí tính toán.
4. 💡 Tip: Sử dụng kỹ thuật quantization và pruning để tối ưu hóa mô hình LLM.