



AI agent攻破Hugging Face、Kimi K3冲顶开源、DeepSeek V4正式上线

头部企业动态

- Hugging Face于7月16日官方披露遭全程由自主AI agent执行的入侵,攻击者经数据集管道两个漏洞进入,执行1.7万余次操作;官方用开源GLM 5.2本地完成取证,确认公开模型与供应链未被篡改。 A • 97% 已核实
- OpenAI于7月9日向公众全量开放GPT-5.6系列(Sol/Terra/Luna三档)并推出面向完整工作交付的ChatGPT Work,7月8日另发布全双工语音模型GPT-Live。 B+ • 75% 多源一致 • 链接探活失败
- DeepMind CEO Hassabis于7月14日呼吁美国牵头设立FINRA式独立标准机构,在年底前对前沿模型发布进行测试把关,必要时协调全行业放缓,7月16日赴华盛顿游说。 B+ • 90% 多源一致
- Meta于7月7日发布Meta Superintelligence Labs首个图像生成模型Muse Image,已上线Meta AI,将陆续接入Facebook/Instagram/WhatsApp;此前7月1日宣布Meta Compute云业务出售富余算力。 A • 96% 已核实

模型发布

- 月之暗面7月16日发布旗舰模型Kimi K3:2.8万亿参数稀疏MoE(896选16)、1M上下文、原生视觉理解、常开思考模式,官方文档称7月27日前开源权重,将成全球最大开源模型。 A • 96% 已核实
- 谷歌7月21日发布Gemini 3.6 Flash(新主力,较3.5 Flash便宜约17%)、3.5 Flash-Lite及面向政府试点的安全专用模型3.5 Flash Cyber;旗舰3.5 Pro继续缺席,并官宣启动Gemini 4预训练。 B+ • 91% 多源一致
- DeepSeek V4正式版据港媒报道于7月20日全量上线,主打代码与推理及极低价格;官方6月29日已公告7月中旬发布并首次引入峰谷定价(高峰时段API价格翻倍)。 B • 78% 待复核
- 字节跳动Seed团队7月8日发布多模态图像创作模型Seedream 5.0 Pro,强化复杂信息可视化、交互式精准编辑与多语种生成,已上线火山方舟,将接入豆包、即梦。 B- • 82% 同源引述

热点与趋势

- 2026世界人工智能大会(WAIC)7月17-20日在上海举行并闭幕:主题'智能伙伴,共创未来',超1100家企业、3000余件展品、300余项全球首发,首设姚期智任主席的WAIC Academic学术会议;Kimi K3等多个模型赶会前发布。 B+ • 90% 多源一致
- AI agent网络攻防升级成本周最大安全议题:Hugging Face事件后其CEO于7月21日公开警告攻击者已在实战使用AI agent;官方指出'不对称问题'——商业API安全限制反而束缚防守方,建议预置可本地运行的强开源模型。 B+ • 91% 多源一致
- 开源阵营对闭源旗舰的追赶显著加速:Kimi K3自称比肩Fable 5并将开源权重、智谱GLM-5.2以MIT协议开源、DeepSeek V4以约数十分之一价格上线,7月形成'开源升级潮'。 B+ • 88% 多源一致

excluded_placeholder

主动剔除(未核实,不外发)

- DeepSeek V4的具体规格传闻(1.6万亿MoE、81% SWE-bench、'成本低50倍'等)仅见SEO聚合站与转述报道,官方未发技术报告,剔除具体数字
- 机器之心公众号《Kimi K3发布,国产Fable 5来了》与夕小瑶HF反击文章均被微信验证墙拦截无法全文核验,仅采用能从官方/独立源证实的事实
- 'GPT-5.6提前向合作伙伴开放系应特朗普政府要求'的说法为单源表述,未能独立复核,不采用
- Gemini 3.5 Pro'8月发布'为传闻,谷歌官方未确认时间表

• Muse Image'Arena文生图榜第二'的排名说法未在Meta官方页出现,仅见二手聚合源,不采用

信息源清单(可审计)

条目	等级	可信度	探活	来源
Hugging Face于7月16日官方披露遭全	A	97%	✓活	huggingface.co/blog/security-incident-july-202...
OpenAI于7月9日向公众全量开放GPT-5.	B+	75%	✗死	axios.com/2026/07/09/ai-openai-gpt-release...
DeepMind CEO Hassabis于7月	B+	90%	✓活	techcrunch.com/2026/07/14/deepmind-ceo-calls-f...
Meta于7月7日发布Meta Superint	A	96%	✓活	about.fb.com/news/2026/07/introducing-muse-ima...
月之暗面7月16日发布旗舰模型Kimi K3:2	A	96%	✓活	platform.kimi.ai/docs/guide/kimi-k3-quickstart...
谷歌7月21日发布Gemini 3.6 Flas	B+	91%	✓活	techcrunch.com/2026/07/21/google-releases-thre...
DeepSeek V4正式版据港媒报道于7月20	B	78%	✓活	unwire.hk/2026/07/21/deepseek-v4-official-rele...
字节跳动Seed团队7月8日发布多模态图像创作模	B-	82%	✓活	donews.com/news/detail/1/6626041.html...
2026世界人工智能大会(WAIC)7月17-2	B+	90%	✓活	business.cctv.com/2026/06/18/ARTIqtjxJlq4F4cdS...
AI agent网络攻防升级成本周最大安全议题:	B+	91%	✓活	forbes.com/sites/timkeary/2026/07/21/hugging-f...
开源阵营对闭源旗舰的追赶显著加速:Kimi K3	B+	88%	✓活	interconnects.ai/p/kimi-k3-the-open-weights-es...

*评分:A 官方一手抓原文 / B+ ≥2独立源 / B 单家权威或未复核 / B- 同源引述 / C 二手(不采)。本期 WebSearch=13
WebFetch=8 成本≈\$2.440316。自动生成,源已分级核验。*