信息 • 趋势 • 感悟

THE POWER OF COMMUNITY STARTS WITH YOU

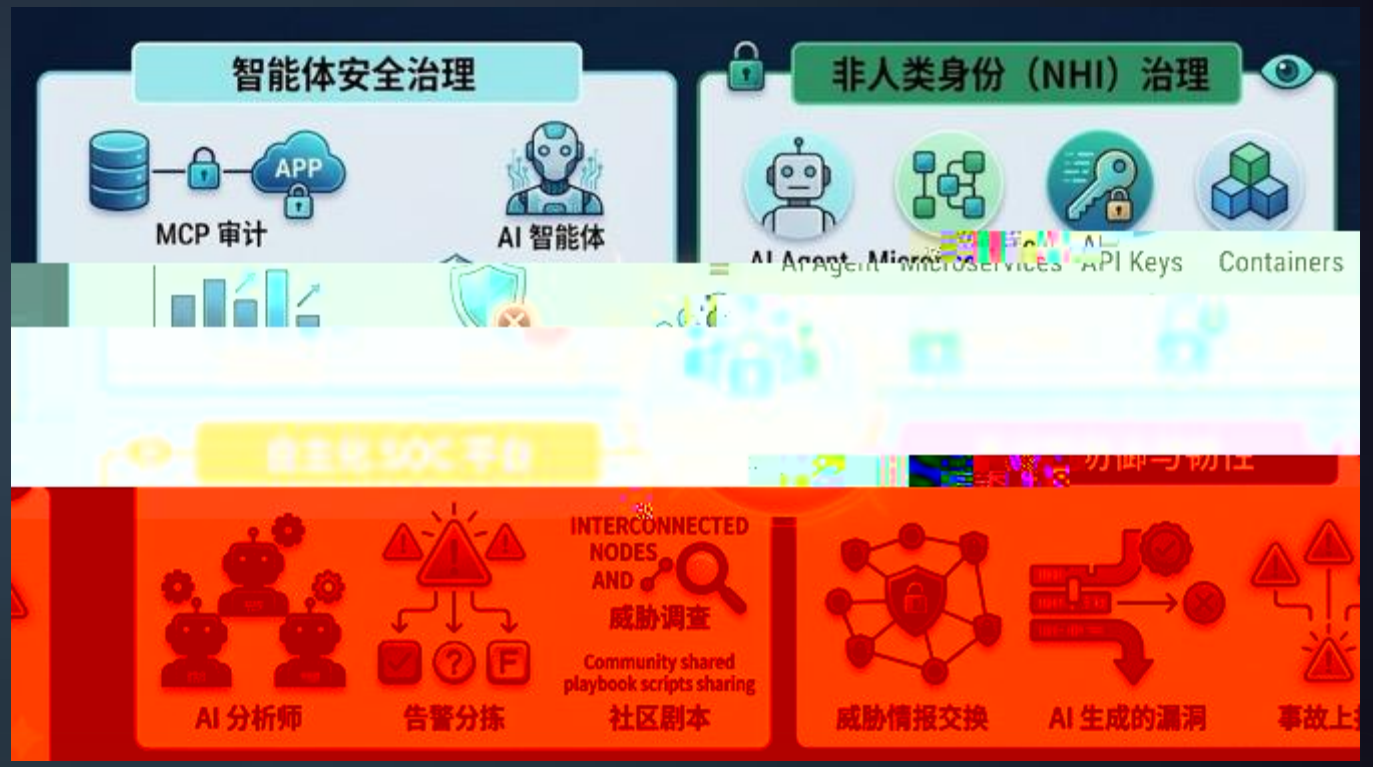
美国2026 RSA热点研讨

暨第十八届信息安全高级论坛

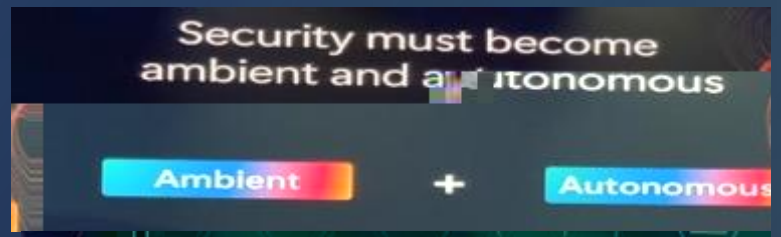
INFORMATION SECURITY FORUM 2026

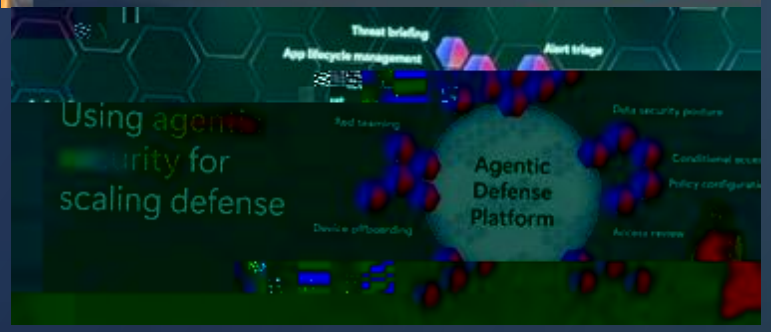

POWER OF
COMMUNITY.

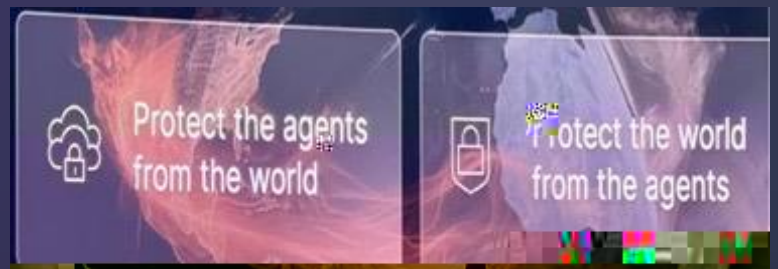

SECURITY
AI
FROM
CYBER
THREAT
AGENTS

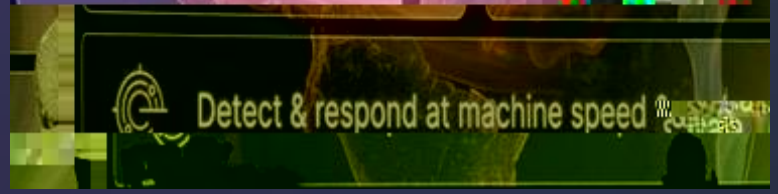

智能体安全治理
APP
MCP 审计
AI 智能体
非人类身份（NHI）治理
API Keys
Containers
INTERCONNECTED
NODES
AND
威胁调查
Community shared
playbook scripts sharing
AI 分析师
告警分拣
社区剧本
威胁情报交换
AI 生成的漏洞

Microsoft

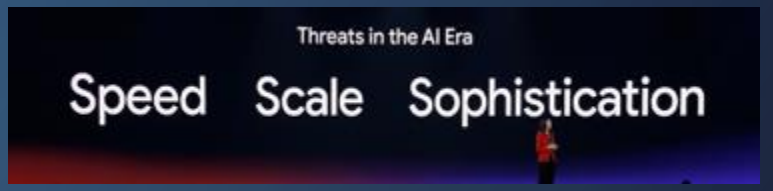








Google




BROADCOM
SYMANTEC & CARBON BLACK
ENTERPRISE-GRADE SECURITY FOR

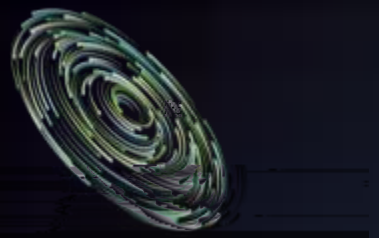

ITALIA
ITALIA


Germany
Germany


KOREA


SINGAPORE
ALICE
ABSOLUTE


NSFOCUS
AUTONOMOUS SECURITY OPERATIONS
24*7 ASOC
Innovation
ERED ENGINE



绿盟科技研究院

01

Beam 引擎

技术原理：注入式治理 (Context Injection)。不同于暴力阻断（Kill Connection），Beam 引擎在内向 AI 上下文窗口注入"确定性约束"。

引导 AI "自我修正"，而非强行关机

让安全成为 AI

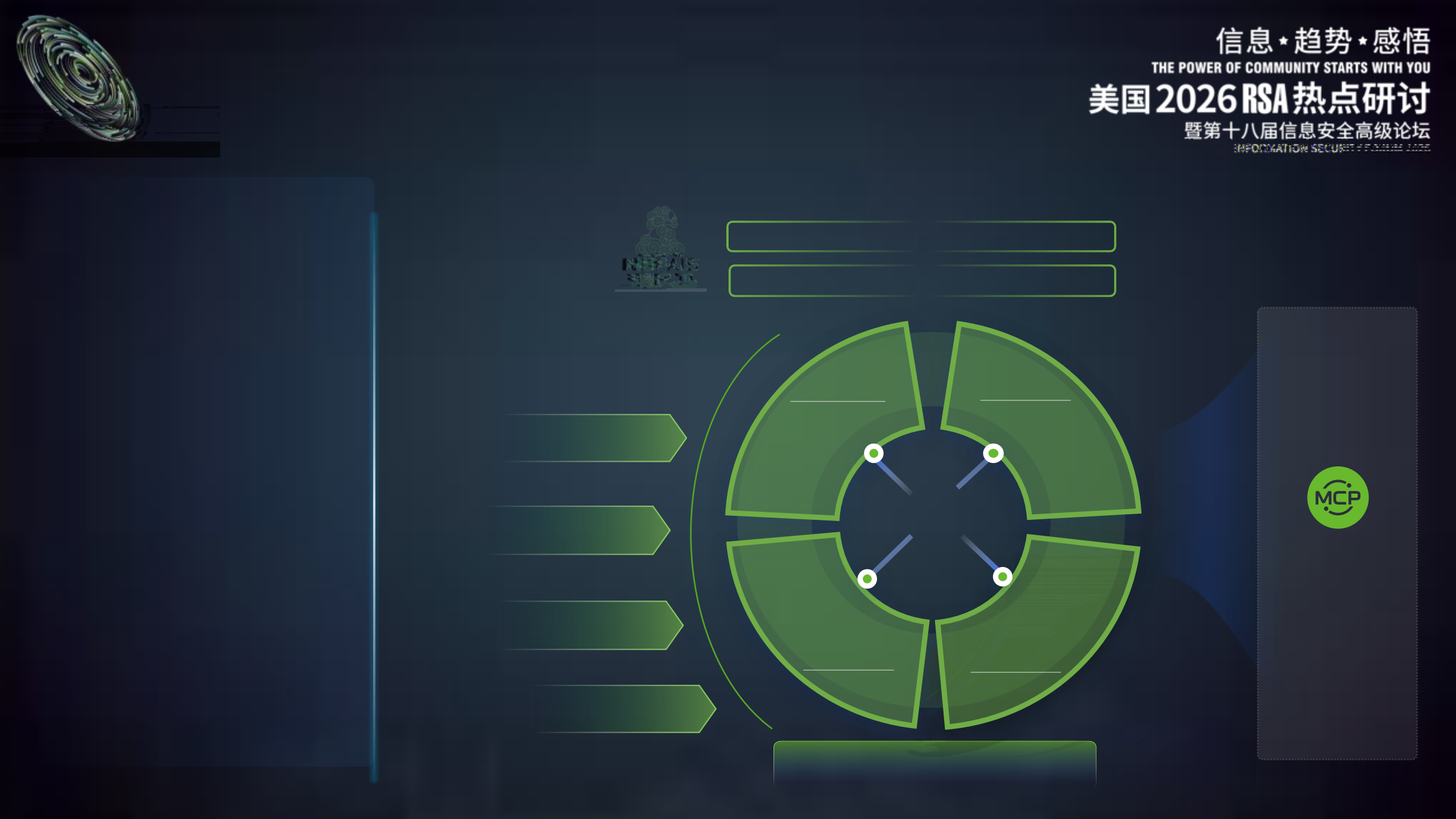
高摩擦

需要人工审核和放行，严重影响效率

，安全成为业务阻力

低摩擦

通过上下文注入引导AI自我修正，而非强制阻断



信息 ★ 趋势 ★ 感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国2026 RSA热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FORUM 2026

NSA

CISA

FBI

RSAC 2025

Jen Easterly

Claude @claudeai

Introducing Claude Code Security, now in limited research preview.

It scans codebases for vulnerabilities and suggests targeted software patches for human review, allowing teams to find and fix issues traditional tools often miss.

Learn more: anthropic.com/news/claude-co...

介绍 Claude 代码安全，现处于有限研究预览阶段。

它扫描代码库……建议针对性的软件补丁供人工审核，帮助团队发现并修复传统工具常忽略的问题。

了解更多：anthropic.com/news/claude-co...

Forbes

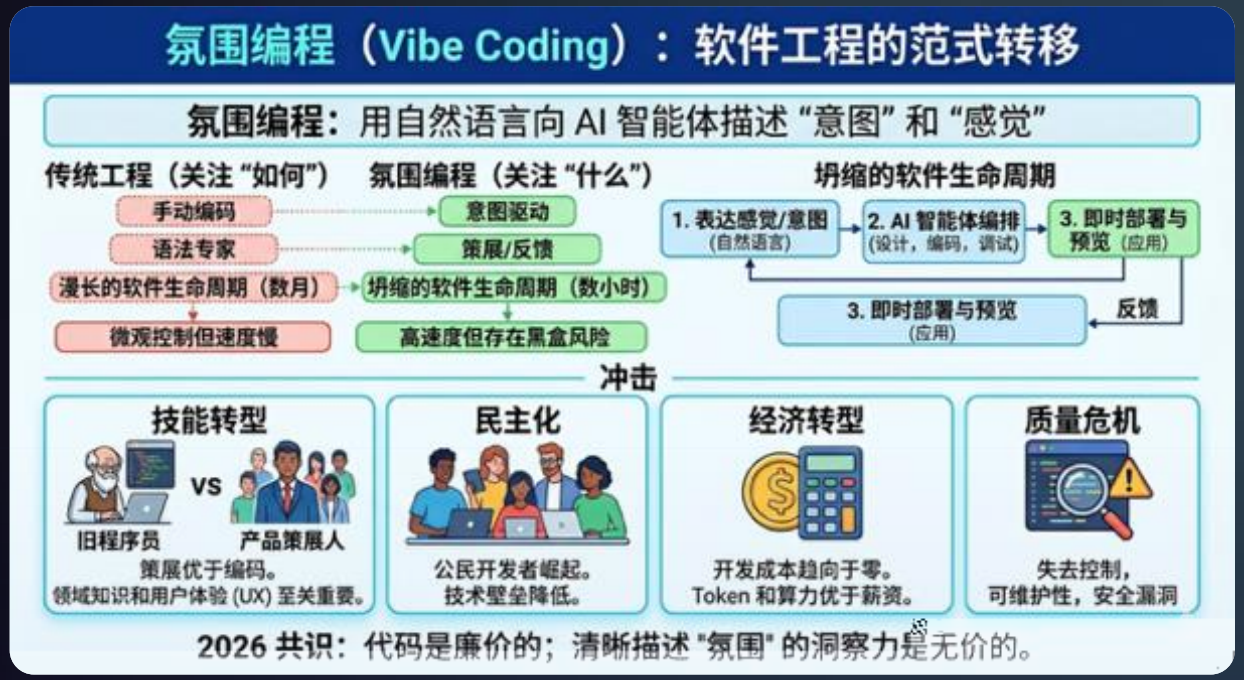
AI Just Hacked One Of The World's Most Secure Operating Systems

By Amir Husain, Contributor. © Founder WQ... Follow Author

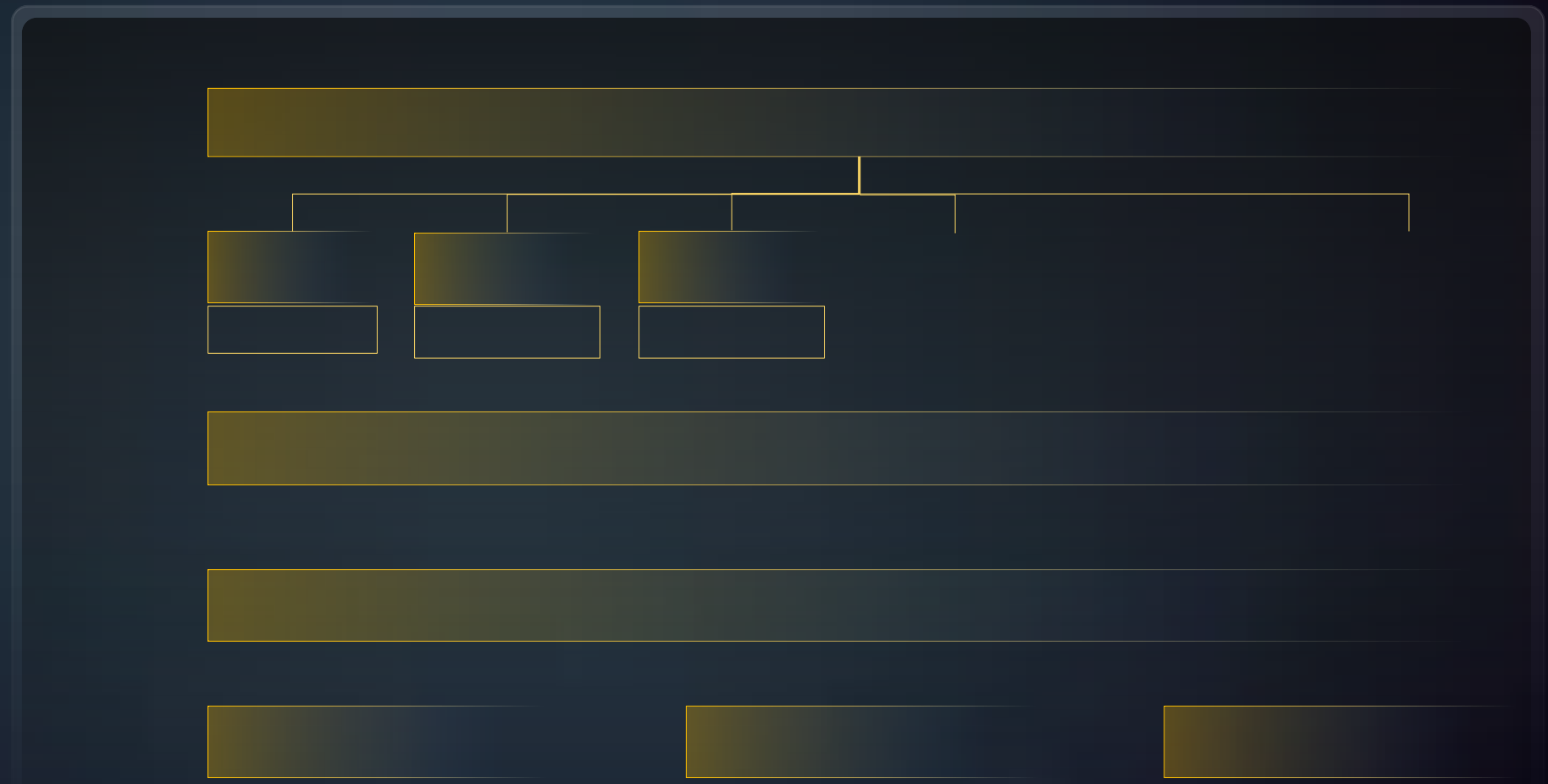
Published Apr 01, 2026, 08:38pm EDT, Updated Apr 01, 2026, 08:39pm EDT

An autonomous agent found, analyzed and exploited a FreeBSD kernel vulnerability in four hours. The implications for software security are profound.

PHOTOTHEK VIA GETTY IMAGES


氛围编程（Vibe Coding）：软件工程的范式转移
氛围编程：用自然语言向 AI 智能体描述“意图”和“感觉”
传统工程（关注“如何”）
手动编码
语法专家
漫长的软件生命周期（数月）
微观控制但速度慢
氛围编程（关注“什么”）
意图驱动
策展/反馈
坍缩的软件生命周期（数小时）
高速度但存在黑盒风险
坍缩的软件生命周期
1. 表达感觉/意图 (自然语言)
2. AI 智能体编排 (设计，编码，调试)
3. 即时部署与预览（应用）
3. 即时部署与预览 (应用)
反馈
冲击
技能转型
VS
旧程序员
产品策展人
策展优于编码。
领域知识和用户体验 (UX) 至关重要。
民主化
公民开发者崛起。
技术壁垒降低。
经济转型
开发成本趋向于零。
Token 和算力优于薪资。
质量危机
失去控制，
可维护性，安全漏洞
2026 共识：代码是廉价的；清晰描述 "氛围" 的洞察力是无价的。


Agent
SKILLS
SPEC
Model Base
MCP
Security Atomic Capabilities



开放性架构

构建标准化、模块化的安全原子能力，支持灵活组合与快速集成

智能体对接

实现与安全智能体的深度对接，支持自动化威胁检测与响应

信息 • 趋势 • 感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国2026 RSA热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY FORUM 2026