

信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

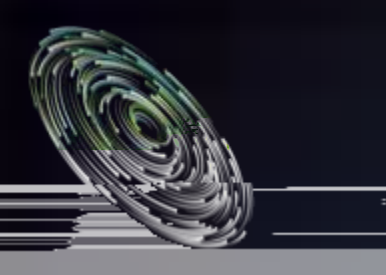
美国2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY LEADERS

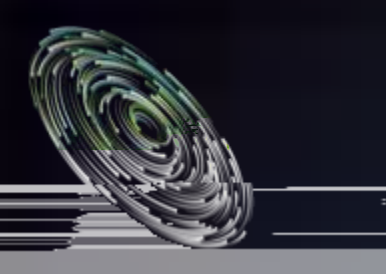
RSAC





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 LEADERS





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 LEADERS



Security must become ambient and autonomous

Ambient + Autonomous

Using agentic security for scaling defense

Agentic Defense Platform

Agents must be secured with the same vigilance that we secure people

Statistic	Value
Of the Fortune 500 have active agents built using low- or no-code tools	80%
Of employees have turned to unsanctioned AI agents for work tasks	29%
Of organizations report having security controls in place around GenAI use	47%

We need to reimagine security for the agentic workforce

Protect the agents from the world

Protect the world from the agents

Detect & respond at machine speed

INTRODUCING DefenseClaw

Secure framework for OpenClaw deployments



Threats in the AI Era

Speed Scale Sophistication

What Disruption Is (And Isn't)

Active Defense # Hacking Back

Imposing Costs On Adversaries

Bringing Partners

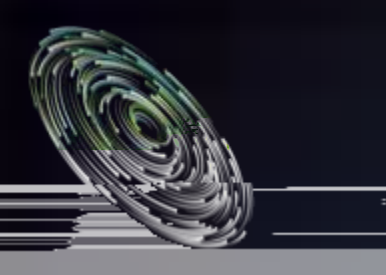
Four Pillars of Disruption

Civil Legal Action

Disinformation Disclosure

Technical Takedowns

Product Hardening



信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国2026 RSA 热点研讨

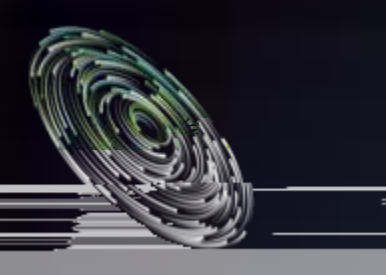
暨第十八届信息安全高级论坛

INFORMATION SECURITY LEADERS

	649	2024	600	2025	650
261	2020		40%		

()						
(TDR/ TI)		117	18%	AI		
AI	(Security for AI)	115	17.7%	LLM	Agent	
(SecOps)		101	15.5%			
(Data Security)		95	14.6%	AI	DSPM	
(IAM)		91	14.0%	(		
(AppSec)		83	12.8%	AI		
(Cloud Security)		82	12.6%	AI		
(GRC/ /)		<60	-	AI		





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 LEADERSHIP





Innovation Sandbox

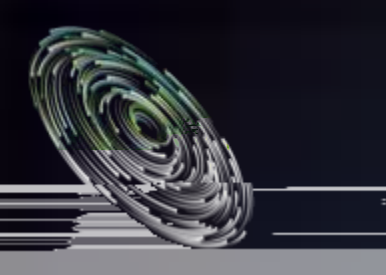
信息·趋势·感悟

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 SUMMIT 2026



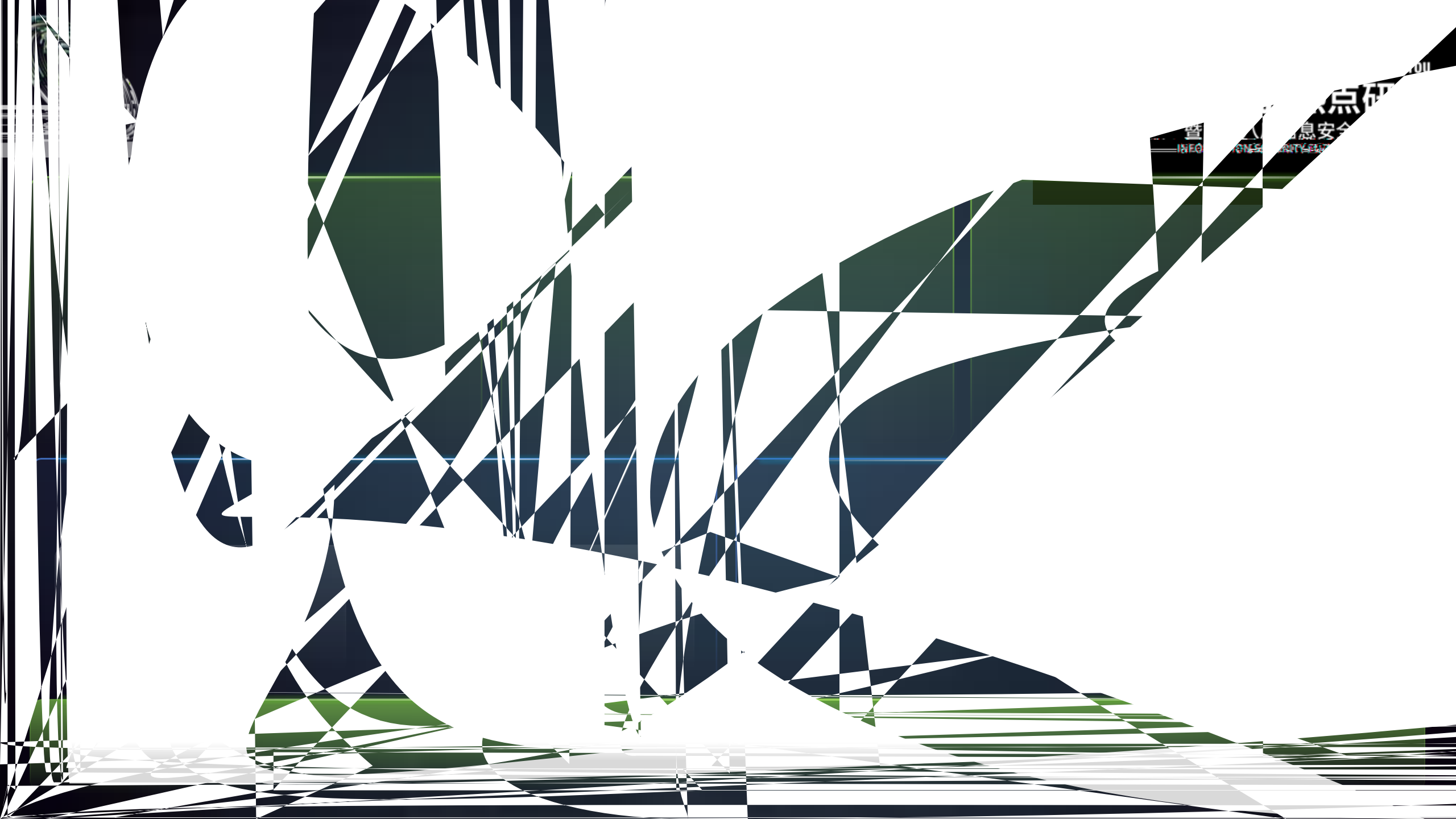
01

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



点研

警

INCO

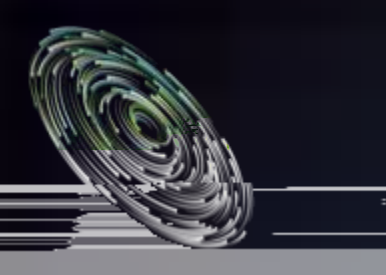
人

GN

息安

STY

on



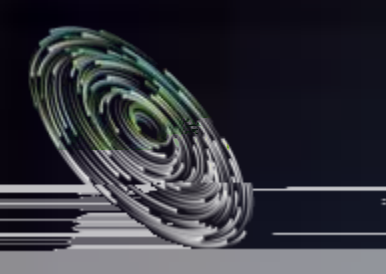
高摩擦

需要人工审核和
放行, 严重影响
效率

AI
, 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



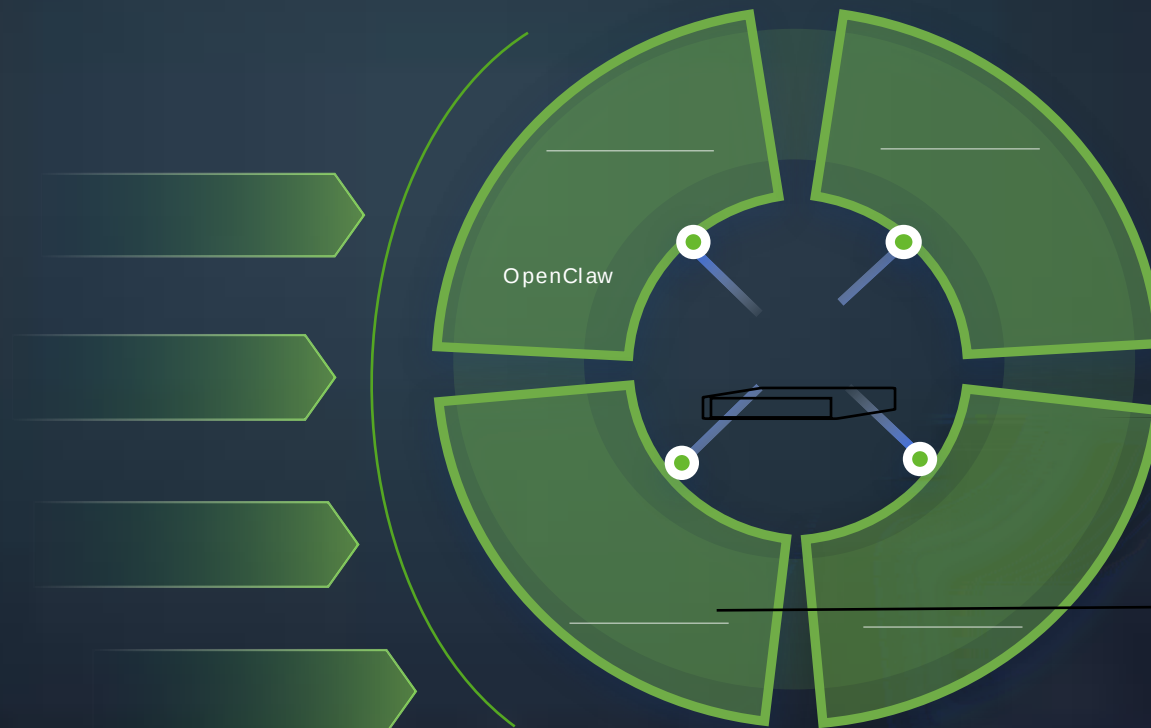
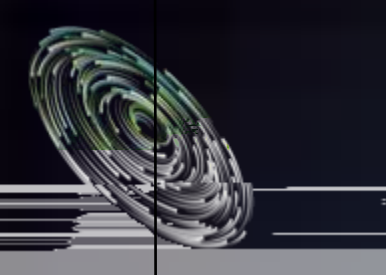
信息·趋势·感悟

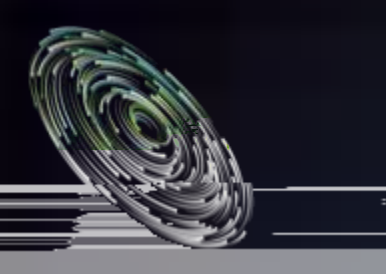
THE POWER OF COMMUNITY STARTS WITH YOU

美国2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY LEADERS





信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

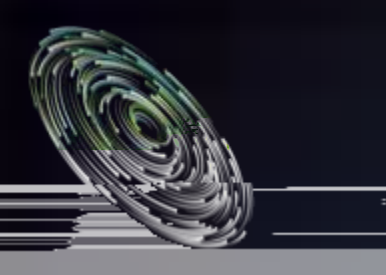
美国 2026 RSA 热点研讨

暨第十八届信息安全高级论坛

INFORMATION SECURITY LEADERS

*AUTONOMOUS
AGENTS*

*SECURITY
AGENT*



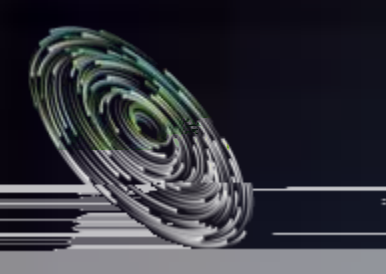
信息·趋势·感悟

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 SUMMIT 2026



信息·趋势·感悟

THE POWER OF COMMUNITY STARTS WITH YOU

美国 2026 RSA 热点研讨

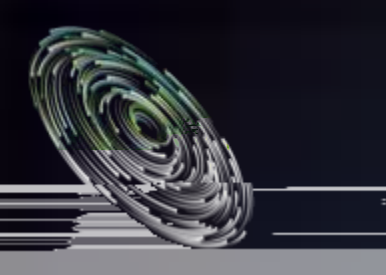
暨第十八届信息安全高级论坛

INFORMATION SECURITY EXPERTS



“ ”





Crypto Panel

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 LEADERS



NSA



CISA



FBI

RSAC 2025

RSAC 2025

Claude



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 that traditional tools often miss.

Learn more: anthropic.com/news/claude-code-security

介绍 Claude 代码安全，现处于有限研究预览阶段。

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

了解更多: anthropic.com/news/claude-code-security

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

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



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

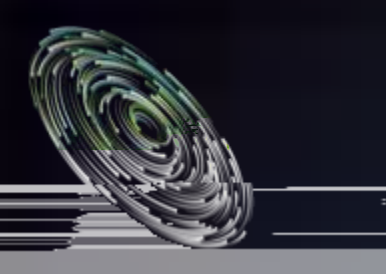
信息·趋势·感悟

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 EXPERTS



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”）

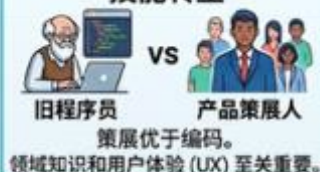
氛围编程（关注“什么”）

坍塌的软件生命周期



冲击

技能转型



民主化



经济转型



质量危机



2026 共识：代码是廉价的，清晰描述“氛围”的洞察力

Security Intelligence Agent

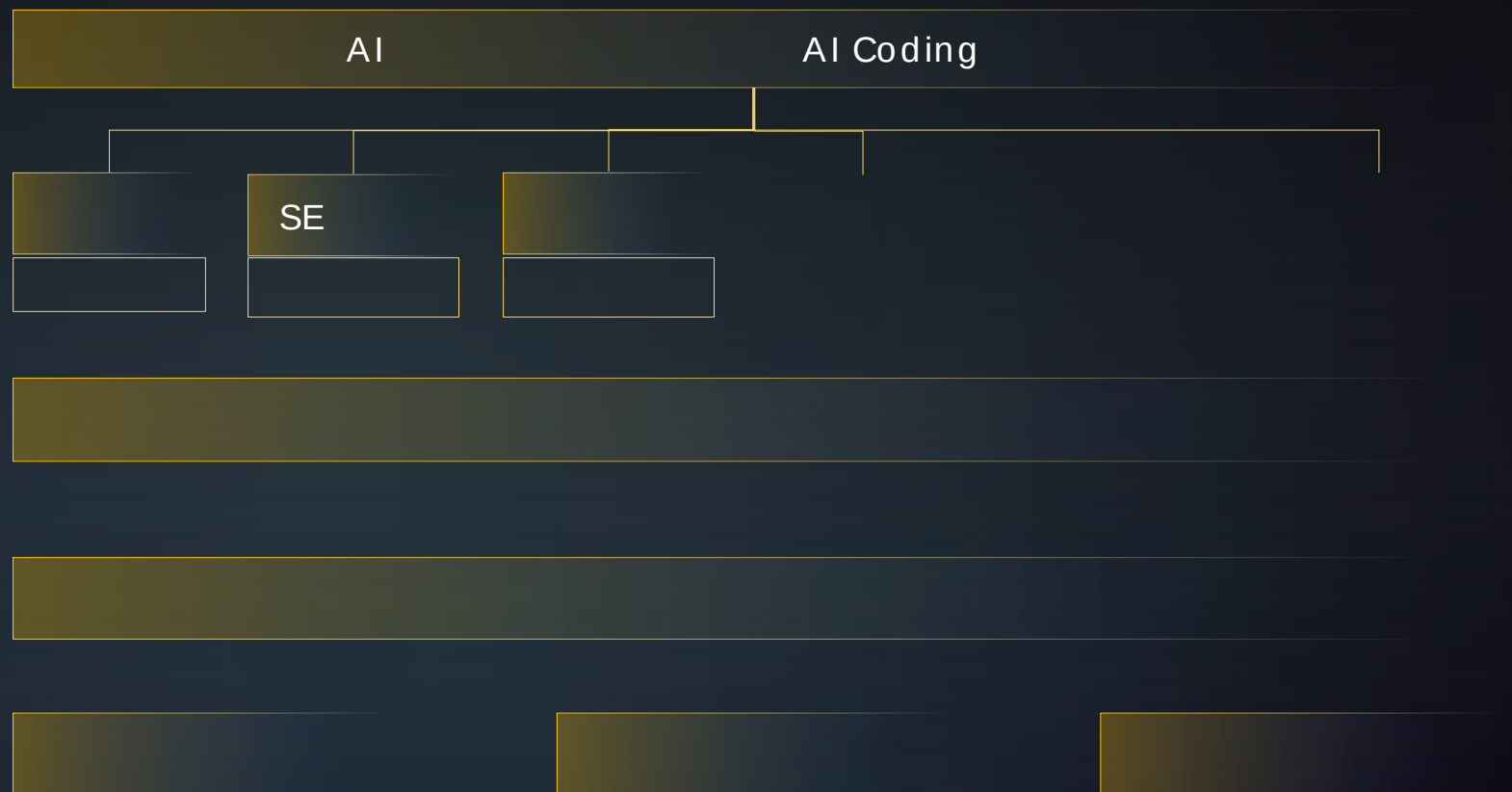
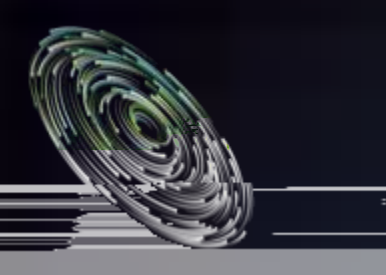
SKILLS

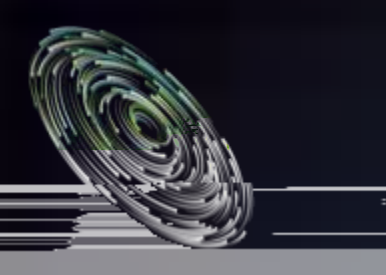
SPEC

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

AI

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 LEADERS

