AI 行业日报

模型与工具能力 · 产业基础设施 · 应用商业化 · 研究开源 · 资本监管 | Data Source: aihot.virxact.com

API耗时: 2s 精选条目: 9 条 焦点: 8 条 快讯: 0 条

Executive Summary

Anthropic的Claude Mythos Preview在安全研究领域取得突破性进展，协助团队在5天内攻破Apple M5芯片macOS内核的安全防护，成功构建首个公开的内存破坏提权利用链，绕过了苹果耗时5年、投入数十亿美元打造的MIE硬件级内存完整性防护。阿里云推出HappyHorse视频生成模型，支持从原始提示词生成1080p多镜头现实感画面，标志着电影级AI视频生成能力的商业化落地。腾讯云公测ArdotAI设计智能体平台，实现一句话生成可编辑设计稿并一键转代码的功能集成。

AI视频生成和设计自动化领域的商业化加速明显，HappyHorse和Ardot分别在视频内容创作和UI设计流程中降低了专业门槛，影响了创意产业的成本结构和产品形态。开源生态持续活跃，yao-weread-skill工具将微信读书数据转化为可视化分析报告，展现了AI在个人数据处理方面的应用拓展。API安全监测方面，api-relay-audit项目针对AI API中转站的安全风险提供透明审计能力，反映了行业对服务质量和安全性的关注提升。

后续需跟踪Claude Mythos Preview的安全研究能力是否会在其他系统漏洞挖掘中复现类似效果，HappyHorse和Ardot的API定价策略及其对传统创意工具市场的冲击程度，以及AI API中转站的安全标准和监管框架是否会因审计工具的普及而发生变化。同时，多模态模型在设计自动化领域的应用深度值得持续观察。

重点 今日核心进展

★ 1. Anthropic Claude 5天攻破Apple M5 macOS内核漏洞：5年数十亿防线，被AI一举击穿

X：Berry Xia (@berryxia) · 昨天 00:06 · 研究与开源进展

Anthropic的Claude Mythos Preview在5天内，协助安全团队Calif成功构建并演示了首个公开的、针对Apple M5芯片macOS内核的内存破坏提权利用链。该攻击绕过了苹果耗时5年、投入数十亿美元打造的MIE硬件级内存完整性防护，从普通用户权限通过纯数据操作即可获得root权限。苹果已在后续更新中修复漏洞并致谢。此事件标志着AI驱动的安全研究能力已能极速突破顶尖硬件防护，

能力进展 基础设施 监管/资本

https://x.com/berryxia/status/2056043674446995887

★ 2. 阿里云推出HappyHorse视频生成模型

X：阿里云 / Alibaba Cloud (@alibaba_cloud) · 23 小时前 · 应用与商业化

电影级AI现已到来。HappyHorse现已登陆Model Studio。从原始提示词到1080p多镜头现实感画面--在统一工作流中体验视频生成的未来。没有阻碍。只有纯粹性能。限时优惠：8折。观看演示并立即开始创作。 立即访问：https：//int.alibabacloud.com/m/1000412936/

能力进展 基础设施 新发布

https://x.com/alibaba_cloud/status/2056182152681644176

★ 3. 腾讯 AI 设计智能体 Ardot 公测：一句话生成可编辑设计稿，一键转代码

IT之家（RSS） · 21 小时前 · 应用与商业化

腾讯云正式公测自研AI设计智能体平台Ardot。该平台核心功能包括：用户通过一句话指令即可生成App页面、官网、海报等可编辑设计稿；支持调用团队自有组件库生成规范稿，并能直接导入Figma文件保留原有设计。同时，Ardot具备设计稿一键转换为代码的能力，可对接CodeBuddy等开发工具实现代码还原。平台还提供多人在线实时评论、标注反馈和版本对比等协作功能，其微信小程序即将上线。

能力进展 基础设施

https://www.ithome.com/0/951/677.htm

★ 4. 开源微信读书数据可视化工具yao-weread-skill发布

X：Vista (@vista8) · 昨天 00:33 · 观点、资本与监管

开发者姚老师开源了微信读书Skill--yao-weread-skill。该工具能将用户的微信读书数据生成本地可视化报告，核心功能包括分析近两年的阅读时长与节律、书架书籍构成、阅读分类与作者偏好，并对笔记和想法进行语义分析。报告最终通过词云、热力图、雷达图等26种图表形式呈现，所有代码已在GitHub公开。

能力进展 基础设施 新发布

https://x.com/vista8/status/2056050473392902430

★ 5. 开源工具揭露AI API中转站安全风险与检测差异

X：Berry Xia (@berryxia) · 23 小时前 · 观点、资本与监管

针对AI API中转站可能存在的"掺水"、"造假"等安全风险，开源项目api-relay-audit通过双论文锚定路线，对AC-1工具调用改写、AC-2错误响应泄漏、上下文截断等常见攻击进行可验证的三态判定，并提供透明日志。对比hvoy.ai和cctest.ai等工具，其透明度和可审计性更为可靠。项目作者已将完整方法论、对比结果和功能速查表公开，并开源了该检测工具。

能力进展 监管/资本 新发布

https://x.com/berryxia/status/2056173473588994392

★ 6. 一键生成韩国棒球AI视频模板爆火

X：PixVerse (@PixVerse_) · 21 小时前 · 应用与商业化

那个热狗需要自己的座位 【引用 @MrDasOnX】：这可能是最简单的病毒式AI编辑。 PixVerse → 上传自拍 → 即时生成韩国棒球镜头视频 无需指令。无需编辑。 只需一键点击。 @PixVerse_ 上的K-Baseball Sprint模板太疯狂了。

能力进展

https://x.com/PixVerse_/status/2056198882321904098

★ 7. Hermes 可配置的国内外 AI 模型及使用方法

X：Vista (@vista8) · 23 小时前 · 观点、资本与监管

Hermes 支持配置多种国内外主流 AI 模型，包括 OpenAI GPT-5.5、xAI Grok-4.3、谷歌 Gemini 系列、DeepSeek V4 系列、智谱 GLM-5 系列、Kimi K2.6 以及小米 Mimo V2.5-pro。用户需通过相应服务的订阅或 API 进行配置，完成后可使用 /model 指令指定模型及提供者来切换对话模型，例如输入"/model gpt-5.5

能力进展 新发布

https://x.com/vista8/status/2056170241147977741

★ 8. 让 Codex 自己做了一条视频介绍了一下这个视频生成方案

X：歸藏 (@op7418) · 昨天 22:36 · 观点、资本与监管

该方案整合了藏师傅的PPT Skill（视觉与动效）、HyperFrames（时间线与渲染）、Listenhub Skill（配音）以及即梦CLI（补充片段）。核心在于，用户可通过Codex直接基于文本提示生成带动效的解释视频，并能在聊天界面内预览，极大提升了制作效率，特别适合产品介绍等视频内容。

能力进展

https://x.com/op7418/status/2056021133477163298

产业 产业与基础设施

1. 人机快递分拣对决直播

X：小互 (@xiaohu) · 23 小时前

Figure 直播机器人 VS 人类 挑战 快递分拣任务 目前人类稍稍领先…😊

https://x.com/xiaohu/status/2056172740873511139

应用 应用与商业化

1. 阿里云推出HappyHorse视频生成模型

X：阿里云 / Alibaba Cloud (@alibaba_cloud) · 23 小时前

电影级AI现已到来。HappyHorse现已登陆Model Studio。从原始提示词到1080p多镜头现实感画面--在统一工作流中体验视频生成的未来。没有阻碍。只有纯粹性能。限时优惠：8折。观看演示并立即开始创作。 立即访问：https：//int.alibabacloud.com/m/1000412936/

能力进展 基础设施 新发布

https://x.com/alibaba_cloud/status/2056182152681644176

2. 腾讯 AI 设计智能体 Ardot 公测：一句话生成可编辑设计稿，一键转代码

IT之家（RSS） · 21 小时前

腾讯云正式公测自研AI设计智能体平台Ardot。该平台核心功能包括：用户通过一句话指令即可生成App页面、官网、海报等可编辑设计稿；支持调用团队自有组件库生成规范稿，并能直接导入Figma文件保留原有设计。同时，Ardot具备设计稿一键转换为代码的能力，可对接CodeBuddy等开发工具实现代码还原。平台还提供多人在线实时评论、标注反馈和版本对比等协作功能，其微信小程序即将上线。

能力进展 基础设施

https://www.ithome.com/0/951/677.htm

3. 一键生成韩国棒球AI视频模板爆火

X：PixVerse (@PixVerse_) · 21 小时前

那个热狗需要自己的座位 【引用 @MrDasOnX】：这可能是最简单的病毒式AI编辑。 PixVerse → 上传自拍 → 即时生成韩国棒球镜头视频 无需指令。无需编辑。 只需一键点击。 @PixVerse_ 上的K-Baseball Sprint模板太疯狂了。

能力进展

https://x.com/PixVerse_/status/2056198882321904098

研究 研究与开源进展

1. Anthropic Claude 5天攻破Apple M5 macOS内核漏洞：5年数十亿防线，被AI一举击穿

X：Berry Xia (@berryxia) · 昨天 00:06

Anthropic的Claude Mythos Preview在5天内，协助安全团队Calif成功构建并演示了首个公开的、针对Apple M5芯片macOS内核的内存破坏提权利用链。该攻击绕过了苹果耗时5年、投入数十亿美元打造的MIE硬件级内存完整性防护，从普通用户权限通过纯数据操作即可获得root权限。苹果已在后续更新中修复漏洞并致谢。此事件标志着AI驱动的安全研究能力已能极速突破顶尖硬件防护，

能力进展 基础设施 监管/资本

https://x.com/berryxia/status/2056043674446995887

格局 观点、资本与监管

1. 开源微信读书数据可视化工具yao-weread-skill发布

X：Vista (@vista8) · 昨天 00:33

开发者姚老师开源了微信读书Skill--yao-weread-skill。该工具能将用户的微信读书数据生成本地可视化报告，核心功能包括分析近两年的阅读时长与节律、书架书籍构成、阅读分类与作者偏好，并对笔记和想法进行语义分析。报告最终通过词云、热力图、雷达图等26种图表形式呈现，所有代码已在GitHub公开。

能力进展 基础设施 新发布

https://x.com/vista8/status/2056050473392902430

2. 开源工具揭露AI API中转站安全风险与检测差异

X：Berry Xia (@berryxia) · 23 小时前

针对AI API中转站可能存在的"掺水"、"造假"等安全风险，开源项目api-relay-audit通过双论文锚定路线，对AC-1工具调用改写、AC-2错误响应泄漏、上下文截断等常见攻击进行可验证的三态判定，并提供透明日志。对比hvoy.ai和cctest.ai等工具，其透明度和可审计性更为可靠。项目作者已将完整方法论、对比结果和功能速查表公开，并开源了该检测工具。

能力进展 监管/资本 新发布

https://x.com/berryxia/status/2056173473588994392

3. Hermes 可配置的国内外 AI 模型及使用方法

X：Vista (@vista8) · 23 小时前

Hermes 支持配置多种国内外主流 AI 模型，包括 OpenAI GPT-5.5、xAI Grok-4.3、谷歌 Gemini 系列、DeepSeek V4 系列、智谱 GLM-5 系列、Kimi K2.6 以及小米 Mimo V2.5-pro。用户需通过相应服务的订阅或 API 进行配置，完成后可使用 /model 指令指定模型及提供者来切换对话模型，例如输入"/model gpt-5.5

能力进展 新发布

https://x.com/vista8/status/2056170241147977741

4. 让 Codex 自己做了一条视频介绍了一下这个视频生成方案

X：歸藏 (@op7418) · 昨天 22:36

该方案整合了藏师傅的PPT Skill（视觉与动效）、HyperFrames（时间线与渲染）、Listenhub Skill（配音）以及即梦CLI（补充片段）。核心在于，用户可通过Codex直接基于文本提示生成带动效的解释视频，并能在聊天界面内预览，极大提升了制作效率，特别适合产品介绍等视频内容。

能力进展

https://x.com/op7418/status/2056021133477163298