FOR YOU / 今日重点 · 主编导读

当 AI 接上外部系统，测试该看什么？

OpenAI 和 Hacktron 把第三方服务连接列为安全测试重点。实验室里的另两项研究则分别检查模型怎样解读原始数据、机器人能否从实物反馈中修订动作。

部署前分开验证访问权限、结果质量和故障恢复；实验得分与生产可靠性各需自己的证据。

第三方连接进入测试

双方将共同选定测试目标，后续跟踪漏洞披露。

OpenAI · Hacktron

从真机反馈中更新技能

作者报告八项真机任务平均成功率为 91.1%。

arXiv · PyRUA-REAL

01 / AI公司

2026-11-06 · 本期更新

OpenAI 与 Hacktron 将联合测试第三方服务连接

OpenAI 与 Hacktron 将共同选定第三方服务连接的测试重点，并通过 Daybreak Red 扩大 Hacktron 的模型访问权限。

合作公告确定了研究范围，具体漏洞仍要看此后的披露和修复记录。

OpenAI · Hacktron

2026-11-06 · 近72小时

BioBasicsBench 用原始实验数据考查模型

OpenAI 与 Ligo 设计了 100 项常见湿实验分析任务，包括识别对照异常和证据不足。在 xhigh 设置下，Astra 获得可得分数的 66.7%，Sol 为 43.8%。

这个指标是平均得分比例，不能直接读成独立完成实验的成功率。

OpenAI · BioBasicsBench

2026-11-05 · 近72小时

Claude 在美国试行只读金融账户连接

Anthropic 公布 Personal Finance 公测，面向美国部分个人订阅用户逐步开放。用户选择连接账户后可就余额与交易提问。

这个入口支持分析，不能发起转账；试用前应查看历史聊天和解除账户连接的分别处理方式。

Anthropic · Personal Finance

02 / 热点 AI 产品追踪

产品	版本 / 日期	变化与来源
Claude Code	2.1.319 2026-11-07 本期更新 · stable	在相关设置下，自动模式遇到服务端无法检查的调用时改为询问或拒绝；发布说明保留了特定云平台例外。 Anthropic · Claude Code
Claude Personal Finance	Public beta 2026-11-05 近期版本 · beta	近期公开测试，逐步向合资格美国个人订阅用户开放。 Anthropic · Personal Finance

03 / AI芯片

2026-11-03 · 近7日观察

江波龙预告宽温工业 mSSD

江波龙称，将在 11 月 10 至 13 日慕尼黑电子展展示其首款宽温工业 mSSD。系统级封装把主控、闪存和无源器件集成在同一封装内。

设计针对边缘设备的空间与环境约束，采购仍要核实工作温区、耐久指标和供货日期。

Longsys · electronica

04 / 具身智能

2026-11-05 · 近72小时

PyRUA-REAL 将真机尝试转成可重复执行的技能

研究团队让编程智能体根据实物操作反馈修订程序，把经验保留为记忆与可执行技能。作者报告八项真机任务平均成功率 91.1%；另在 RoboDojo 的 42 项任务上报告 84.4%。

两组评估的任务和环境不同，仍需在新物体与新工位复验。

arXiv · PyRUA-REAL

05 / 基础设施

2026-11-06 · 本期更新

AWS 政府云可在同一资源组管理多种算力预留

AWS GovCloud（美国）把面向机器学习的 EC2 Capacity Blocks 和可中断预留纳入容量预留资源组。团队可为 Fleet 和 Auto Scaling 指定优先顺序，并配置预留用尽后的按需回退。

此功能便于调度已有预留，实际可用容量与实例费用仍须逐项确认。

AWS · EC2 Capacity Reservations

06 / 监管政策

2026-11-01 · 近7日观察

中国联邦学习标准明确跨框架互操作范围

YD/T 7118—2026 于 7 月 15 日发布、11 月 1 日实施，涵盖联邦学习算法跨框架互操作的架构、操作模式和流程。

多方协作项目可以据此设计接口验收测试，实际部署仍需验证各参与方选用的软件版本与配置。

YD/T 7118—2026

07 / 商业动态

2026-11-02 · 近7日观察

Lumentum 披露光互连采购承诺与季度营收

Lumentum 报告 2027 财年第一季度净营收约 12.6 亿美元，并称其第二个重要 NPO/CPO 项目获得超过 50 亿美元的采购承诺。公司将泵浦激光器和光路交换机列为增长的主要贡献者。

后续交付与收入确认决定这些承诺如何反映到财报中。

Lumentum · Q1 FY2027

08 / AI股市

AMD、美光反弹，亚洲存储股收跌

11月6日，AMD 涨11.04%，美光涨5.19%，西部数据跌1.51%。A股长鑫科技跌4.98%，港股中芯国际跌4.04%。韩国三星电子跌6.35%，SK海力士跌10.44%。

四地收盘时间不同，30家公司以 USD、CNY、HKD、KRW 原币列示。商汤收于1.16港元，来源未列日涨跌幅。清单不代表行业指数。各行链接至 Stock Analysis 或《首尔经济日报》。

存储与内存

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
美光 / MU	US / USD	690.43	+5.19%	2026-11-06 美光 · Stock Analysis
Sandisk / SNDK	US / USD	834.59	+3.49%	2026-11-06 Sandisk · Stock Analysis
SK海力士 / 000660	KR / KRW	1,132,000	-10.44%	2026-11-06 首尔经济日报 · 11月6日收盘
三星电子 / 005930	KR / KRW	188,700	-6.35%	2026-11-06 首尔经济日报 · 11月6日收盘
长鑫科技 / 688825	CN / CNY	40.41	-4.98%	2026-11-06 长鑫科技 · Stock Analysis

存储设备及配套

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
西部数据 / WDC	US / USD	263.60	-1.51%	2026-11-06 西部数据 · Stock Analysis
希捷 / STX	US / USD	460.94	-1.20%	2026-11-06 希捷 · Stock Analysis
澜起科技 / 688008	CN / CNY	150.10	-8.36%	2026-11-06 澜起科技 · Stock Analysis
兆易创新 / 603986	CN / CNY	239.49	-8.99%	2026-11-06 兆易创新 · Stock Analysis
江波龙 / 301308	CN / CNY	214.77	-4.87%	2026-11-06 江波龙 · Stock Analysis
佰维存储 / 688525	CN / CNY	126.00	-5.90%	2026-11-06 佰维存储 · Stock Analysis

算力芯片与制造

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
博通 / AVGO	US / USD	293.34	+0.62%	2026-11-06 博通 · Stock Analysis
台积电ADR / TSM	US / USD	375.13	+6.24%	2026-11-06 台积电ADR · Stock Analysis
NVIDIA / NVDA	US / USD	186.71	+2.81%	2026-11-06 NVIDIA · Stock Analysis
AMD / AMD	US / USD	449.03	+11.04%	2026-11-06 AMD · Stock Analysis
Intel / INTC	US / USD	56.30	+7.75%	2026-11-06 Intel · Stock Analysis
寒武纪 / 688256	CN / CNY	802.90	-4.98%	2026-11-06 寒武纪 · Stock Analysis
海光信息 / 688041	CN / CNY	189.50	-1.71%	2026-11-06 海光信息 · Stock Analysis
中芯国际 / 00981	HK / HKD	45.58	-4.04%	2026-11-06 中芯国际 · Stock Analysis

互联与供电散热

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
Arista / ANET	US / USD	170.75	+7.28%	2026-11-06 Arista · Stock Analysis
Vertiv / VRT	US / USD	182.82	+3.44%	2026-11-06 Vertiv · Stock Analysis

平台与应用

公司 / 代码	市场 / 币种	收盘	日涨跌	交易日 / 来源
微软 / MSFT	US / USD	530.62	-0.99%	2026-11-06 微软 · Stock Analysis
Alphabet / GOOGL	US / USD	284.68	+0.75%	2026-11-06 Alphabet · Stock Analysis
Meta / META	US / USD	610.15	+0.84%	2026-11-06 Meta · Stock Analysis
亚马逊 / AMZN	US / USD	259.42	-0.30%	2026-11-06 亚马逊 · Stock Analysis
科大讯飞 / 002230	CN / CNY	38.25	-2.30%	2026-11-06 科大讯飞 · Stock Analysis
百度 / 09888	HK / HKD	78.20	-3.04%	2026-11-06 百度 · Stock Analysis
阿里巴巴 / 09988	HK / HKD	104.90	-3.85%	2026-11-06 阿里巴巴 · Stock Analysis
腾讯 / 00700	HK / HKD	419.80	-2.46%	2026-11-06 腾讯 · Stock Analysis
商汤 / 00020	HK / HKD	1.16	—	2026-11-06 商汤 · Stock Analysis

后续跟踪合作披露的具体漏洞、真机跨工位复验和宽温存储器的供货规格。