AI 行业日报

模型 · 产品 · 产业 · 研究 · 观点 | Data Source: aihot.virxact.com

API耗时: 1s 精选条目: 41 条 焦点: 8 条 快讯: 0 条

Executive Summary

今日重点

HappyHorse在阿里云Model Studio上线，这是基准测试排名第一的AI视频生成模型，主打闪电速度和原生音视频同步，号称能终结排队等待AI视频的时代。Peekaboo 3.0正式发布，专注macOS电脑的操作与界面检测，统一了截图和界面检测功能，为AI代理操作提供了更强的底层支持。Google Fitbit Air开放全新Health API，提供31种健康数据点，支持Webhooks实时推送，为健康应用开发提供了更丰富的数据接口。

技术动向

OncoAgent开源肿瘤临床决策支持系统采用双层多智能体框架，结合LangGraph拓扑与四阶段Corrective RAG流程，能检索超过70份权威临床指南。系统根据查询复杂度路由至不同参数规模模型，9B模型优化速度，27B模型深度推理。Redis创始人开源ds4推理引擎，仅用几千行C代码实现DeepSeek V4 Flash的高效推理，通过MoE专家不对称2-bit量化、KV Cache移至SSD、Apple Silicon Metal优化三项技术突破内存限制。

近期关注

Qwen3.5和Qwen3.6系列全尺寸模型已在SiliconFlow平台上线，覆盖9B到397B参数范围，包括MoE与Dense架构。Hermes Agent已登顶OpenRouter全球令牌使用排名第一，显示其在实际应用中的强劲势头。工信部启动的人工智能科技伦理审查先导计划将在国家人工智能产业创新应用先导区展开具体实践。

今日焦点

★ 1. HappyHorse上线阿里云，AI视频无需等待

X：阿里云 / Alibaba Cloud (@alibaba_cloud) · 7 小时前 · 模型发布/更新

基准测试排名第一。闪电速度。原生音视频同步。 排队等待AI视频的时代结束了。HappyHorse现已在阿里云Model Studio上线。当别人还在渲染时，你已完成。 立即构建：https：//int.alibabacloud.com/m/1000412167/

https://x.com/alibaba_cloud/status/2053153199561863454

★ 2. ERNIE 5.1发布，预训练成本仅需对标模型6%

X：百度 Baidu (@Baidu_Inc) · 16 小时前 · 模型发布/更新

ERNIE 5.1 刚刚发布。 基于 ERNIE 5.0 的预训练基础，我们最新的基础模型升级了搜索、推理、知识问答、创意写作和智能体能力，而预训练成本仅需对标模型的约 6%。 更多内容详见主题帖

https://x.com/Baidu_Inc/status/2053009538769735774

★ 3. Google 开放 Fitbit Air 的全新 Health API

X：Berry Xia (@berryxia) · 31 分钟前 · 产品发布/更新

Google 随新款 Fitbit Air 发布了全新的 Health API 并向开发者开放。该 API 提供了涵盖运动、睡眠、心率、血氧等维度的 31 种健康数据点，支持 Webhooks 实时数据推送、精细的读写权限控制以及按时间范围查询和汇总数据。开发者可利用该 API 基于个人真实健康数据构建 AI Agent、MCP Server、CLI 或实时监控系统等应用，从而创建实用的个人健康自

https://x.com/berryxia/status/2053256690498433146

★ 4. 帕累托代码：免费实验性编码路由工具

X：OpenRouter (@OpenRouter) · 6 小时前 · 产品发布/更新

推出帕累托代码：一款全新、免费、实验性的编码路由工具 在请求中设置 `min_coding_score`，即可路由至符合您标准且成本最低的编码模型，排名由 @ArtificialAnlys 提供。 实时查看帕累托前沿的变化

https://x.com/OpenRouter/status/2053170520087024109

★ 5. Hy3预览版免费期结束 三项指标居首

X：腾讯混元 (@TencentHunyuan) · 12 小时前 · 产业与资本

@OpenRouter 的免费期已结束。 这两周期间，Hy3预览版达成： 总令牌使用量排名第一 代码生成排名第一 工具调用排名第一 在所有供应商中占据15.4%市场份额 Hy3预览版仍可在OpenRouter以有竞争力的价格使用。继续创造--并请持续反馈。 https：//openrouter.ai/tencent/hy3-preview

https://x.com/TencentHunyuan/status/2053073752431403482

★ 6. 工信部启动人工智能科技伦理审查与服务先导计划，加快推动审查工作落地实施

IT之家（RSS） · 15 小时前 · 产业与资本

工业和信息化部近日启动人工智能科技伦理审查与服务先导计划，旨在依托国家人工智能产业创新应用先导区，探索审查服务的落地路径与协同治理机制。该计划部署了四项重点任务：细化省级伦理审查制度、指导创新主体建设伦理委员会、开展审查实践与标准研制、构建部省市三级联动治理网络。同时，将设立全国伦理风险监测服务网络，编制培训教材并开设"伦理课堂"，以提供智力支持，推动人工智能负责任创新和产业高质量发展。

https://www.ithome.com/0/948/246.htm

★ 7. OncoAgent：一个用于隐私保护肿瘤临床决策支持的双层多智能体框架

Hugging Face：Blog（RSS） · 5 小时前 · 论文与研究

研究团队发布了开源肿瘤临床决策支持系统OncoAgent。该系统采用双层多智能体框架，结合LangGraph拓扑与四阶段Corrective RAG流程，检索超过70份权威临床指南。系统根据查询复杂度，将任务路由至9B参数的速度优化模型或27B参数的深度推理模型，两者均通过QLoRA在AMD MI300X硬件上使用包含26万余病例的数据集进行微调。系统强制执行严格的零受保护健康信息政策，并通过三层

https://huggingface.co/blog/lablab-ai-amd-developer-hackathon/oncoagent-official-paper

★ 8. 菲尔兹奖得主称 ChatGPT 5.5 Pro 在无人帮助下两小时内完成"博士级"数学研究

The Decoder：AI News（RSS） · 9 小时前 · 论文与研究

菲尔兹奖得主蒂莫西·高尔斯让 ChatGPT 5.5 Pro 尝试解决数论中的开放性问题。该模型在不到一小时内，将一个问题中的指数界限改进为多项式界限。一位参与的 MIT 研究员认为其核心想法"完全具有原创性"。高尔斯总结指出，未来数学贡献的门槛将变为证明某些是大语言模型无法完成的工作。

https://the-decoder.com/fields-medalist-says-chatgpt-5-5-pro-delivered-phd-level-math-research-in-under-two-hours-with-zero-human-help

模型 模型发布/更新

1. HappyHorse上线阿里云，AI视频无需等待

X：阿里云 / Alibaba Cloud (@alibaba_cloud) · 7 小时前

基准测试排名第一。闪电速度。原生音视频同步。 排队等待AI视频的时代结束了。HappyHorse现已在阿里云Model Studio上线。当别人还在渲染时，你已完成。 立即构建：https：//int.alibabacloud.com/m/1000412167/

https://x.com/alibaba_cloud/status/2053153199561863454

2. ERNIE 5.1发布，预训练成本仅需对标模型6%

X：百度 Baidu (@Baidu_Inc) · 16 小时前

ERNIE 5.1 刚刚发布。 基于 ERNIE 5.0 的预训练基础，我们最新的基础模型升级了搜索、推理、知识问答、创意写作和智能体能力，而预训练成本仅需对标模型的约 6%。 更多内容详见主题帖 ☒

https://x.com/Baidu_Inc/status/2053009538769735774

3. StepAudio 2.5 TTS 在语音竞技场盲测中跻身全球前三

X：阶跃星辰 StepFun (@StepFun_ai) · 19 小时前

StepFun 推出的 StepAudio 2.5 TTS 在 Artificial Analysis 语音竞技场盲测排行榜中位列全球第三，Elo 评分为 1187 分，仅次于 Inworld TTS 1.5 Max 与 Google Gemini 3.1 Flash TTS。该模型语音自然度较前代显著提升，并以 8 分优势超越 Eleven v3。其定价为每百万字符 85 美元，生成速度为每秒

https://x.com/StepFun_ai/status/2052963182587584878

4. Ring-2.6-1T发布：万亿参数思维模型专为复杂任务设计

X：蚂蚁百灵 (@antLingAGI) · 昨天 01:52

Ring-2.6-1T是一款万亿参数的旗舰思维模型，专为现实世界复杂任务和生产环境构建。该模型具备可调节思维努力功能，通过动态计算机制灵活平衡认知深度、token成本和执行速度。它针对代理优化，适用于高频工作流，提供快速多步执行和工具编排，并具有SOTA稳定性。深度思维特性解锁了模型的最大能力上限，特别适合严格数学逻辑和科学研究。

https://x.com/AntLingAGI/status/2052808934390661134

5. EMO：为涌现模块化预训练的专家混合模型

Hugging Face：Blog（RSS） · 昨天 00:03

EMO是一种新型专家混合模型，通过端到端预训练使模块化结构直接从数据中涌现，无需依赖人类定义的先验。该模型允许在特定任务中仅使用12.5%的专家子集（即8个活跃专家中的部分），同时保持接近全模型的性能；当所有128个专家共同使用时，它仍作为强大的通用模型。EMO具有1B活跃参数和14B总参数，训练数据达1万亿令牌。与标准MoE相比，EMO通过文档级路由约束，鼓励专家形成领域专业化组，从而支持选择性

https://huggingface.co/blog/allenai/emo

产品 产品发布/更新

1. Google 开放 Fitbit Air 的全新 Health API

X：Berry Xia (@berryxia) · 31 分钟前

Google 随新款 Fitbit Air 发布了全新的 Health API 并向开发者开放。该 API 提供了涵盖运动、睡眠、心率、血氧等维度的 31 种健康数据点，支持 Webhooks 实时数据推送、精细的读写权限控制以及按时间范围查询和汇总数据。开发者可利用该 API 基于个人真实健康数据构建 AI Agent、MCP Server、CLI 或实时监控系统等应用，从而创建实用的个人健康自

https://x.com/berryxia/status/2053256690498433146

2. 帕累托代码：免费实验性编码路由工具

X：OpenRouter (@OpenRouter) · 6 小时前

推出帕累托代码：一款全新、免费、实验性的编码路由工具 在请求中设置 `min_coding_score`，即可路由至符合您标准且成本最低的编码模型，排名由 @ArtificialAnlys 提供。 实时查看帕累托前沿的变化

https://x.com/OpenRouter/status/2053170520087024109

3. Peekaboo 3.0 正式发布 专注操作与界面检测

X：Peter Steinberger (@steipete) · 9 小时前

Peekaboo 3.0 现已上线。这是自 2.0 以来最重要的版本。 ⚡ 以操作为先的 macOS 电脑使用体验 统一的截图 + 界面检测功能 CLI + MCP 间更简洁的 JSON 交互 更好的快照功能 我去年就开始了这项工作，但当时的模型还不够好。现在它们已经准备好了。https：//peekaboo.sh

https://x.com/steipete/status/2053114837698249190

4. Qwen系列多尺寸模型登陆SiliconFlow平台

X：硅基流动 SiliconFlow (@SiliconFlowAI) · 15 小时前

思小建大@Alibaba_Qwen 3.5 和 Qwen3.6 系列现已在 SiliconFlow 上线 9B 到 397B • MoE 与 Dense • 原生多模态 Qwen3.6-35B-A3B • Qwen3.6-27B Qwen3.5-397B-A17B • Qwen3.5-122B-A10B Qwen3.5-35B-A3B • Qwen3.5-27B • Qwen3

https://x.com/SiliconFlowAI/status/2053035285974487369

5. Grok 升级推出全平台连接器功能

X：Elon Musk (@elonmusk, xAI) · 昨天 05:01

Grok 升级 【引用 @grok】：… 今天就在 iOS、Android 和 http：//grok.com 上的所有计划中添加您的连接器到 Grok。

https://x.com/elonmusk/status/2052856431611941200

6. OpenRouter SDK新增人工审核工具

X：OpenRouter (@OpenRouter) · 昨天 05:00

OpenRouter Agent SDK 新增功能：人工介入工具。 自动处理常规工具调用。暂停高风险调用以供审核。 返回值可保持代理运行。返回 null 则将该调用提交至您的应用以获取人工输入。

https://x.com/OpenRouter/status/2052856129961758917

7. 仅凭人声能否创作流行歌曲?

X：Suno (@suno) · 昨天 04:31

你能只用你的声音创作一首流行歌曲吗?

https://x.com/suno/status/2052848941260058808

8. Gemini笔记本助您高效组织复杂任务

X：Gemini (@GeminiApp) · 昨天 01:38

Gemini中的笔记本功能为复杂任务带来条理性。 以研究生院申请流程为例：通过笔记本，您可以将成绩单、文书草稿和录取要求集中在一处，让Gemini帮助追踪截止日期、提供反馈并评估您的进展。

https://x.com/GeminiApp/status/2052805372050604187

9. Codex切换功能正式上线

X：OpenAI (@OpenAI) · 昨天 01:19

就把这个留在这里。 https：//chatgpt.com/codex/switch-to-codex/

https://x.com/OpenAI/status/2052800507727781979

产业 产业与资本

1. Hy3预览版免费期结束 三项指标居首

X：腾讯混元 (@TencentHunyuan) · 12 小时前

@OpenRouter 的免费期已结束。 这两周期间，Hy3预览版达成： 总令牌使用量排名第一 代码生成排名第一 工具调用排名第一 在所有供应商中占据15.4%市场份额 Hy3预览版仍可在OpenRouter以有竞争力的价格使用。继续创造--并请持续反馈。 https：//openrouter.ai/tencent/hy3-preview

https://x.com/TencentHunyuan/status/2053073752431403482

2. 工信部启动人工智能科技伦理审查与服务先导计划，加快推动审查工作落地实施

IT之家（RSS） · 15 小时前

工业和信息化部近日启动人工智能科技伦理审查与服务先导计划，旨在依托国家人工智能产业创新应用先导区，探索审查服务的落地路径与协同治理机制。该计划部署了四项重点任务：细化省级伦理审查制度、指导创新主体建设伦理委员会、开展审查实践与标准研制、构建部省市三级联动治理网络。同时，将设立全国伦理风险监测服务网络，编制培训教材并开设"伦理课堂"，以提供智力支持，推动人工智能负责任创新和产业高质量发展。

https://www.ithome.com/0/948/246.htm

3. Hermes Agent登顶OpenRouter全球令牌排名

X：OpenRouter (@OpenRouter) · 19 小时前

祝贺@NousResearch！ 【引用 @NousResearch】：Hermes Agent 现已在全球 @OpenRouter 令牌排名中位列第一。 虽然我们的旅程才刚刚开始，但我们想借此机会感谢我们的贡献者、支持者和用户，感谢他们为我们走到今天所做的一切。

https://x.com/OpenRouter/status/2052966744952897750

4. Claude Mythos评估显示16小时风险时距

X：Ethan Mollick (@emollick) · 22 小时前

嗯。 【引用 @METR_Evals】：我们于2026年3月的有限窗口内评估了Claude Mythos Preview的早期版本进行风险评估。在我们的任务套件上，我们估计其50%时间范围至少为16小时（95%置信区间8.5小时至55小时），这处于我们无需新任务即可测量的上限。

https://x.com/emollick/status/2052924556264796163

5. DeepSeek融资70亿美元创纪录，创始人个人出资30亿

X：Rohan Paul (@rohanpaul_ai) · 昨天 08:02

DeepSeek正以500亿美元估值进行高达70亿美元的融资，创下中国AI领域最大单轮融资纪录。创始人梁文锋个人出资30亿美元，占本轮融资的40%，同时仍保留公司90%的所有权。该公司最初诞生于其本人成功的对冲基金内部。本轮融资将主要用于获取大规模计算资源，以加速发布V4.1等新模型，并投资企业级产品，目标是推动公司实现营收转正，其发展路径与OpenAI和Anthropic类似。

https://x.com/rohanpaul_ai/status/2052901878728659037

论文 论文与研究

1. OncoAgent：一个用于隐私保护肿瘤临床决策支持的双层多智能体框架

Hugging Face：Blog（RSS） · 5 小时前

研究团队发布了开源肿瘤临床决策支持系统OncoAgent。该系统采用双层多智能体框架，结合LangGraph拓扑与四阶段Corrective RAG流程，检索超过70份权威临床指南。系统根据查询复杂度，将任务路由至9B参数的速度优化模型或27B参数的深度推理模型，两者均通过QLoRA在AMD MI300X硬件上使用包含26万余病例的数据集进行微调。系统强制执行严格的零受保护健康信息政策，并通过三层

https://huggingface.co/blog/lablab-ai-amd-developer-hackathon/oncoagent-official-paper

2. 菲尔兹奖得主称 ChatGPT 5.5 Pro 在无人帮助下两小时内完成"博士级"数学研究

The Decoder：AI News（RSS） · 9 小时前

菲尔兹奖得主蒂莫西·高尔斯让 ChatGPT 5.5 Pro 尝试解决数论中的开放性问题。该模型在不到一小时内，将一个问题中的指数界限改进为多项式界限。一位参与的 MIT 研究员认为其核心想法"完全具有原创性"。高尔斯总结指出，未来数学贡献的门槛将变为证明某些是大语言模型无法完成的工作。

https://the-decoder.com/fields-medalist-says-chatgpt-5-5-pro-delivered-phd-level-math-research-in-under-two-hours-with-zero-human-help

3. 教克劳德"为什么"

Hacker News 热门（buzzing.cc 中文翻译） · 21 小时前

Anthropic公司发布了Claude模型的新研究"Teaching Claude Why"。该研究通过让模型学习解释自身推理过程中的"为什么"，显著提升了其推理能力和输出结果的准确性。实验表明，经过此项训练后，模型在多项基准测试中的表现得到改善，其推理步骤的透明度和逻辑连贯性增强。这项技术旨在推动AI向更可解释、更可靠的方向发展。

https://www.anthropic.com/research/teaching-claude-why

4. OpenAI分析意外思维链评分对模型影响

X：OpenAI (@OpenAI) · 昨天 04:19

思维链监控器是防御AI智能体错位的关键层。为保持可监控性，我们在RL期间避免惩罚错位推理。 我们发现少量意外思维链评分影响了已发布模型，现分享相关分析。 https：//alignment.openai.com/accidental-cot-grading/

https://x.com/OpenAI/status/2052845764507062349

观点 技巧与观点

1. AI放大能动性差异，用户两极分化加剧

X：Francois Chollet (@fchollet) · 6 小时前

主观能动性向来具有自我增强的特性，而AI正在放大这种效应。 低能动性的AI使用者进一步丧失能动性，高能动性的AI使用者则进一步增强能动性。

https://x.com/fchollet/status/2053169711341551936

2. GPT-Realtime-2语音控制CRM集成方案

X：OpenAI Developers (@OpenAIDevs) · 6 小时前

以下介绍如何集成GPT-Realtime-2为CRM工作流添加语音控制功能。

https://x.com/OpenAIDevs/status/2053161503470366881

3. Tesla利用视觉AI提前预判碰撞，大幅降低伤亡风险

X：Elon Musk (@elonmusk, xAI) · 8 小时前

Tesla通过分析真实车队碰撞数据，结合视觉系统与传感器，实现了安全系统的突破。传统碰撞传感器需要时间确认，降低阈值可能导致误触发。而视觉系统能提前"看到"即将发生的碰撞，与传感器协同，使约束控制器能更早、更准确地启动安全气囊和安全带预紧器。通过仿真重放碰撞并测量人体模型受力，团队发现提前部署能优化保护时机。这一改进使预测伤害严重程度整体显著下移，并通过OTA更新实现，是前所未有的安全提升。

https://x.com/elonmusk/status/2053141290989318335

4. 手机扫描与AI Agent技术颠覆房地产与专业领域

X：阿易 AI Notes (@AYi_AInotes) · 8 小时前

一项名为"3D高斯泼溅"的技术，允许用户仅用手机扫描整栋房屋，即可生成可在浏览器中直接浏览的沉浸式3D模型。其成本极低、文件小巧，为房产等行业带来新机会。同时，AI在垂直专业领域正通过Agent范式取得突破。例如Tianfu Agent在专业命理大赛中接近人类顶尖水平，其通过构建专用工具集而非依赖通用模型硬记规则的方法，为法律、中医等规则密集型领域的AI化提供了可迁移的新路径。

https://x.com/AYi_AInotes/status/2053139580572856328

5. YC CEO开源个人AI操作系统GBrain，构建知识复利"第二大脑"

X：Berry Xia (@berryxia) · 8 小时前

Y Combinator CEO Garry Tan开源其个人AI操作系统GBrain，旨在将AI打造成具备复利效应的"第二大脑"。该系统通过"Book Mirror"、"Meeting Prep"等模块化技能，在五个月内深度处理了20多本书、自动预习会议，并管理着超10万页持续增长的结构化知识。其架构清晰，分为轻量路由层、可组合技能层与丰富数据层，并能按任务智能调用不同AI模型。Garry Ta

https://x.com/berryxia/status/2053136924244836455

6. Redis创始人用C语言引擎将大模型"装进"个人电脑

X：阿易 AI Notes (@AYi_AInotes) · 9 小时前

Redis创始人Antirez开源了专为DeepSeek V4 Flash设计的原生推理引擎ds4。该引擎仅用几千行C代码，通过三项关键技术：对MoE专家进行不对称2-bit量化、将KV Cache移至高速SSD突破内存限制、为Apple Silicon进行纯Metal原生优化，成功在128GB MacBook Pro上流畅运行具备1M上下文窗口的模型，实测达27 tok/s。此举将原本依赖云端G

https://x.com/AYi_AInotes/status/2053121974734291359

7. 用Codex并行调试验证修复

X：Peter Steinberger (@steipete) · 15 小时前

每当调查bug时，我让codex在临时crabbox中重建精确状态，验证bug，修复它，再验证修复。 没有混乱状态因为本地系统可能被污染，也没有速度下降因为我并行运行10个会话。http：//crabbox.sh

https://x.com/steipete/status/2053032450138276274

8. Show HN： 适用于人工智能代理的 Git

Hacker News 热门（buzzing.cc 中文翻译） · 16 小时前

开源项目"适用于人工智能代理的 Git"发布，旨在为AI代理提供类似Git的版本控制系统。该系统允许AI代理跟踪和管理其代码、提示词、模型权重等资产的变更历史，支持分支、合并与回滚操作。项目已在GitHub开源，并在Hacker News上获得100点热度。这一工具试图解决AI开发中工作流复杂、迭代难以追溯的问题，为多代理协作与实验管理提供标准化方案。

https://github.com/regent-vcs/re_gent

9. 养龙虾最蠢的事，就是每次都重复说同一句话

X：阿易 AI Notes (@AYi_AInotes) · 18 小时前

YC创始人Garry Tan公开了OpenClaw提示词，旨在将AI代理从一次性工具转化为永久自动系统。其核心规则包括禁止一次性工作、遵循MECE原则、以重复询问作为失败判定，并采用标准六步流程，促使AI自我学习并积累技能库，实现复利增长。用户实践表明，系统能自动处理日报、邮件等重复任务。此外，有观点指出，在AI时代，HTML正取代Markdown成为更高效的沟通语言，因其能生成交互式彩色表格、流

https://x.com/AYi_AInotes/status/2052983074514723067

10. Codex Chrome插件安装与使用经验分享

X：Vista (@vista8) · 20 小时前

用户成功使用Codex Chrome插件完成购物任务，验证了其可用性。安装过程存在关键注意事项：必须将Codex更新至最新版本，并切换为官方订阅登录模式，第三方API模式不支持安装。插件对网络节点有要求，例如香港地区不支持。安装后，必须在Codex对话中通过"@ Chrome"指令来调用插件功能。此外，将Chrome设置为默认浏览器有助于安装流程顺利进行，遇到连接问题时重启电脑可能有效。

https://x.com/vista8/status/2052953667817578581

11. GPT Image 2 Prompt：水墨风格 Slides/PPT

X：宝玉 (@dotey) · 20 小时前

本文介绍一个用于生成水墨风格幻灯片画图提示词的模板。该模板结构清晰，包含标题、关键要点、视觉元素、布局偏好、文字层级和延续性说明，旨在指导AI（如Codex）生成具有统一美学风格的幻灯片图像。视觉元素强调宣纸背景、水墨山水等东方元素，整体风格追求静谧、克制、佗寂或当代东亚奢华。通过应用此模板，用户可以简化AI驱动的设计流程，快速获得视觉一致且富有美感的水墨风格PPT素材。文末提供了一个简短的应用示

https://x.com/dotey/status/2052948362668732781

12. GPT Image 2 Prompt：中文科技新闻爆款封面生成器

X：宝玉 (@dotey) · 21 小时前

这是一个用于生成中文科技新闻爆款封面图的详细提示词框架。它要求AI扮演顶级视觉设计师，根据输入的文章内容自动提取核心新闻、关键数字、产品及行业情绪等信息。设计需融合中国科技媒体头图、B站爆款缩略图等风格，强调强烈的视觉冲击与高信息密度，确保3秒内传递重点。构图包含顶部新闻区、中央超大标题区、主视觉产品区、数据卡片区和底部总结区，配色、字体、背景均需根据文章行业、品牌和情绪动态调整，最终输出专业的1

https://x.com/dotey/status/2052942818570543550

13. Claude Code实践：HTML输出格式的卓越效果

Simon Willison 博客 · 昨天 05:00

Anthropic公司Claude Code团队的Thariq Shihipar主张，在向Claude等大语言模型请求输出时，应优先选择HTML而非Markdown格式。HTML允许模型直接生成包含SVG图表、交互式组件和页面内导航等丰富元素的文档，显著提升信息呈现的交互性与清晰度。作者以GPT-5.5生成一个Linux安全漏洞的交互式HTML解释页面为例，展示了该方法的实际效果。这促使长期习惯使

https://simonwillison.net/2026/May/8/unreasonable-effectiveness-of-html

---

14. CyberSecQwen-4B：为何网络防御需要小型、专业化、本地可运行的模型

Hugging Face：Blog（RSS） · 昨天 01:41

Lablab.ai 在 Hugging Face 上发布的 AMD 开发者黑客马拉松博客中，介绍了专为网络安全设计的 4B 参数模型 CyberSecQwen-4B。该模型强调小型化、专业化与本地可运行特性，旨在降低部署门槛并提升实时防御效率。其紧凑结构适用于资源受限环境，同时针对安全任务进行优化，以应对动态威胁场景。这一方向反映了当前防御型 AI 向轻量化、领域专用化的发展趋势。

https://huggingface.co/blog/lablab-ai-amd-developer-hackathon/cybersecqwen-4b

---

15. 发布智能体技能构建内部手册

X：Perplexity (@perplexity_ai) · 昨天 00:25

我们已发布构建智能体技能的内部手册。 开发者需要以全新思维方式构建技能。 https：//research.perplexity.ai/articles/designing-refining-and-maintaining-agent-skills-at-perplexity

https://x.com/perplexity_ai/status/2052786858774630665

---

16. 抖音"法天象地"特效：从图片生成到视频优化的突破

X：歸藏 (@op7418) · 昨天 22:57

抖音近期流行的"法天象地"户外照片特效多基于图片生成，但实际测试表明直接生成视频效果更佳。作者通过优化提示词实现了这一改进，关键采用了 GPT-Image-2.0 与 C-Down 3.0 技术组合，并将优化后的图片提示词附在视频内容后供参考。这一方法提升了特效的动态表现力与视觉冲击力。

https://x.com/op7418/status/2052764933696475279

---

17. 机器人终局：物理AGI路线图与LLM类比

X：Jim Fan (@DrJimFan) · 昨天 22:32

演讲者以"Robotics： Endgame"为题，提出解决物理AGI的路线图，直接类比LLM的成功路径。核心观点包括视频世界模型作为第二预训练范式、世界行动模型（WAM）、机器人数据收集策略（类似FSD的物理数据飞轮）、EgoScale和灵巧性缩放定律、物理强化学习 bridging the last mile，以及DreamDojo端到端神经物理引擎。预测物理AGI的实现比预期更近，并提及20

https://x.com/DrJimFan/status/2052758642781487237

---

18. 在OpenAI安全运行Codex

OpenAI：官网动态（RSS · 排除企业/客户案例） · 昨天 20:30

OpenAI通过沙盒隔离、人工审批流程、严格网络策略与原生代理遥测四层防护机制，确保Codex代码生成模型的安全运行。沙盒环境完全隔离执行代码，所有生产请求需经人工审核批准，网络策略限制外部依赖访问，实时遥测系统监控代理行为异常。该安全框架使企业能够合规采用AI编程助手，在保障代码安全性的同时维持开发效率。

https://openai.com/index/running-codex-safely
