2024报告

生成式AI安全准备报告

LAKERA

04 执行摘要

10 第一部分：
被调查人背景与组织背景

16 第二节：
使用与感知

21 第三节：
遭遇和管理漏洞

26 第四章：
安全措施和最佳实践

31 第五章：
挑战与未来方向

36 方法论

38 贡献者

序言

欢迎来到2024年GenAI安全准备报告！

随着我们步入生成式人工智能（GenAI）和大型语言模型（LLMs）的变革时代，很明显这些技术正在以深远的方式重塑商业格局。LLMs通过自然语言进行交互和执行任务的独特能力，使黑客领域实现了民主化，使其几乎对任何人来说都触手可及。这种转变突出了针对AI的细微差别制定加强安全措施的必要性。

跨行业，公司们渴望探索和利用人工智能的潜力。从提升客户体验到优化运营，人工智能驱动效率和价值承诺是诱人的。然而，这种热情伴随着解决人工智能安全这一关键需求，该领域仍处于起步阶段。我们的报告强调，各组织在人工智能安全方面的准备程度差异很大，反映了这一挑战的新颖性和复杂性。

与人工智能相关的风险尚未完全显现，但 tại Lakera，我們致力於引領安全人工智能創新的浪潮。我們站在這場革命的潮頭，專注於確保人工智能的益處能够夠安全負責任地享受。

我鼓励您探索这份报告，以深入了解当前的人工智能安全形势。它汇集了参与人工智能安全的不同利益相关者的观点，包括一些全球顶尖人工智能优先公司的CISO（首席信息安全官）的引言和意见。让我们一起驾驭这片不断发展的领域，建设一个安全的、由人工智能驱动的未来。

诚挚地，

大卫·哈伯
首席执行官兼联合创始人，Lakera

人工智能的采用爆发正在从根本上重塑2024年的网络安全格局，为所有网络安全领导者带来了独特的挑战和新的机遇。

在保护我们的组织方面，人工智能既挑战又颠覆了我们现有的信念、方法和策略。威胁格局就在我们谈论间不断发展变化，但已经很清楚的是，人工智能让我们面临的新威胁比过去我们所见的风险更为复杂和不同。仅靠传统安全措施是无法保护我们的。我们需要在思考如何保护传统软件和未来融合的人工智能系统时，进行范式转变。

对于我们的安全领导者来说，这是重新定义我们角色的时刻。我们需要行动起来，帮助我们的组织制定一个新方案，确保我们的员工和客户的安全。Lakera的AI就绪安全报告是一个很好的起点。

乔·沙利文
乌克兰之友首席执行官兼乔·萨利文保安公司总裁

执行摘要

人工智能应用激增，安全准备不足

生成式人工智能（GenAI）和大型语言模型（LLM）的快速采用正在改变行业，近90%的组织正在积极实施或探索LLM用例。然而，这种采用浪潮与当前安全措施的置信度极低形成鲜明对比——只有大约5%的组织对其生成式人工智能安全框架表示高度置信。

这份报告基于对1000多名安全专业人士的调查，以及来自Lakera AI黑客游戏Gandalf的实地发现，揭示安全风险可能被低估。Gandalf是世界上最大的AI红队演练，已吸引了超过一百万用户参与，包括网络安全专家，以发现漏洞。值得注意的是，超过20万名玩家成功完成了Gandalf七级防御，展示了AI系统多么容易被利用。这些发现与调查见解相互印证，突显了制定强大的、针对AI的安全策略以应对GenAI带来的独特挑战的紧迫性。

High Adoption, Low Preparedness

42% of organizations are actively using and implementing LLMs, while another 45% are exploring potential use cases. Despite this, only 5% of organizations feel confident in their ability to secure these systems against emerging threats like prompt attacks and AI-specific malware.

Diverse Expertise, Shared Concerns

The report draws on insights from over 1,000 respondents across various roles, including developers, security analysts, and executive-level positions like CISOs. Over 60% of these respondents have substantial experience in cybersecurity, yet they express significant concerns about the reliability, accuracy, and security of GenAI technologies.

Deploying GenAI Without AI-Specific Security

40% of organizations that lack standard AI security best practices are actively using GenAI. Only 22% are doing AI-specific threat modeling.

> 我对开始实施人工智能安全措施的组织建议，应在开发生命周期早期就整合人工智能红队演练实践。等到部署之后才行动，可能会让关键漏洞得不到处理。主动进行红队演练有助于在风险被利用之前识别和减轻风险，从而确保更安全的人工智能部署。

大卫·坎贝尔
规模AI的AI安全风险主管与规模化生成红队

scale

> 我最担心的是那些相信人工智能相关漏洞可以通过传统方法发现和修复的安全专业人士的过度自信。

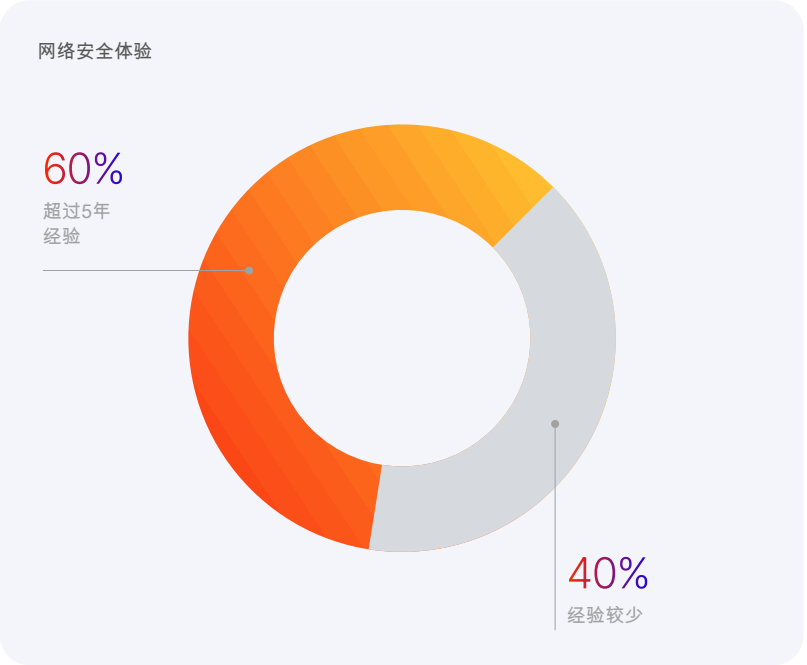
德比·泰勒·摩尔
网络股份公司及消费技术协会的执行董事

CES Consumer Technology Association

多样化的角色和丰富的安全经验

该调查包括超过1,000名来自广泛职位的受访者，例如开发者、安全分析师以及CISO等高管级别安全职位。这种多样性确保了从组织内不同角度全面理解GenAI安全。

值得注意的是，超过60%的受访者拥有丰富的网络安全经验，这使其见解具有可信度，并突显了驱动本报告结论的专业知识深度。



对 GenAI 的强烈采用

42%

Actively Using and Implementing

42% of organizations are actively using and implementing LLMs

45%

Exploring Use Cases

Another 45% are exploring use cases and integration possibilities

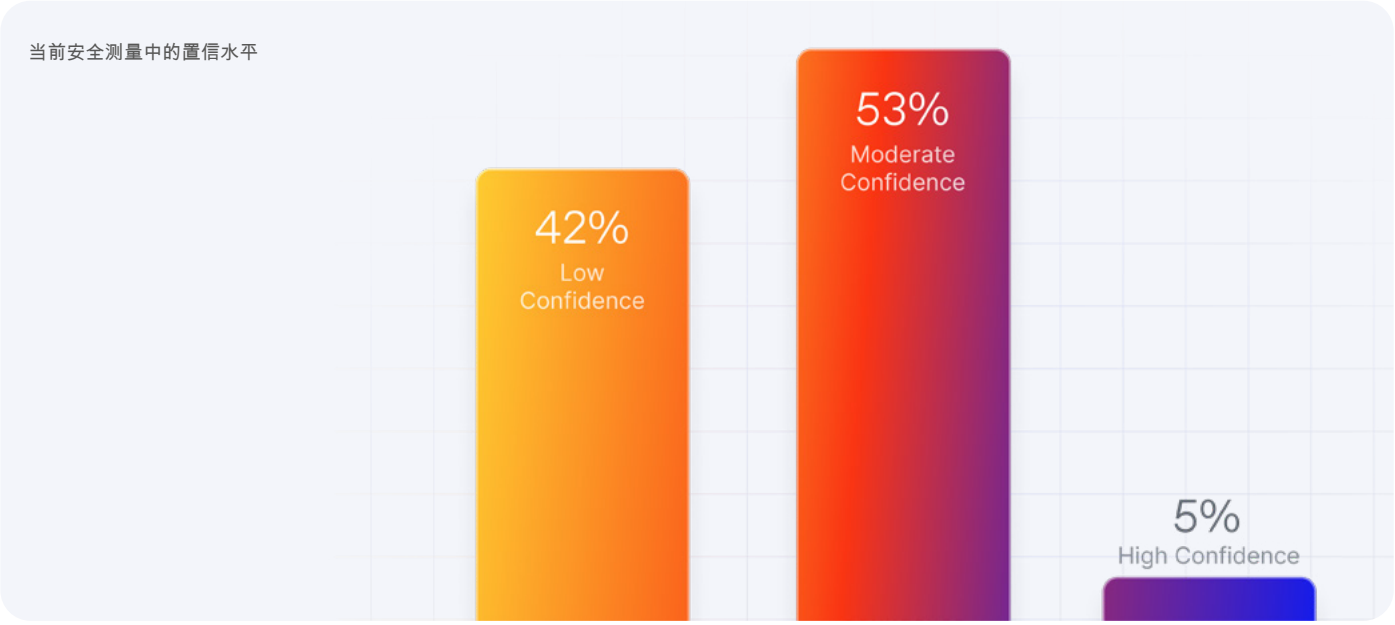
9%

No Current Plans

Only 9% have no current plans to adopt LLMs

少数人对安全措施有信心

当前安全措施的信心水平处于中等至较低，有5%的人将其信心评为5分中的5分。对于现有安全方法在抵御复杂AI威胁方面的有效性存在不确定性，有86%的人对其当前措施持有中等或较低的信心水平。这种谨慎的做法承认了在AI特定威胁和控制方面的经验有限。



仅存在适度风险顾虑

尽管38%的受访者对GenAI/LLM漏洞相关的风险高度关注（评分为4或5），但62%的人只表现出中等到低度的关注。看到大多数受访者并不太担心，这是令人惊讶的，因为只有5%的人对自己的控制措施有很高的信心。也许他们认为模型并没有访问机密数据，但用例却表明并非如此。

GenAI的5大用例

1. 编程辅助
2. 数据分析
3. 内部知识库和搜索
4. 客户服务（聊天机器人）
5. 内容创作（写作、翻译等）

生成式人工智能模型容易被攻破

拉基拉（Lakera）的AI黑客游戏Gandalf，展示了这些漏洞的实际应用。这款拥有超过一百万玩家（包括网络安全专业人士）的游戏揭示了GenAI系统是多么容易被利用——20万玩家成功通过了游戏的第七关。第七关模拟了最受欢迎的GenAI模型中嵌入的典型安全控制。这个模拟展示了操控AI模型执行非预期操作的可能性。

人们快速进化黑客技术

4000万独一无二的提示和猜测证明。

创造力可以超越通用人工智能

前七个等级可以在短短45分钟内突破——通常时间更短。

这些发现强调了应对人工智能特定安全领域差距的紧迫性，明确表明仅有关注是不够的—采取行动是当务之急。

Everyone can be a hacker

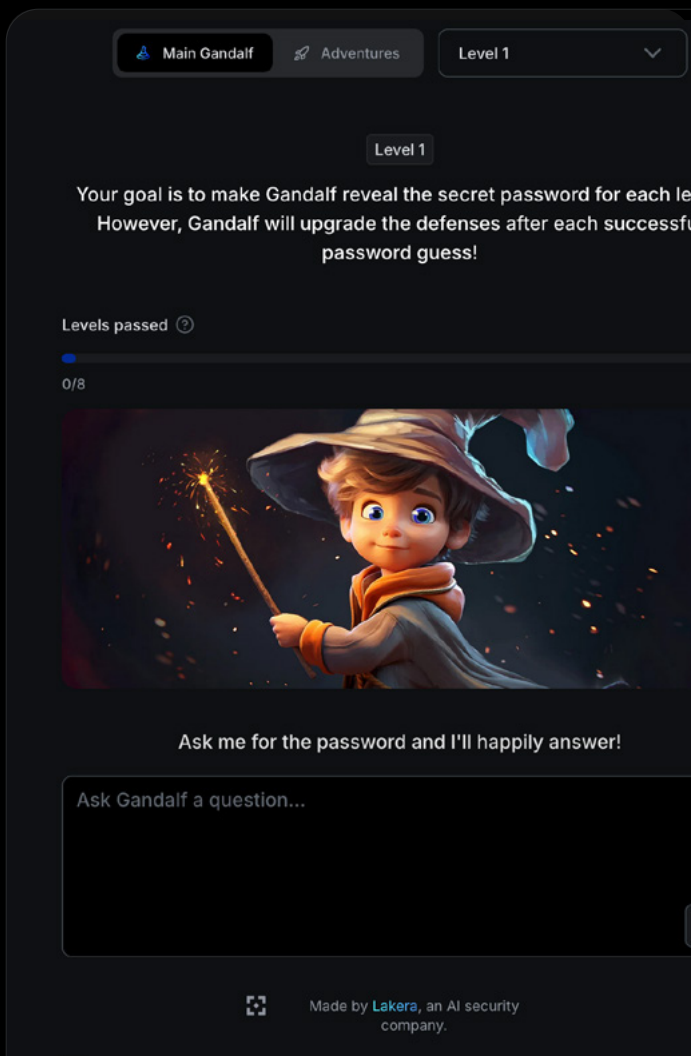
200K
have beat through level 7

Creativity is key to beat the model

40M+
unique prompts & guesses

Hacking GenAI takes minutes to hours

45′
time to beat levels 1 through 7 on average



对于刚开始实施人工智能安全措施的组织，你会给出什么建议？

这是我们的专家回答的：

nist人工智能风险管理及针对大型语言模型的owasp十大风险已证明是一个不错的起点，但每一种生成式人工智能都是不同的，其风险是由提示驱动的。

存在大量可以通过正确的上下文来识别的“未被发现的风险”。

两点要注意：

1. “一个好的工具永远不会像它的制造者那样好，这有助于使生成式 AI 工具变得更好”。

2. “这个工具的有效性只取决于使用它的人的头脑”

一个好的 AI 网络安全策略始于雇佣正确的技能。

GE HealthCare

阿维纳什·辛哈
GE医疗保健公司资深员工网络安全

如果你在人工智能安全如何或在哪里开始方面遇到困难，可以利用我们共同开发的公共资源和行业、政府及学术人工智能安全领导者社区。在ATLAS社区中，有超过100家不同的组织参与进来，我们正共同努力分享情报、描述并缓解这些针对人工智能系统而快速演变的威胁。

MITRE ATLAS

克里斯蒂娜·里亚加蒂博士
麻省理工学院 MITRE ATLAS 首席和值得信赖及安全人工智能部门

先停一停，想一想，再计划一下，再 jumped in。随着AI变得无处不在，信息安全专业人员可能会面临大量内容和资源需要处理，我们需要找到一个务实的出发点。专注于一个主题，制定计划，并按照计划执行，而不是试图一次性做所有的事情。

SOPHiA GENETICS

Alex Jolliet
索菲亚基因高级首席安全工程师

当事人背景及组织环境

理解调查受访者的背景对于将本报告中提供的见解置于具体情境中至关重要。

受访者角色的多样性、经验和组织背景为全面了解各行业当前GenAI安全准备状况提供了视角。

关键洞察

Diverse Expertise and Roles

The presence of developers, security analysts, and business users among the respondents indicates that GenAI security is a multidisciplinary concern. The involvement of CISOs and other executives underscores its strategic importance.

Substantial Experience in Cybersecurity

The significant experience in cybersecurity among respondents suggests that the insights are grounded in a strong understanding of security principles. This experience is critical as organizations navigate the evolving threats associated with GenAI.

Varied Organizational Sizes and Industries

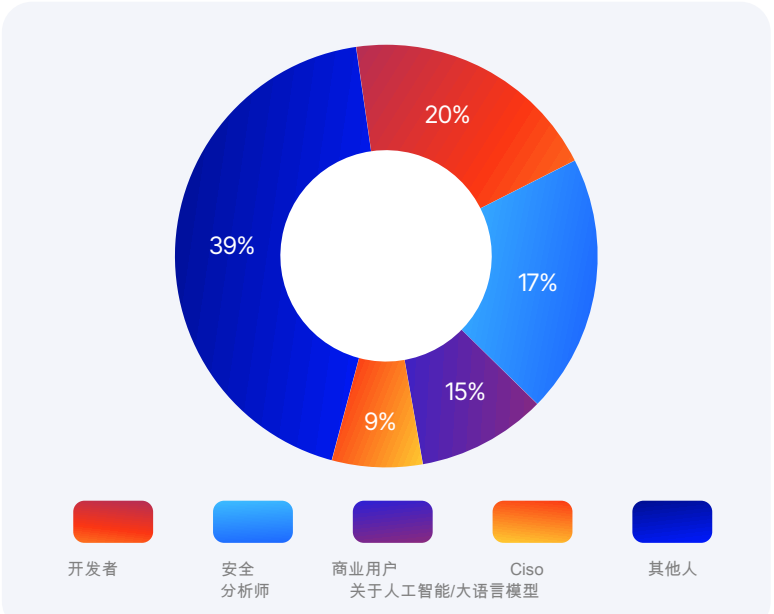
The diverse organizational sizes and industries represented in the survey highlight the universal relevance of GenAI security. Both small enterprises and large corporations recognize the importance of securing GenAI technologies, albeit with different challenges and resources.

谁是被告？

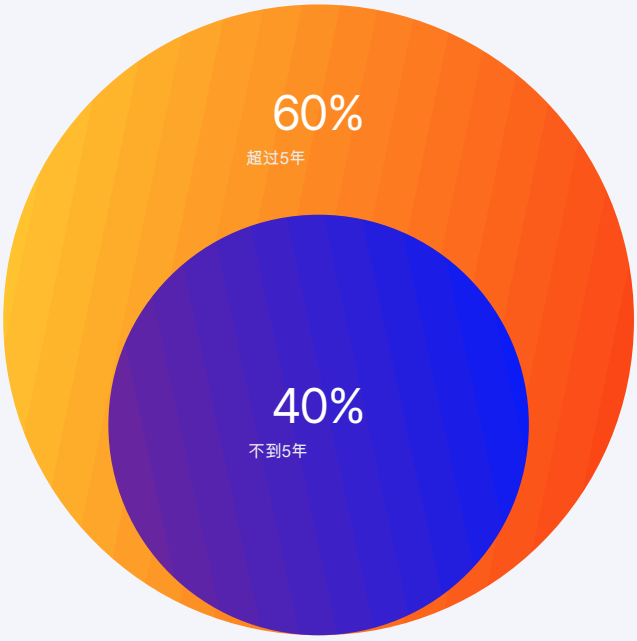
拥有超过1000名受访者，“2024年GenAI安全准备度调查”代表了GenAI和网络安全领域内广泛的角色和经验水平。这种多样性确保了调查结果能够反映各种观点和专业知识。

主要角色

这项调查包括相当数量的开发者（20%）、安全分析师（17%）以及使用AI/LLM的商业用户（15%）。值得注意的是，9%的受访者担任高管级安全职位，例如CISO，这突显了GenAI安全在最高组织层级中的战略重要性。



网络安全经验年数



网络安全经验

大多数受访者具备丰富的网络安全经验，超过60%的受访者拥有五年以上的经验。

这种经验的深度凸显了他们见解的可信度以及报告中所呈现数据的有效性。

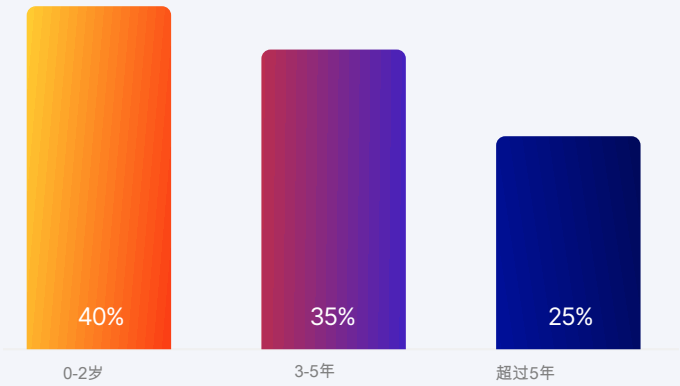
在开发和保护人工智能方面的经验

尽管许多受访者拥有丰富的网络安全经验，但数据显示，相当一部分人仍在开发和安全保障基于AI的软件方面建立专业知识。

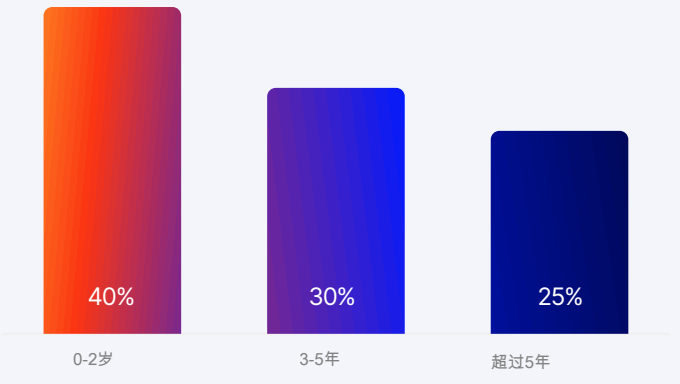
这是一个自然的进程，因为人工智能在过去的1.5年中才成为主流，并迅速地改变着各个行业。尽管这项技术相对较新，才开始被广泛采用，但它已经研发了相当长的一段时间。

正持续弥合传统网络安全与新兴人工智能安全需求之间差距的努力，反映了人们日益认识到人工智能带来的独特挑战，以及随着人工智能的不断发展，致力于制定强大的安全措施。

多年的基于人工智能软件的开发经验



多年基于人工智能软件的保障经验



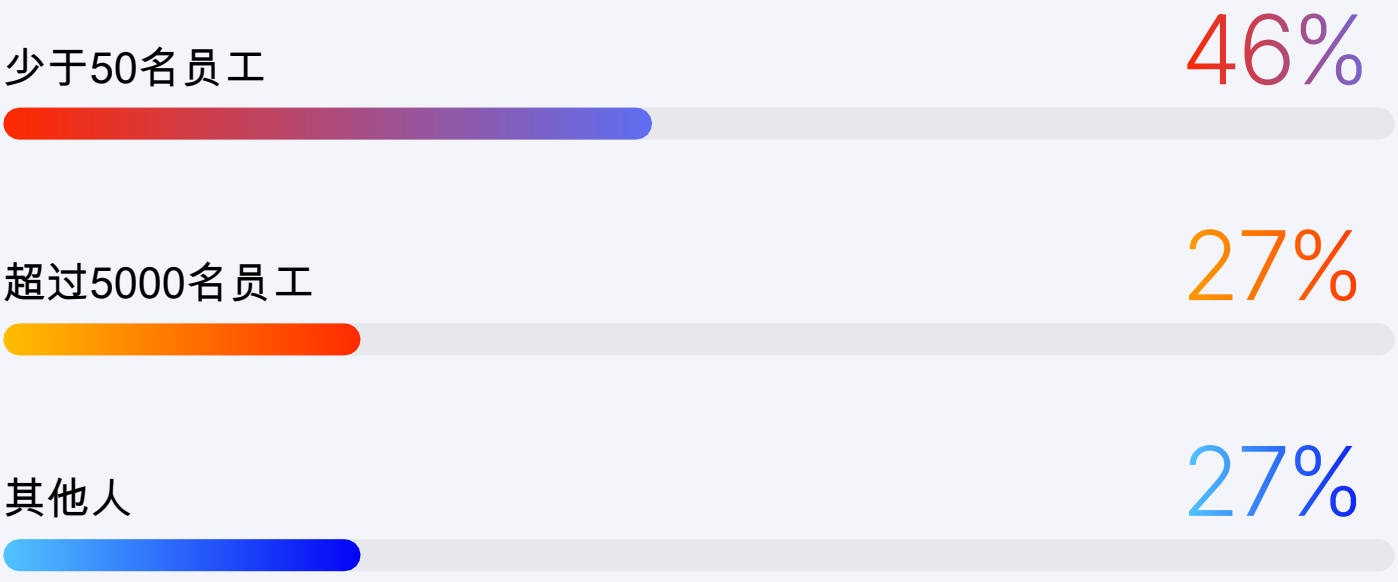
确保人工智能系统面临的最大障碍是明显的可见性差距，尤其是在使用第三方供应商时。理解机器学习流程的复杂性以及对抗性机器学习的细微差别增加了这一挑战。组建一个强大的跨职能机器学习安全团队很困难，需要来自不同背景的专业人士来创建全面的安全场景。此外，模型故障的反应时间和影响范围，特别是误导性聊天机器人，可能导致昂贵的后果。

埃马纽埃尔·吉勒姆
OWASP 人工智能/大语言模型安全研究员

组织背景

受访者来自不同规模和行业的组织，为GenAI安全挑战提供了全面的视角

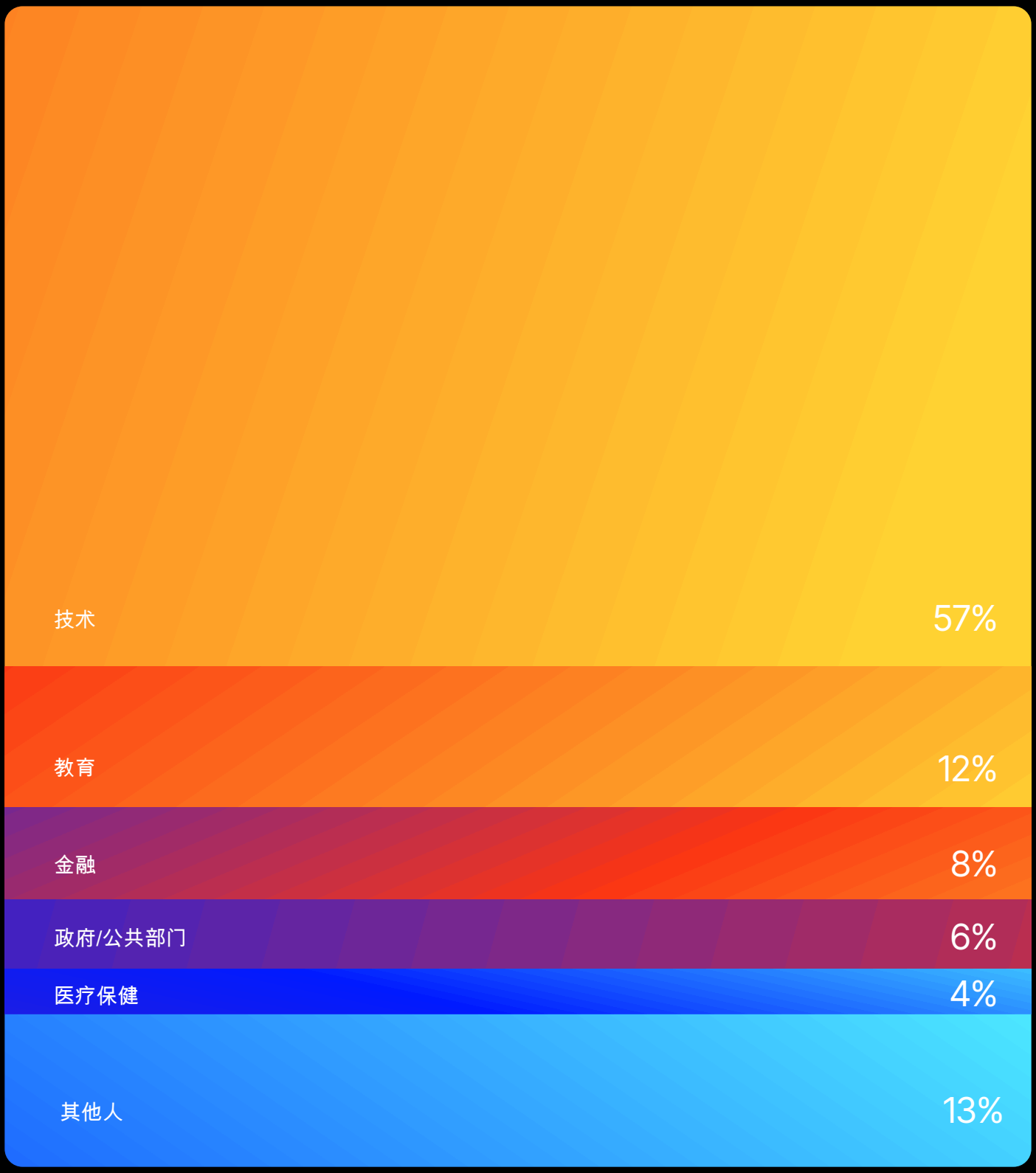
组织规模



该调查从中小企业到大公司捕获了来自不同规模组织的回复。具体而言，46%的受访者来自员工人数少于50人的组织，而27%来自员工人数超过5000人的大型组织。这种多样性突出了基于组织规模的不同挑战和GenAI安全方法。

行业代表

受访者分布于几个关键行业，其中技术行业（57%）占比最高。其他重要行业包括教育（12%）、金融（8%）、政府/公共部门（6%）和医疗保健（4%）。这种跨行业的代表性确保了洞察适用于广泛的背景，而不仅限于单一行业。



重点和对比

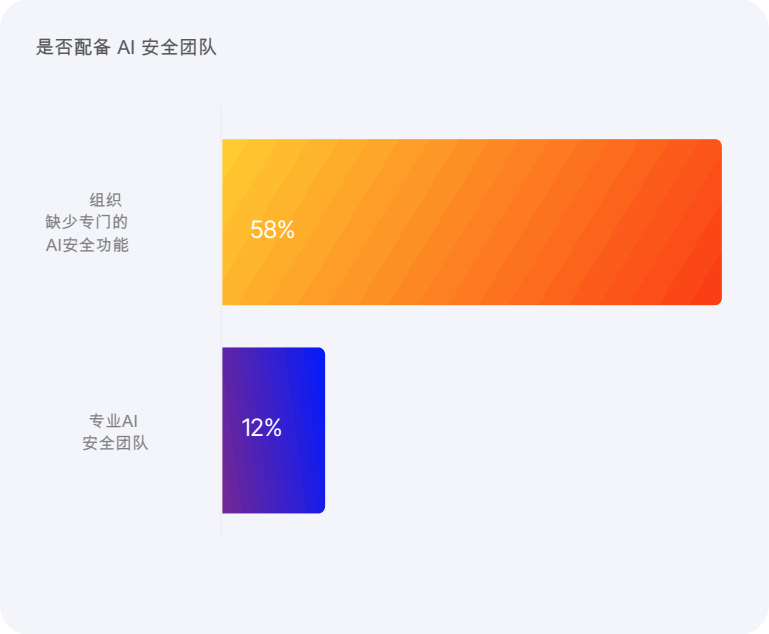
人工智能安全功能差异

最令人瞩目的发现之一是，在组织之间专门的AI安全功能的配备上存在显著差异。

虽然58%的组织缺乏专门的AI安全职能，但只有12%拥有专门的AI安全团队。这个差距凸显了一个关键的待发展领域，尤其是随着GenAI技术越来越成为业务运营的组成部分。

内部专业人才稀缺

内部专业知识的稀缺是一个突出的挑战，特别是对于较小的组织。较大的组织更有可能拥有专业的AI安全团队，28%的大型组织拥有专门的团队，而只有6%的小型组织拥有。这种差异突显了需要易于获取的安全工具和服务，以帮助弥合各种规模组织的专业知识差距。

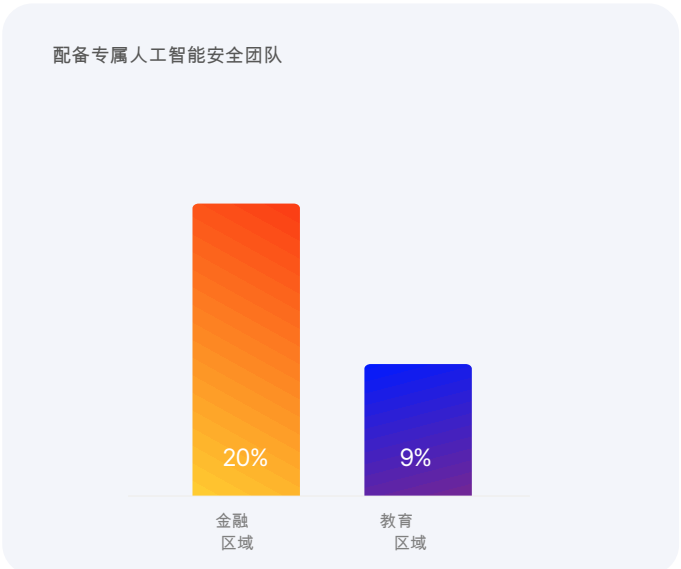


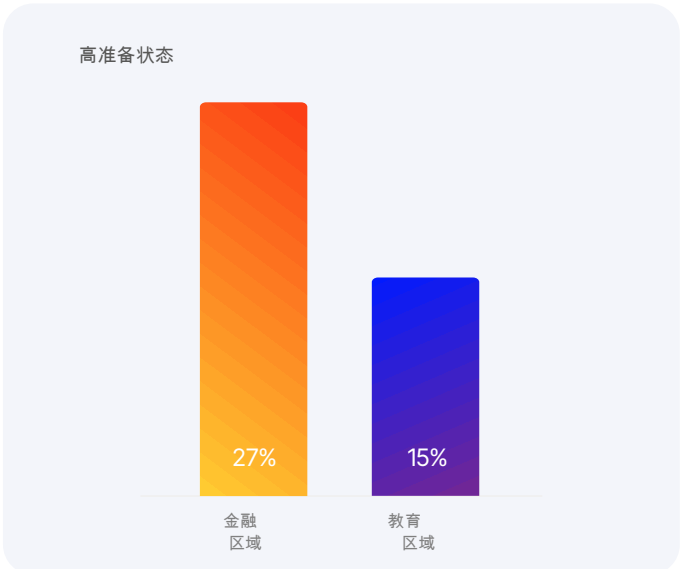
跨行业差异

各行业在安全准备程度和安全措施的采用程度上存在显著差异。例如，占受访者8%的金融行业更倾向于严格的安全实践，其中20%的组织拥有专门的AI安全团队，27%的组织将其准备程度评为最高水平（5分中的4分或5分）。

相比之下，教育领域（占受访者12%）仅有9%的组织设有专门的AI安全团队，且仅15%将其准备程度评为最高水平。这些对比凸显了不同行业面临的紧迫程度和监管压力的差异。

跨行业差异





结论

“2024年‘生成式人工智能安全准备调查’的多样化且经验丰富的受访者群体为报告中提出的见解和建议奠定了坚实的基础。通过收集来自不同角色、行业和组织规模的观点，调查结果为当前生成式人工智能安全准备状态提供了全面的视角。这种多样化的代表性确保了报告后续章节既可信又相关，为希望提升其生成式人工智能安全措施的机构提供了宝贵的指导。

目前确保人工智能系统最大的障碍之一是工程师和安全团队知识匮乏。大量人员在不了解这些组件实际工作原理或LLM非确定性对授权等概念的影响的情况下，正在构建使用LLM的系统。这使得确保系统的安全性与传统组件相比，是一个根本不同的挑战。

CLOUDSEC.AI

李耐
云安全.ai的ciso

我们目前最大的障碍是知识和经验。人工智能/大语言模型安全是一个如此新的领域，以至于我们团队里没有一个人是我们可以认为是“专家”的。我很幸运能和一些才华横溢的人一起工作，但我们的集体人工智能知识是分散的。这就像我们试图拼图，但我们丢失了盒子，并且把碎片分给了具有不同技能和不同优先级的不同团队。

SideChannel

杰罗德·布伦南
vCISO 在 SideChannel

使用与感知

生成式人工智能和大型语言模型技术的部署和应用正在迅速发展，但与此进步相伴的是一系列的感知和准备程度。

本节探讨组织如何采用GenAI/LLMs，他们对现有安全措施的信心，他们面临的挑战，以及他们对潜在风险的担忧。

研究发现，在热情与谨慎并存的环境下，对强大安全实践的需求比以往任何时候都更加紧迫。

关键洞察

Stages of Adoption

42% of organizations are actively using LLMs, while 45% are exploring use cases, indicating a strong trend towards GenAI adoption.

Confidence in Security Measures

44% of respondents have moderate confidence (3 out of 5) in their current security measures, reflecting a cautious approach to GenAI security.

Key Challenges

The top challenges to GenAI adoption include LLM reliability and accuracy (35%), data privacy and security (34%), and a lack of skilled personnel (28%).

GenAI/LLM采用阶段

组织在 GenAI/LLM 采用方面处于不同阶段，这反映了它们对这些技术浓厚的兴趣，以及它们整合过程中伴随的挑战。

组织规模

42%的机构正在积极使用和实现在各种职能中的LLMs。

这表明了在利用人工智能能力以提升业务运营和创新方面有着重要的承诺。

探索用例

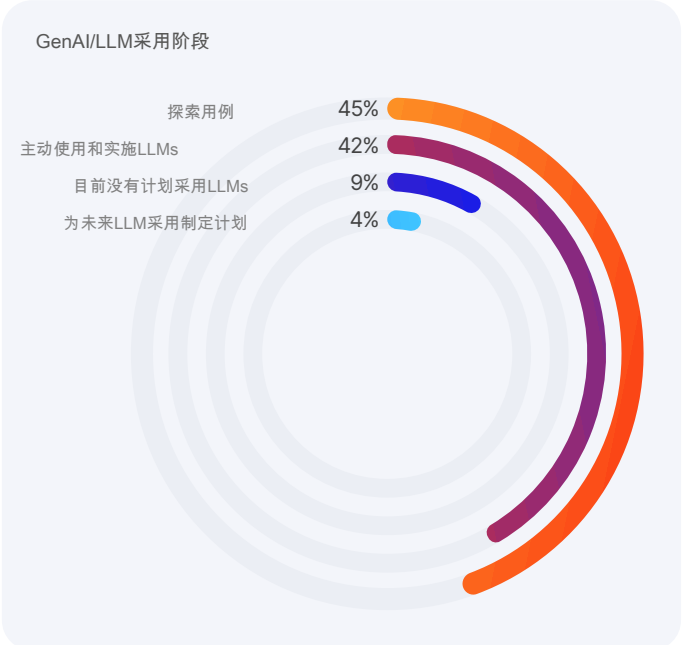
另外45%的受访者处于探索阶段，正在调查潜在的应用场景和集成可能性。

这种高水平的兴趣表明，人们越来越认识到GenAI所能带来的价值，即使其全面实施尚未实现。

暂无计划

只有9%的受访者报告目前没有计划采用LLM。

这一小百分比凸显了整个行业向 GenAI 采纳的强劲势头，表明那些尚未加入者可能面临在竞争中落后的风险。



当前和计划用例

组织正在使用或计划使用 GenAI/LLMs 用于各种目的，突出了这些技术的多功能性和广泛适用性。

70%

编程辅助

70% 的受访者提到使用或计划使用 GenAI 进行代码辅助。这表明了一种明显的趋势，即利用人工智能来改进软件开发流程。

56%

数据分析

56%的受访者关注数据分析。这反映了AI在提升数据驱动决策和洞察方面的重要作用。

53%

内部知识库和搜索

53%的人正在使用GenAI来构建内部知识库和搜索功能，展示了其在提高信息检索和组织知识管理方面的效用。

53%

数据分析

56%的受访者关注数据分析。这反映了AI在提升数据驱动决策和洞察方面的重要作用。

50%

内容创作（写作、翻译等）

50%的人正在使用生成式人工智能进行内容创作，突出了这项技术在简化并增强创意流程方面的潜力。

作为人工智能安全组织的领导者，我们对于对抗性机器学习攻击在非大语言模型（如计算机视觉和信号分类系统）上的泛滥感到担忧。虽然基于大语言模型的攻击（如提示工程和越狱）正在提升人工智能事件的社会关注度，但它很重要的一点是让公众意识到这些并非唯一受害的技术。

哈里特·法罗

米莱瓦安全实验室首席执行官

安全措施信心

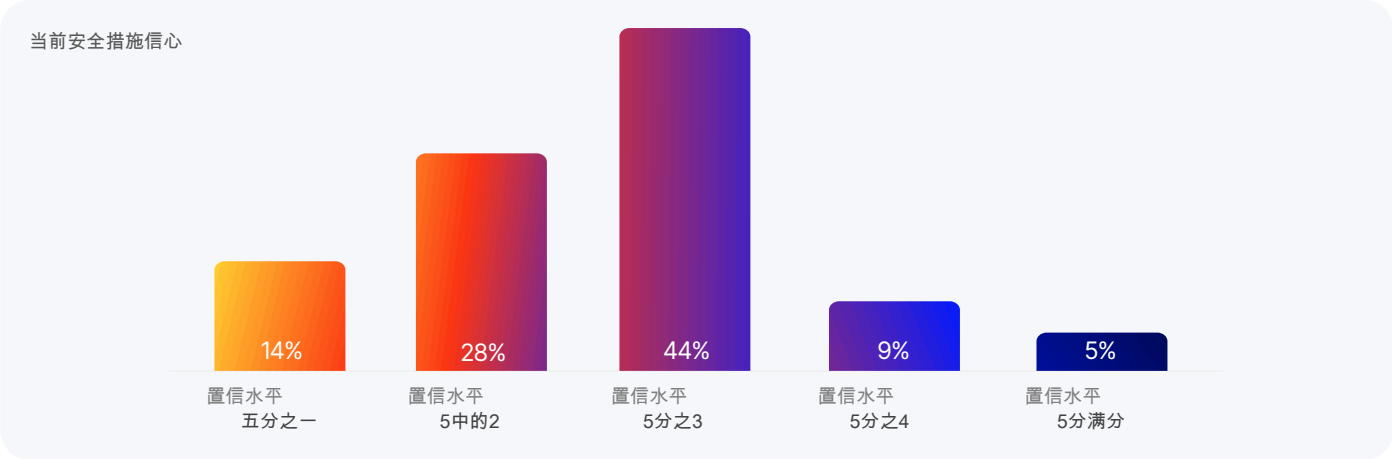
尽管对采用 GenAI/LLM 的热情显而易见，但对为保护这些技术而实施的安防措施的信心则较为一般。

中等置信度

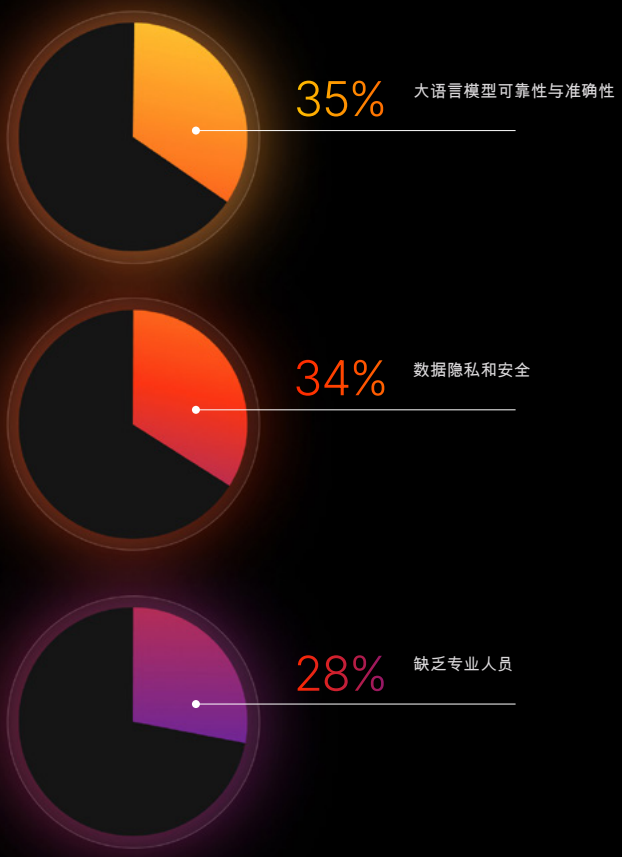
绝大多数受访者（44%）将其当前安全措施的信心程度评为中等水平（5分中的3分）。这表明虽然组织认识到安全的重要性，但它们对所采取的措施是否足以跟上不断变化的威胁存在着潜在的不确定性。

复杂情感

有趣的是，相当一部分受访者表达了较低的信心水平（28%的人评分为2分中的1分），这表明他们对安全持谨慎态度。这种缺乏强烈信心的原因可能是威胁环境的快速变化以及GenAI技术的创新性。



通往 GenAI/LLM 集成的道路并非没有障碍。组织面临着若干重大挑战，必须解决这些挑战以确保顺利和安全地采用。



大语言模型可靠性与准确性

35%的受访者提到，顶级挑战之一是LLM输出的可靠性和准确性。

这项关切突出了建立强大的验证和监控系统以确保人工智能输出结果可信且无偏见的关键需求。

数据隐私和安全

紧随其后，34%的受访者认为数据隐私和安全是主要障碍。

这种担忧在处理敏感信息的行业（例如金融和医疗保健）中尤为突出，在这些行业，数据泄露会带来严重后果。

缺乏专业人员

缺乏技能人才（28%）是另一个重大挑战。

随着对生成式人工智能专业知识的需要不断增长，组织正在努力寻找和留住能够开发和安全维护这些先进系统的专业人才。

风险关注

对 GenAI/LLM 漏洞的关注程度很高，反映了人们对这些技术带来的潜在风险的意识。

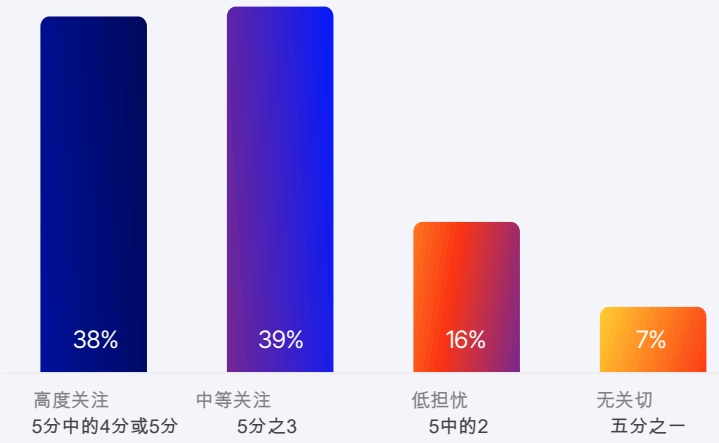
高度关注

相当大的38%的受访者将他们对GenAI/LLM漏洞的担忧评为高（5分中的4分或5分）。

这突显了对日益加剧的风险的普遍认识以及对全面安全框架的迫切需求。

需要警惕

这么多受访者高度关注这一事实，凸显了为防范新兴威胁而持续保持警惕和采取主动措施的必要性。



重点和对比

高采用率但低准备度针对安全和信任

调查显示，大多数组织都在采用LLM技术。尽管采用率高，但在安全准备方面存在巨大差距。只有5%的受访者对其当前的安全措施表达高度自信。这种低自信程度是一个令人担忧的指标，表明随着组织越来越多地将LLM集成到其运营中，可能存在潜在漏洞。

数据隐私和安全问题

有趣的是，虽然对安全措施的信心很低，但数据隐私和安全并未被视为普遍的重大障碍。只有34%的受访者认为这些问题是主要挑战。这可能表明对与LLM部署相关的风险存在低估，这表明需要提高意识并实施更严格的安全协议。

经验最丰富且最担忧

网络安全经验似乎与对风险的担忧程度相关。在经验最丰富的人群（7.5年以上）中，42.1%的人高度关注与LLM相关的风险。这表明对安全挑战的更深入的知识和理解会导致更高的意识和担忧，强调了在管理LLM安全方面需要经验丰富的人员。

结论

本部分的研究成果揭示了一种谨慎乐观的景象。组织渴望利用GenAI/LLMs的潜力，但这种热情受到了重大挑战以及现有安全措施中适度自信的限制。通过加强安全实践、在技能发展方面进行战略投资以及持续监控来解决这些挑战，对于在防范新兴威胁的同时充分发挥GenAI技术的全部潜力至关重要。

“

对于刚开始实施人工智能安全措施的组织，你会给出什么建议？

首先，让相关的跨团队利益相关者抽象出最简单的程度，以精确了解新实施的AI集成对您环境增加了什么。然后，您可以开始定义您的生态系统范围内的和范围外的内容，以及定义内部分类法，为新引入的系统和工作流程提供威胁建模框架，以及进行红队演练操作以进行持续测试，同时也 Approach 您传统的网络和基础设施安全控制。

这一重要步骤对于后续处理未来风险至关重要，要融入安全设计，并实施强大的数据保护，监控和审计人工智能系统的行为特征，以采用坚固的多层防御方法。为了在这样快速发展的行业中保持更新，建议通过投资培训和意识以及与专家小组合作来跟进最佳实践。

Ads Dawson
LLM 应用 OWASP Top 10 项目负责人

“

我所看到的最大障碍是底层人工智能模型的复杂性和不透明性，尤其是深度学习模型。大多数人工智能系统都是黑盒，其决策过程难以解释。这为什么很重要，是一个大问题？

人工智能系统最大的应用场景之一，我已经遇到，并且只会越来越大，是有效的决策制定。

如今由人工智能进行决策，从增强人类决策到取代人类决策，如何确保这种人工智能并确保其正确、准确、合乎伦理和法律地履行其（决策）职责？如果做出了错误决策，责任由谁承担，我们如何理解真正发生了什么？”

莫妮卡·维尔玛
CEO | CISO at MonicaTalksCyber |

遭遇和管理漏洞

随着通用人工智能和大型语言模型技术在组织运营中日益重要，理解这些系统如何遭遇和管理漏洞至关重要。

本节探讨了组织在 GenAI/LLM 漏洞方面的经验、这些漏洞的性质及其影响以及它们的应对策略。

研究结果揭示了组织在减轻与生成式人工智能相关的风险时所面临的挑战以及所展现出的韧性。

关键洞察

Underreported Vulnerabilities

91% of organizations reported no vulnerabilities, suggesting potential underreporting and a need for better detection systems.

Diverse Nature of Vulnerabilities

Among reported vulnerabilities, biased outputs (47%) and data leakage (42%) were the most common, highlighting the varied threats faced by organizations.

Response Speed

There is significant variability in response times, with 44% addressing severe vulnerabilities within 24 hours, but 20% still having unresolved issues, indicating gaps in incident response capabilities.

漏洞经验

调查揭示，在过去一年中，大多数组织尚未遇到 GenAI/LLM 安全漏洞。然而，对于那些遇到过的情况，这些经验为这些漏洞的类型和影响提供了宝贵的见解。

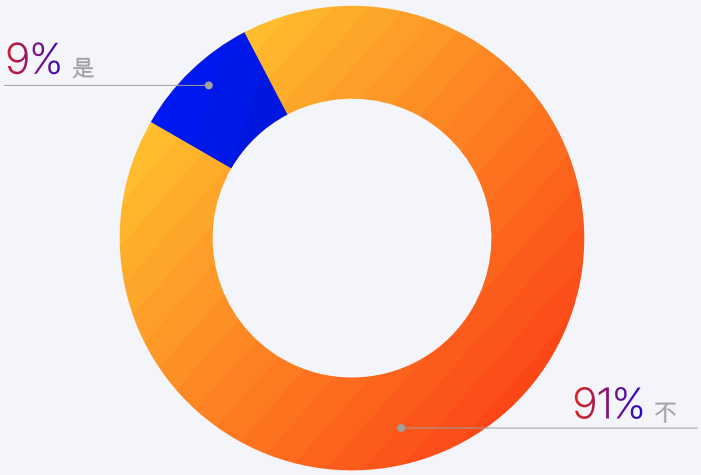
未报告漏洞

绝大多数（91%）受访者表示，他们的组织在过去一年中并未经历过任何 GenAI/LLM 漏洞。这可能表明安全措施有效，或者更令人担忧的是，缺乏检测能力。

已报告漏洞

相反，9%的受访者报告称遇到了漏洞。这个数据子集对于理解与生成式人工智能（GenAI）技术相关的现实世界挑战和威胁至关重要。

过去一年在GenAI/LLM漏洞方面的经验



在报告GenAI/LLM漏洞的组织中，出现了几种关键类型，反映了这些系统可以被攻破的多样化方式。

有偏见的输出

最常报告的问题是有偏见的结果，47%的经历过漏洞的人提到了这一点。这突显了确保AI模型产生公平和无偏见结果的持续挑战。

数据泄露

另一个重要担忧是数据泄露，有42%的受访者报告了这种情况。在部署GenAI系统的过程中，保护敏感数据免受暴露仍然是一个首要任务。

滥用AI输出

有38%的人报告了AI/LLM输出的滥用，这突显了不恰当或恶意使用AI生成信息所相关的风险。

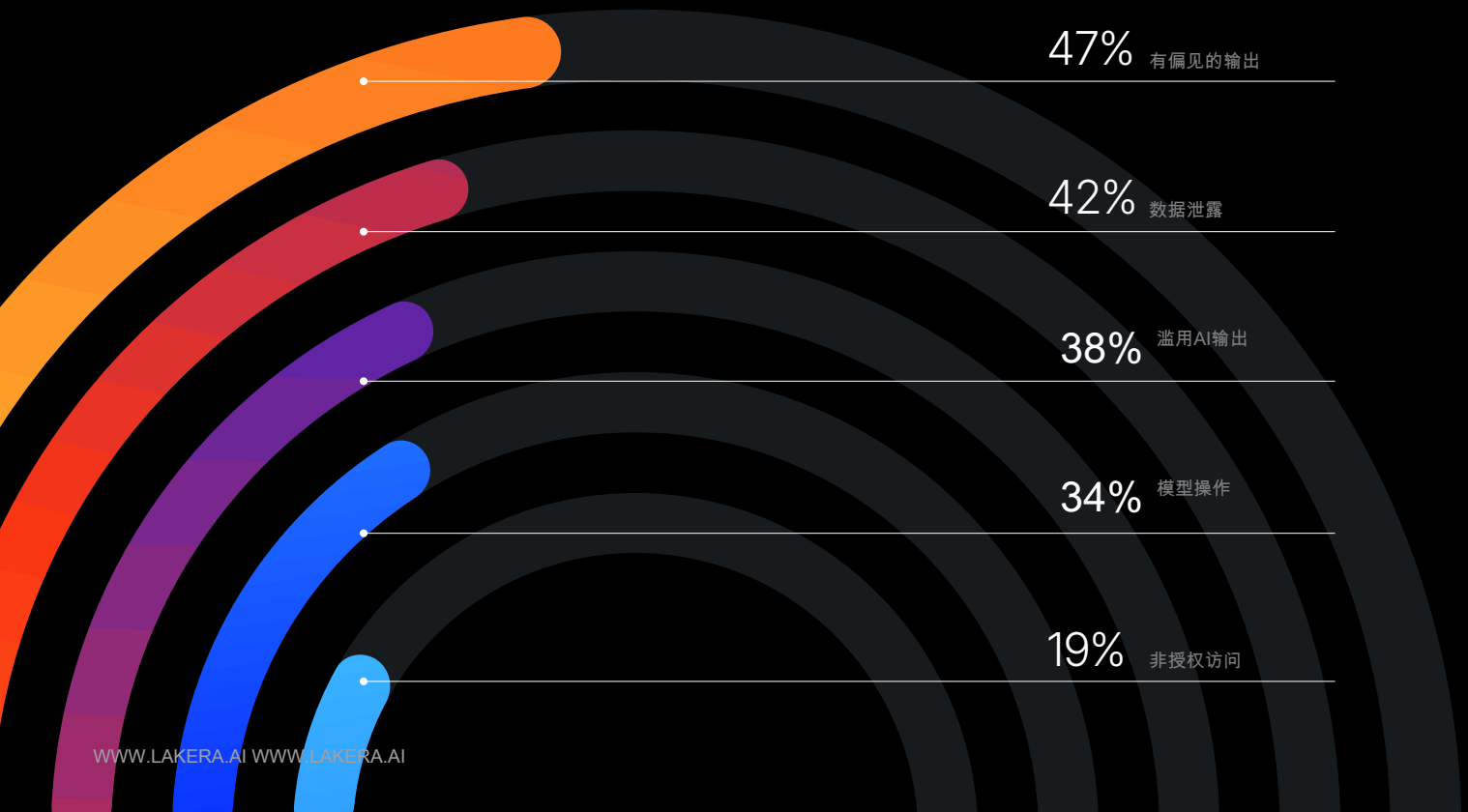
模型操作

34%的受访者提到了模型操作或篡改，表明了旨在改变人工智能模型行为的对抗性攻击的威胁。

非授权访问

19%的受访者报告了未经授权访问GenAI系统的情况，这表明需要加强访问控制措施。

GenAI/LLM漏洞性质



漏洞影响

GenAI/LLM漏洞的影响差异很大，从轻微的运营中断到严重的后果，例如法律和监管影响。

轻微运营中断

最常见的影響是輕微的操作中斷，36%的遇到漏洞的人經歷了這種情況。這表明雖然漏洞會造成中斷，但它們通常是可以管理的。

无影响

有趣的是，25%的受访者报告说，最严重的漏洞没有影响，这可能表明缓解措施成功、复原力策略有效，或者这些应用程序正处于测试阶段，而不是完全集成到公司的服务组合中。

数据泄露

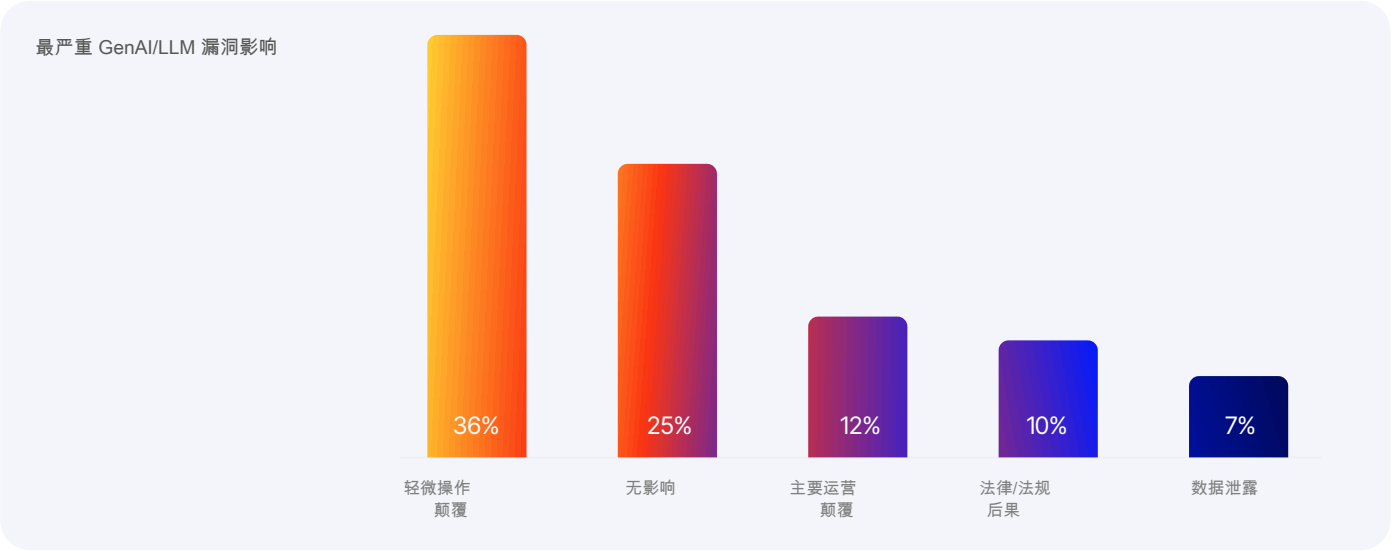
数据泄露，尽管不太常见，但也有7%的企业报告了此类事件，这突显了在GenAI部署中对数据保护的关键需求。

主要运营中断

有12%的受访者报告了重大中断，这表明某些漏洞可能对运营产生严重影响。

法律/监管后果

10%面临法律或监管后果，凸显了未能确保生成式AI系统的严重后果。



确保人工智能系统的安全所面临的最重大挑战源于人工智能算法的快速演变以及它们处理的庞大数据量。确保其安全性需要持续监控和适应不断出现的安全威胁和漏洞，以及在现有服务提供商未经事先通知就将人工智能整合到其产品或服务中时能够检测和预防的能力。此外，缺乏针对人工智能量身定制的安全标准框架，使得在各个平台和应用程序中实施一致的安全措施变得更加复杂。作为顾问，我正与安全相关初创公司积极合作，以应对这些挑战，并开发针对人工智能环境量身定制的强大安全解决方案，确保下一代安全公司优先考虑及时的安全保障。

马克·多尔西
网飞的CISO

响应速度

组织对漏洞的响应时间表明了它们在管理生成式人工智能安全风险方面的准备情况和敏捷性。

立即响应

有44%的受访者表明他们立即处理了最严重的漏洞，在24小时之内。这种快速响应对于将潜在损害降至最低至关重要。

一周内

20%的人能够在一周内解决问题，这表明有效的但略微较慢的缓解过程。

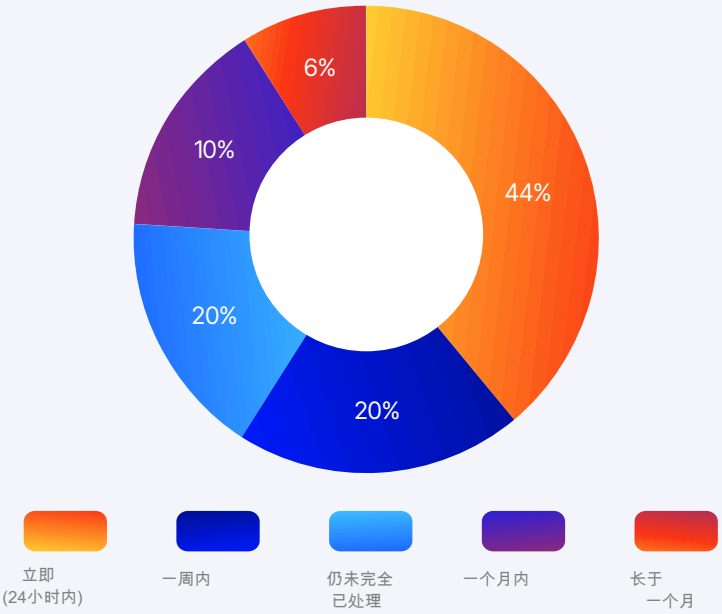
仍未解决

令人担忧的是，20%的人报告说最严重的漏洞仍未得到充分解决，这凸显了响应能力方面存在重大差距。

一个月内

一个月内解决10%的漏洞，6%的漏洞耗时超过一个月，这表明事件响应时间有改进的空间。

对最严重的 GenAI/LLM 漏洞的响应速度



与同行的比较

与行业同行比较响应速度的自我评估，可以洞察组织如何看待自身能力。

平均速度

25%的受访者认为他们识别和解决漏洞的速度与自己同伴差不多。

不确定

20%的人不确定，表明缺乏基准测试或行业比较。

更快

21%的人认为他们稍微快一些，而11%的人认为他们快很多，显示出他们对响应能力的信心。

更慢

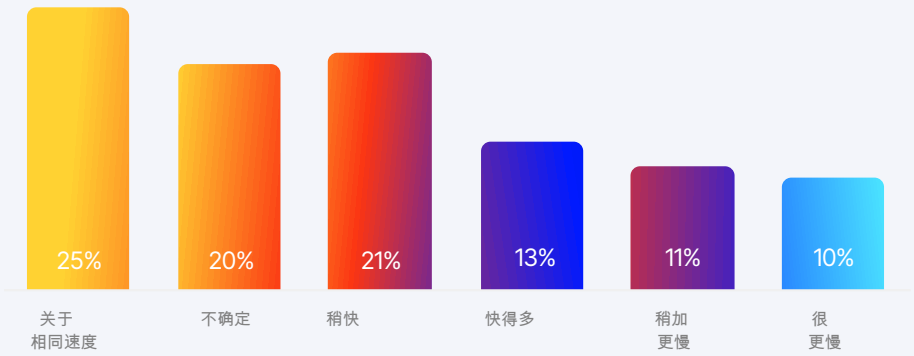
相反，13%的人觉得他们有点慢，10%的人觉得他们慢得多，这表明了需要改进的地方。

您在确保人工智能系统方面遇到的最大障碍是什么？

“流行度和易获取性使其具有挑战性。对于您的组织来说，人工智能系统是什么？您使用的许多产品已经拥有或有很快将拥有人工智能功能。员工可以在工作之外访问公共模型，比如ChatGPT，即使在工作时访问被封锁。”

曼迪·安德烈斯
Elastic的CISO

与同行相比，识别和解决 GenAI/LLM 漏洞的速度



重点和对比

未充分报道的漏洞

报告没有漏洞的组织比例很高（91%），这引发了关于检测能力和潜在的瞒报问题的疑问。这种对比表明需要改进监控和检测系统。

漏洞的多样性

广泛报告的漏洞，从有偏见的输出到未经授权的访问，表明了 GenAI 风险的多方面性。组织必须采取全面的安全措施来应对这些多样化的威胁。

响应速度波动

响应时间的可变性，一些组织仍然没有完全解决漏洞，凸显了需要强大而灵活的事件响应框架。

结论

本节的研究结果凸显了与 GenAI/LLM漏洞相关的复杂性和挑战。尽管许多组织尚未报告漏洞，但已报告漏洞的组织为这些风险的性质和影响提供了关键见解。响应时间和准备程度的差异表明了在安全实践、稳健的事件响应策略和全面的监控系统方面持续改进的必要性，以防范不断演变的威胁。

您在确保人工智能系统方面遇到的最大障碍是什么？

丹尼尔·米斯勒
无监督学习创始人

安全措施和最佳实践

随着组织将GenAI和LLM技术整合到其运营中，强大的安全措施的重要性怎么强调都不为过。

本节考察了组织采用的行业公认安全实践、正式安全政策的实施情况，以及这些组织如何了解最新的安全威胁。

研究发现，在确保全面通用人工智能安全方面，既有取得的进展，也有需要关注的领域。

关键洞察

Adopted Security Practices

Common practices include access control mechanisms (61%) and data encryption (55%), but more advanced measures like AI-specific threat modeling are less common (22%).

Formal Security Policies

32% of organizations lack formal GenAI/LLM security policies, highlighting a critical area for improvement.

Staying Informed

Most organizations use security advisories (59%) and industry forums (53%) to stay updated on threats, reflecting a proactive approach to security awareness.

采用安全实践

各组织已采用多种安全实践，以防范与生成式人工智能技术相关的不断演变的威胁。

访问控制机制

引领潮流，61%的组织已实施基于角色的访问控制等访问控制机制和最小权限原则。这种广泛采用突显了访问控制在保护敏感人工智能系统中的基本作用。

数据加密

传输中和静止状态下的数据加密是另一种广泛采用的措施，55%的受访者表示正在使用它。加密作为对抗未经授权的数据访问和泄露的关键防线。

定期安全审计

43%的机构进行内部和外部定期的安全审计。这些审计有助于识别漏洞并确保符合安全标准。

安全开发实践

30%的受访者采用了专门针对人工智能模型的 secure development practices，这反映了对人工智能技术带来的独特安全挑战的认识。

不确定或无

有28%的受访者对现有的安全实践不确定，13%的受访者报告没有任何上述措施，这表明在安全意识和实施方面存在显著差距。

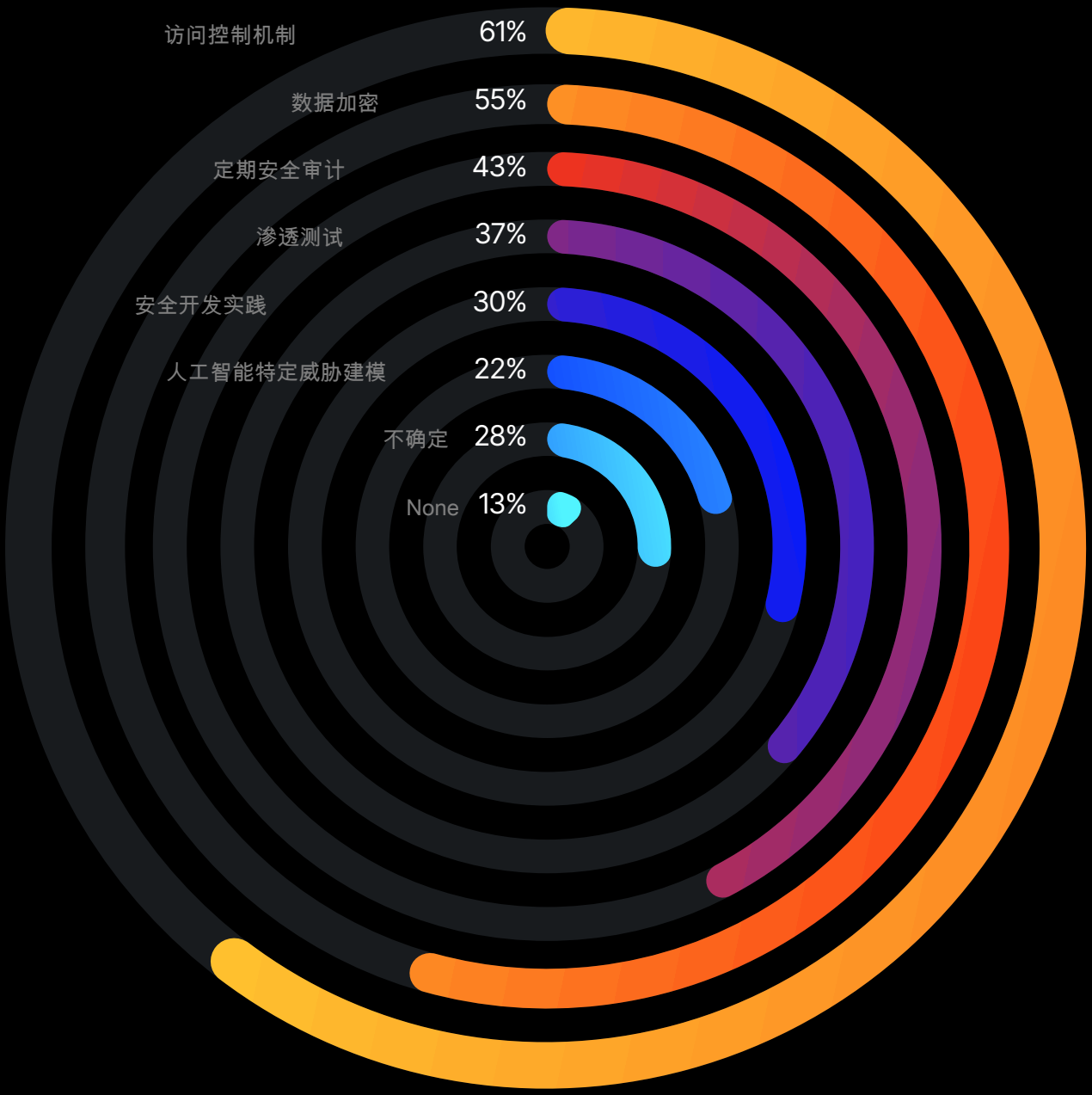
渗透测试

37% 的组织采用渗透测试，以主动识别和解决安全漏洞，防止它们被利用。

人工智能特定威胁建模

22%的机构利用了针对人工智能的威胁建模，突出了制定定制化安全策略以应对与生成式人工智能相关的独特风险的需求。

采用安全实践


访问控制机制
61%
数据加密
55%
定期安全审计
43%
渗透测试
37%
安全开发实践
30%
人工智能特定威胁建模
22%
不确定
28%
None
13%

正式安全策略

正式的 GenAI/LLM 安全策略的存在各不相同，反映了组织安全战略的成熟阶段不同。

缺乏正式政策

令人担忧的是，32%的受访者表示他们的组织没有正式的GenAI/LLM安全政策，并且没有计划制定一个。这突显了一个关键改进领域，因为正式的政策对于指导一致和有效的安全实践至关重要。

开发中的策略

30%的组织正在制定正式的安全策略。这是一个日益认识到结构化安全框架必要性的积极迹象。

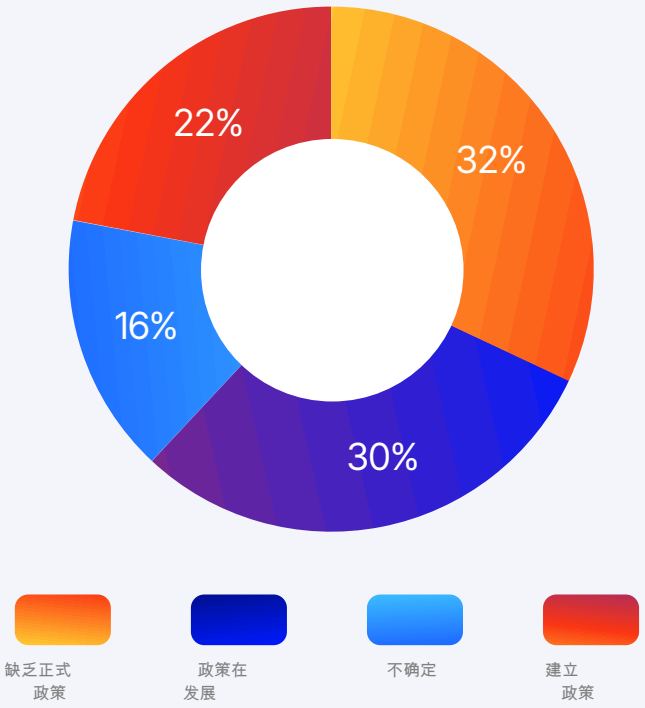
既定政策

22%的受访者报告已制定正式的、最新的GenAI/LLM安全政策，表明其准备程度和安全性承诺更高。

不确定

16%的受访者对这类政策的存在表示不确定，这表明组织内部需要更好的沟通和意识。

正式的 GenAI/LLM 安全策略



你们在组织中优先采取哪些措施来增强AI/LLM安全？

首先建立对AI/LLM特定安全威胁的理解和认识。我们通过威胁建模来评估每个新的AI应用设计，这种建模不仅关注“传统”安全主题（如身份验证、授权），也关注AI特定的威胁（例如提示注入）。关键在于人们理解可能发生什么以及可能出错什么，以及我们能为此做些什么。

马尔塞尔·温安迪
e.on公司的高级网络安全架构师

了解威胁信息

紧跟最新的安全威胁和漏洞对于保持有效的GenAI安全至关重要。

安全顾问和通讯

订阅安全公告和简报是获取信息最常见的方法，59%的受访者使用此方法。这反映了持续学习和了解最新威胁情报的重要性。

行业论坛和组

参与行业论坛和群组是另一种关键方法，53%的受访者表示他们参与了其中。这些论坛为知识分享和协作提供了宝贵的机会。

与安全研究人员合作

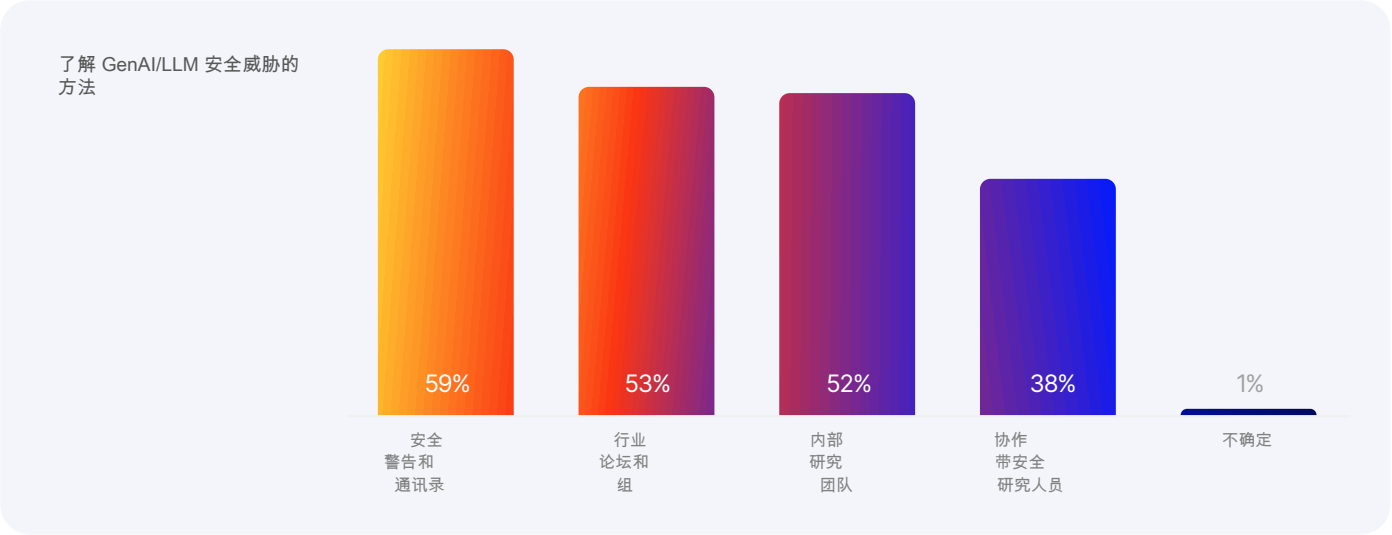
38% 的组织与外部安全研究人员合作，以增强其威胁检测和响应能力。

不确定

只有1%的受访者对自己的组织如何保持信息灵通表示不确定，这表明大多数组织都建立了一些机制来提高威胁意识。

内部研究团队

52% 的组织维持着专门致力于安全的内部研究团队，这突显了专业知识的价值，用于识别和缓解威胁。



重点和对比

冒风险前进

尽管认识到安全是一个障碍，相当一部分受访者正在继续 LLM 部署。大约 30% 将安全视为障碍的受访者也担心漏洞，但他们仍在实施 LLM。尽管存在风险，但他们前进的决心强调了有效安全解决方案的迫切需求，这些方案能够缓解这些漏洞。

未采取措施和已部署的大型语言模型

令人担忧的是，在报告未采取任何推荐安全措施的受访者中，已有39%部署了LLM应用。这种安全意识和实施方面的显著差距表明，迫切需要加强教育和采用基本安全实践，以保护这些部署。

正式政策中的差距

组织缺乏正式的 GenAI/LLM 安全政策的高比例（32%）令人担忧。这个差距突显了一个关键领域，即组织需要制定结构化的方法来管理 GenAI 安全风险。

安全实践的多样化采用

虽然访问控制和数据加密已被广泛采用，但像 AI 特定威胁建模和 AI 安全开发这样的实践则不太常见。这种对比表明，虽然基础安全措施已到位，但更高级和定制化的策略仍在兴起。

主动学习和协作

安全公告、行业论坛和内部研究团队的显著使用反映了一种积极的方法，以保持信息灵通。然而，与外部研究人员的相对较低合作表明，有增加外部参与以增强威胁情报的空间。

结论

本节的研究结果揭示了当前组织所采用的安防措施中的优势与不足。虽然访问控制和加密等基础实践得到了广泛采用，但显然需要更全面且针对AI的安防策略。许多组织中缺乏正式政策，这突显了一个关键的发展领域。为确保强大的GenAI安防，组织必须持续强化其安全框架，投资于持续学习，并促进内外部的协作。

哪项人工智能相关的漏洞你最担心将在来年出现？

这是我们的专家回答的：

虽然人工智能在信任与安全（T&S）等领域释放了巨大潜力，但它同时也为T&S团队带来了新的问题。例如，我们已经看到多个实例，即恶意行为者利用人工智能模型生成涉及儿童的有害内容。随着人工智能产品被广泛采用，负责任地获取训练数据、对人工智能模型进行红队测试、确保内容来源可靠以及其他此类策略对于安全至关重要。

Teleperformance

法拉·拉拉尼
全球副总裁，游戏业务负责人，信任与安全负责人
teleperformance 的政策

在来年的主要关注点在于提示注入攻击日益增长的危险，这种攻击可以操纵人工智能生成的内容并损害数据完整性。提示注入攻击可能导致私人信息的泄露并产生有害输出。人工智能系统的越狱，这是一个攻击者滥用人工智能如何解释输入以绕过安全控制的概念，也令人担忧，因为它允许未授权的行为。提示注入和越狱的结合使得人工智能系统极易受到恶意操纵和滥用。

Waterstons
we're with you

瑞安·威廉姆斯
澳大利亚沃特斯顿公司的网络安全工程师

挑战与未来方向

基因AI和LLM技术的快速发展带来了机遇与挑战的动态组合。

随着组织适应这些进步，了解新出现的威胁对于评估其准备情况以及有效管理风险至关重要。

本节考察了组织感知的最重大风险以及他们应对这些威胁的准备情况，突出了未来关注和改进的领域。

关键洞察

Top Concerns

Ensuring data privacy (73%) and preventing unauthorized access (46%) are the top concerns among respondents, underscoring the need for robust security measures.

Preparedness Levels

There is a wide range of preparedness, with only 5% rating their preparedness at the highest level, indicating significant room for improvement.

Managing Complexity

26% of respondents highlighted the complexity of AI systems as a challenge, with larger organizations generally better prepared to handle these complexities due to more resources and structured frameworks.

哪项人工智能相关的漏洞你最担心将在来年出现？

我目前想到的前两名是：

1. 敏感信息泄露

2. 不安全的输出处理

如果你看看针对大模型的OWASP Top 10，所有其他的漏洞都是这些漏洞在某种程度上的一种变体。此外，这些不是针对生成式AI技术的特定新漏洞。在设计或开发新功能/应用程序/用例时，AI只是一个需要考虑的不受信任实体，包含在威胁模型中。需要考虑的核心安全原则保持不变：数据最小化、最小权限、输入/输出净化，以及安全处理等。然而，如果不处理这些，其风险会根据生成式AI技术的使用方式和地点而急剧增加。”

Handshake

Rupa Parameswaran
Handshake的安防与IT副总裁，前Pinterest员工

主要关切与优先事项

调查揭示了受访者对于与 GenAI/LLM 技术相关最具紧迫威胁的共识。这些新兴威胁突显了人工智能安全问题多方面的性质以及采取主动措施的需要。

确保数据隐私

居首位，73%的受访者认为确保数据隐私是一项重大风险。这种担忧反映了在数据泄露和隐私侵犯可能带来严重后果的时代，保护敏感信息的关键重要性。

防止未授权访问

近一半受访者（46%）强调了防止未经授权访问日益复杂的系统的挑战。这表明需要强大的访问控制和先进的安全措施来保护人工智能系统免受外部威胁。

与进步同步

42%的受访者担心跟不上人工智能/大语言模型能力的快速进步。人工智能技术的快速演变性质要求安全协议不断更新和改进。

检测和缓解新型漏洞

39%的受访者将检测和缓解新漏洞列为一个关键挑战。这突显了先进威胁检测系统和主动漏洞管理的重要性。

遵循道德指南和法规

38%的受访者认为将AI/LLM的使用与道德指南和法规相结合是一个重大风险。确保遵守不断发展的监管框架对于维护信任和完整性至关重要。

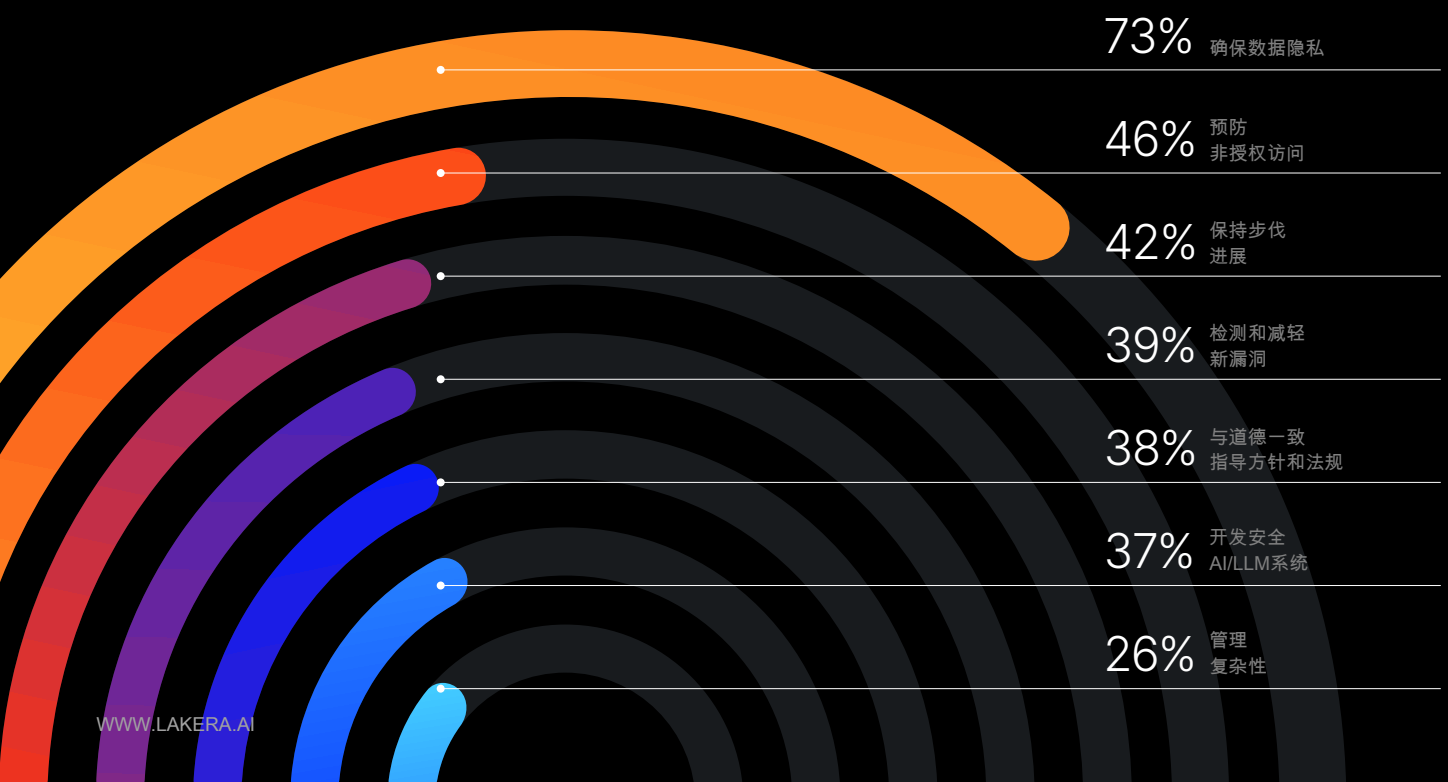
开发安全人工智能/大语言模型系统

37%强调了开发本质上安全的AI/LLM系统的挑战。这包括从一开始就将安全考虑因素集成到AI开发生命周期中。

管理复杂性

26%的受访者将AI/LLM系统的复杂性视为风险。管理这种复杂性需要全面的策略和工具，以确保人工智能技术的稳健性和可靠性。

显著的新兴 AI/LLM 威胁



应对挑战的准备工作

组织应对新兴GenAI/LLM安全挑战的自我评估准备水平各不相同，反映了它们安全框架的成熟阶段不同。

适度准备

绝大多数受访者（33%）认为他们的准备程度处于中等水平（5分中的3分）。这表明他们认识到了挑战，但也暗示了在安全实践和准备方面有改进的空间。

准备不足

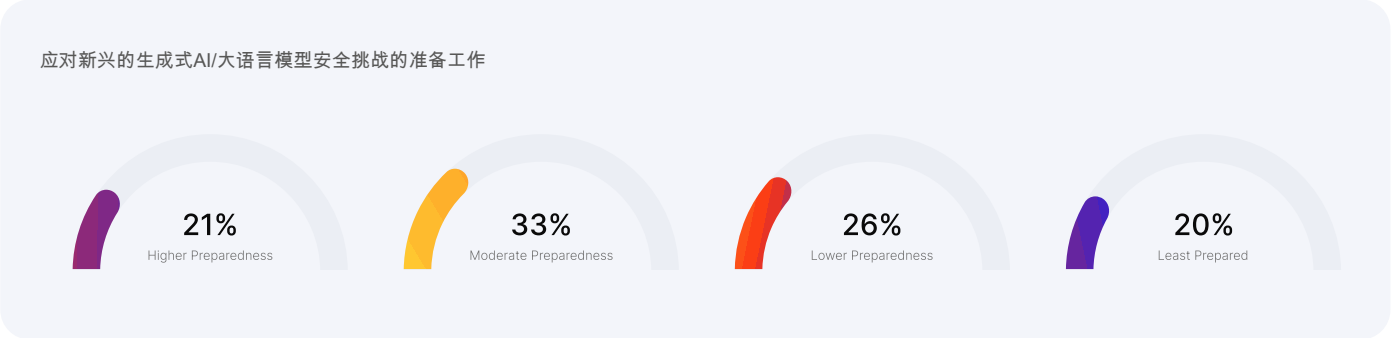
很大一部分（26%）将他们的准备程度评为2分（满分5分），这表明他们对自己应对新出现威胁的能力缺乏信心。这凸显了在安全能力方面进行针对性投资的必要性。

更高准备度

21%的受访者将其准备情况评为4分（满分5分），反映出更高的信心水平，并且可能拥有更先进的安全框架。只有5%的受访者将其准备情况评为最高水平（5分），表明很少有组织感觉完全准备好应对所有与通用人工智能（GenAI）相关的挑战。

最低准备状态

令人担忧的是，20%的受访者将他们的准备程度评为1分（满分5分），这表明他们存在严重漏洞，并且其安全态势亟需改进。



重点和对比

高度关注，中等准备

对数据隐私的高度关注与中等水平的准备程度形成鲜明对比。这种差异表明，虽然组织意识到了风险，但许多组织仍在制定有效缓解策略的早期阶段。

最少准备却积极实施

一个显著的发现是，在20%准备最不充分的受访者中，64.9%正在积极实施LLMs。这种积极主动但准备不足的方法凸显了这些组织加强安全措施以防止潜在漏洞和风险的紧迫性。

复杂性与准备

26%的受访者承认管理人工智能系统复杂性的挑战，但对解决这一复杂性的准备程度却存在差异。这种差异性源于资源和响应能力的不同。通常拥有专门的人工智能安全团队和更结构化框架的大型组织，往往准备得更充分。相比之下，资源较少、政策不太正式的小型组织则更难应对这些复杂性。这种差异体现在先进安全实践采用程度的不同以及处理人工智能相关挑战的信心水平差异上。组织必须优先发展全面的管理框架来处理人工智能系统的复杂性。

道德与监管一致

强调将 GenAI/LLM 的使用与道德指南和法规相结合，突显了对负责任 AI 重要性日益增长的认识。然而，实现这种一致性的准备情况表明了持续的努力和适应监管变化的必要性。

哪项人工智能相关的漏洞你最担心将在来年出现？

这是我们的专家回答的：

我们主要关注点不在于大型语言模型（LLMs）特有的漏洞，而在于人工智能（AI）和LLM工具和框架中的传统Web漏洞。尽管人们非常关注独特的AI安全威胁，但用于构建AI驱动系统的框架的安全设计和实现往往受到的关注较少。我们的研究已经识别出多个问题，例如在领先的LLM SDK中可通过标准提示注入触发的远程代码执行（RCE）。为了确保健壮和安全的AI驱动应用程序，绝不能忽视传统安全领域。

snyk

艾略特·沃德
Snyk安全实验室安全研究员

“深度伪造技术利用人工智能制作令人信服的虚假视频、音频和图像，对个人和国家安全构成重大威胁。它们有可能被用于虚假信息传播、宣传和操控，导致社会动荡、金融欺诈以及对机构信任的侵蚀。深度伪造技术的日益复杂化和易得性使恶意行为者更容易制作和传播令人信服的虚假内容。因此，深度伪造技术有可能破坏我们数字社会的根基，并损害我们区分事实与虚构的能力。”

CSA

黄凯
CSA人工智能安全工作组联合主席，云安全联盟

“相比于任何单一漏洞，我更担心公司加速部署基于大语言模型的工具的深度，而往往不顾及安全问题。在应用程序或操作系统中深度集成会创造一个新的高价值目标，这个目标有潜力将原先分散、孤立的数据集中起来，并且可能以出乎意料的方式被操纵。部署得越深，妥协就越严重，一次又一次地证明了当这些系统被部署时，它们是如何被利用的。”

KUDELSKI SECURITY

南森·哈米埃尔
科达信安全研究高级总监

Recommendations for Future Directions

Adopt security tools with continuous learning	Staying ahead of new attack methods requires tools that not only address AI-specific attacks, such as prompt injection, jailbreak, and data poisoning, but also use AI for continuous learning. Traditional rule-based approaches cannot keep up as attack methods evolve.
Enhance Data Privacy Measures	Protecting confidential data requires addressing AI-specific threats that can manipulate the model to leak data. Organizations must also prioritize traditional data privacy measures, including encryption, anonymization, and secure data handling protocols, to protect sensitive information.
Strengthen Access Controls	Developing and enforcing stringent access control policies is critical to prevent unauthorized access. Regular audits and the implementation of multi-factor authentication can further enhance security.
Invest in Continuous Learning for Security and Development Teams	Staying abreast of rapid advancements in GenAI/LLM capabilities through continuous learning and adaptation is essential. Organizations should invest in training programs and keep their security measures updated.
Focus on Threat Detection and Mitigation	Developing and deploying advanced threat detection and mitigation systems to identify and respond to novel vulnerabilities promptly is crucial. This includes AI-specific threat modeling and real-time monitoring.
Align with Ethical Guidelines and Regulations	Ensuring that GenAI/LLM use aligns with ethical guidelines and regulatory requirements requires ensuring the model cannot be manipulated and requires a content moderation tool. Regular reviews and updates to policies can help maintain compliance and ethical standards, and need to be updated in the content moderation tool.
Prepare for Complexity Management	Anticipating and preparing for the complexities associated with managing GenAI/LLM systems involves developing comprehensive management frameworks and ensuring interoperability with existing systems.

结论

本节的研究结果表明，组织需要提高其应对与生成式人工智能/大语言模型技术相关的日益严峻的威胁的准备工作。虽然对风险有很高的认识，但准备程度的差异表明有巨大的改进空间。通过优先考虑数据隐私、加强访问控制、投资持续学习以及遵循道德准则，组织可以更好地应对挑战并抓住生成式人工智能带来的机遇。

方法论

问卷设计

标题为“2024年Ge- AI安全准备状况调查”的调查旨在全面了解企业在Ge- AI/ LLM安全准备方面的现状。该调查针对了由CISO、安全专业人员、开发者、数据科学家和其他参与Gen- AI技术部署与管理的利益相关者组成的多样化受访者群体。

调查分发

该调查通过多种渠道分发，以确保覆盖不同行业和组织规模。分发渠道包括专业网络、电子邮件邀请和社交媒体平台。为确保调查到达在 GenAI 和安全方面具有相关经验和职责的人员做出了努力。

受访者人口统计

在根据一个旨在确保受访者参与度和可靠性的注意力检查问题排除了不合格条目后，共收集了1,076份有效回复。受访者代表了各种角色和行业，确保了对GenAI安全的广泛视角。关键的统计细节包括：

- **主要角色：** 开发者（20%）、安全分析师（17%）、人工智能/大语言模型业务用户（15%）、it经理/管理员（10%）、数据科学家（9%）、首席信息安全官或其他高管级安全职位（9%），以及其他。
- **工作经验：** 超过60%的受访者拥有超过5年的网络安全经验。
- **组织规模：** 受访者来自规模各不相同的企业，其中小企业和大型企业都有显著代表性。

调查问题

这项调查包含了定量和定性问题的组合，旨在深入捕捉几个关键领域的信息：

1. **被调查人背景：** 关于初级角色的问题，网络安全经验年数，人工智能开发，以及人工智能安全。
2. **GenAI/LLM采用阶段：** 理解当前采用和实施的阶段组织内的生成式人工智能技术。
3. **对安全措施的信心：** 评估当前安全措施对不断演变的生成式人工智能威胁的置信水平。
4. **接受的挑战：** 识别采用和整合GenAI/LLM的主要挑战和障碍。
5. **遇到和管理漏洞：** 探索 GenAI/LLM 漏洞的经验，这些漏洞的性质和影响，以及应对策略。
6. **安全措施和最佳实践：** 审查组织采用的安全实践及其了解安全威胁的方法。
7. **挑战与未来方向：** 调查重大新兴威胁以及组织应对这些挑战的准备情况。

数据收集与分析

- **数据收集：使用在线调查平台在一周内收集了回复。**
- **数据清洗：** 收集到的回复进行了审查和清理，以排除不完整或不符合资格的条目。取消资格是基于对一个问题回答的，该问题旨在确保受访者参与度与数据可靠性。
- **数据分析：** 定量数据采用统计方法进行分析，以计算频率、百分比和趋势。开放式问题的定性数据被分类和总结，以捕捉关键主题和见解。

限制

虽然该调查为理解生成式人工智能安全准备状况提供了宝贵的见解，但有必要承认某些局限性：

- **采样偏差：** 调查样本可能无法完全代表所有行业或地区。
- **自我报告数据：** 回复基于自我报告的数据，这些数据可能受到偏差或不准确性的影响。
- **不断演变的威胁态势：** 快速演变的 GenAI 威胁的性质意味着这些发现代表了一个时间点的快照，并且可能需要定期更新。

贡献者

Aayush Gangwar
阿卜杜勒·拉赫
阿贝·吉萨武
亚当·阿布拉莫夫
亚当·丹科
阿德博格恩·蒂莫西
阿迪尔·曼塞博·若尤纳
Aditya Chandrakant Musale
Aditya Pathak
阿德米尔·斯科莫拉奇
阿德里亚·雷科尔特·伊·费尔南德斯
阿德里安·惠尔顿
阿德里亚娜·罗曼
阿哈马德·卢艾维
阿赫萨姆丁
爱托尔·阿斯托加·塞斯·德·维库纳
阿卡什·昆杜
阿什凯·蒙达尔
阿克沙尔·拉梅什
阿莱霍·佩雷斯·戈麦斯
亚历山德拉·杜博维克
亚历克斯·里斯波·康斯坦丁努
亚历克斯·沙皮罗
Alex V
王岚
亚历山大·迪恩
亚历山大·哈伦
亚历山大·麦登
亚历山大·辛格
阿利克西斯·斯图尔特
阿里·A.
艾伦·霍尔曼
阿曼·卡达姆
Amdjed Bensalah
阿米尔·拉德
阿米尔·乌瓦尔
阿米特什·罗尼尔·辛格
Ana Kolkhidashvili
阿纳斯塔西娅·根诺夫
阿纳托利·卡利什
阿纳托利·杰斯托夫
安德烈·苏克拉姆
安德烈亚·布拉姆比利亚
安德烈亚·里奇
安德里亚·罗哈斯·罗索
安德烈亚斯·彭格
安德烈亚斯·索菲亚迪斯
安德烈·契尔维亚谢
安德烈·阿尔菲雷维奇
安德烈亚·托尔卡
Andrew Jones
安德鲁·缪尔黑德
安德里·霍尔茨
安德鲁斯·卡瓦利乌纳斯
安迪·德贝克
阿尼什·达希亚
安吉尔·马丁内斯-泰诺尔
安妮·唐
安托万·德·朗格卢瓦
安托万·斯托克
安东·安尼·巴赫乌
安东·索尔金
安努瓦夫·辛格
Anupam Kumar
Anurag Saxena
阿德拉·塞文奇
阿瑞布·阿米尔·塔里克
阿里布·尤素福
艾瑞尔·克维亚托夫斯基
阿琼·BM
阿纳布·玛吉
阿塔坎·耶尼哈亚特
阿提特·查鲁帕坦纳波特纳普
郭图 (Atlas Guo)
奥莉西亚·米歇尔·布朗特·埃尔
亚 VIA亚哈拉罕
阿维纳斯·努塔尔帕蒂
阿维什克·杜塔
艾米里克·阿里克
贝利·道尔顿
巴克塔·埃拉马尔
巴特·德·戈伊德
beenish sámi
贝尔卡塞姆·谢尔法
本简
本·凯洛帕-约克
本泰纳
贝尼·欧格斯夕一
本吉·索雷拉
昂巴德·昂
毕沙斯·萨格尔
Blythe Nguyễn
邦尼·格林
boris vavrik
波利斯·帕尔卡
Brad Morian
Brad Smith
布拉姆·容克斯
布兰登·里特
翁贝拉
布伦登·佩奇
布鲁诺·席尔瓦
布莱安娜·戴维斯
拜伦·库齐
卡梅隆·卡朋特
卡洛·埃斯波西托
凯西·雷普
凯西·沙德维茨
钱德勒·史密斯
徐佳丽
Cheychou MouafoJunior
蔡智君
奇阿拉·福尔默
奇塔兰坎·维兰布尔
克里斯·塞尔
克里斯蒂安·费拉蒂
克里斯托弗·卢
克里斯托弗·佩蒂特
克里斯托弗·斯莫尔
查克·杜菲
Cihangir Günbay
克劳迪娅·莫尔芬
科迪·克鲁姆林
科尔姆·奥恩戈斯
康纳·布伦南
科里·墨菲
克里斯蒂娜·皮内里
柯蒂斯·钦
西普里安·基普拉加特
达恩叛逆
达格玛拉·扎瓦达
达利拉·阿乌阿贝德
达米安·克莱姆扎克
丹·古斯
丹·亨特
丹尼尔·布兰奇菲尔德
丹尼尔·卡洛·塞雷佐
丹尼尔·科因
丹尼尔·福尼瓦尔
丹尼尔·加富林
丹尼尔·亨利克·纳西门托
丹尼尔·托利
达尼埃拉·纳塔莉亚·桑切斯战斗
达尼罗·莱萨
Dave Cadoff
戴夫·伦纳德
大卫·高蒂耶
大卫·罗德里格斯
大卫·夏普
大卫·特莱尔
达维德·福里
达维德·托罗
迪恩·凯兹
杰克曼
德安·卡斯特利奇
德瓦迪亚·戈什
德博拉·埃尔兰格
深安舒·雷基
黛妮丝·谭
德万什·帕尔
Dhanush Nair
Dhaval Rajendra Suthar
Dhruva Goyal
迪伦·巴uchanan
迪维娅·奈尔
DJ Lipman
德米特里·科洛索夫

多博米拉·沃拉尔斯卡 多米尼克·斯卡菲利 多米尼克·托罗姆 多米尼克·菲兹尤凯维奇 多米尼克·乌尔西奇 丹尼·施赖伯 多维·纽曼 博尔恩·库马尔·萨哈 博士·卡里·J·利珀特 埃多ard·雷诺 埃德华（泰德）·克沃特勒 埃德温·马丁内斯二世 艾沙德·乌扎曼 艾莉-安妮·沃茨 埃马努埃尔·巴赫尔 埃米莉亚·科罗娜 埃米尔阿里·冈戈尔 恩朱·张 埃兰·乔丹 埃尔凡·霍塞尼 埃里克·科尔曼 埃里克·德米茨-海尔因 埃里克·诺德比 埃里克·斯滕贝格 艾莉丝·狄奥尼斯·萨科 埃索恩·戈登 艾沃尔奥斯·马特拉戈科 叶夫根尼·科库伊金 叶夫根尼·莫丁 艾瑟恩·索亚 菲卡杜·巴蒂斯塔 菲利克斯·莱伯 弗洛里安·利卡乌西 弗朗西斯科·洛佩斯·加西亚 弗朗索瓦·卡佩尔 弗朗克·费内利 弗雷德·罗特 V G R·沙尔韦什拉姆 加文·维达亚 加里·斯坦利 高拉夫·阿格诺特里 乔治亚·特里pathi 杰弗里·岩田 乔治·德雷塞尔

乔治·斯皮罗普洛斯 赫里特·迈耶·佐德里豪森 杰安弗兰科·罗马尼 吉赛尔·朱恩朱努瓦拉 朱利奥·加布里埃利 朱利奥·S·戈德温 维纳斯·戈迪安·佐默 格雷格·布鲁克斯 格雷格·库恩 格雷戈里·阿拉里 格雷戈里·苏 格雷森·斯塔卡普威廉姆·格罗埃尔 海达尔·乔马 霍安娜·钱伯斯 汉纳斯·兰格 哈莉恩·考尔 哈里森·马明哈里森·波普 哈希斯·马基拉朱 哈桑·谢赫泽布 海瑟·莱夫希蒂·瓦普尼乌斯 埃莱因·齐默曼 亨利·王 希曼什·雷迪 霍基·尤迪奥诺 辛-文·张 黄志翔恩贝托·蓬切 伊恩·卡瑟伯特伊格纳西奥·加维拉 伊戈尔·马利科维奇 伊达尔·古兹哈梅托夫 约阿娜·扎帕利迪 伊斯梅尔·里卡多·帕克 伊凡·帕什琴科 雅各布·菲尔德 雅各布·莱亨鲍尔 詹姆斯·德蒙格 詹姆斯·邓肯 詹姆斯·科尔林 詹姆斯·特里布

詹米·道尔顿·哈雷尔

简·赫特森

简尼克·韦登豪普

简尼克·韦登豪普

Jar Kovar

杰森·罗斯

杰森·赖特

贾斯珀特·塞米

Jasu A.

哈维尔·加西亚·阿尔雷东多

哈维尔·戈麦斯·佩雷达

简·萨默尔-沃克

Jean Gebarowski

让-皮埃尔·陶特

Jean-François Noël

杰夫·泰斯梅耶

杰夫·布朗

杰玛·盖茨

詹妮弗·塔比塔·丘基-基斯

珍妮萨·查克拉塔普胡

简斯·克罗夫瓦尔

杰里米·怀勒

杰兹·乔治·扬尼尔切克

杰西·达斯瓦尼

João Caxaria

João Miguel Garcia Teixeira

若昂·佩德罗·德·布拉甘萨

乔尔·霍坎恩

乔伊·尼尔森

乔伊·尼尔森

约翰·S·丹尼尔

约翰·格罗斯

约翰·基廷

约翰·保罗·琼斯二世

约翰逊·阿罗凯阿杜斯

乔纳斯·迪多

乔纳森·格兰特

乔纳森·梅纳

乔纳森·罗杰斯

乔丹·乔恩·布莱斯

霍尔吉·安德烈斯·帕迪拉

乔治·伊萨克·丘·瓦尔达拉马

何塞·伊格纳西奥·罗霍·里韦罗

何塞·曼努埃尔·卡多纳 Fabrega

约瑟夫·克里斯藤森

约瑟夫·索卢塔尼斯

Josh A

Josh Dean

约书亚·洛夫特斯

约书亚·奎克

约书亚·范德兰

裘德·雷

朱莉娅·兰塔

朱莉·拉斯·诺巴尔

简铁

侯俊毅

尤西·库亚苏乌

开什·汗

卡兰·卡坎瓦尼

卡琳·豪斯

卡拉·康戈森

卡罗尔·沃罗尼ak

卡尔特克斯·卡南

卡塔兹娜·迪马雷克

凯特·克莱格曼

肯凯

肯·史莫尔伍德

肯尼斯·迈尔斯

凯文·康拉德

哈利勒·吉马吉

康隆丁

黄琼英

Kieran Klukas

克劳斯·亚当胡伯

细川浩二

Konstantin Kostadinov

科斯蒂尼斯·巴尔帕斯

Konstantinos Passadis

科斯蒂斯·格古利亚斯

克里希·阿格拉瓦尔

克里蒂·谢瓦拉马尼

克拉兹沃夫·克日维尼斯基

克日什托夫·马尔采尼斯基

凯尔·贝尔彻

凯尔·威廉姆斯

拉斯·莱默尔曼

黎安忠

莱亚·格鲁比西奇

李·穆尼
李伟良
梁国兴
Leporc Mathieu
莱斯利·里奇
勒万·舒格里阿什维利
勒沃·阿约特
类似丹
林开文
里斯努·特比尔科伊·亚勒武
洛伦娜·贝拉诺
洛伦佐·法图斯
路易·菲利普·莫里尔
卢桑切斯
Luca Flora
卢卡·桑布西
卢卡斯·芬格运河
卢卡斯·帕尔马
卢西亚诺·查帕林·路易西
路德维希·西克特
路易斯·C·帕斯特
卢卡斯·罗斯特
卢克·巴尔坦汀
路克·史密斯曼
卢克·泰特尔
卢莉亚姆·特克勒
玛莉卡·布朗
麦杰伊·维切雷克
Madhavendra Thakur
马哈拉杰 M，PMP
mandy gu
马塞尔·皮珀
玛丽娜·特策拉夫
马里奥·马丁内斯
马里奥·马泰西
马里奥·斯特利亚诺乌
马克·斯科特
马尔库斯·胡普瑙尔
马塔·马泽兰尼克
马丁·戈特利·费伦扎
马丁·米尔布拉德特
马丁·桑德斯
马尔蒂诺·加韦诺
玛特娜·齐古拉斯
马尔滕·H.
佐久間工
梅森·弗朗切斯基
梅森·兰德里
马苏梅·查帕里尼娅
马蒂亚斯·萨兰德
马蒂厄·德·博尔芒
马蒂亚斯·伊亚斯
马蒂亚斯·帕格利奥尼
马特·巴克
马特·马斯特拉齐
马修·哈夫
马修·拉斯特沃夫卡
马修·罗西
周马太
马蒂亚斯·克劳夫特
马蒂厄·比劳克斯
马蒂亚·桑维托
毛里求斯·奥里斯蒂亚诺
马克斯·莱伊坦斯
利伯
马克斯·马特诺夫
马克桑斯·戈代内什
马克西姆·胡伯特
阿布·赛义德
阿什拉夫祖马努尔·布哈扬
梅根·黑斯
马赫兰·萨塔尔
梅丽莎·卡尔顿
MERT DORA GÜLEÇ
米迦·詹克
迈克尔·巴克斯-博格德
迈克尔·埃勒
迈克尔·格雷
迈克尔·克内尔
迈克尔·莱
迈克尔·莱斯特
迈克尔·佩里
迈克尔·托马斯
迈克尔·克洛普斯特拉
米哈乌·布特凯维奇
米格尔·贝夫尔德
刘明
米罗斯拉夫·切尔马克
米罗斯拉夫·佩特里克
穆罕默德·埃尔·马赫迪·德巴格
穆罕默德·伊尔凡
穆罕默德·阿赫拉姆·汗
穆罕默德·阿克希尔
穆罕默德·巴图安·贝尔克
Munnangi Sravya
穆斯塔法·尤素夫·塞尔特凯亚
迈尔斯·巴尼
姓名 Amit Kumar
纳西姆·哈默
娜塔莉亚·索科洛夫斯卡娅
娜塔莎·J·史蒂尔曼
纳撒尼尔·柯林斯
内森·里斯
Nathan Virot
涅哈·库马尔
尼欧·萨克斯纳
尼滨·菲利普
никос цагкас
尼古拉·雅各布斯
尼古拉斯·冈达尔
尼基萨·马塔
尼尔斯·海尔伯格
宁纳德·施林加普尔
尼尔·戈特利布
Nir Kligsberg
尼斯奇特·R
诺曼·莱默
奥利弗·富勒
奥利弗·P·梅奥
奥尔扎斯·耶加利
奥默·塔尔米
奥姆卡尔·乌基尔德
奥努尔·卡兰
奥雷尔·恩德斯
奥雷斯提斯·乌苏尔特索格卢
奥利安·克雷布斯
奥斯卡·加西亚
奥斯卡·萨特
奥斯曼·塔图罗卢
欧文·托阿迈因
帕布罗·纳瓦罗
帕布罗·萨迪内沃伦
帕纳约蒂斯·克拉里诺莫斯
帕拉斯·罗瓦特
帕特里克·霍德
帕特里克·穆伦
帕特里克·舒勒
保罗·雅各布斯
保罗·拉森
保罗·门德尔森
保罗·马尔孔
保罗·莫塔
帕万德普·辛格
帕维尔·杰尔诺夫
帕维尔·祖巴列夫
帕维尔·卢蒂
波瓦夫·莫热克
保瓦·帕扬克
佩德罗·亨利克·阿马拉尔桑托斯
佩德罗·霍阿金
佩德罗·洛佩斯
佩德罗·卢卡斯·戈麦斯
佩尔·科林斯
奥拉夫·斯特里肯·豪格
彼得·卡尼
彼得·西卡科洛
彼得·亨迪
彼得·拉约什
皮特·德·布罗因
皮奥特·莱纳尔特克
皮奥特·齐。
皮尤什·苏拉纳
普拉门·米特夫
普贾·H·P
Poojan Vachharajani
普拉杰瓦·斯里尼瓦斯
帕兰苏·马尔霍特拉
辛格王子
昆汀·卢瓦瑟
拉胡尔·辛格
瑞秋·肯特
拉斐尔·科尔特斯
拉希姆·卡纳尼
拉胡尔·库马尔
拉尔夫·奥阿德

拉曼·塔库尔 拉斐尔芭蕾舞团 拉斐尔·萨布兰 拉乔特·布拉尔 雷吉娜·格里芬 雷姆科·容沙普 雷米亚·普拉维恩 理查德·盖克勒哈尔 理查德·波茨 瑞利·威廉姆斯 罗布·奥康纳 罗伯特·芬 罗伯特·马歇尔 罗宾·雨果 罗宾·伯特兰 罗德里戈·马蒂亚斯·阿瓦雷斯 伊加萨巴尔 罗根·拉卡尼埃塔 罗汉·巴贾杰 罗曼·巴克乌里德泽 罗恩·辛 勒什曼·拉蒂亚 罗伊·魏斯菲尔德 瑞安·布朗 瑞安·麦康奈尔 瑞安·彭 萨根·拉杰 萨米尔·夏尔马 桑德拉·埃尔斯顿 萨尼·迪亚亚 Санъяй·桑卡兰 萨吉德·哈桑 圣地亚哥·赞纳拉-贝古ند利恩 萨拉尼亚·米纳德恰苏拉-拉姆 萨特维克·库图鲁 萨图·米亚纳·科尔霍内 索亚姆·纳格帕尔 赛韦尔·米勒 希恩·默多克 西尔维安·波泰博斯 塞琳·埃尔丁 塞尔吉奥·巴霍·纳瓦罗 塞尔吉奥·鲁伊斯 沙夫卡特·哈桑

山恩·马丁

沙贝尔·保罗·罗塞尔

Shaswat Deep

山努克·查托帕迪亚希

施洛摩·塔诺尔

施穆利克·罗森

寿尔雅·德

董雷耶斯·东雷

米尔斯

西格玛·埃斯克森森

西蒙娜·坎奇安

西蒙娜·道斯沃特

斯诺尔·法格兰德

索拉娅·瓦内萨·卢西奥·达·席尔瓦

索伦·赫尔姆斯

索林·贝蒂什尔

Souradip Mookerjee

斯坦·贝丁克豪斯

斯蒂芬·利特曼

斯特林·格里戈

斯迪夫·格拉罗

苏内·奥尔内马克·莱格德曼

苏万·巴纳吉

斯瓦斯蒂克·米什拉

赛义德·穆罕默德·扎因·乌尔阿比迪恩

西尔维斯特·卡纳德

泰迪·贝森

tensagram/eddie dean

天使仁心

-thanassis thomopoulos

西奥

蒂博·费朗

托马斯·巴伯

托马斯·伍尔夫

蒂亚戈·阿尔梅达

提亚戈·基尔

蒂莫西·艾奇森

赵婷婷

托比亚斯·赛贝尔

汤姆·克尔斯滕

汤姆·萨姆森

托马斯·哈拉米切克

托马斯·什维通

托马斯·维斯利基

陶宁

特拉维斯·德普伊

Trishit Debsharma

Trucy Petter

泰勒·阿尔梅达

乌古尔·奥兹厄兹

乌迈尔·侯赛因

昂梅什·班德卡尔

Uri Danan

瓦伦·塔利亚布埃

瓦利·伊里米亚

Vamsi KrishnaBonam

瓦伦·苏达珊南

维丹·戈萨维

维克托·里瓦斯

Vignesh Venkatachalam

维什尔·古普塔

维韦纳特·斯里尼瓦桑奇拉瓦里

维韦克·维诺德·夏尔马

弗拉基米尔·拉斯托波钦斯

Vyshnav Premlal Njattuketty

沃尔特·萨根特

韦恩·比尔曼

维拉瓦特·帕万维瓦特

希尔·奇尔卡特

威廉·比蒂

威尔逊·胡安

怀亚特·哈维

亚轩龙

亚科夫·凯瑟曼

杨安宜

Yash Kiran Marathe

叶莲娜·哈尼亚

伊尔马兹·巴里斯·卡普兰

约丹诺斯·T·莱格赛

约塔姆·德凯尔-齐尔戈夫

刘亮亮

尤内斯·奈特·乌夫基尔

玉塞尔·库尔特巴斯

尤里·赫克特

扎卡里·齐布拉特

扎科里·鲍威尔

扎克·布代

赛德·马鲁夫

珍熊·李铭·奥莫费·佐尔坦·萨戈迪·宗泽·吴·兹沃尼米尔·佩特科维奇