BIS - MT · 03/07/2026

Bản Tin AI Hằng Ngày

Cập nhật công nghệ AI mới nhất

“Kiến tha lâu đầy tổ.”

— Tục ngữ Việt Nam

Tích lũy từng chút một mỗi ngày — dù nhỏ bé, sự kiên trì sẽ tạo nên kết quả lớn theo thời gian.

TIN TỨC NỔI BẬT

1 Các nhà nghiên cứu bảo mật cảnh báo về lỗ hổng trong code do AI tạo ra

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 lo ngại về các lỗ hổng trong code do AI tạo ra. Theo một báo cáo gần đây, các công cụ hỗ trợ bởi AI đang ngày càng được sử dụng để tạo ra code, nhưng code này thường chứa các lỗi và lỗ hổng bảo mật. Các nhà nghiên cứu cảnh báo rằng việc phụ thuộc vào code do AI tạo ra có thể khiến người dùng gặp rủi ro bị tấn công mạng. Báo cáo nhấn mạnh rằng code do AI tạo ra có thể không được kiểm thử hoặc review kỹ lưỡng, dẫn đến các vấn đề bảo mật tiềm ẩn. Ngoài ra, việc sử dụng code do AI tạo ra cũng có thể gây khó khăn trong việc xác định nguyên nhân gốc rễ của một vấn đề bảo mật, vì code có thể không dễ hiểu đối với các developer con người. Các nhà nghiên cứu đang kêu gọi các developer thận trọng khi sử dụng code do AI tạo ra và kiểm thử, review kỹ lưỡng code trước khi deploy. Họ cũng khuyến nghị các developer cần hiểu rõ về các công cụ AI đang được sử dụng và những rủi ro tiềm ẩn liên quan đến chúng.

2 Agent Factory: Kết nối các agent, ứng dụng và dữ liệu bằng các chuẩn mở mới như MCP và A2A

Agent Factory: Connecting agents, apps, and data with new open standards like MCP and A2A

Microsoft Azure Đọc bài viết →

Microsoft đã giới thiệu Agent Factory, một sáng kiến mới nhằm kết nối các agent, ứng dụng và dữ liệu thông qua các chuẩn mở. Nền tảng này sử dụng các chuẩn Cloud PC (MCP) và Application-to-Application (A2A) của Microsoft để tạo điều kiện tương tác liền mạch giữa các thành phần khác nhau. Agent Factory cho phép các developer tạo và quản lý các agent thông minh có thể tương tác với nhiều ứng dụng và nguồn dữ liệu. Điều này cho phép tạo ra các workflow phức tạp và tự động hơn, nâng cao năng suất và hiệu quả. Việc sử dụng các chuẩn mở như MCP và A2A đảm bảo khả năng tương tác và tính linh hoạt, cho phép các developer xây dựng các giải pháp có thể tích hợp với nhiều hệ thống và dịch vụ. Động thái này của Microsoft có khả năng có những tác động đáng kể đến sự phát triển của các ứng dụng thông minh và bối cảnh kỹ thuật số rộng lớn hơn.

3

AWS mở mã nguồn MCP server cho Bedrock AgentCore nhằm tinh gọn 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 MCP (Multi-Cloud Platform) server cho Bedrock AgentCore, một framework được thiết kế để tinh gọn quá trình phát triển AI agent. MCP server là một thành phần quan trọng của Bedrock AgentCore, cho phép các developer xây dựng và deploy các AI agent trên nhiều nền tảng cloud khác nhau. Bằng cách mở mã nguồn MCP server, AWS đặt mục tiêu đẩy nhanh quá trình phát triển AI agent và thúc đẩy sự hợp tác trong cộng đồng developer. MCP server là một phần cốt lõi của Bedrock AgentCore, cung cấp một giao diện thống nhất để xây dựng, deploy và quản lý các AI agent. Với việc MCP server hiện đã được mở mã nguồn, các developer có thể truy cập code và đóng góp vào quá trình phát triển của nó, cho phép đổi mới và cải tiến nhanh hơn. Động thái này dự kiến sẽ mang lại lợi ích cho các developer làm việc trong các dự án AI, vì họ sẽ có quyền truy cập vào một MCP server được sử dụng rộng rãi và được duy trì tốt. Việc mở mã nguồn MCP server là một bước tiến đáng kể hướng tới việc làm cho quá trình phát triển AI trở nên dễ tiếp cận và hiệu quả hơn.

4 PamStealer mới được phát hiện không phải là malware macOS thông thường

Newly discovered PamStealer isn't your typical macOS malware

Ars Technica Đọc bài viết →

> Các nhà nghiên cứu tại Jamf đã phát hiện một loại malware macOS mới có tên PamStealer, kết hợp các kỹ thuật tinh vi để lây nhiễm vào máy Mac bằng code đánh cắp credential được phát triển tùy chỉnh và hoạt động ẩn mình. Malware này được phân phối theo hai giai đoạn, với giai đoạn đầu tiên ngụy trang thành một clipboard manager cho máy Mac có tên Maccy, được phân phối dưới dạng disk image. Khi mở, disk image sẽ thực thi code độc hại bên trong một AppleScript, sử

5 ChatGPT đã được chấp nhận rộng rãi như thế nào

How ChatGPT adoption has expanded

OpenAI Blog Đọc bài viết →

> Theo dữ liệu gần đây từ OpenAI Signals, việc áp dụng ChatGPT đang mở rộng trên toàn cầu. Nền tảng này đã chứng kiến sự tăng trưởng về mức độ tương tác của người dùng, với các cá nhân không chỉ sử dụng dịch vụ này thường xuyên hơn mà còn khám phá các khả năng khác nhau của nó. Sự tăng trưởng này được thúc đẩy trên các khu vực và ngôn ngữ khác nhau, cho thấy việc áp dụng công nghệ này một cách rộng rãi và phổ biến. Dữ liệu cung cấp thông tin về phạm vi mở rộng của ChatGPT, nhấn mạnh sự phổ biến và sử dụng ngày càng tăng của nó trên toàn thế giới.

6 Bản nhại 'Infowars' của The Onion đã ra mắt. Alex Jones chắc chắn sẽ ghét nó

The Onion’s ‘Infowars’ Parody Is Here. Alex Jones Is Going to Hate It

Wired Đọc bài viết →

> The Onion, một kênh tin tức châm biếm, đã ra mắt một phiên bản nhái của mạng lưới Infowars của nhà lý thuyết âm mưu Alex Jones. Chương trình phát trực tiếp hàng tuần, cũng được gọi là Infowars, được phát vào thứ Năm lúc 8 giờ tối theo giờ ET trên các nền tảng như Twitch, YouTube và Instagram. Chương trình này là một phiên bản hài hước về văn hóa internet và cánh hữu cực đoan, với trọng tâm là nhái lại phong

cách bình luận của Jones. Giám đốc sáng tạo của The Onion, Tim Heidecker, sẽ tiếp tục dẫn dắt dự án, nhằm mục đích chế giễu văn hóa internet âm mưu đã lan rộng trên các nền tảng truyền thông xã hội. Tập đầu tiên của chương trình nhái này có một phiên bản hài hước về cái chết của Jones, với nhân vật này phát nổ sau khi ăn quá nhiều Whataburger. The Onion đã mua lại quyền sử dụng tên Infowars trong một phiên đấu giá phá sản, nhưng thỏa thuận này đã bị một thẩm phán liên bang chặn lại tạm thời. Kênh này dự định sử dụng chương trình nhái này để quyên tiền cho các gia đình của các nạn nhân trong vụ nổ súng tại trường Sandy Hook, những người đã được trao hơn 1 tỷ đô la trong các bản án chống lại Jones. Giám đốc điều hành của The Onion, Ben Collins, cho biết chương trình nhái này là một cách để "phá vỡ sự ngớ ngẩn" của văn hóa internet âm mưu đã trở nên như thế nào.

7

GitHub đã dùng secret scanning để đạt "inbox zero" như thế nào

How GitHub used secret scanning to reach inbox zero

GitHub Blog Đọc bài viết →

GitHub, một nền tảng hàng đầu cho các developer, đã đạt được "hộp thư đến zero" cho các cảnh báo quét bí mật trong vòng chín tháng. Ban đầu, đội an ninh của công ty đã phát hiện hơn 20.000 cảnh báo quét bí mật trên 15.000 kho lưu trữ. Để giải quyết vấn đề này, GitHub Security đã khởi xướng một sáng kiến để cải thiện vệ sinh bí mật và thử nghiệm khả năng Secret Scanning. Sau đó, đội tập trung vào việc xác định các rủi ro thực sự, phân công quyền sở hữu và khắc phục an toàn các bí mật. Nỗ lực này đã dẫn đến việc đạt được zero cảnh báo mở. Kinh nghiệm của công ty này nhấn mạnh tầm quan trọng của việc quản lý bí mật hiệu quả và những thách thức mà nó mang lại. Cách tiếp cận của GitHub đối với việc quản lý bí mật đã phát triển theo thời gian, và thành công của công ty chứng minh lợi ích của việc triển khai các biện pháp bảo mật mạnh mẽ.

8

llm-coding-agent 0.1a0

llm-coding-agent 0.1a0

Simon Willison Đọc bài viết →

> Một thư viện Python mã nguồn mở mới, llm-coding-agent 0.1a0, đã được phát hành. Thư viện này là một thử nghiệm trong việc xây dựng một tác nhân mã hóa (coding agent) sử dụng một khung khổ mô hình ngôn ngữ lớn (LLM). Tác nhân này được thiết kế để hỗ trợ các nhiệm vụ mã hóa, bao gồm đọc và chỉnh sửa tệp, thực thi lệnh, và thực hiện một phong cách mã hóa tương tự như Claude Code. Thư viện cung cấp một tập hợp các công cụ, chẳng hạn như chỉnh sửa tệp, thực thi lệnh, liệt kê tệp, đọc tệp và tìm kiếm tệp, có thể được sử dụng để tự động hóa các nhiệm vụ mã hóa. Thư viện này được xây dựng sử dụng một kho lưu trữ mẫu và tuân theo phương pháp phát triển dựa trên thử nghiệm (TDD). Nó đã được gửi đến PyPI và có thể được cài đặt và sử dụng như bất kỳ thư viện Python nào khác. Tác giả đã chứng minh khả năng của thư viện bằng cách sử dụng nó để tạo một ứng dụng CLI SwiftUI đơn giản để hiển thị thời gian dưới dạng nghệ thuật ASCII. API của thư viện dựa trên lớp CodingAgent, cung cấp một giao diện Python để tương tác với tác nhân mã hóa.

TIPS & TRICKS CHO DEV

Chain-of-Thought Prompting

Vấn đề: Khi cần thực hiện các nhiệm vụ phức tạp, đòi hỏi nhiều bước suy nghĩ.
Cách làm: Sử dụng kỹ thuật chain-of-thought, ví dụ "Let's think step by step to solve this math problem...".
Đánh giá: Hiệu quả khi giải quyết vấn đề phức tạp, nhưng đòi hỏi thiết kế prompt tốt.

Few-Shot Learning

Vấn đề: Khi dữ liệu huấn luyện hạn chế cho mô hình AI.
Cách làm: Sử dụng few-shot learning, ví dụ "Write a story about a character who learns to play the guitar in 3 sentences.".
Đánh giá: Hiệu quả khi dữ liệu hạn chế, nhưng đòi hỏi chất lượng dữ liệu cao.

System Prompt Design

Vấn đề: Khi cần thiết kế hệ thống AI có tính tùy chỉnh cao.
Cách làm: Sử dụng system prompt design, ví dụ "Act as a personal assistant and respond to user queries."
Đánh giá: Hiệu quả khi xây dựng hệ thống AI tùy chỉnh, nhưng đòi hỏi thiết kế cẩn thận.

BÀI HỌC AI HÔM NAY CHO DEV

1. **Tích hợp AI API vào ứng dụng**

2. Tích hợp AI API vào ứng dụng giúp nâng cao khả năng tự động hóa và phân tích dữ liệu. Dev cần biết cách tích hợp AI API để tạo ra các ứng dụng thông minh hơn. Điều này cũng giúp giảm thiểu thời gian và công sức phát triển.

3. Ví dụ, sử dụng thư viện như TensorFlow hoặc PyTorch để tích hợp mô hình AI vào ứng dụng, cho phép thực hiện các nhiệm vụ như nhận diện hình ảnh hoặc phân tích ngôn ngữ tự nhiên.

4. Tip hoặc bước tiếp theo: Sử dụng các nền tảng như Google Cloud AI Platform hoặc AWS SageMaker để dễ dàng tích hợp AI API vào ứng dụng và giảm thiểu công việc backend.