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: 0s 精选条目: 11 条 焦点: 8 条 快讯: 0 条

Executive Summary

今日AI行业面临重大安全挑战，TrapDoor供应链攻击同时袭击npm、PyPI和Crates.io三大平台，34个恶意包通过注入CLAUDE.md和.cursorrules配置文件窃取开发者敏感信息，标志着AI助手成为新型攻击载体。StepAudio 2.5 Realtime发布，实现副语言感知能力，可深度理解语气、语速等特征并支持数百万种人格化组合。OpenClaw 2026.5.22版本将API响应时间降至5毫秒，显著提升服务效率。

Anthropic即将完成超300亿美元融资，估值有望突破9000亿美元超越OpenAI，预计Q2营收达109亿美元环比增长超一倍。DeepSeek对其旗舰模型实施永久性75%折扣，大幅降低使用成本。Replit Agent与Squidler集成实现全自动化AI质量保障闭环，Luma Agents已能规模化生成真实UGC风格广告内容，显示AI Agent在商业应用中的成熟度提升。

后续需关注供应链安全防护机制的演进、大型AI公司融资节奏与估值变化、模型API价格竞争态势、AI Agent商业化落地速度以及针对新兴攻击面的安全标准制定。

重点 今日核心进展

★ 1. TrapDoor供应链攻击：AI助手成新型攻击面

X：Kim (@kimmonismus) · 7 小时前 · 产业与基础设施

一场名为"TrapDoor"的协调供应链攻击同时袭击了npm、PyPI和Crates.io，涉及34个恶意包，旨在窃取加密货币、AI和安全开发者的钱包、SSH密钥和云凭证。攻击的新手段是向流行开源项目提交Pull Request，注入被操纵的`CLAUDE.md`和`.cursorrules`配置文件。当开发者克隆仓库并使用Claude Code或Cursor等AI助手时，AI智能体会将这些文件当

能力进展 基础设施 监管/资本

https://x.com/kimmonismus/status/2058584943052161488

★ 2. OpenClaw 2026.5.22发布：性能优化与安全加固

X：OpenClaw (@openclaw) · 20 小时前 · 应用与商业化

OpenClaw 2026.5.22 已上线 ⚡ Gateway/模型启动路径更精简 ☒models 响应时间降至约5毫秒 ☒npm包现提供锁定依赖项 ☒Windows安装/更新路径更安全 等待更少，意外更少。 https：//github.com/openclaw/openclaw/releases/tag/v2026.5.22

能力进展 监管/资本 新发布

https://x.com/openclaw/status/2058397616124072274

★ 3. StepAudio 2.5实时语音发布：副语言感知与人格化交互

X：阶跃星辰 StepFun (@StepFun_ai) · 昨天 05:45 · 应用与商业化

StepAudio 2.5 Realtime是一款实时语音模型，能够深度理解用户语音中的语气、语速、停顿乃至微表情等副语言特征。它支持通过API接入自定义人格，允许设定个性、背景故事和语言风格，并提供了上万种原生人格选项，可组合出数百万种特征。产品还内置了5个可直接体验的预设人格，并经过RLHF调优，确保在复杂的角色扮演压力测试中也能保持角色一致性。该模型支持中文和英文。

能力进展 新发布

https://x.com/StepFun_ai/status/2058303294544425197

★ 4. 格雷格·布罗克曼：那段差点让OpenAI覆灭的72小时

Hacker News 热门（buzzing.cc 中文翻译） · 10 小时前 · 观点、资本与监管

Hacker News 热门（buzzing.cc 中文翻译）披露：格雷格·布罗克曼：那段差点让OpenAI覆灭的72小时。该条属于观点、资本与监管方向，后续关注其对模型能力、产品形态或产业链节奏的影响。

能力进展 监管/资本 新发布

https://fs.blog/knowledge-project-podcast/greg-brockman

★ 5. 消息称 Anthropic 最快下周完成逾 300 亿美元融资，有望推动估值反超 OpenAI

IT之家（RSS） · 昨天 23:12 · 产业与基础设施

据彭博社报道，Anthropic即将完成一轮超300亿美元的融资，最快可能于下周敲定。此轮融资将使其估值突破9000亿美元，正式超越OpenAI，成为全球估值最高的AI初创企业。融资的迅速推进反映了市场的强烈追捧。同时，公司营收高速增长，预计第二季度营收将达109亿美元，环比增长超一倍，有望迎来首个盈利季度。

监管/资本 新发布

https://www.ithome.com/0/954/452.htm

★ 6. DeepSeek将对其旗舰AI模型实施永久性75%折扣

Hacker News 热门（buzzing.cc 中文翻译） · 6 小时前 · 产业与基础设施

Hacker News 热门（buzzing.cc 中文翻译）披露：DeepSeek将对其旗舰AI模型实施永久性75%折扣。该条属于产业与基础设施方向，后续关注其对模型能力、产品形态或产业链节奏的影响。

能力进展

https://www.bloomberg.com/news/articles/2026-05-23/deepseek-to-make-permanent-75-discount-on-flagship-ai-model

★ 7. Replit Agent与Squidler集成，实现全自动化AI质量保障

X：Replit (@Replit) · 昨天 03:00 · 应用与商业化

Replit Agent与Squidler已完成集成，形成一套完整的AI驱动质量保障闭环。用户可通过自然语言描述应用功能，由Replit Agent负责构建。构建完成后，Squidler会像真实用户一样对线上应用进行自动化测试，无需编写任何测试脚本。测试中发现的问题会自动反馈给Replit Agent进行修复。该流程已通过Squidler加入Replit的MCP库正式上线，实现了从构建、测试到修复

能力进展

https://x.com/Replit/status/2058261705998602548

★ 8. Luma Agents 实现规模化真实 UGC 广告生成

X：Luma AI (@LumaLabsAI) · 2 小时前 · 应用与商业化

规模化的真实性曾是矛盾，如今已成现实。 定义简报，设定风格，Luma Agents 从这里构建每一条 UGC 风格广告。 让它真实 → http：//lumalabs.ai/app

能力进展

https://x.com/LumaLabsAI/status/2058672731705503959

产业 产业与基础设施

1. TrapDoor供应链攻击：AI助手成新型攻击面

X：Kim (@kimmonismus) · 7 小时前

一场名为"TrapDoor"的协调供应链攻击同时袭击了npm、PyPI和Crates.io，涉及34个恶意包，旨在窃取加密货币、AI和安全开发者的钱包、SSH密钥和云凭证。攻击的新手段是向流行开源项目提交Pull Request，注入被操纵的`CLAUDE.md`和`.cursorrules`配置文件。当开发者克隆仓库并使用Claude Code或Cursor等AI助手时，AI智能体会将这些文件当

能力进展 基础设施 监管/资本

https://x.com/kimmonismus/status/2058584943052161488

2. 消息称 Anthropic 最快下周完成逾 300 亿美元融资，有望推动估值反超 OpenAI

IT之家（RSS） · 昨天 23:12

据彭博社报道，Anthropic即将完成一轮超300亿美元的融资，最快可能于下周敲定。此轮融资将使其估值突破9000亿美元，正式超越OpenAI，成为全球估值最高的AI初创企业。融资的迅速推进反映了市场的强烈追捧。同时，公司营收高速增长，预计第二季度营收将达109亿美元，环比增长超一倍，有望迎来首个盈利季度。

监管/资本 新发布

https://www.ithome.com/0/954/452.htm

3. DeepSeek将对其旗舰AI模型实施永久性75%折扣

Hacker News 热门（buzzing.cc 中文翻译） · 6 小时前

Hacker News 热门（buzzing.cc 中文翻译）披露：DeepSeek将对其旗舰AI模型实施永久性75%折扣。该条属于产业与基础设施方向，后续关注其对模型能力、产品形态或产业链节奏的影响。

能力进展

https://www.bloomberg.com/news/articles/2026-05-23/deepseek-to-make-permanent-75-discount-on-flagship-ai-model

应用 应用与商业化

1. OpenClaw 2026.5.22发布：性能优化与安全加固

X：OpenClaw (@openclaw) · 20 小时前

OpenClaw 2026.5.22 已上线 ⚡ Gateway/模型启动路径更精简 ☒/models 响应时间降至约5毫秒 ☒npm包现提供锁定依赖项 ☒Windows安装/更新路径更安全 等待更少，意外更少。 https：//github.com/openclaw/openclaw/releases/tag/v2026.5.22

能力进展 监管/资本 新发布

https://x.com/openclaw/status/2058397616124072274

2. StepAudio 2.5实时语音发布：副语言感知与人格化交互

X：阶跃星辰 StepFun (@StepFun_ai) · 昨天 05:45

StepAudio 2.5 Realtime是一款实时语音模型，能够深度理解用户语音中的语气、语速、停顿乃至微表情等副语言特征。它支持通过API接入自定义人格，允许设定个性、背景故事和语言风格，并提供了上万种原生人格选项，可组合出数百万种特征。产品还内置了5个可直接体验的预设人格，并经过RLHF调优，确保在复杂的角色扮演压力测试中也能保持角色一致性。该模型支持中文和英文。

能力进展 新发布

https://x.com/StepFun_ai/status/2058303294544425197

3. Replit Agent与Squidler集成，实现全自动化AI质量保障

X：Replit (@Replit) · 昨天 03:00

Replit Agent与Squidler已完成集成，形成一套完整的AI驱动质量保障闭环。用户可通过自然语言描述应用功能，由Replit Agent负责构建。构建完成后，Squidler会像真实用户一样对线上应用进行自动化测试，无需编写任何测试脚本。测试中发现的问题会自动反馈给Replit Agent进行修复。该流程已通过Squidler加入Replit的MCP库正式上线，实现了从构建、测试到修复

能力进展

https://x.com/Replit/status/2058261705998602548

4. Luma Agents 实现规模化真实 UGC 广告生成

X：Luma AI (@LumaLabsAI) · 2 小时前

规模化的真实性曾是矛盾，如今已成现实。 定义简报，设定风格，Luma Agents 从这里构建每一条 UGC 风格广告。 让它真实 → http：//lumalabs.ai/app

能力进展

https://x.com/LumaLabsAI/status/2058672731705503959

格局 观点、资本与监管

1. 格雷格・布罗克曼：那段差点让OpenAI覆灭的72小时

Hacker News 热门（buzzing.cc 中文翻译） · 10 小时前

Hacker News 热门（buzzing.cc 中文翻译）披露：格雷格・布罗克曼：那段差点让OpenAI覆灭的72小时。该条属于观点、资本与监管方向，后续关注其对模型能力、产品形态或产业链节奏的影响。

能力进展 监管/资本 新发布

https://fs.blog/knowledge-project-podcast/greg-brockman

2. 面向 Codex 的自我优化提示词框架

X：Greg Brockman (@gdb) · 7 小时前

这是一个结构化的提示词，用于指导 Codex 自动分析其历史记录以识别并固化重复工作流。该框架要求 Codex 回顾会话、Memories 等数据，找出重复、耗时且有明确复用价值的任务。筛选标准包括至少出现两次、输入稳定、可提升效率等。最终，Codex 应以"技能"、子智能体或自动化工具等最小实用形式创建或扩展现有资产，避免冗余。流程包括生成候选清单、执行创建，并汇报结果与待验证项。

能力进展

https://x.com/gdb/status/2058598608224858442

3. Pixverse角色设计工作流测试

X：PixVerse (@PixVerse_) · 9 小时前

在Pixverse中进行角色设计工作流测试 使用GPT Image 2.0为Lucas创建视觉形象，使用Seedance 2.0制作动画弹跳表演。 从静态概念图到电影级动态效果。 RT + Follow + Reply = 工作流

能力进展

https://x.com/PixVerse_/status/2058564994669727803

4. Claude Code自动模式：多任务并行的关键技巧

X：Boris Cherny (@bcherny) · 12 小时前

人们常问我，用好Claude Code的最大技巧是什么。 如今我的头号技巧是：使用自动模式。 自动模式意味着不再有权限提示。它是实现"多Claude并行"的关键构件：启动一个会话，然后在其运行时，并行处理另一个会话。

能力进展

https://x.com/bcherny/status/2058519809214607704