

2026 年网络安全现状

全球劳动力、资源与网络安全运营更新报告



目录

4	执行摘要
4	调查方法
6	网络安全人才队伍考量
	7 / 招聘与职位空缺
	10 / 职业倦怠与人才留任
15	人才梯队
	16 / 技能缺口
20	网络安全运营
	21 / 预算
	22 / 董事会与网络安全优先事项
23	网络风险与网络攻击
	27 / 网络风险
29	AI 与网络安全
34	结论：网络安全承压，正值关键转折期
36	致谢

内容摘要

《2026 年网络安全现状：全球劳动力、资源与网络安全运营更新报告》呈现了 ISACA 年度全球网络安全状况调查的结果，该调查于 2026 年第二季度进行。本调查报告重点呈现网络安全人才招聘、人员配置和预算趋势，以及网络风险与威胁、网络安全运营和人工智能（AI）在网络安全工作中的作用。部分调查结果与往年基本一致，但也有一些结果显示，网络安全运营和整体人才队伍趋势正在发生显著变化。

执行摘要

ISACA 全球网络安全状况调查已连续开展十二年，聚焦网络安全领域面临的挑战、发展趋势与机遇。今年的调查报告重点分析网络安全技能、人才招聘与预算、网络风险，以及人工智能（AI）在网络安全领域的作用。

部分调查结果与去年基本一致，另一些结果则显示，网络安全专业人员的工作方式正在发生变化。今年的调查受访者对 AI 给网络安全带来的影响，以及网络安全专业人员日益扩大的技能缺口表示担忧。

主要发现包括：

- 网络安全人才队伍的工作压力依然居高不下。68% 的调查受访者表示，过去五年来，其工作压力有所增加。这一比例较 2024 年和 2025 年的 66% 略有上升。日益复杂的威胁形势是工作压力增加的首要原因。将其列为压力来源的受访者比例从 2025 年的 63% 上升至 2026 年的 71%。这一变化与此前的趋势形成反差：2024 年至 2025 年，将这一因素列为压力来源的受访者比例曾下降 18 个百分点，从 81% 降至 63%。
- 软技能仍是网络安全专业人员最突出的技能缺口，但报告存在这一缺口的企业比例今年有所下降（2025 年为 59%，2026 年为 57%）。调查结果显示，LLM

SecOps 已成为第二大技能缺口（45%），较 2025 年的 33% 大幅上升。

- 今年，最重要的五项安全技能有所调整。数据安全继续位居首位，而云计算跌出前五，取而代之的是事件响应。优先级最高的技术技能主要聚焦于降低核心风险，包括数据安全（56%）、威胁检测与响应（54%）、漏洞管理（53%）、身份与访问管理（51%）以及事件响应（49%）。
- 受访者指出的安全专业人员最重要的软技能与去年一致，但认为这些技能重要的受访者比例均有所上升。排名前五的软技能分别是批判性思维（59%）、沟通能力（57%）、问题解决能力（53%）、团队合作能力（47%）以及适应能力/灵活性（43%）。
- AI 在安全运营中的应用正在加速，但 AI 治理和事件响应的成熟度仍明显偏低。AI 在安全运营中的主要应用场景包括自动化威胁检测与响应（41%）、自动执行日常安全任务（40%）以及端点安全（33%）。13% 的企业尚未在安全运营中应用 AI。
- AI 相关准备工作尚未跟上 AI 应用的步伐。仅 8% 的企业定期开展 AI 相关事件响应演练。随着 AI 在安全运营和攻击者战术中的应用日趋常态化，企业的相关准备能力与实际需求之间正逐渐形成差距。

调查方法

2026 年第二季度，ISACA 面向全球网络安全专业人员发出在线调查邀请。受邀者包括持有 ISACA 注册信息安全经理认证（CISM）的专业人员，以及职位登记为信息安全相关岗位的 ISACA 会员。

调查涵盖以下领域：

- 人员配置与技能
- 安全运营
- AI
- 网络安全预算
- 网络攻击与网络威胁
- 网络风险与障碍

共有 1,888 名受访者完整完成了调查问卷，其回答均纳入本报告。本次调查在 95% 置信区间内的误差范围为 $\pm 2\%$ 。调查数据匿名收集，每个问题的回复率各不相同。

在所有受访者中，56% 表示网络安全是其主要专业职责领域。

图 1 展示了调查受访者的人口统计信息，图 2 展示了受访者所代表的行业。

图 1: 受访者基本情况

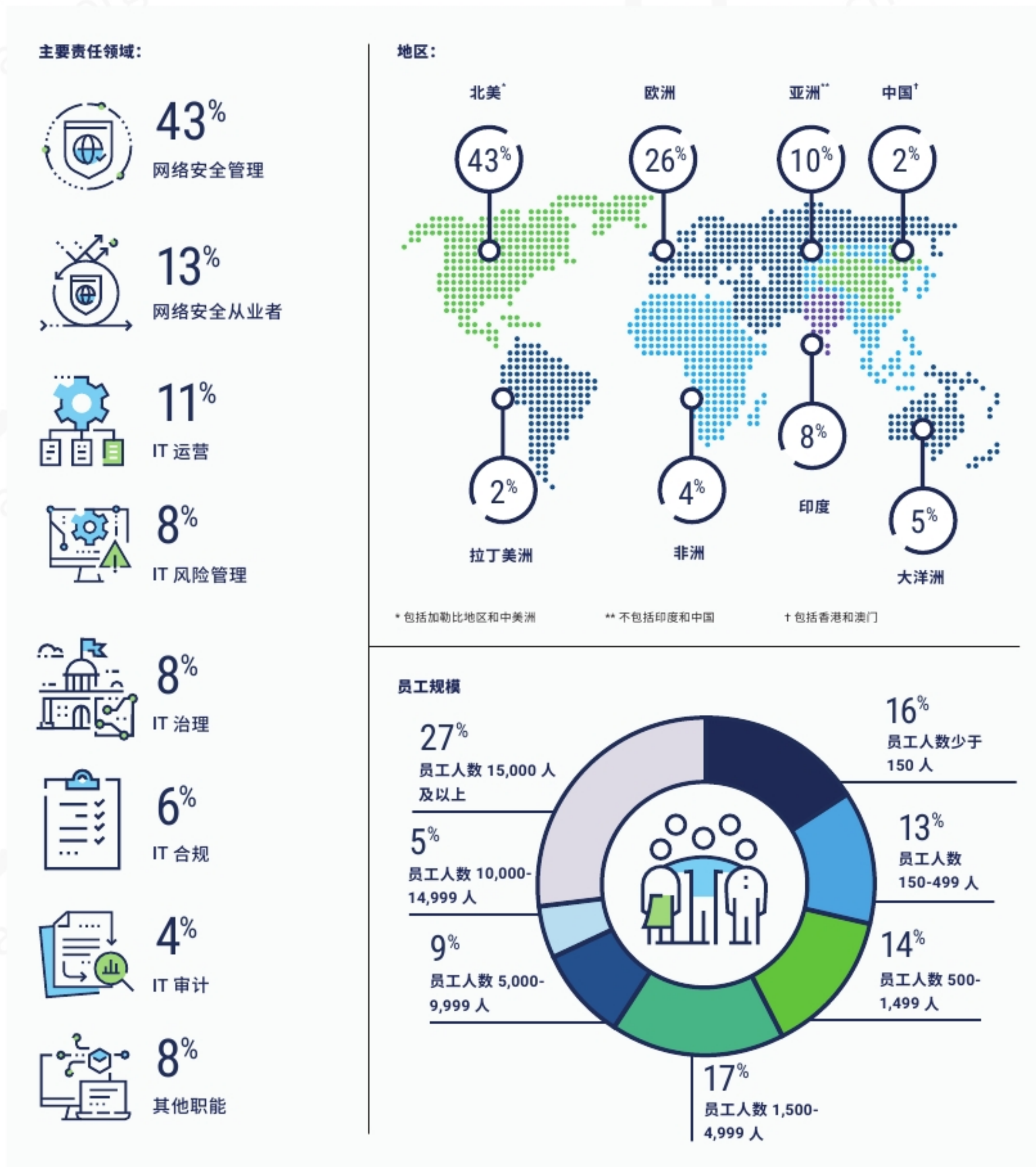
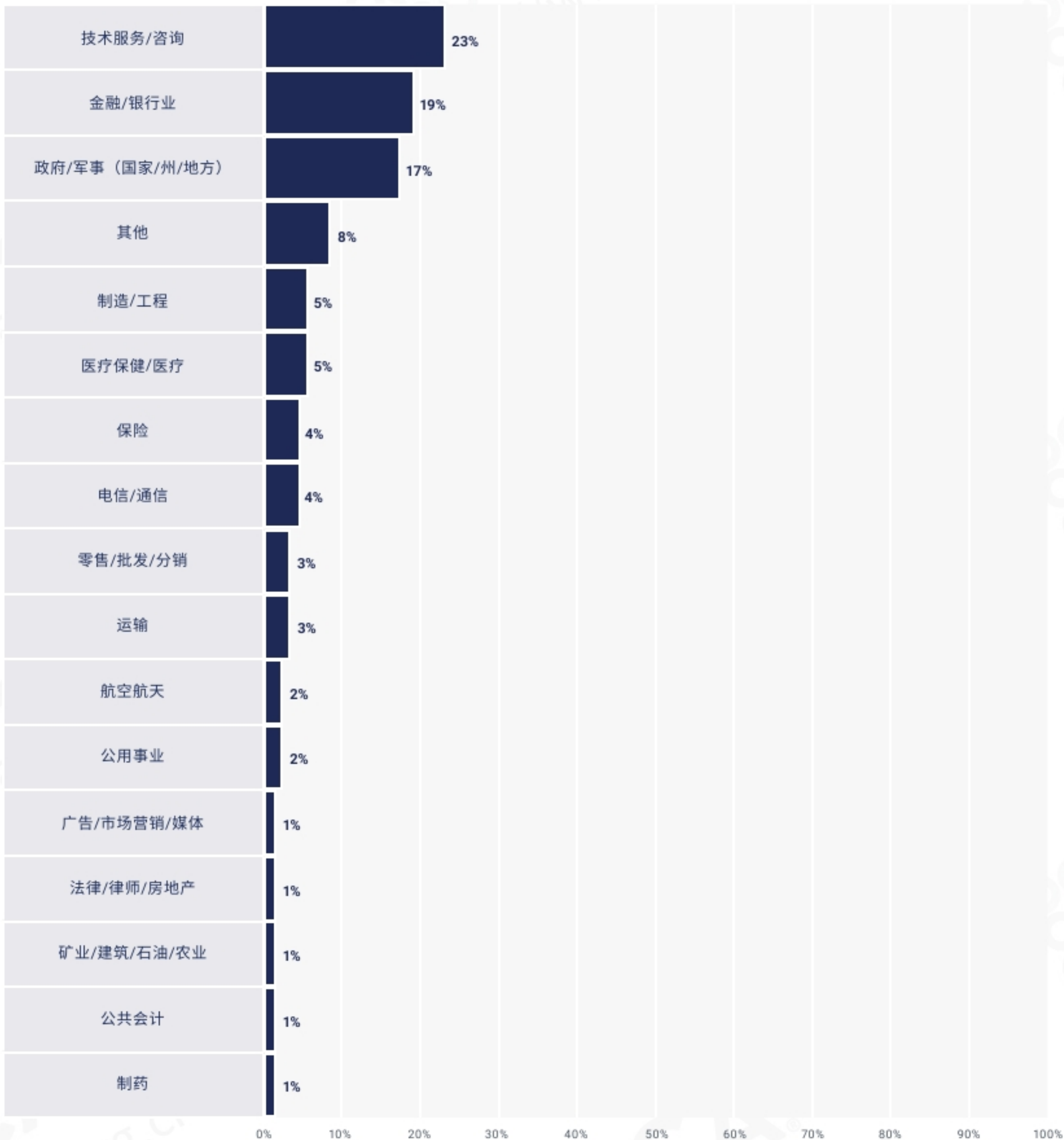


图 2：代表的行业

请说明贵组织所在主要行业。



网络安全人才队伍考量

与往年一样，越来越多的受访者对网络安全人员配置表示担忧。58% 的受访者表示，其网络安全团队人员不足，较去年的 55% 略有上升。

在员工人数为 500 至 10,000 人的企业中，网络安全人员短缺问题更为突出，60% 的受访者表示其网络安全团队人员严重不足或有所不足。

认为网络安全团队人员配置合理或人员过剩的受访者比例与过去两年基本持平。安全团队人员规模中位数保持不变，仍为 8 人。

招聘与职位空缺

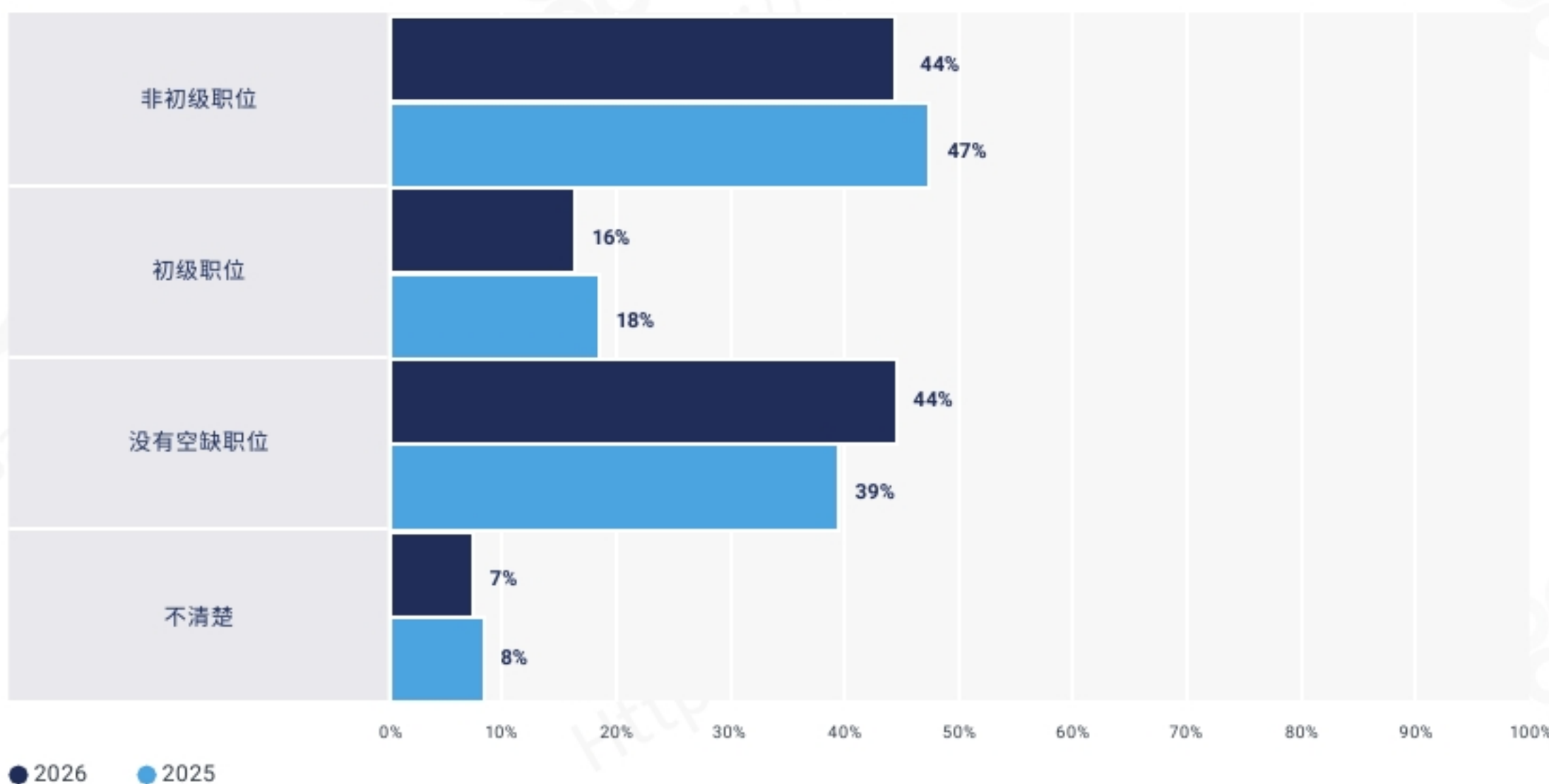
近半数（49%）的受访者表示，其所在企业存在网络安全职位空缺。值得注意的是，表示没有职位空缺的企业比例较去年上升 5%。图 3 展示了存在网络安全职位空缺的企业比例及空缺职位的

级别。与 2025 年相比，存在初级职位空缺的企业比例下降 2%，存在非初级职位空缺的企业比例下降 3%。

无论职位级别如何，招聘到最符合要求的网络安全人才仍需要较长时间。对于初级职位，38% 的受访者表示，通常需要三至六个月才能招聘到合格人才；12% 的受访者表示，招聘过程平均需要六个月以上。

图 3：职位空缺

贵组织是否有尚未填补（空缺）的网络安全职位？



非初级职位的招聘周期略长。在受访者中，40% 表示招聘到合格人才填补此类职位需要三至六个月，24% 表示需要六个月以上。调查结果显示出一定的地区差异：亚洲和欧洲分别有 28% 和 30% 的受访者表示，填补非初级职位空缺需要六个月以上。

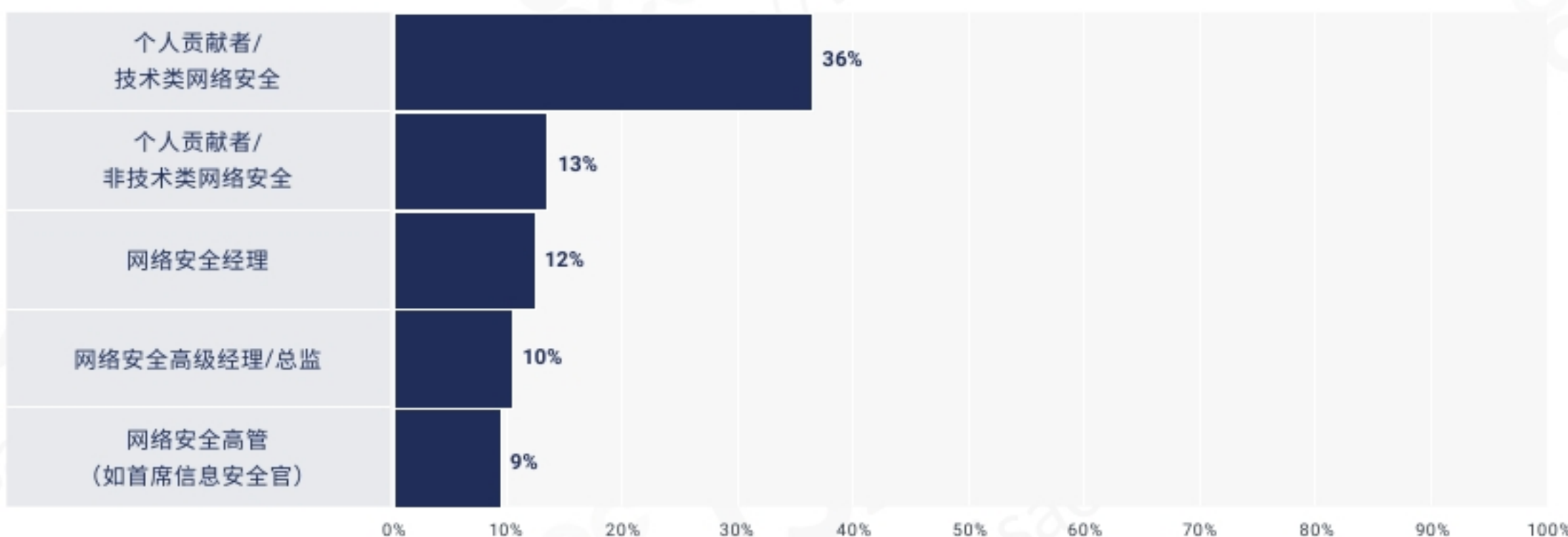
就网络安全职位空缺的整体招聘周期而言，22% 的受访者表示招聘周期有所延长，44% 表示基本

不变，17% 表示有所缩短。与去年相比，这些数据略有变化：去年有 21% 的受访者表示招聘周期有所延长，43% 表示基本不变，17% 表示有所缩短。

图 4 展示了受访者所在企业大部分或全部网络安全职位空缺所处的职级。

图 4：网络安全职位空缺职级

贵组织在以下级别有多少未填补（空缺）的网络安全职位？百分比为选择“全部”或“大部分”的受访者占比。



对许多企业而言，吸引具备所需网络安全专业能力的求职者仍非易事。仅 31% 的调查受访者表示，大多数网络安全职位求职者都具备所申请职位所需的资质；23% 的受访者表示，符合其要求的求职者比例不超过 25%。

图 5 展示了网络安全专业人员在评估候选人是否符合任职要求时非常看重的因素。调查受访者表示，候选人需要具备较强的适应能力（67%）、拥有网络安全相关工作经验（62%），并与组织相契合（61%）。紧随其后的重要因素是持有相关认证（34%）。

调查结果也凸显了人脉推荐的重要性。18% 的受访者表示，在评估候选人是否符合空缺职位的任职要求时，来自前雇主以外其他人士的推荐非常重要，其重要性略高于前雇主的推荐。人脉推荐尤为重要，因为利用 AI 筛选候选人的现象越来越普遍，而研究表明，一些筛选方式可能存在偏见，在某些情况下甚至会阻碍候选人进入后续招聘环节。¹

人脉推荐尤为重要，因为利用 AI 筛选候选人的现象越来越普遍，而研究表明，一些筛选方式可能存在偏见，在某些情况下甚至会阻碍候选人进入后续招聘环节。

最受重视的前三项因素与其他因素之间存在明显差距，这表明，与其他一些因素相比，适应能力、网络安全相关工作经验以及与组织的契合度更能体现候选人是否符合任职要求。

预计不同资历级别的网络安全职位需求将呈现不同变化。如图 6 所示，对网络安全一线技术专业人员的需求最有可能增加。

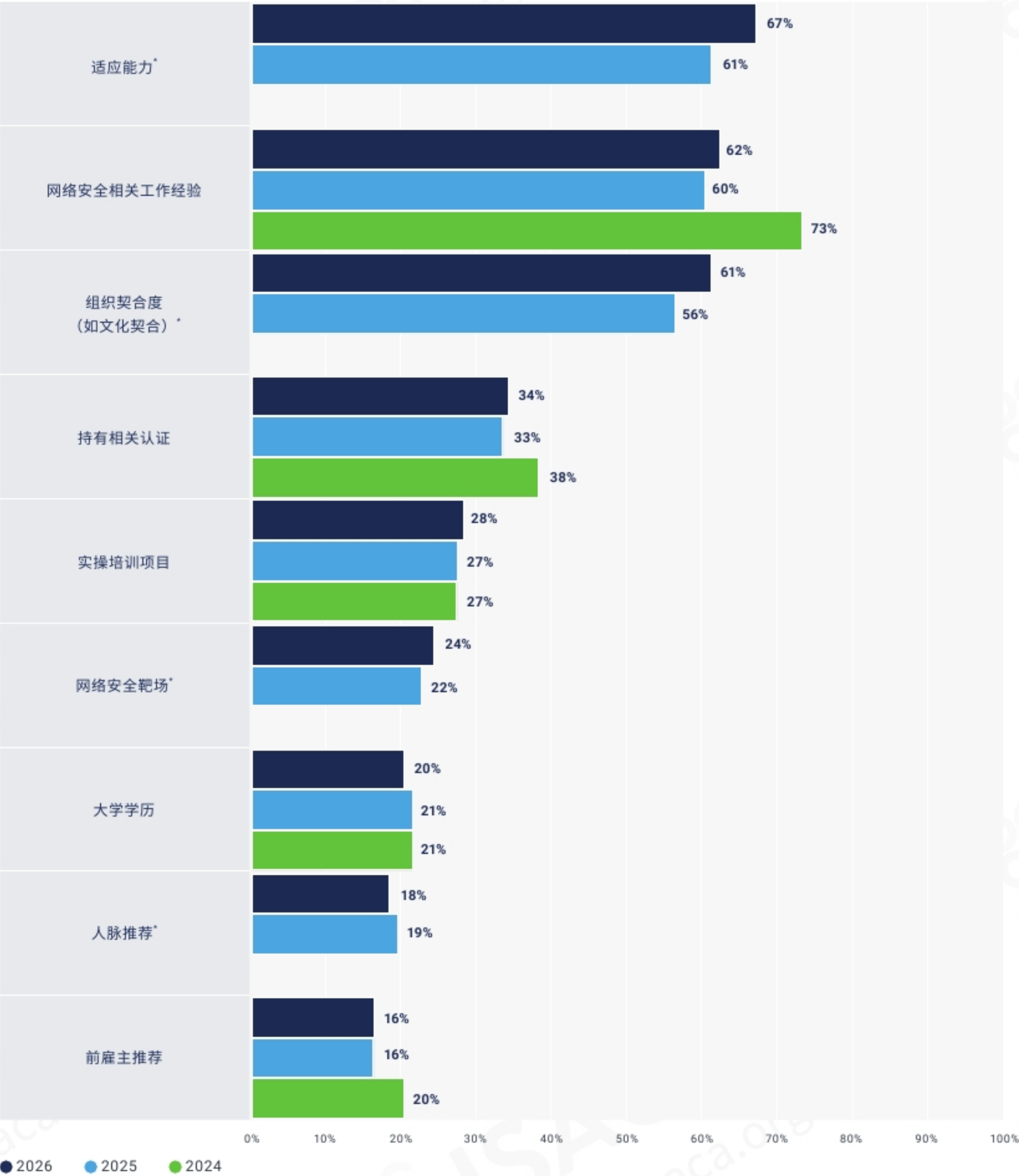
非技术从业人员和管理层岗位配置的调整，可能与 AI 的应用、对安全运营中的 AI 应用进行人工监督的需求，以及为应对日益加剧的攻击活动而增加技术开发与维护人员有关。²

1 Bommasani, R.; Bana, S. 等；《招聘中的算法单一化》，《2026 年 ACM 公平、问责与透明度会议论文集》，2026 年，<https://digitaleconomy.stanford.edu/publication/algorithmic-monocultures-in-hiring/>

2 Salvi, V.；《AI 如何为更多人才打开网络安全领域的大门》，世界经济论坛，2026 年 5 月 5 日，www.weforum.org/stories/cybersecurity/how-ai-could-open-up-cybersecurity-to-a-wider-workforce/

图 5：候选人资质评估因素

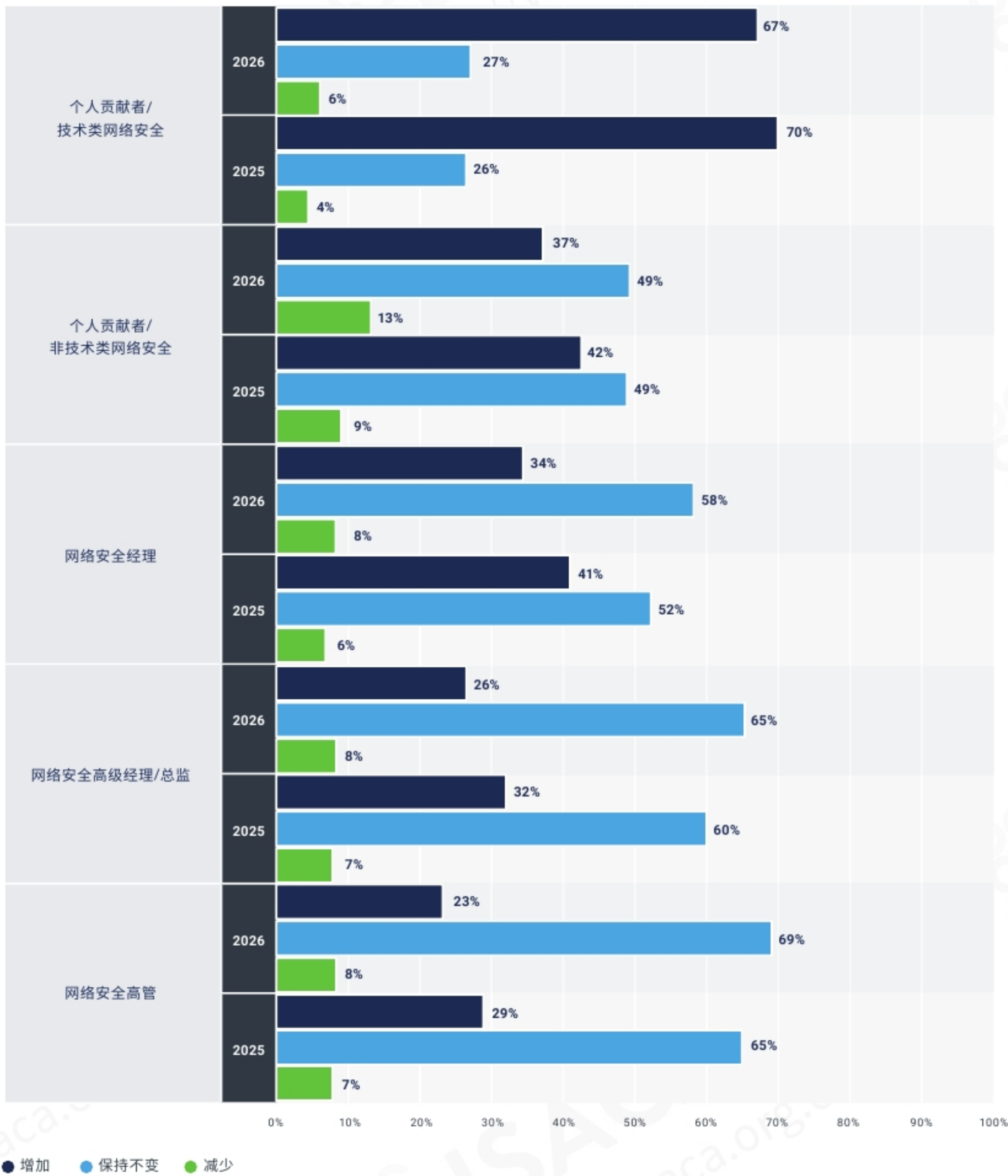
在判断网络安全职位候选人是否符合任职要求时，以下各项因素的重要程度如何？
百分比为认为这些因素“非常重要”的受访者占比。



* 2025 年调查新增因素

图 6：网络安全职位预期需求

未来一年，您认为以下各职级网络安全职位的需求将增加、减少还是保持不变？



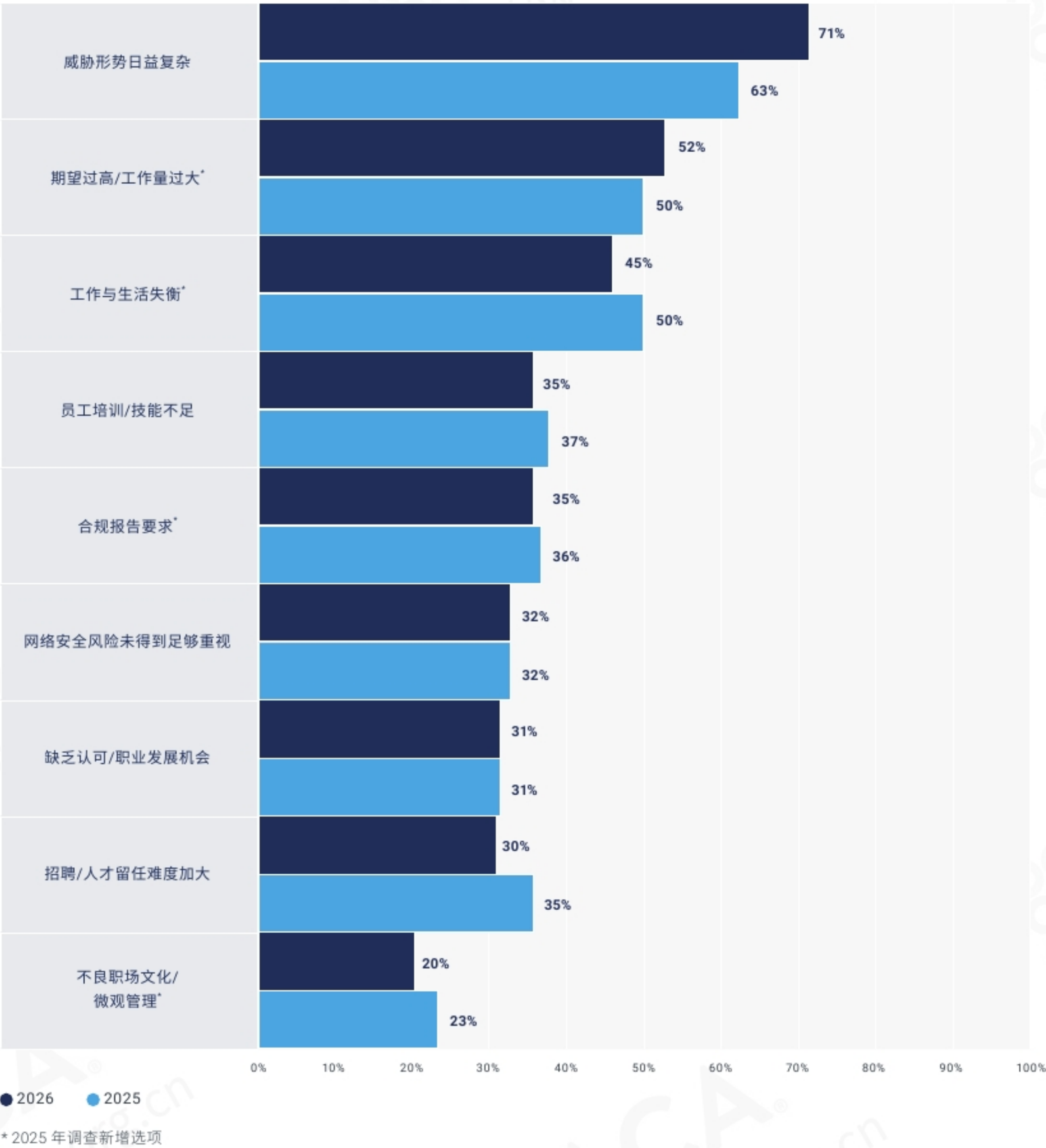
职业倦怠与人才留任

大多数调查受访者表示，与五年前相比，如今的工作压力更大，这与去年的调查结果一致。40%

的受访者表示，与五年前相比，如今的工作压力“显著增加”，高于去年的 37%。图 7 列出了如今网络安全工作压力增加的主要原因。

图 7：工作压力来源

请说明为什么与五年前相比，如今您的工作压力更大。



日益复杂的威胁形势仍是最主要的压力来源（71%），其影响在 2025 年有所下降后再次上升。今年，将工作与生活失衡视为压力来源的受访者比例下降了 5%，这可能表明雇主正在采取措施，帮助员工更好地平衡工作与生活。招聘和人才留

任方面的挑战（30%）继续呈改善趋势，较 2025 年下降 5 个百分点，较 2024 年下降 15 个百分点。高压压力引发的员工职业倦怠是许多企业关注的问题。

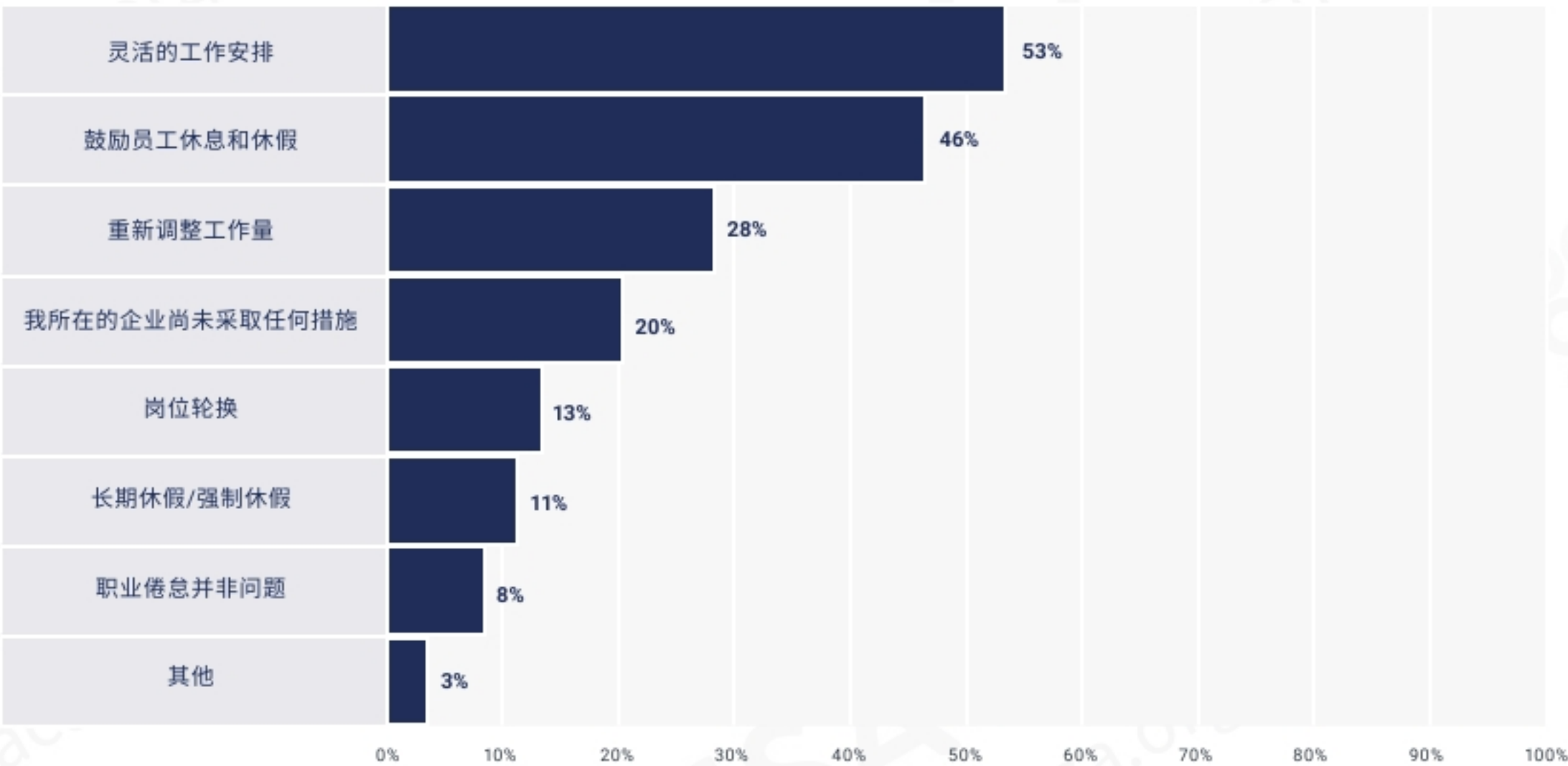
高压力引发的员工职业倦怠是许多企业关注的问题。

调查受访者表示，雇主主要通过两种方式缓解职场压力——提供灵活的工作安排（53%）以及鼓

励员工休息和休假（46%）（图 8）。尽管健康研究³ 通常建议增加休息和休假时间，以缓解压力并帮助员工恢复精力和专注力，但不同地区为此提供的时间存在差异。⁴

图 8：员工职业倦怠缓解措施

贵企业采取了以下哪些措施来缓解员工职业倦怠？



表示难以留住合格网络安全专业人员的受访者比例上升至 55%（图 9）。这一结果扭转了此前人才留任难度持续下降的趋势：从 2022 年的 60% 持续降至 2025 年的 50%。鉴于全球各地就业市

场存在差异，不同地区的人才留任难度也有所不同（图 10）。北美地区面临的人才留任挑战最少，而在非洲、拉丁美洲和亚洲，人才留任则是受访者面临的一大挑战。

3 Giridharan, S.; Pandiyan, B.; 《最大限度促进恢复：频繁休假在提升幸福感与工作表现方面的优势》，Cureus, 第 17 卷, 2025 年第 7 期, www.cureus.com/articles/385949-maximizing-recovery-the-superiority-of-frequent-vacations-for-well-being-and-performance

4 平等未来 (Equal Futures), 《带薪年假与每周休息日》, 《平等未来基础简报系列》, 2026 年 6 月, https://www.equalfutures.org/sites/default/files/2026-06/EqualFutures_RightToPaidTimeOff_30Jun26.pdf

图 9：人才留任难度（2020-2026 年）

贵组织在保留合格网络安全专业人员方面是否遇到困难？

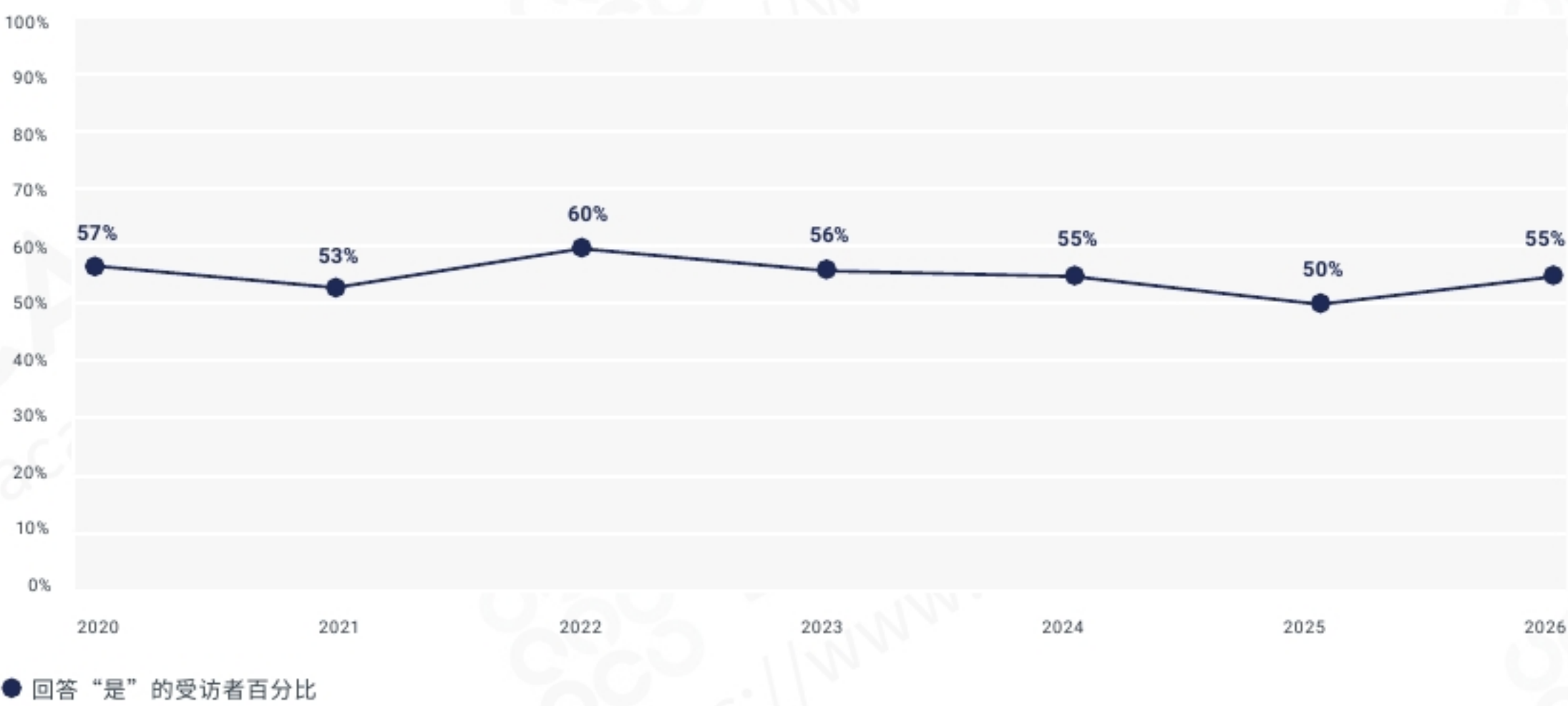
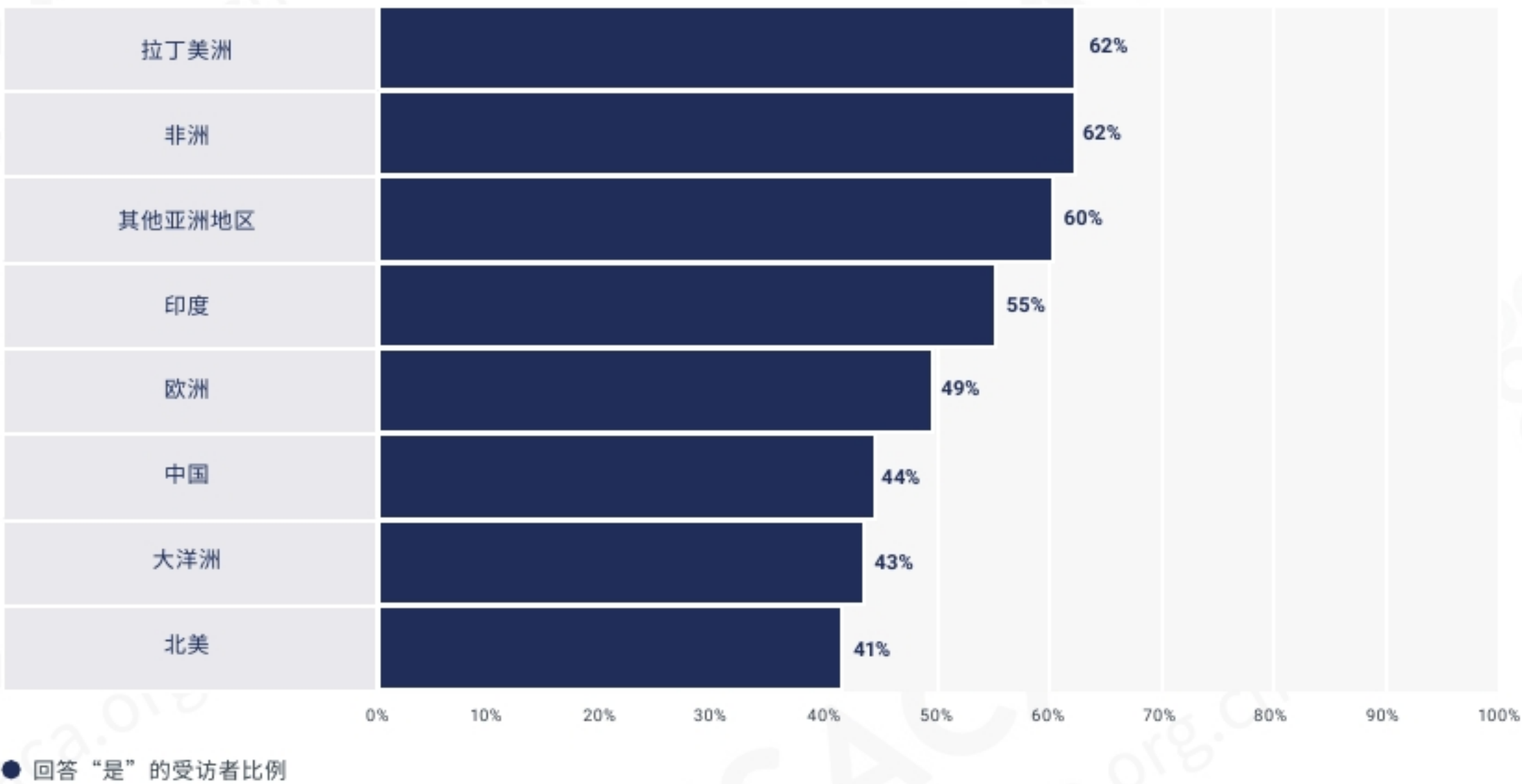


图 10：按地区划分的人员保留难度

贵组织在保留合格网络安全专业人员方面是否遇到困难？



网络安全工作的性质往往会形成高压的工作环境，因为从业者通常需要时刻警惕潜在的攻击活动。⁵网络安全专业人员选择离职的三大原因分别是工作压力大（52%）、晋升和发展机会有限

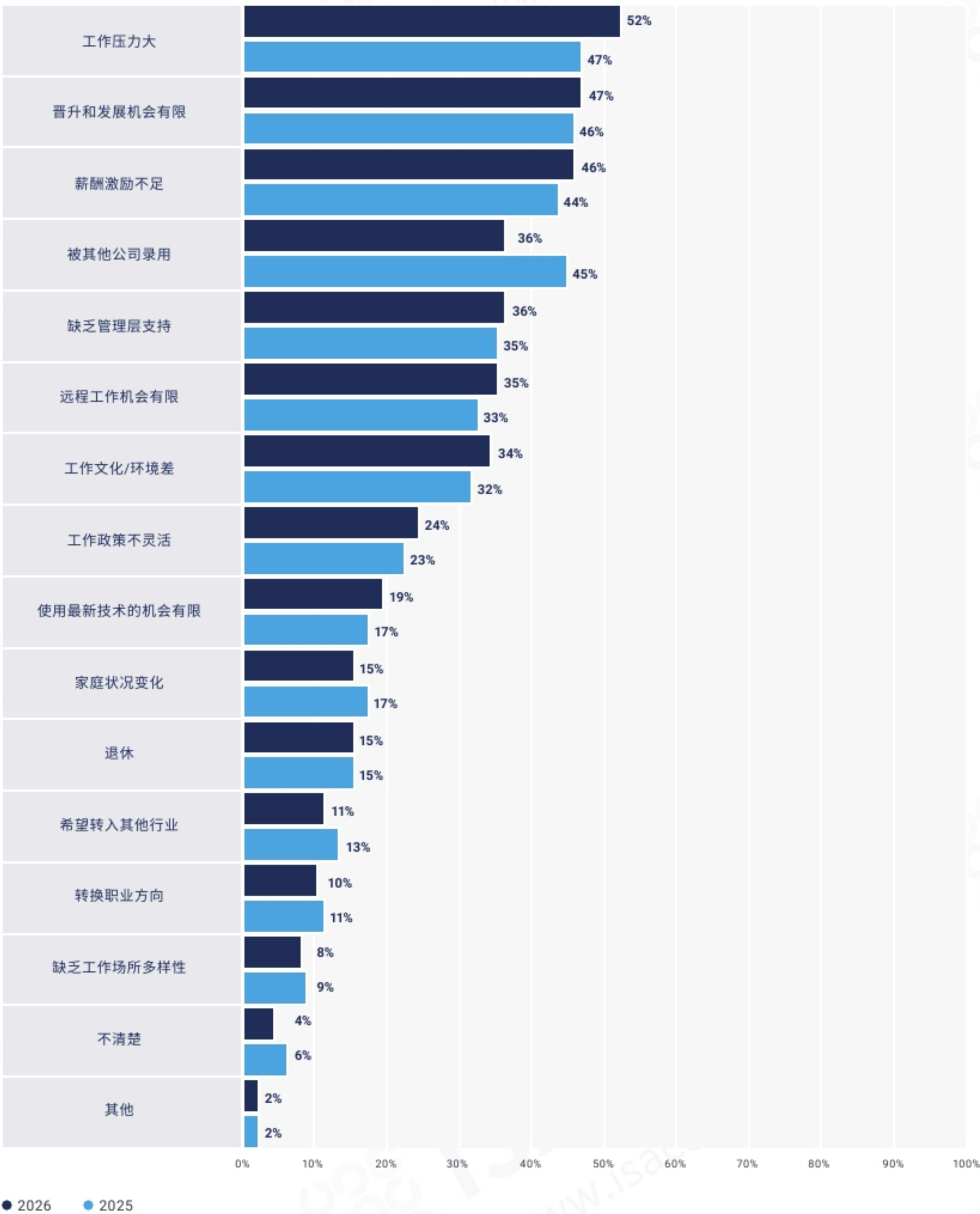
（47%）以及薪酬激励不足（46%）。35% 的受访者表示，缺乏远程办公选择会导致人才离职。

图 11 列出了可能导致网络安全专业人员离职的全部原因。

5 Nobles, C.; 《网络安全领域的压力、职业倦怠与安全疲劳：一个人为因素问题》，《HOLISTICA——商业与公共管理杂志》，第 13 卷，2022 年第 1 期，第 49-72 页，<https://www.semanticscholar.org/paper/Stress%2C-Burnout%2C-and-Security-Fatigue-in-A-Human-Nobles/3f00a50f9515f28b5469ee0fee394e4187ce0f7b>

图 11：离职原因

您认为以下哪些因素（如有）会导致网络安全专业人员离开当前职位？

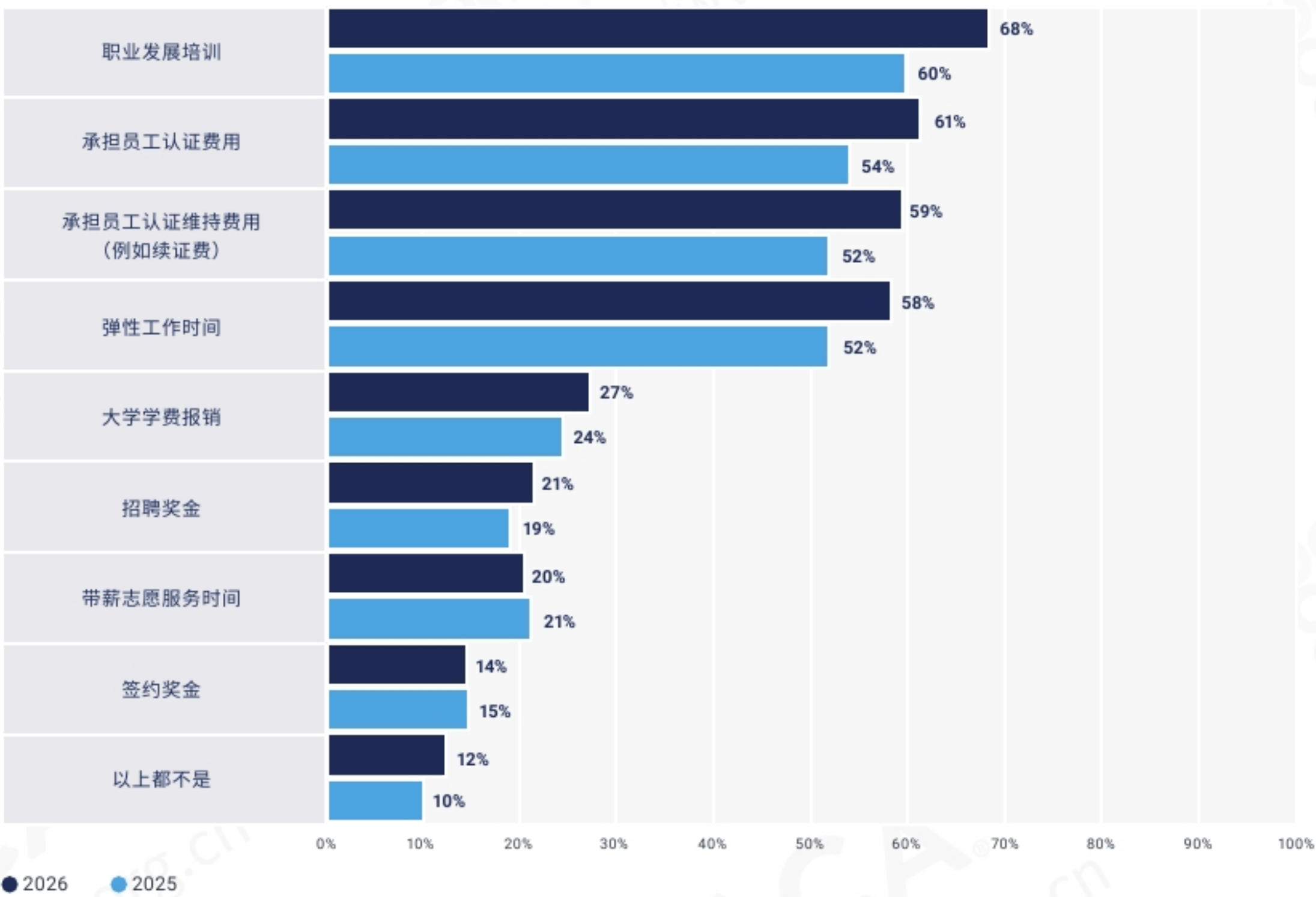


从雇主提供的各项福利来看（图 12），职业发展和认证相关支持最为普遍，且提供比例持续上升。职业发展培训的提供比例从 2025 年的 60% 上升至 2026 年的 68%，认证费用支持从 54% 上升至 61%，认证维持费用支持从 52% 上升至 59%。

提供弹性工作时间的比例也从 52% 上升至 58%，而学费报销、招聘奖金、带薪志愿服务时间和签约奖金等福利仍相对较少。总体而言，调查结果表明，雇主在员工福利策略中正更加重视技能发展和认证支持。

图 12：雇主福利

您的雇主提供以下哪些福利？请选择所有适用项。



无论是通过职业发展培训还是专业认证提升技能，都是雇主为网络安全专业人员提供的主要福利之一。

无论是通过职业发展培训还是专业认证提升技能，都是雇主为网络安全专业人员提供的主要福利之一。

根据调查受访者的反馈，技能提升经费主要来自：

- 运营预算（40%）
- 视具体情况由运营预算和人力资源预算共同承担（36%）
- 人力资源预算（13%）

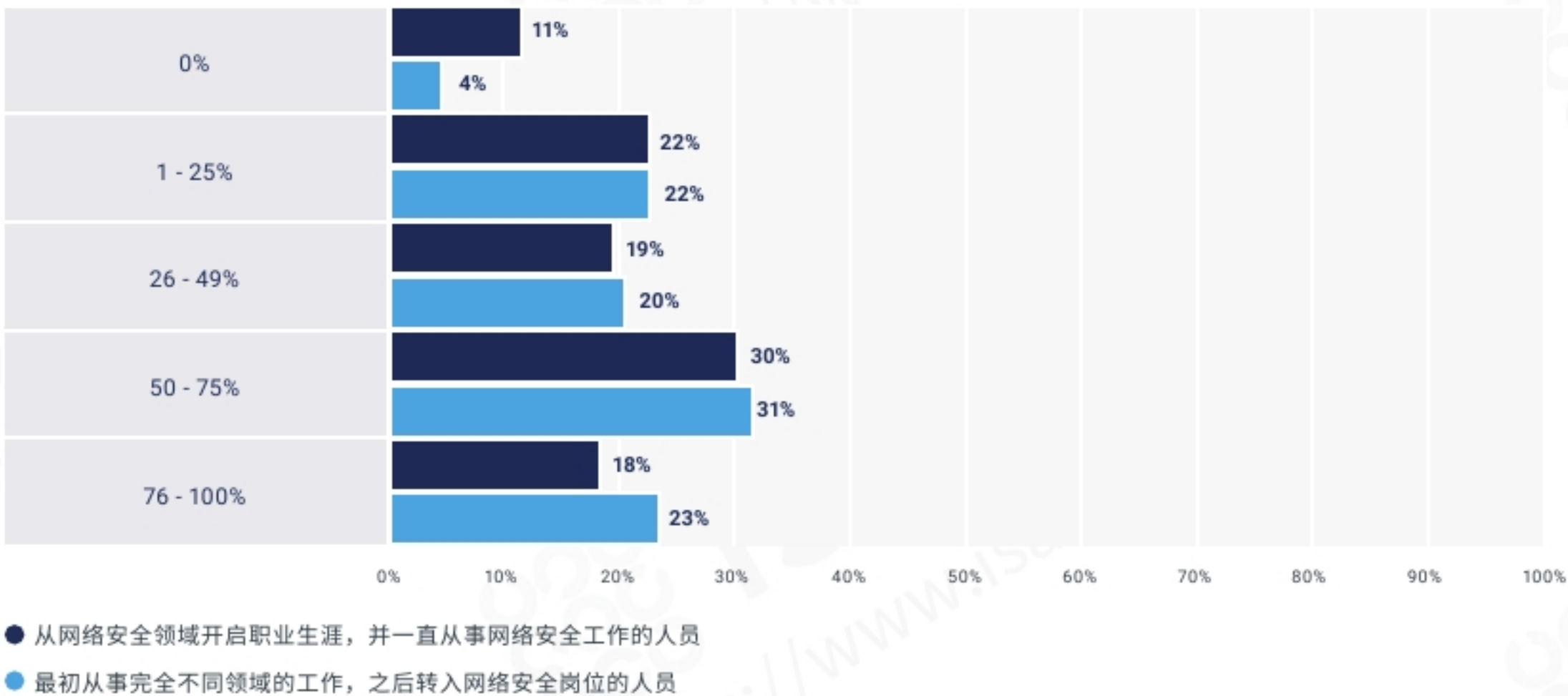
人才梯队

进入网络安全领域的职业路径多种多样。48% 的受访者表示，其网络安全员工中有一半或以上从网络安全领域开启职业生涯，并一直从事网络安

全工作至今；54% 的受访者表示，其网络安全员工中有一半或以上最初从事完全不同领域的工作，之后转入网络安全岗位（图 13）。

图 13：网络安全员工职业背景

您的网络安全员工中，以下各类人员分别占多大比例？



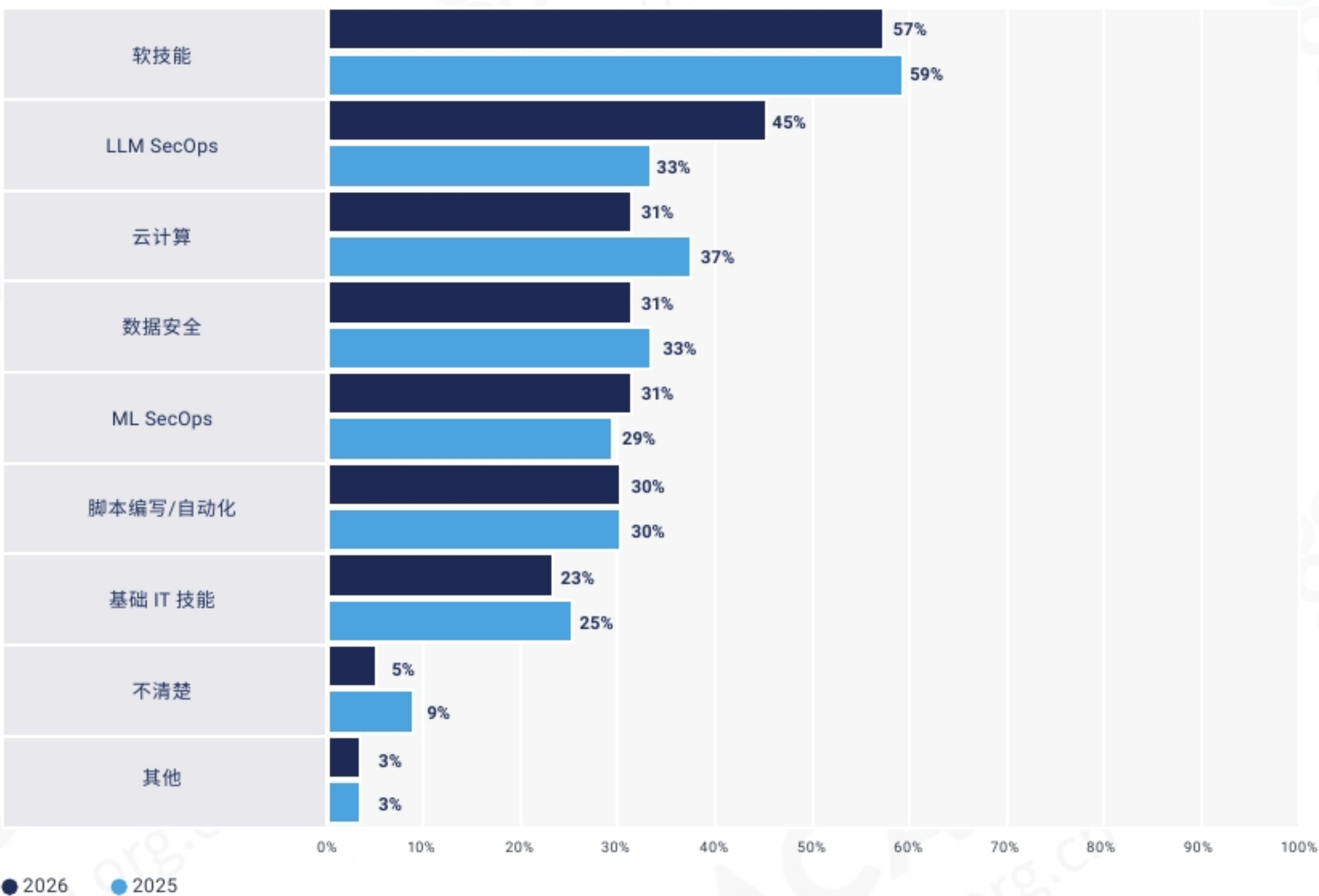
技能缺口

AI 已显著改变了调查受访者所观察到的网络安全专业人员技能缺口。2026 年，45% 的受访者认为 LLM SecOps 存在技能缺口，较 2025 年上升

12 个百分点，较 2024 年上升 21 个百分点。今年，软技能再次位居首位，57% 的受访者认为这是网络安全专业人员最突出的技能缺口之一（图 14）。

图 14：当前网络安全专业人员的技能缺口

您认为当前网络安全专业人员最主要的技能缺口有哪些？



软技能仍受到安全专业人员的高度重视。

软技能仍受到安全专业人员的高度重视。

安全专业人员最需要具备的五项软技能是：

- 批判性思维：59%
- 沟通能力（倾听、表达、冲突解决）：57%
- 问题解决能力：53%
- 团队合作（协作与配合）：47%
- 适应能力/灵活性：43%

其他重要软技能还包括自我激励（32%）、诚信/诚实（32%）、领导力（31%）、敬业精神（30%）、态度（28%）、组织能力（25%）、写作能力（16%）以及同理心（12%）。

为弥补网络安全专业人员在这些非技术技能方面的缺口，企业正在采取以下措施：

- 利用在线学习平台（49%）
- 开展导师辅导（40%）
- 开展企业培训活动（32%）
- 提供学费报销（18%）

22% 的受访者表示，其所在企业尚未采取任何措施弥补这一技能缺口；6% 的受访者表示，其所在企业不存在非技术技能缺口。

网络安全专业人员需要全面提升自身能力和专业素养。调查受访者认为最重要的五项安全技能是：

- 数据安全：56%
- 威胁检测与响应技术：54%
- 漏洞管理：53%

- 身份与访问管理：51%
- 事件响应：49%

图 15 列出了完整的调查结果。

2025 年，应对网络安全技术技能缺口最常用的措施是聘用合同制人员（30%）。今年，这一措施降至第三位（26%），延续了 2024 年至 2025 年的下降趋势。2026 年，更多依赖 AI 或自动化跃居首位——35% 的受访者选择了这一应对措施，较去年上升 12 个百分点。培训有意转岗至安全岗位的非安全人员仍位居第二（27%）。其他弥补这些技能缺口的措施与去年相比变化不大，包括：

- 更多采用技能再培训项目（21%）
- 更多采用基于实际表现的培训，以验证实际技能掌握程度（18%）
- 利用学徒制/实习项目（18%）
- 更多依赖专业认证，以验证实际专业能力（16%）

2026 年，超过半数的受访者（54%）表示，初级网络安全专业人员通常需要具备大学学历（图 16）。今年，拉丁美洲对大学学历的要求大幅下降 17 个百分点。受访者对大学毕业生是否已为从事网络安全工作做好准备看法不一，但与 2025 年的调查结果基本一致。2026 年，仅 4% 的受访者“非常同意”、22% 的受访者“同意”大学毕业生已为应对组织内的网络安全挑战做好充分准备。大多数受访者表示“既不同意也不反对”（38%），另有 21% 表示“不同意”，7% 表示“非常不同意”（图 17）。

图 15：最重要的安全技能

请选择贵组织当前安全专业人员最需要具备的五项安全技能。

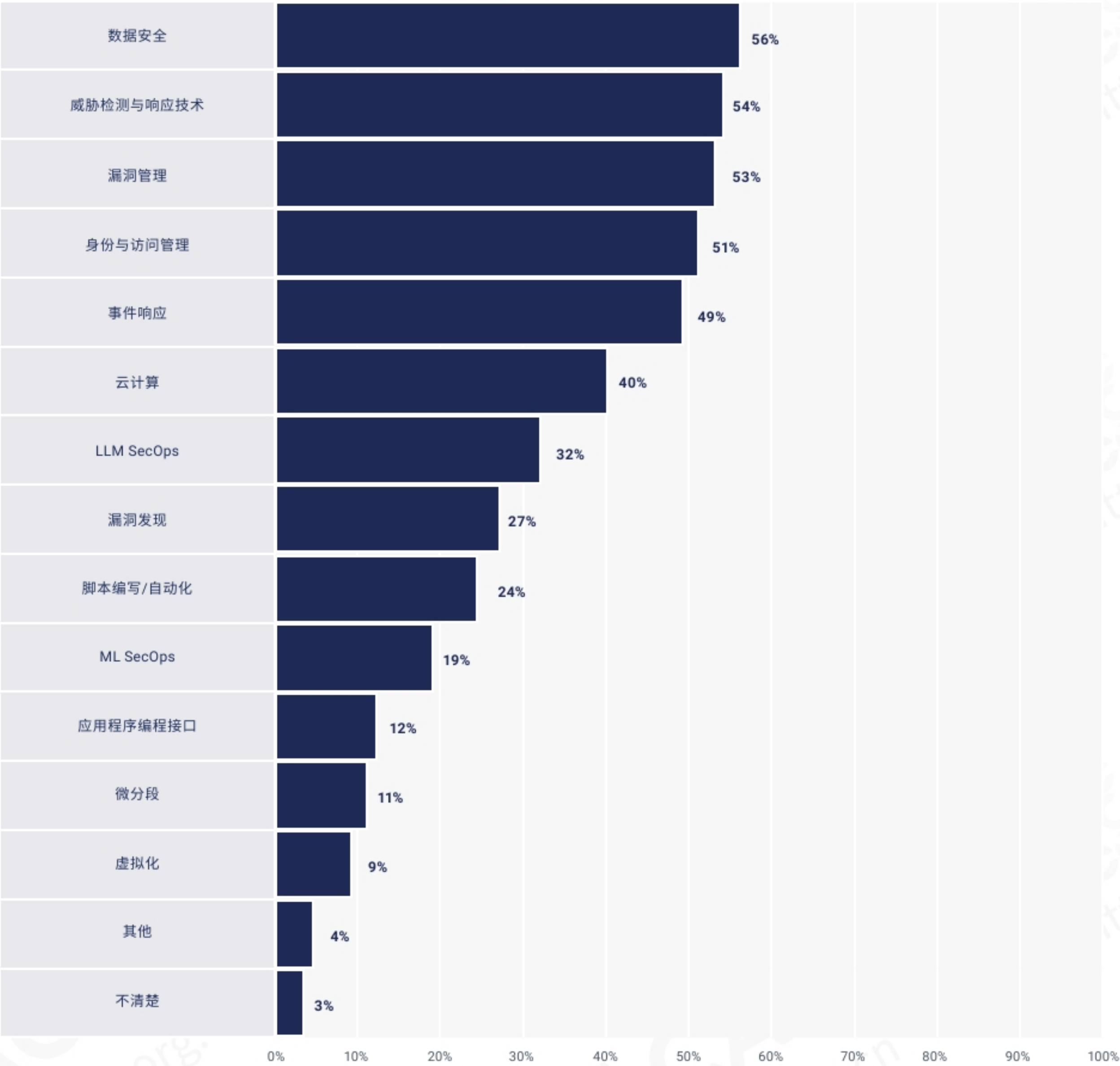


图 16: 全球大学学历要求

贵组织通常是否要求初级网络安全职位的候选人具备大学学历？

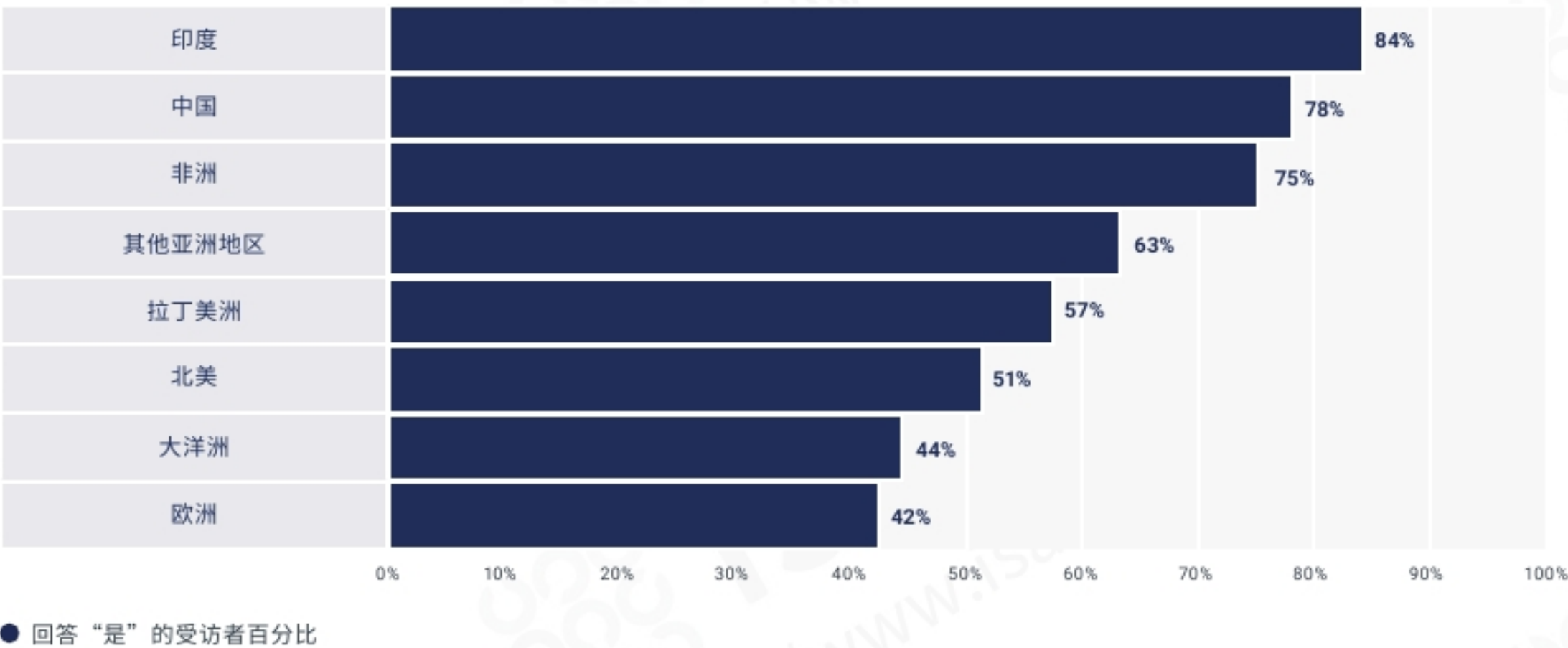


图 17: 职业准备情况

您在多大程度上同意或不同意以下说法：网络安全专业应届毕业生已为应对贵组织面临的网络安全挑战做好充分准备？

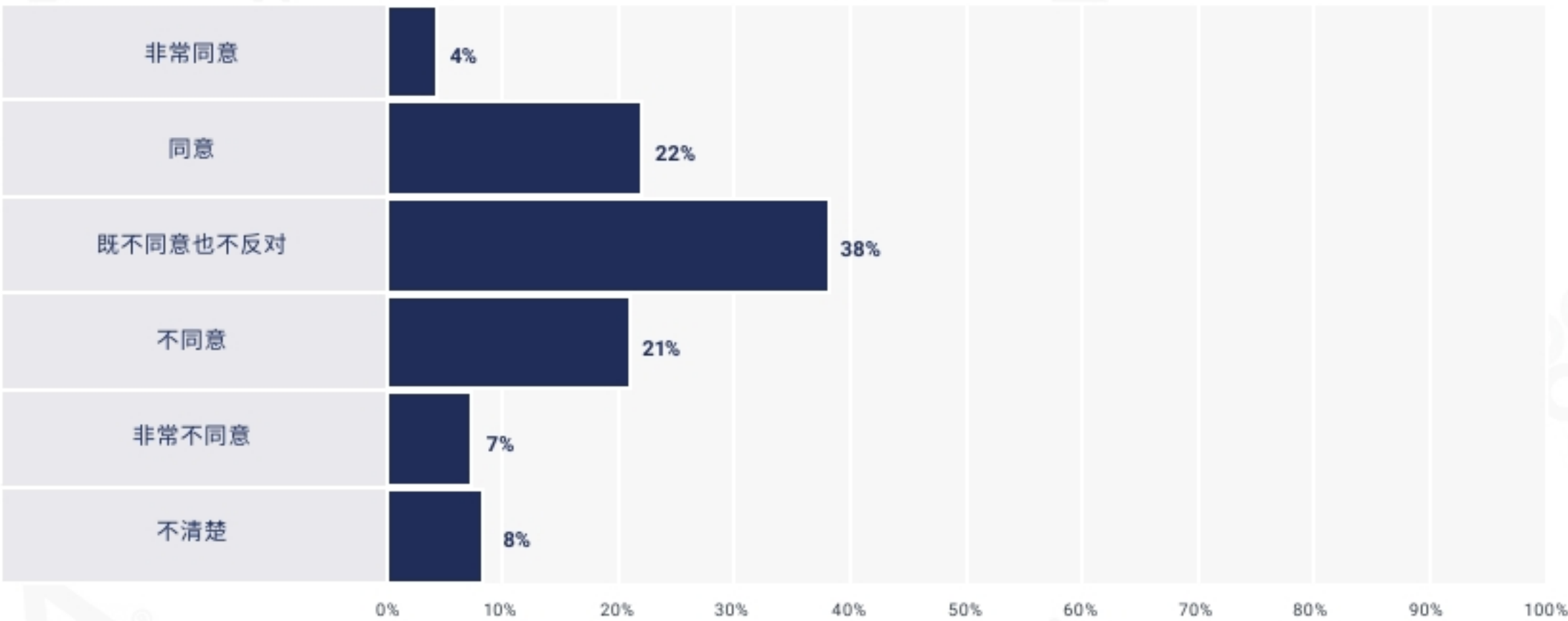


图 18 列出了应届毕业生常见的技能缺口。调查结果表明，有必要深入理解并应对 AI 安全带来的复杂问题——LLM SecOps 较 2025 年上升 9 个百分点，事件响应上升 4 个百分点，威胁检测与响应上升 6 个百分点。鉴于 2026 年 LLM 在企业中的应用持续拓展并不断演进，网络安全专业人员也需要不断适应新的运行环境，因此这一结果符合预期。数据安全及其他技能缺口较 2025 年也略有上升。

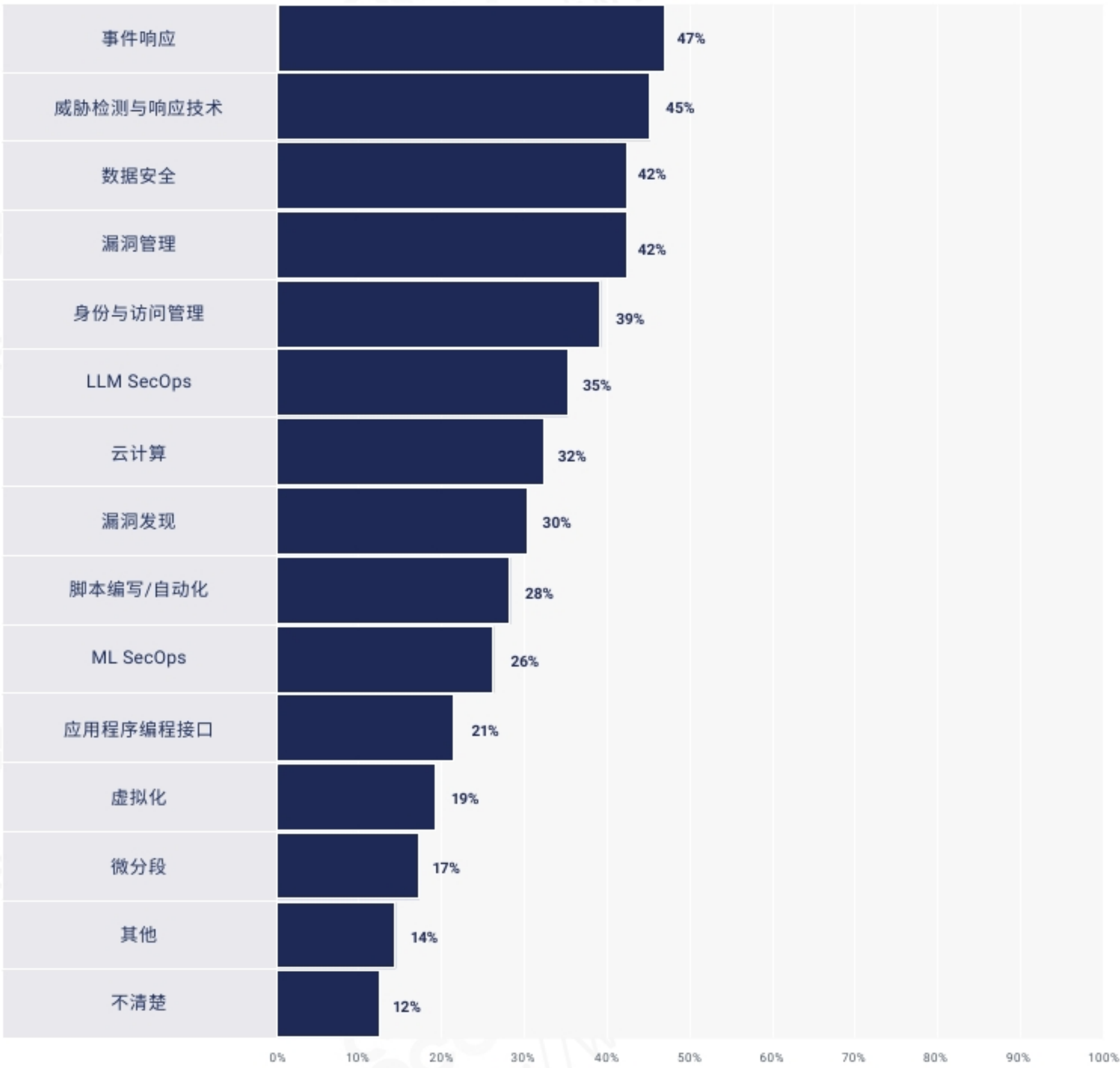
42% 的调查受访者所管理的安全人员工作经验不足三年。

受访者认为，这些员工最需要加强专业发展和培训的领域包括：

- 事件响应（54%）
- 数据安全（50%）
- 漏洞管理（45%）
- 身份与访问管理（43%）
- 威胁检测与响应技术（43%）

图 18：高校应届毕业生常见技能缺口

您在应届毕业生中注意到以下哪些技能缺口？



网络安全运营

大多数调查受访者表示，其所在组织的首席信息安全官（CISO）和高级管理岗位并未呈增长趋势。企业是否设有 CISO 与企业规模密切相关——员工人数少于 499 人的小型企业中，近 60% 设有 CISO；员工人数为 500 至 5,000 人的企业中，这一比例为 73%；员工人数为 5,000 至 10,000 人的企业中，则达到 87%。企业未设 CISO，并不意味着其未将信息风险纳入考量，也不意味着企

业降低了对信息安全重要性的重视程度。中小型企业不设置专职 CISO 的情况并不少见，但相关职责通常由总监级负责人或信息安全经理承担。⁶

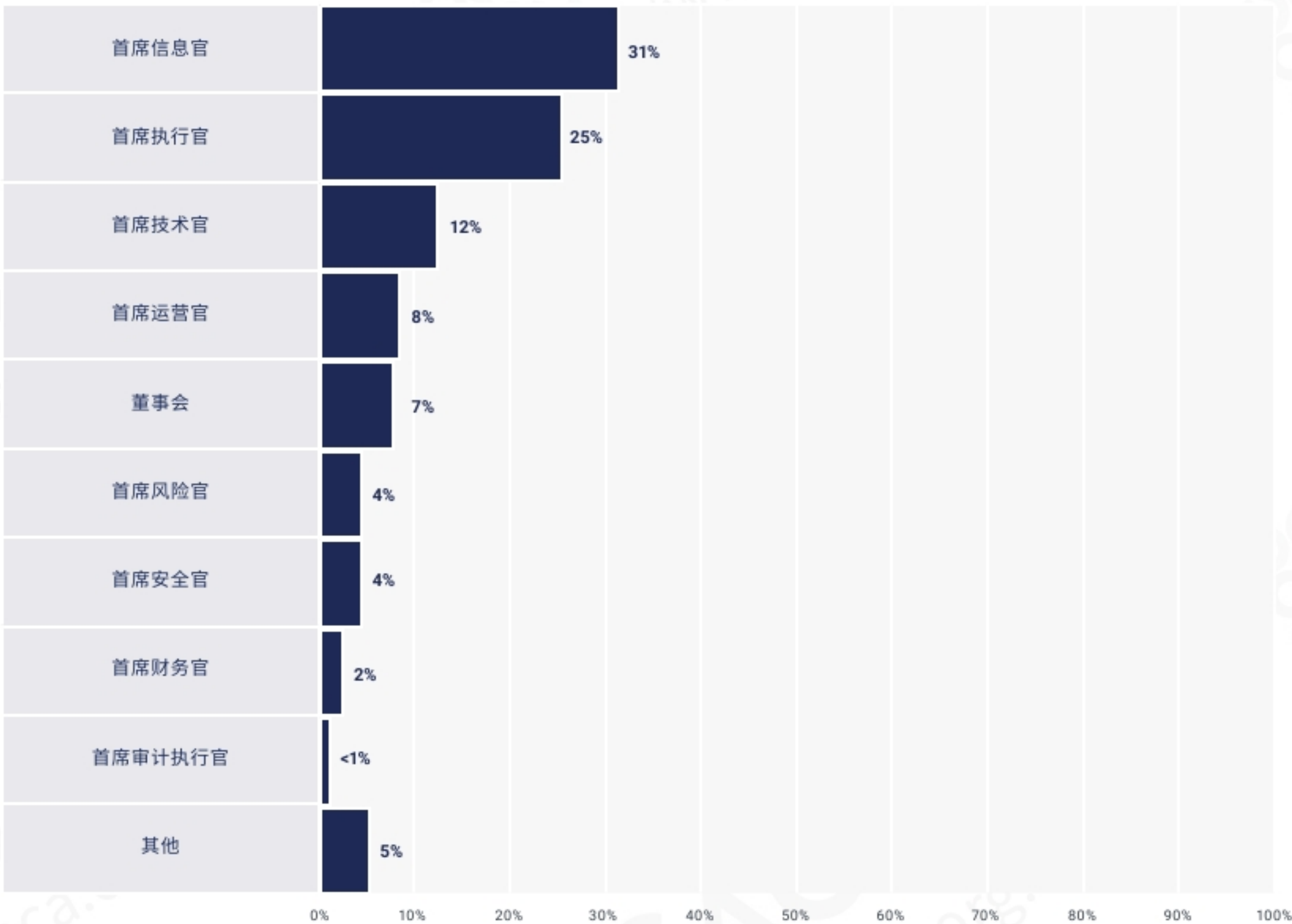
图 19 展示了 CISO 的汇报对象。

在未设 CISO 的组织中，安全团队通常向其他高管汇报。最常见的汇报对象包括首席信息官（31%）、首席执行官（25%）和首席技术官（12%）。

6 IANS, 《IANS 与 Artico Search 最新报告显示：尽管 2024 年市场放缓，CISO 薪酬依然保持强劲》，2024 年 10 月 2 日，www.iansresearch.com/resources/press-releases/detail/new-report-from-ians-research-and-artico-search-reveals-ciso-compensation-remains-strong-despite-2024-market-slowdown

图 19: CISO 汇报关系

贵组织的 CISO 向谁汇报？



预算

与去年的调查结果一致，41% 的受访者表示其网络安全预算资金充足，55% 的受访者表示其预算

资金略显不足或严重不足（图 20）。图 21 显示，大多数受访者预计未来 12 个月网络安全预算将有所增加或保持不变。

图 20: 网络安全预算资金情况

您认为贵组织目前的网络安全预算资金情况如何：

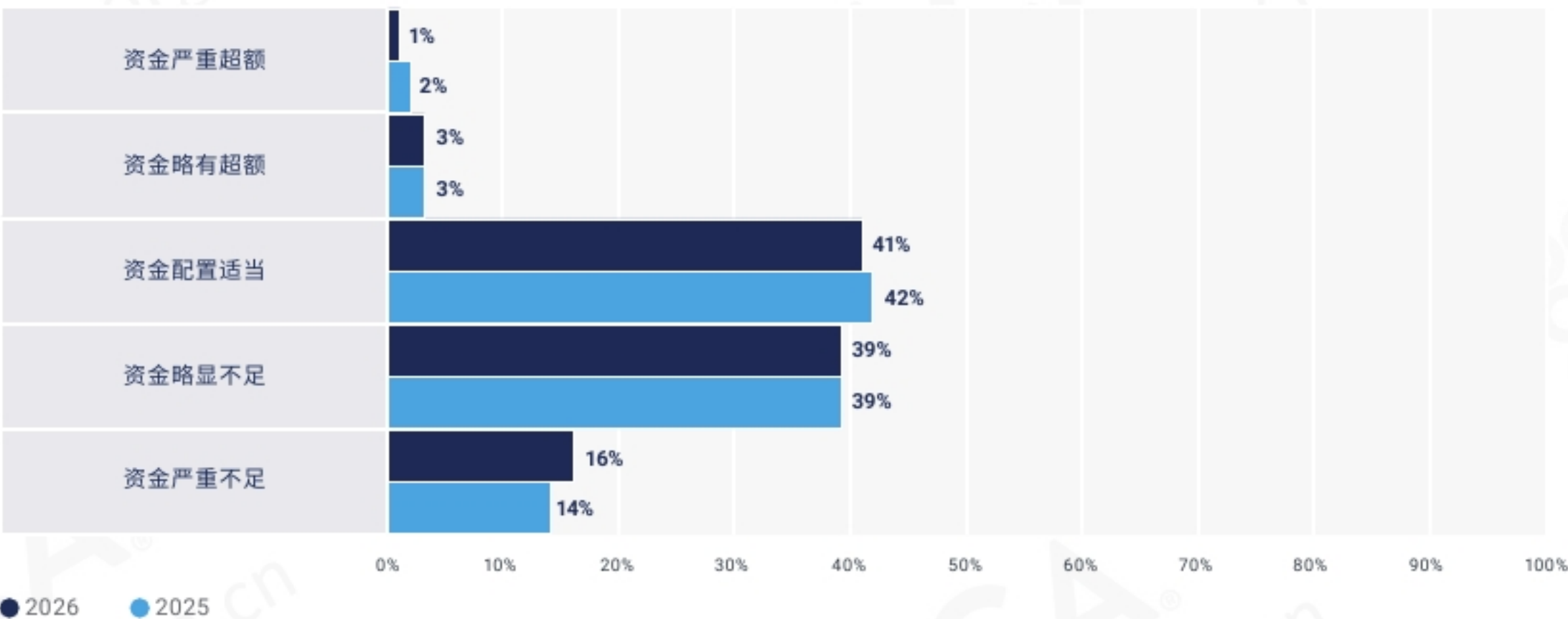
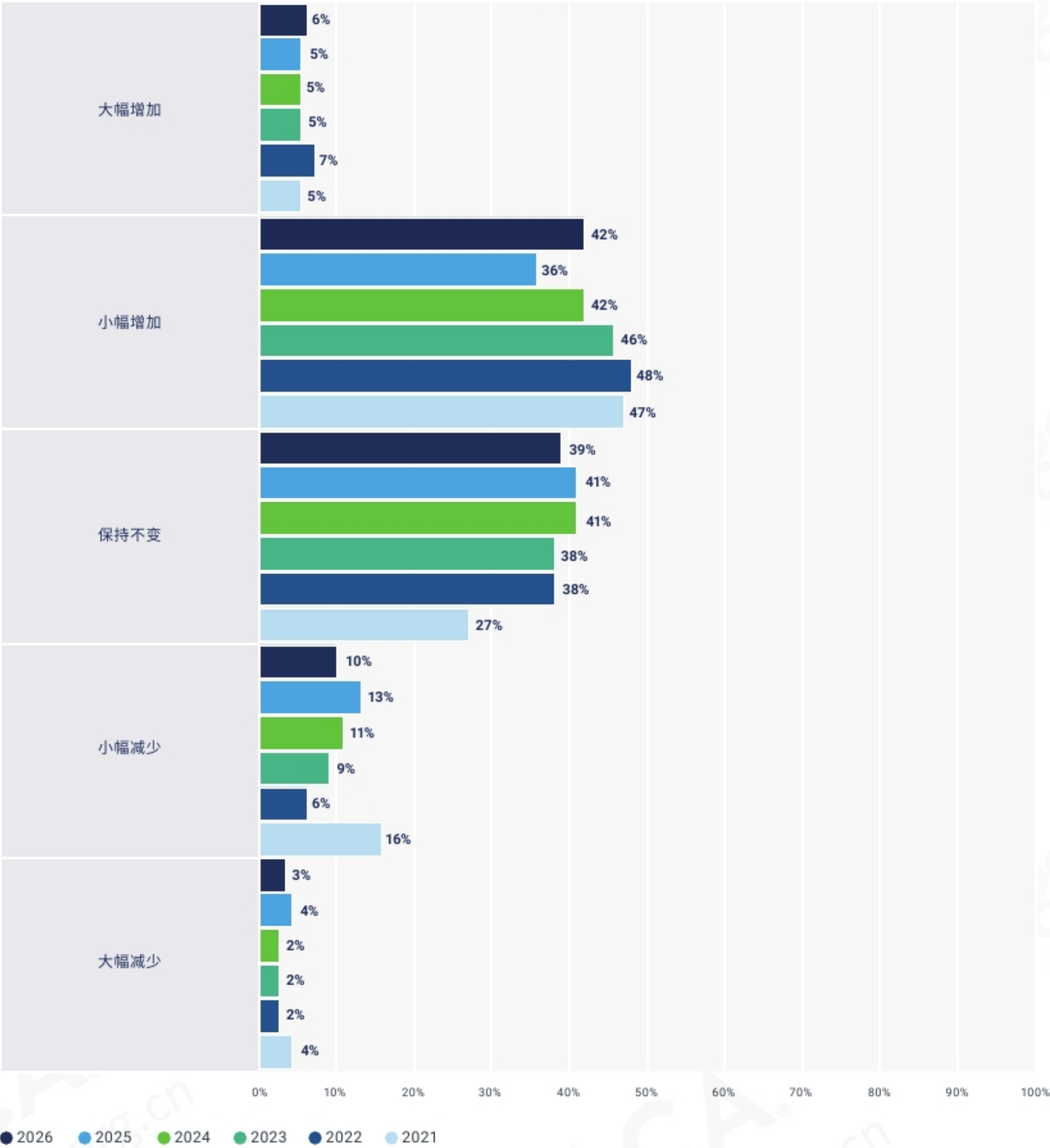


图 21：网络安全预算预测

未来 12 个月，贵组织的网络安全预算预计将如何变化（如有）？



董事会与网络安全优先事项

56% 的受访者表示，其董事会充分重视网络安全；77% 的受访者表示，其企业网络安全战略与组织目标保持一致，略高于去年的 74%。

不出所料，在董事会充分重视网络安全的受访者中，网络安全战略与组织目标保持一致的比例高达 95%。

对比董事会充分重视网络安全与未充分重视网络安全的组织，可以发现一些明显趋势。

重视网络安全的董事会能够为团队提供必要的资源，并增强其对自身网络安全能力的信心：

- 在董事会充分重视网络安全的受访者中，56% 对其网络安全团队识别和应对网络威胁的能力表示完全或非常有信心；而在董事会未充分重视网络安全的受访者中，这一比例仅为 22%。
- 在董事会重视网络安全的受访者中，约 37% 表示其网络安全资金投入不足；而在董事会未充分重视网络安全的受访者中，这一比例高达 85%。
- 与董事会未充分重视网络安全的受访企业相比，董事会重视网络安全的企业更有可能提供具有吸引力的福利，例如职业发展机会以及承担员工认证费用。

与董事会未充分重视网络安全的受访企业相比，董事会重视网络安全的企业更有可能提供具有吸引力的福利，例如职业发展机会以及承担员工认证费用。

- 在董事会充分重视网络安全的受访企业中，仅 48% 面临留住高技能网络安全人才的困难，而在董事会未充分重视网络安全的企业中，这一比例为 67%。

网络风险与网络攻击

35% 的调查受访者表示，与去年相比，其所在企业遭受的网络攻击有所增加（图 22）。这一比例与 2025 年报告网络攻击增加的受访者比例基本一致。

图 23 展示了实施攻击的主要威胁主体，与去年基本一致。黑客和恶意内部人员所占比例均略有下降。

图 22：网络攻击趋势

与一年前相比，贵组织遭受的网络安全攻击有所增加还是减少？

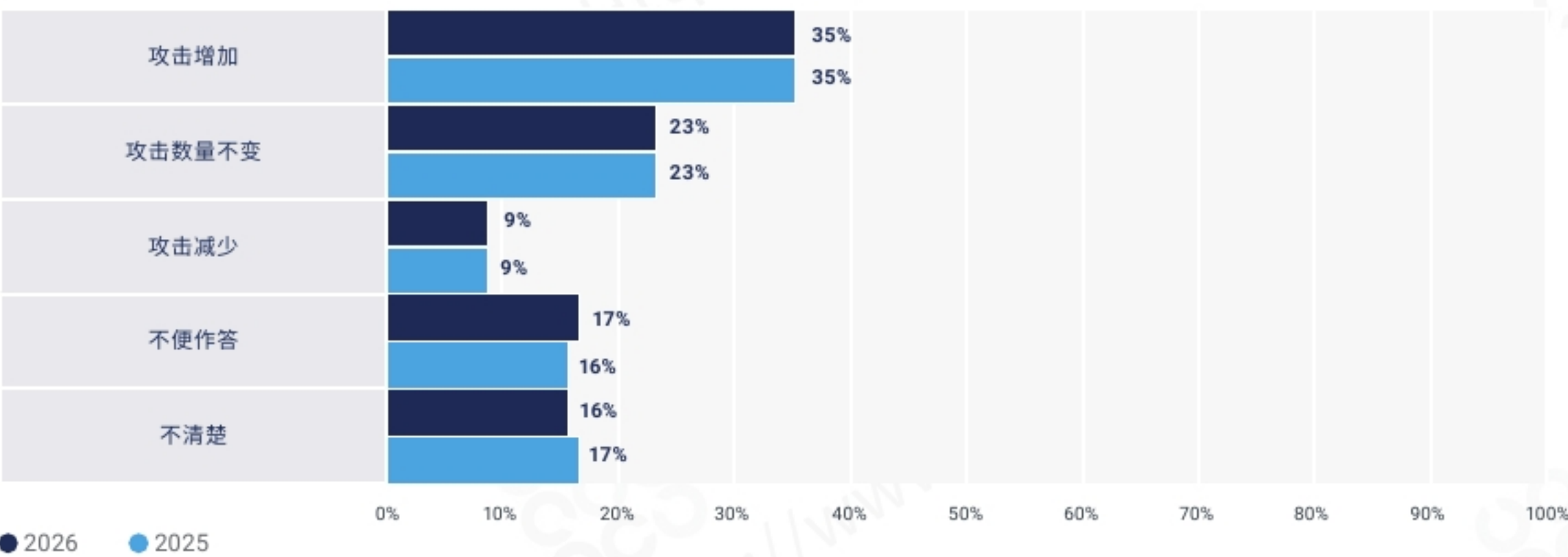
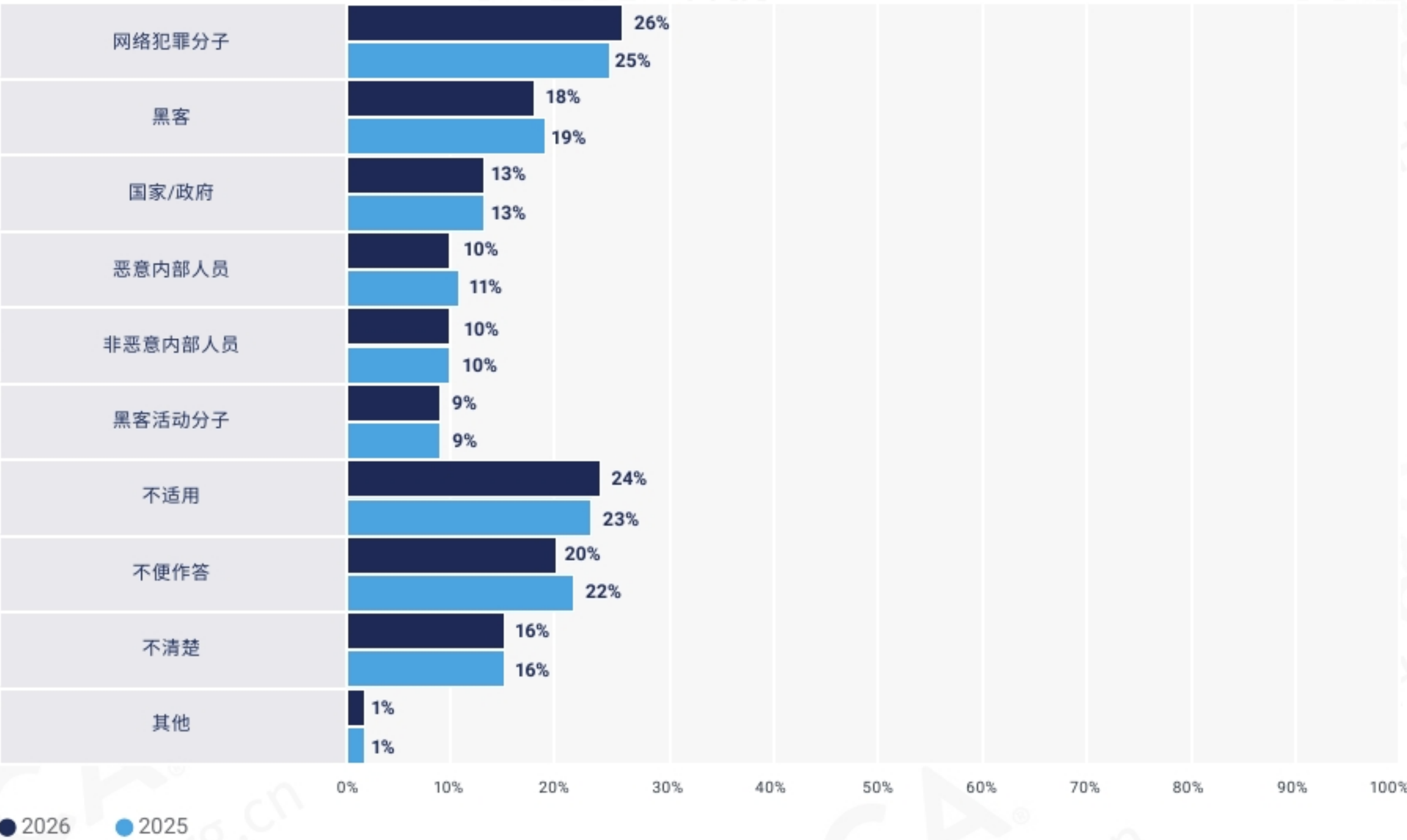


图 23：威胁主体

如果贵组织今年遭受过攻击，以下哪些威胁主体是攻击的实施者？



仅 10% 的受访者表示，自 2025 年 6 月以来，其所在企业曾遭到安全入侵。64% 的受访者表示其所在企业未遭到安全入侵，25% 的受访者表示不知道。图 24 展示了导致企业遭到安全入侵的主要攻击向量。与 2025 年相比，勒索软件所占比例下降 6 个百分点，而远程访问上升 5 个百分点。

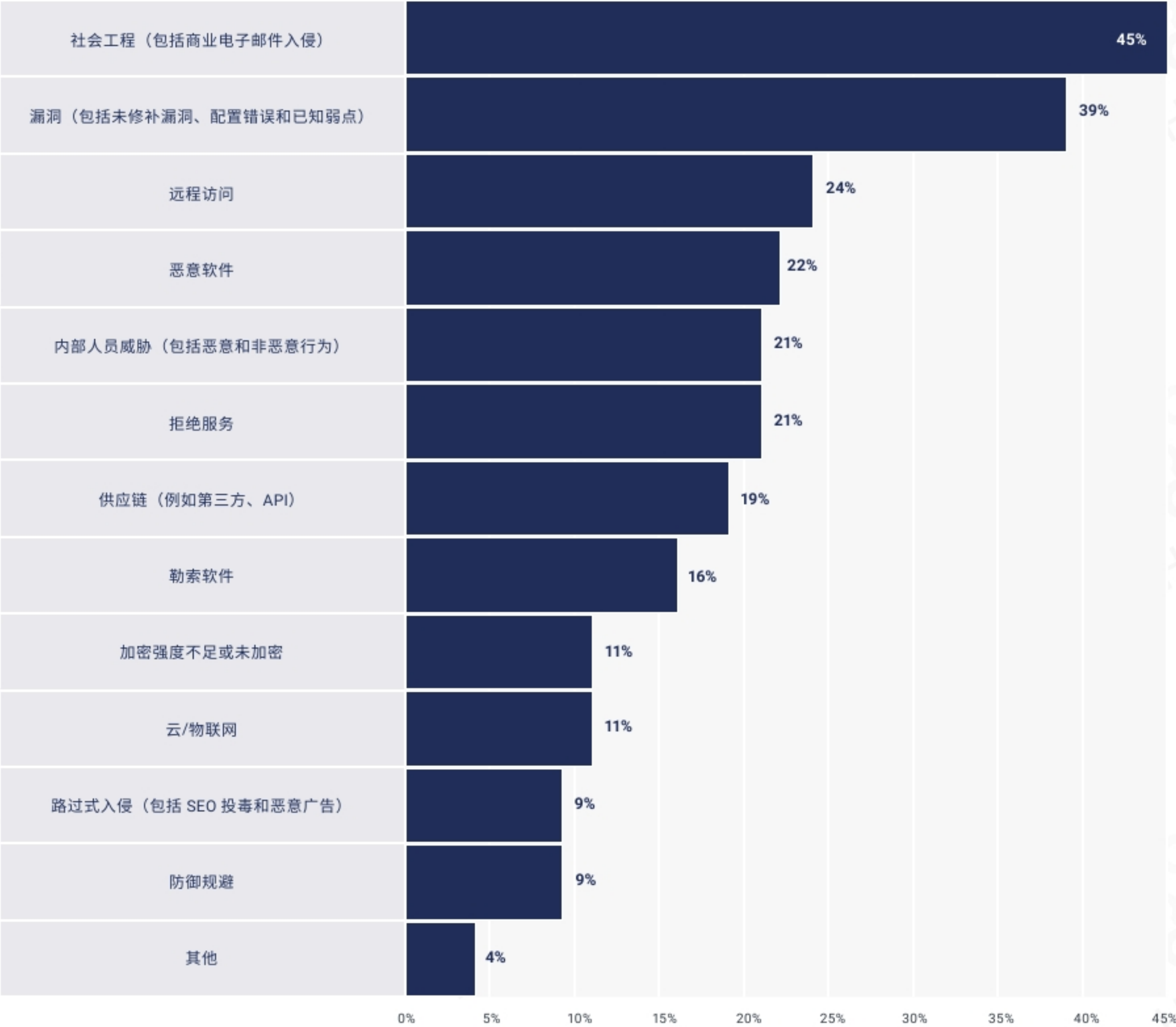
16% 的受访者确认或认为，其所在企业遭受的攻击由 AI 驱动；另有三分之一（33%）的受访者不知道这些攻击是否由 AI 驱动。

近一半（45%）的受访者认为，其所在企业未来一年可能或很可能遭受网络攻击（图 25），这一比例较 2025 年略有上升。

近一半（45%）的受访者认为，其所在企业未来一年可能或很可能遭受网络攻击。

图 24：攻击者使用的攻击向量⁷

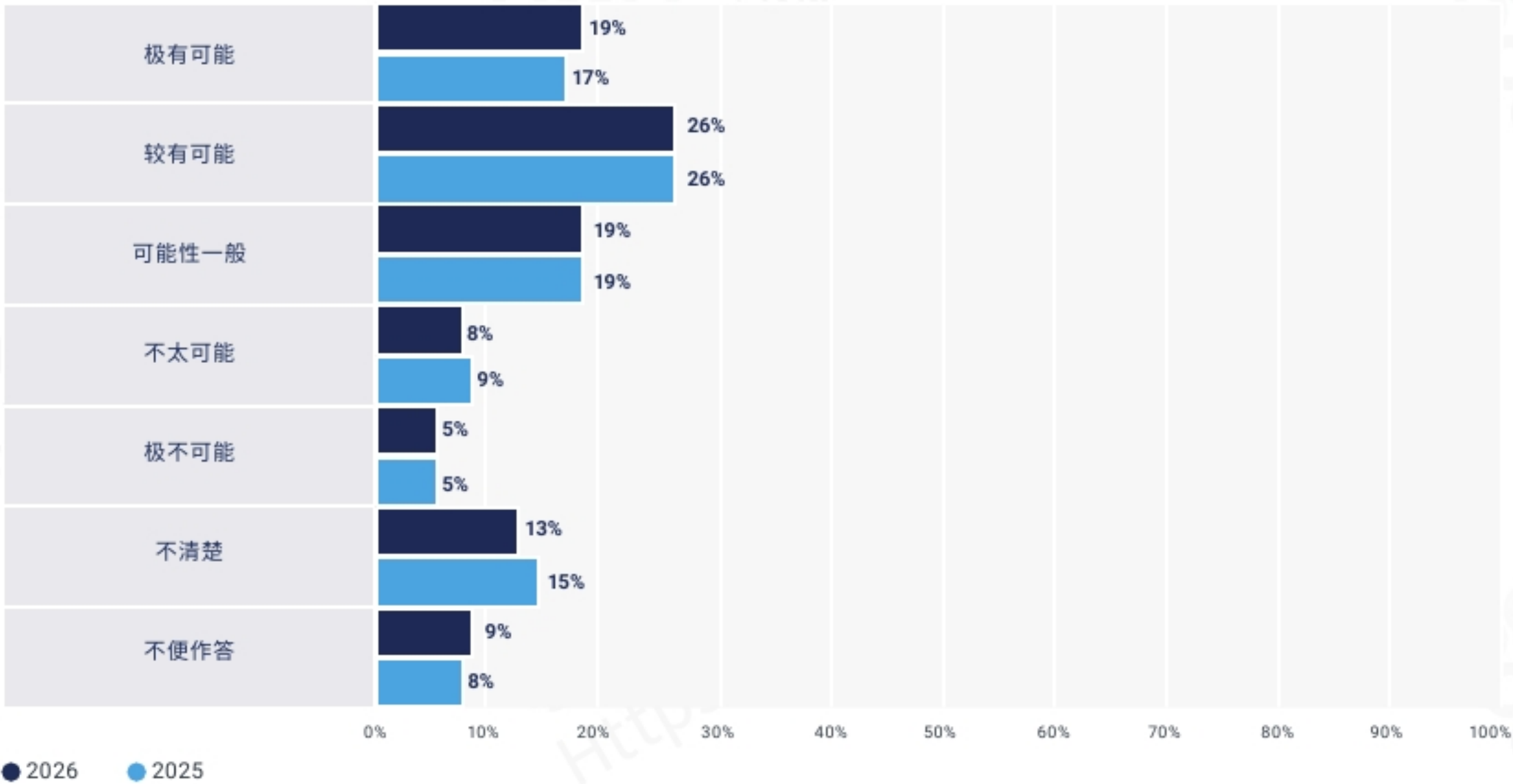
贵组织遭到安全入侵时，攻击者使用了以下哪些攻击向量？



7 本图不包括回答“不知道”以及未回答此问题的受访者。

图 25：遭受网络攻击的可能性

您认为贵组织明年遭遇网络攻击的可能性如何？

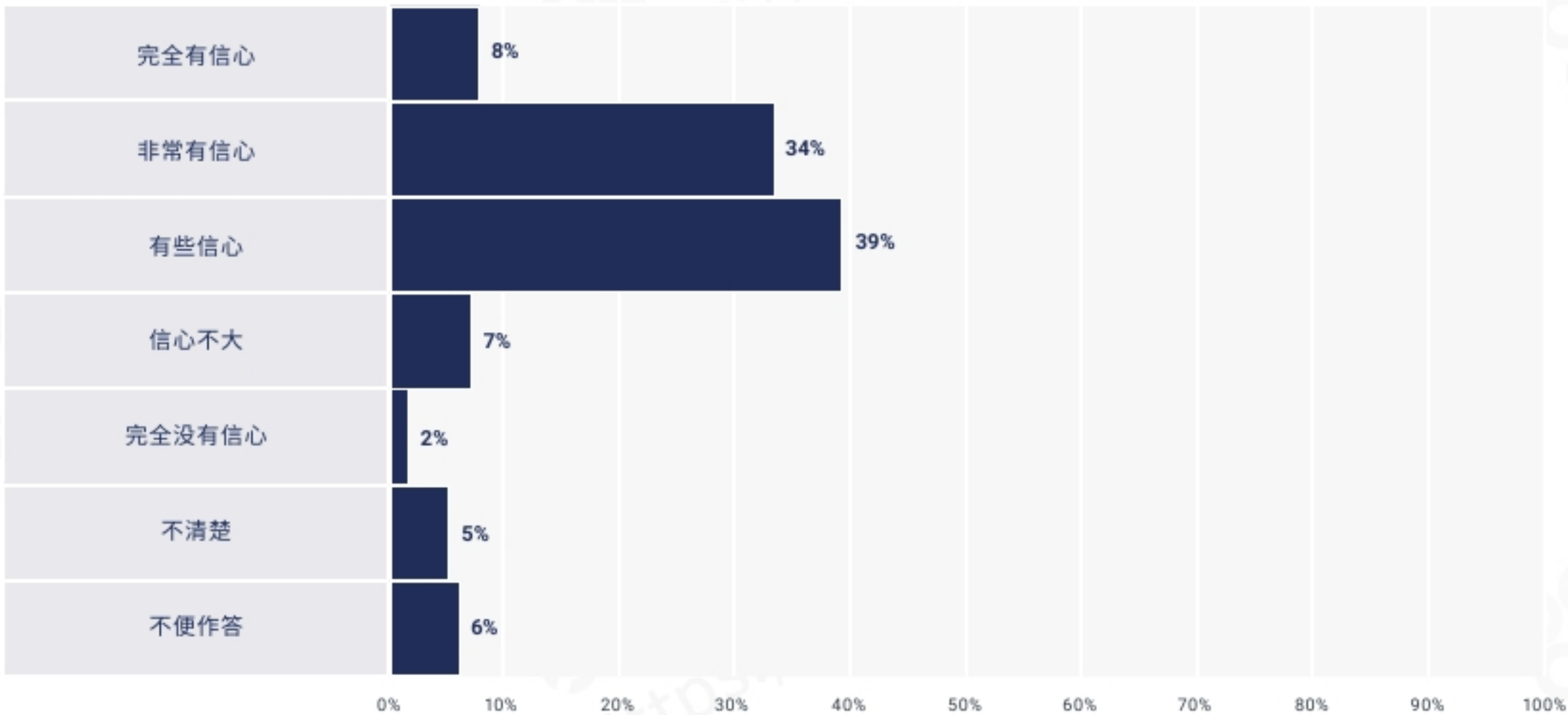


仅 42% 的受访者对其网络安全团队检测和应对网络威胁的能力表示完全有信心或非常有信心（图 26）。在认为网络安全团队人员配置合理的受访

者中，52% 对团队检测和应对网络威胁的能力表示完全有信心或非常有信心；而在员工人数超过 10,000 人的组织中，这一比例为 48%。

图 26：对网络威胁检测与响应能力的信心

您对贵组织的网络安全团队在检测和响应网络威胁方面的整体信心如何？

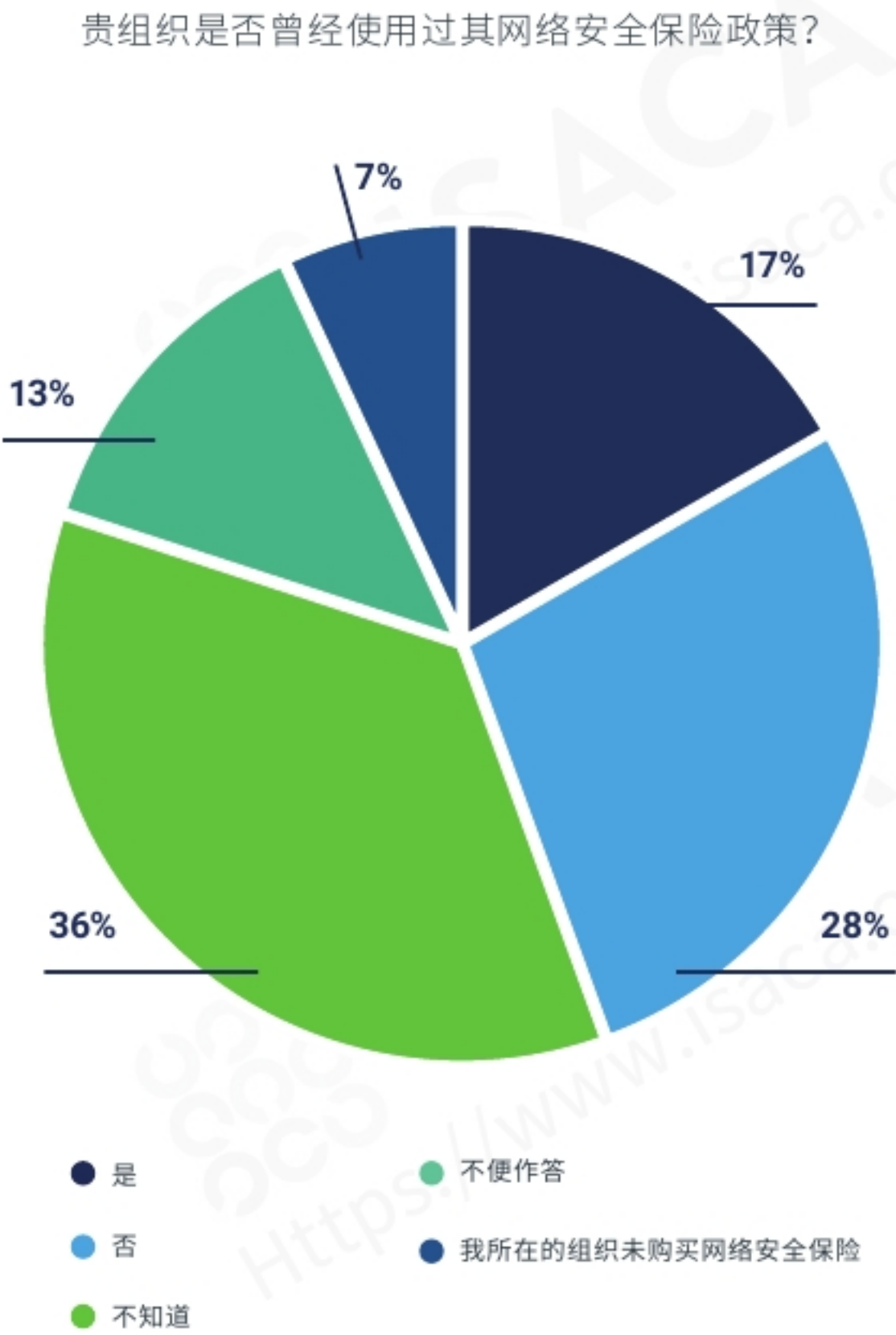


38% 的受访者表示，即使有报告义务，大多数组织仍会少报网络犯罪事件；18% 的受访者表示，即使没有报告义务，组织也会少报网络犯罪事件。仅 20% 的受访者表示，网络犯罪事件能够得到如实报告。

许多企业都购买了网络安全保险，以便在发生网络安全事

件时提供保障，但不少受访者表示，其所在企业从未使用过网络安全保险（图 27）。表示其所在企业曾使用过网络安全保险的受访者比例较去年下降了 4 个百分点。在表示其所在企业去年曾遭受安全入侵的受访者中，28% 表示使用过网络安全保险，19% 表示未使用。

图 27：网络安全保险使用情况



网络风险

今年的调查结果显示，企业正积极从年度风险评估转向更高频的风险评估。

每月开展网络风险评估（13%）或每 1 至 6 个月开展一次网络风险评估（22%）的受访者比例较去年上升 2 个百分点，较 2024 年上升 5 个百分点（图 28）。

图 28：网络风险评估频率

您的组织多久进行一次网络风险评估？

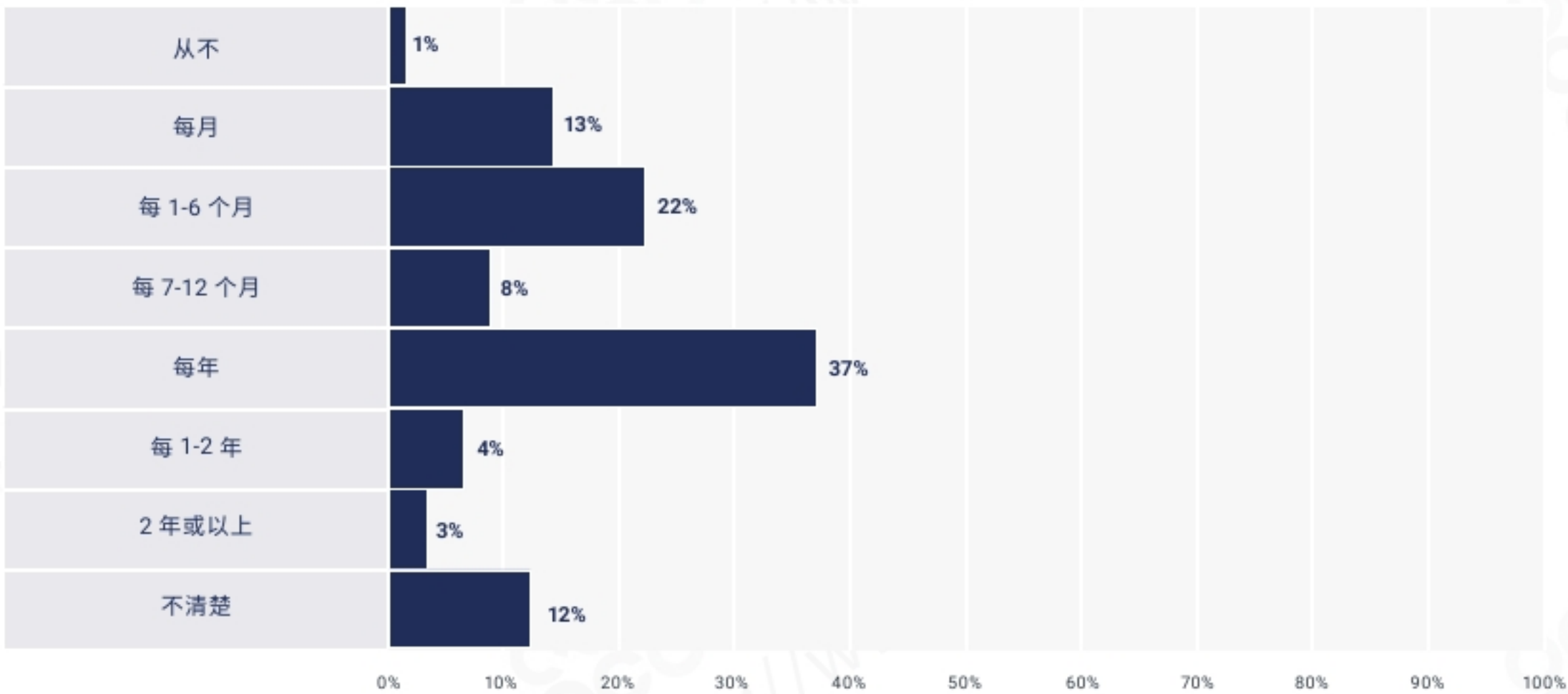
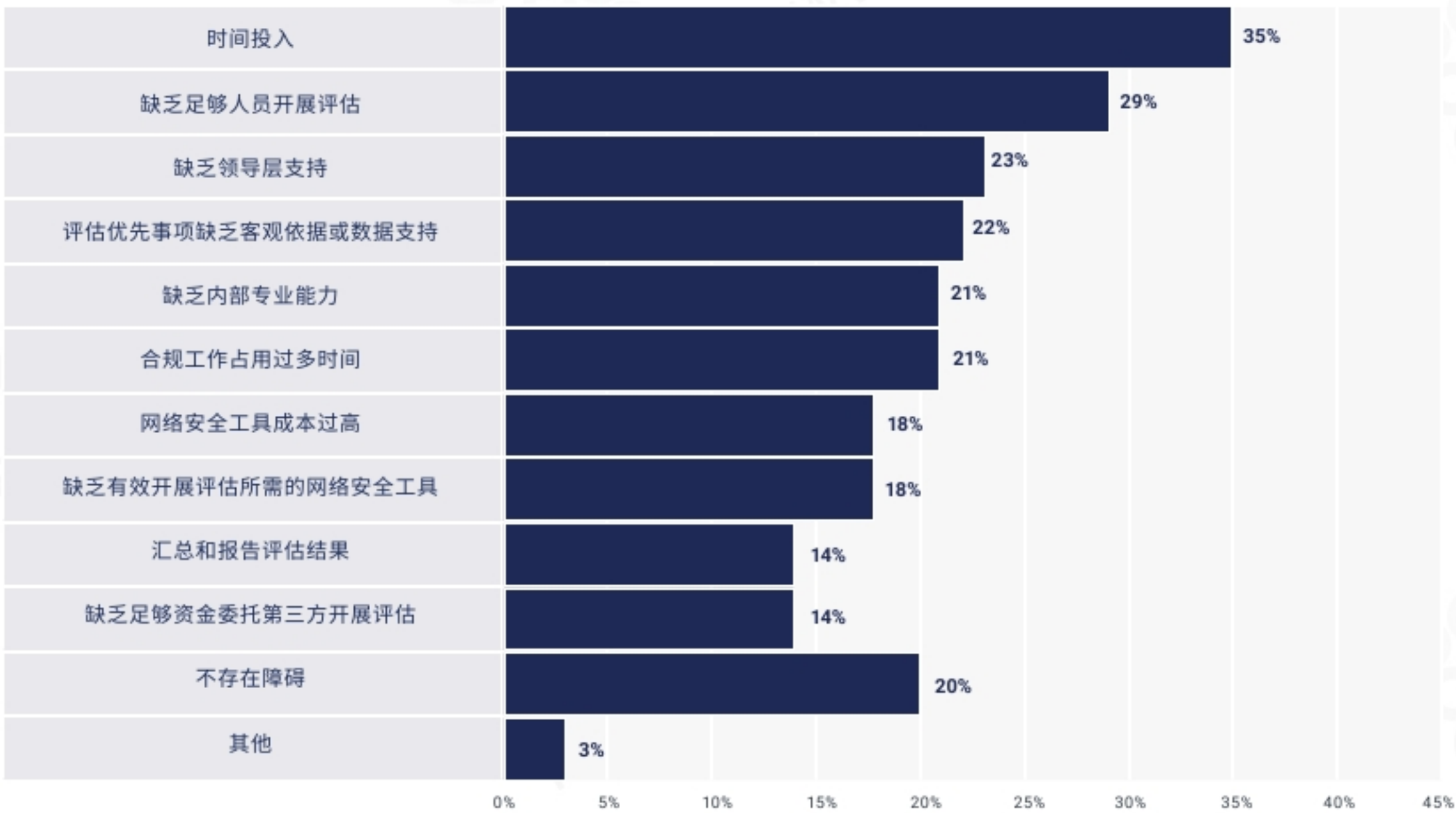


图 29 展示了组织在开展网络风险评估时面临的主要障碍。时间投入（35%）和人员不足（29%）仍是最主要的两项障碍，比例与去年基本持平，但较两年前有所下降，当时这两项比例分别为

41% 和 37%。在网络安全团队人员不足的受访者中，39% 每年开展一次网络风险评估，而人员配置充足有余的团队开展评估的频率更高。

图 29：开展网络风险评估面临的障碍

贵组织在开展网络风险评估时面临以下哪些障碍（如有）？



AI 与网络安全

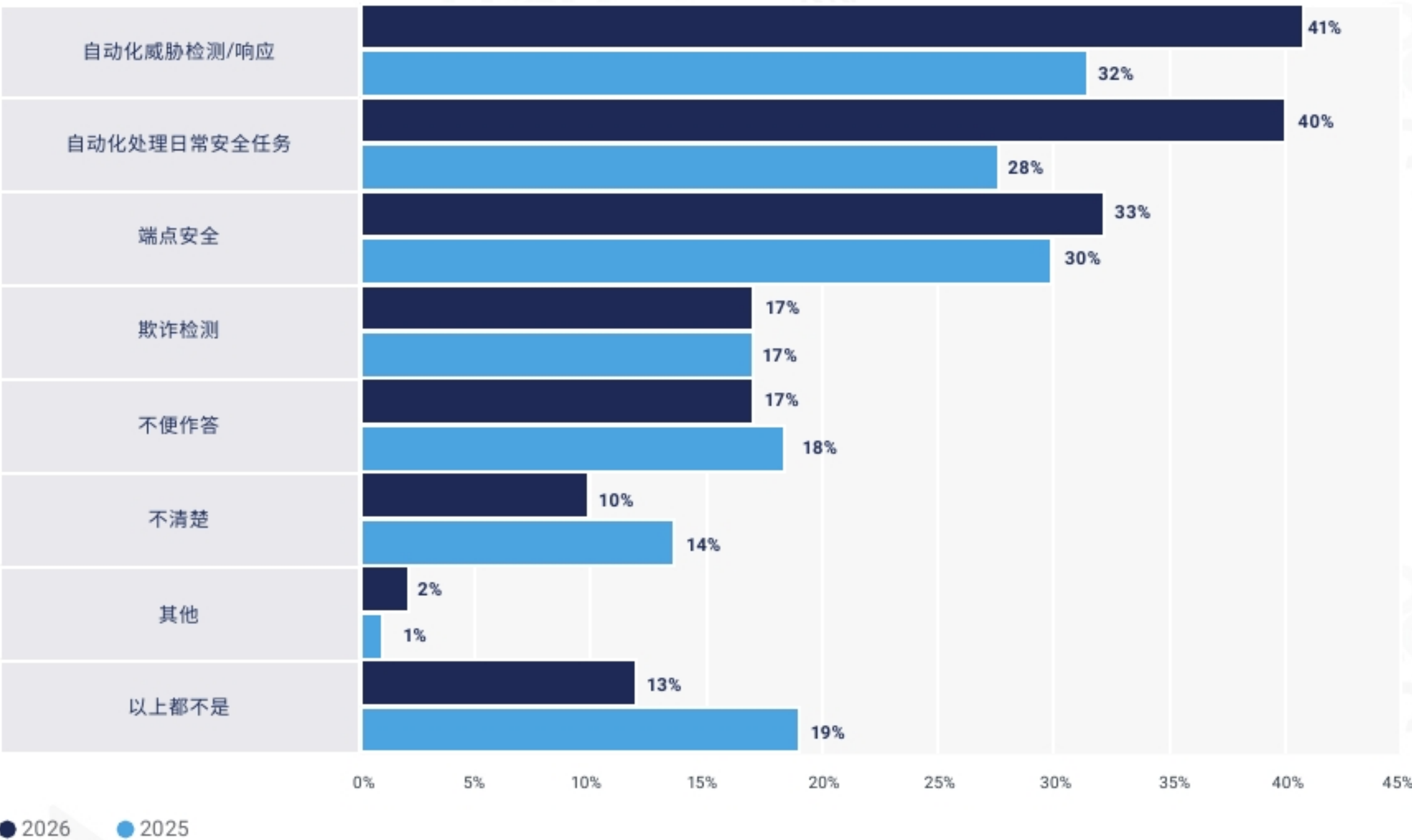
AI 工具在各类安全运营中的应用持续增加（图 30）。

AI 工具在各类安全运营中的应用持续增加。

受访者表示，AI 在安全运营中的两大主要应用领域分别是自动化威胁检测/响应（41%），较 2025 年上升 9 个百分点；以及自动化处理日常安全任务（40%），较 2025 年大幅上升 12 个百分点。

图 30：AI 在安全运营中的应用

贵组织是否在以下任何安全运营场景中使用人工智能（AI）？



超过半数（51%）的受访者表示，他们本人或其团队成员参与了 AI 解决方案的开发、引入或实施，这一比例显著高于去年的 40% 和两年前的 29%

（图 31）。此外，56% 的受访者表示，他们本人或其团队成员参与了所在组织 AI 使用管理政策的制定，较 2025 年上升 9 个百分点（图 32）。

图 31: AI 生命周期参与情况

您或您团队中的任何人是否参与了 AI 解决方案的开发、引入或实施？

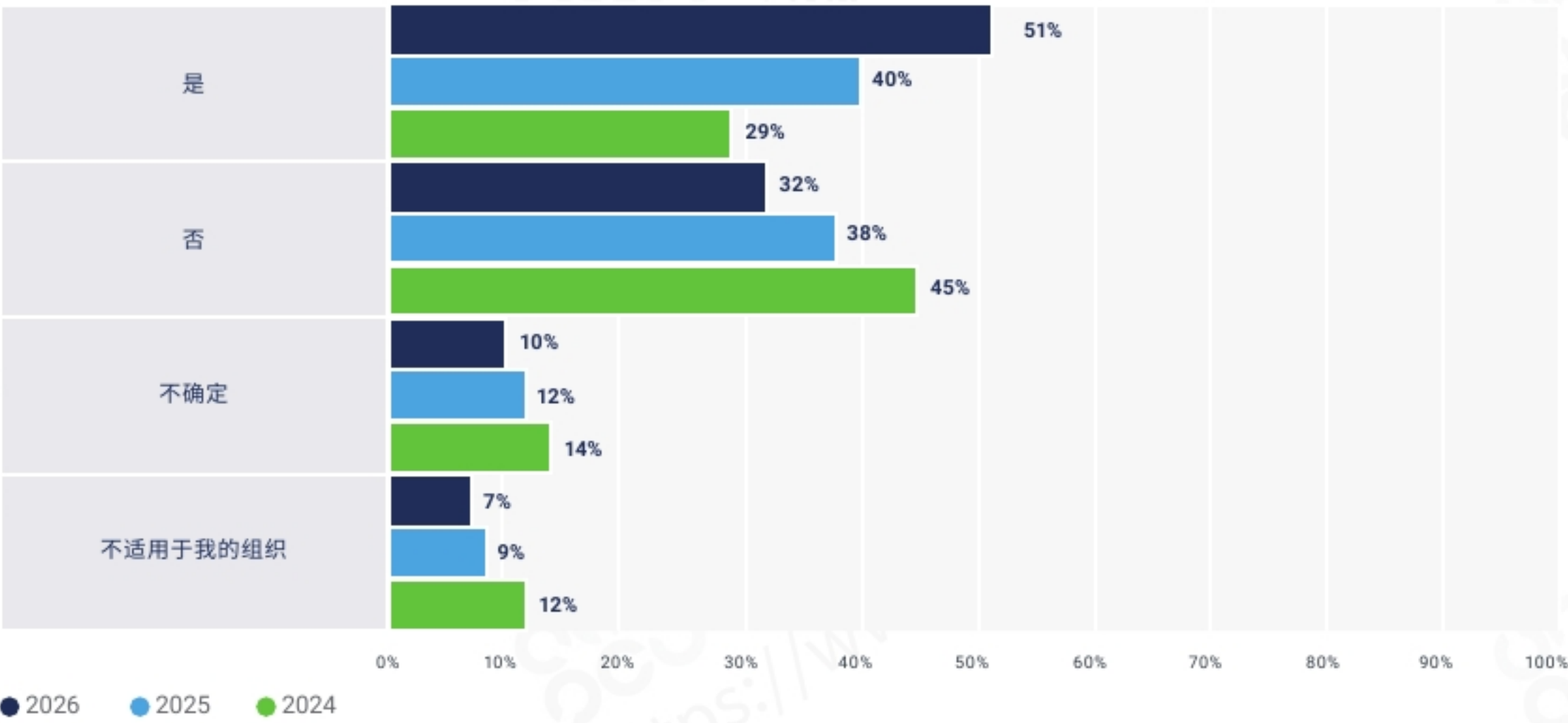
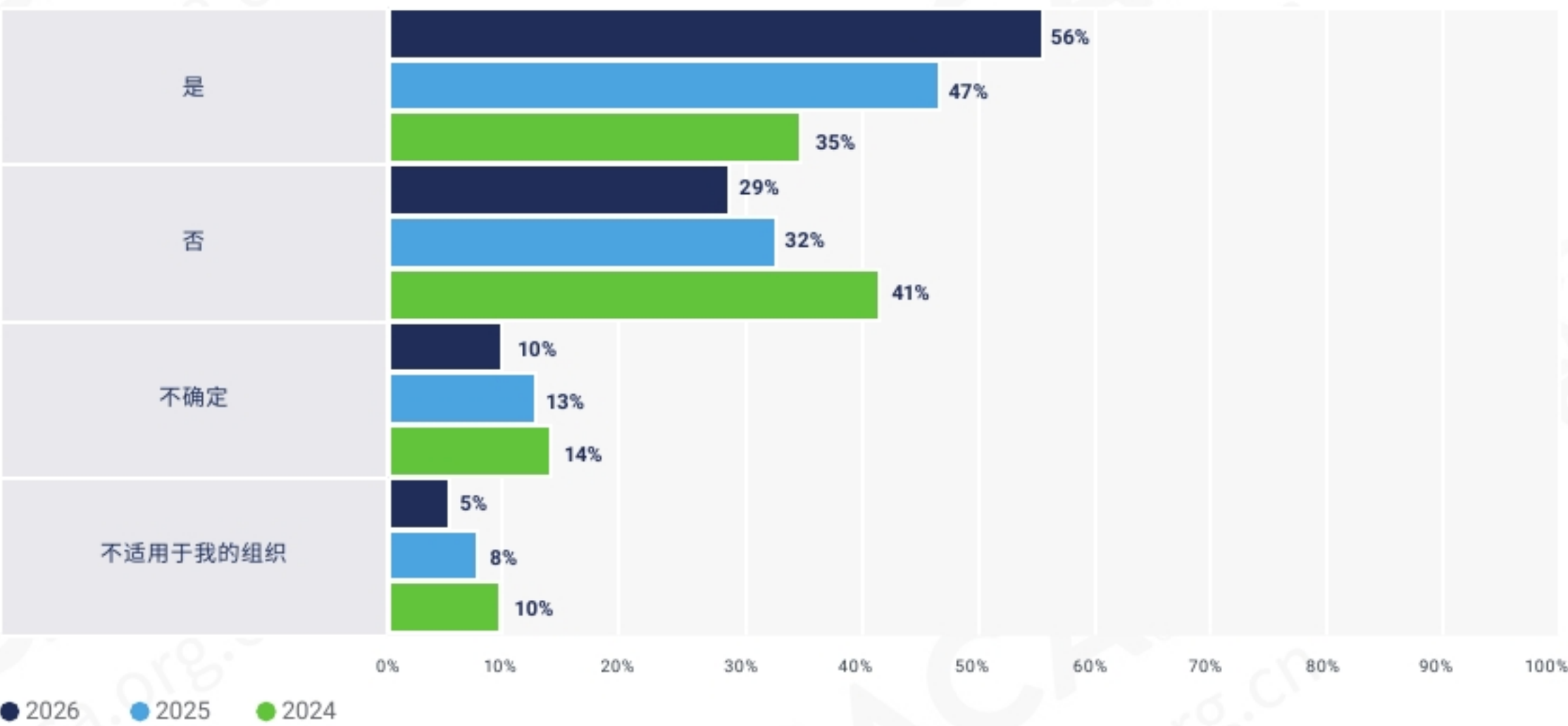


图 32: AI 政策制定参与情况

您或您团队中的任何人是否参与了制定管理您组织中 AI 技术使用的政策？

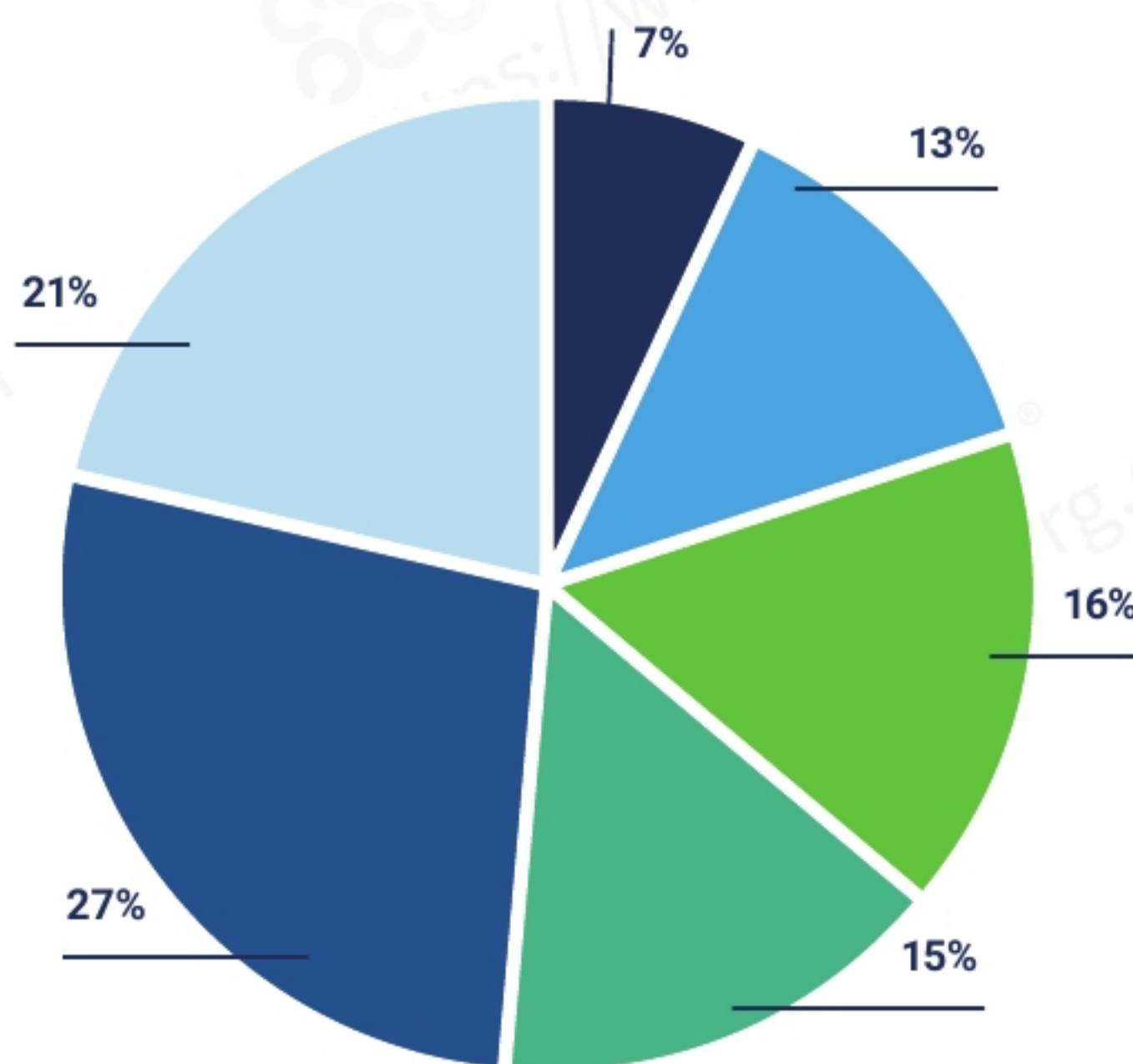


今年的调查新增了有关 AI 解决方案事件响应活动的问题。仅 20% 的受访者表示，其所在组织已建立较为成熟或覆盖范围有限的 AI 专项事件响应预

案/操作手册；27% 的受访者表示，其所在组织目前尚未开展这方面的工作（图 33）。

图 33: AI 事件响应预案/操作手册

贵组织是否已建立针对 AI 事件的响应预案/操作手册？



- 是，我们已针对 AI 专项事件建立成熟、正式的操作手册
- 是，我们已制定部分针对 AI 专项事件的响应措施，但覆盖范围有限
- 我们仅通过现有的通用流程进行处理
- 我们正在制定相关方案，但尚未实施
- 我们目前尚未开展这方面的工作
- 不清楚

2026 年 AI 的应用对网络安全团队产生了影响，这些团队需要负责针对相关解决方案建立新的事件响应机制。10% 的企业至少开展过一次 AI 专项

事件响应演练，仅 8% 的企业定期开展此类演练（图 34）。

图 34：AI 事件响应演练

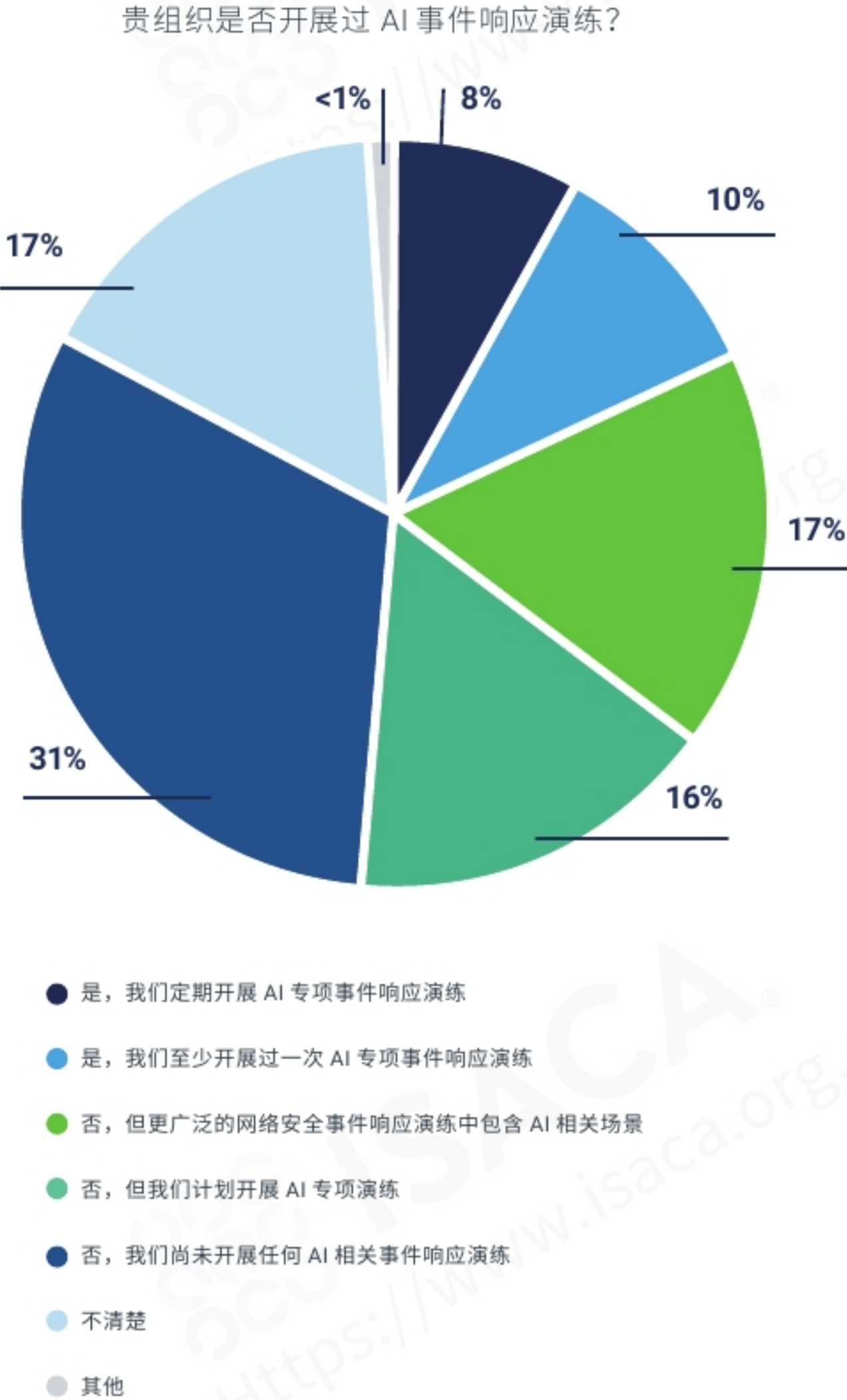
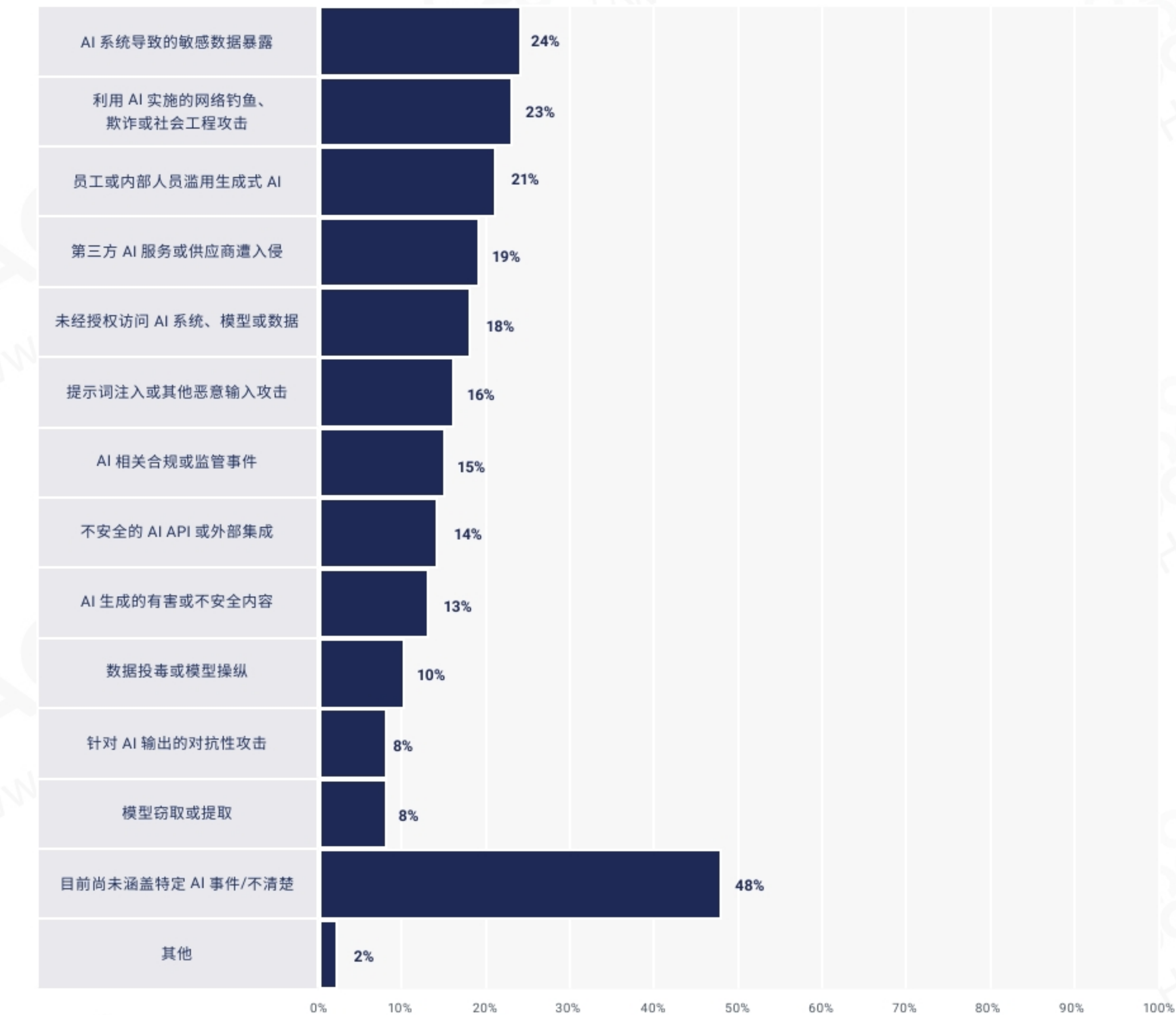


图 35 展示了事件响应演练涵盖的 AI 相关事件类型。最主要的 AI 相关事件包括 AI 系统导致的敏感数据暴露（24%）、利用 AI 实施的网络钓鱼、欺诈或社会工程攻击（23%），以及员工或内部人员滥用生成式 AI（21%）。8% 的受访者表示，

其事件响应演练涵盖针对 AI 输出的对抗性攻击。这些结果表明，在采用 AI 的过程中，行业关注的重点是对能够访问组织内部敏感信息和数据集的用户群体进行管理。

图 35：事件响应演练中的 AI 相关事件类型

贵组织的事件响应演练涵盖以下哪些类型的 AI 相关事件？

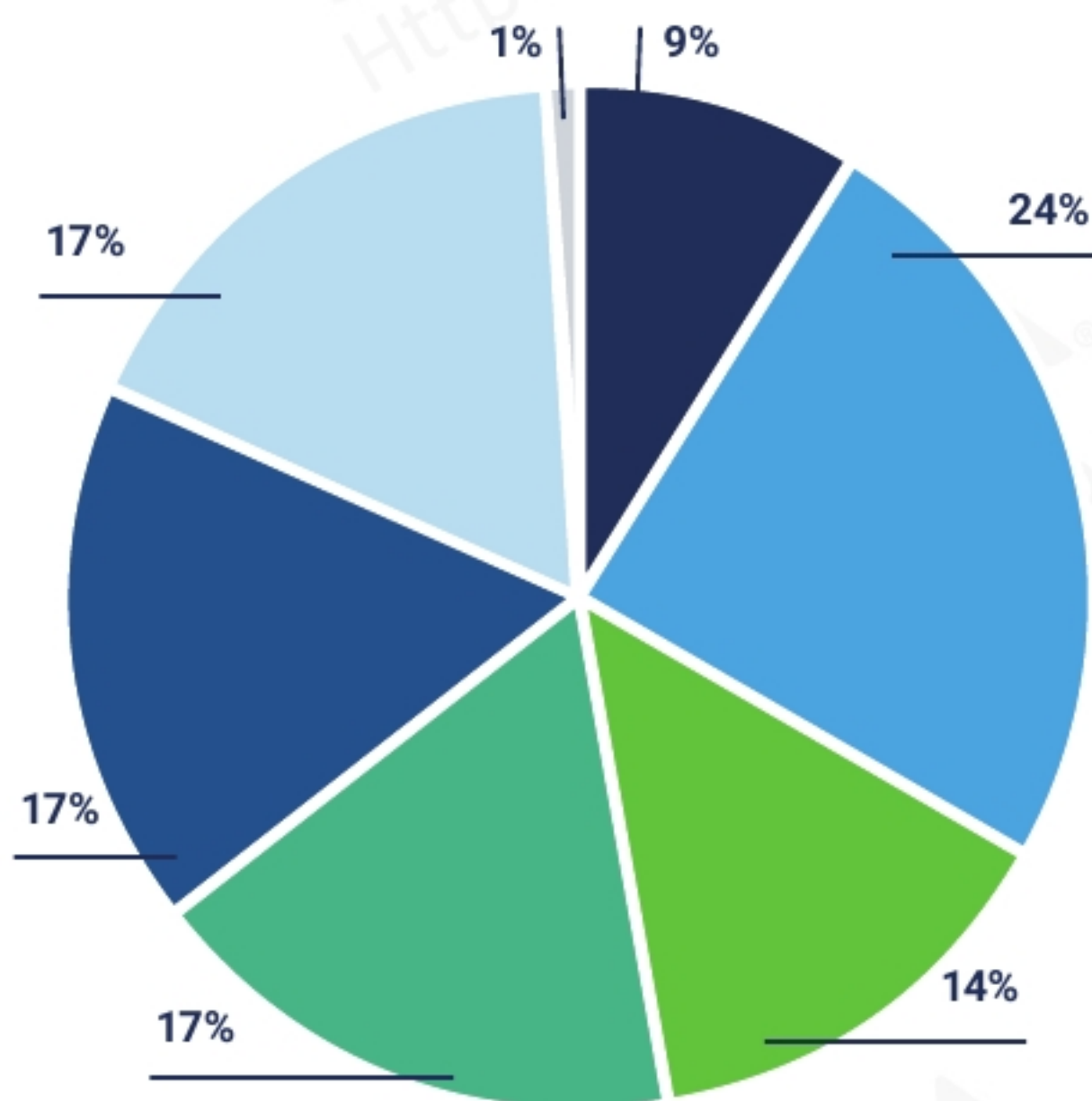


对于已采取一定控制措施的企业而言，其应对第三方和供应商相关 AI 风险的准备仍较为有限（24%）。仅 9% 的受访者表示，其所在企业已建立成熟的管理体系，针对第三方使用的 AI 系统

制定了完善的政策，并开展评估和监控；另有不少企业仍在制定相关方案（17%），或尚未将这一领域纳入其管理体系（17%）。图 36 展示了具体情况。

图 36：第三方使用的 AI 系统网络风险

您如何描述贵组织应对第三方提供商、供应商或合作伙伴所使用的 AI 系统相关网络安全风险的方式？



- 我们已建立成熟、正式的管理体系，制定了 AI 专项政策，并开展相关评估和监控
- 我们已采取部分 AI 专项管控措施，但覆盖范围有限
- 我们仅通过现有的通用第三方风险管理流程进行管理
- 我们正在制定相关方案，但尚未实施
- 我们目前尚未开展这方面的工作
- 不清楚
- 其他

结论： 网络安全承压，正值关键转折期

2026 年调查结果显示，网络安全环境持续承压，长期存在的挑战依然突出。AI 正通过重塑工作流程、改变威胁形势以及增加治理要求进一步加剧这种压力，但 AI 的应用并未降低对高技能从业人员、人工监督和扎实安全基础的需求。

人才队伍方面的调查结果仍值得关注。企业在填补网络安全职位空缺方面仍面临困难，而该行业依然高度依赖从其他领域转入的人才。与此同时，提供初级职位空缺的企业较少，因为市场需求主要集中在经验丰富的从业人员和具备较强技术能力的专业人员。

这种失衡带来了长期隐忧——如果雇主继续优先考虑工作经验，而日常工作又日益自动化，新进入网络安全领域的专业人员可能会更难获得积累实操经验的机会，从而难以掌握进入该领域并实现职业发展所需的技能。这一问题凸显了更有针对性地加强人才队伍培养的必要性。

人才留任仍与工作条件密切相关。受访者指出，工作压力大、晋升和发展机会有限以及薪酬激励不足是网络安全专业人员离职的主要原因。灵活的工作安排和休假有助于留住人才，但这些措施并不能从根本上缓解人员不足、威胁形势复杂以及持续高负荷工作带来的结构性压力。从这个意义上说，人才留任不仅是人才队伍问题，也关系到组织韧性。

人才留任不仅是人才队伍问题，也关系到组织韧性。

在运营和治理层面，AI 的影响已十分明显。安全团队已在一定程度上应用 AI，尤其是在威胁检测、响应支持和日常任务处理方面。然而，AI 的应用速度正在超过相关准备工作的推进速度。许多受访者表示，其在 AI 实施、政策制定和治理方面的参与程度仍较为有限，而开展 AI 专项事件响应演练或制定专项操作手册的企业也相对较少。这并不意味着 AI 需要一套独立的安全模式，而是意味

着必须更加扎实地落实既有安全体系中的各项要求——尤其是数据安全、事件响应、访问管理和治理——从而更全面地应对 AI 相关风险。

有关威胁的调查结果进一步印证了这一点。受访者认为，威胁环境日益复杂，AI 辅助攻击也越来越令人担忧。然而，在曾遭受安全入侵的组织中，最常见的攻击向量仍是较为传统的社会工程和漏洞。这表明，即使攻击方式不断演变，攻击造成的后果仍在很大程度上取决于人为行为、暴露面管理和控制措施落实等基础环节的薄弱之处。对于从业者和管理者而言，结论十分明确：韧性仍有赖于对各项基础工作的严格落实。

然而，在曾遭受安全入侵的组织中，最常见的攻击向量仍是较为传统的社会工程和漏洞。这表明，即使攻击方式不断演变，攻击造成的后果仍在很大程度上取决于人为行为、暴露面管理和控制措施落实等基础环节的薄弱之处。

总体而言，今年的调查结果显示，网络安全行业正在适应新的要求，而长期存在的挑战并未因此缓解。AI 如今已成为网络安全运营的现实组成部分，但调查结果并不支持仅凭技术就能解决网络安全核心挑战的观点。为了持续提升数字信任与韧性，组织需要在人才队伍培养、治理、运营和风险管理方面采取更加有力的措施。

致谢

主要编撰人

ISACA 内部出版物

董事会

Massimo Migliuolo, 主席

Cedro 和 Kibe 创始人兼董事, 马来西亚

Jamie Norton, 副主席

CISA、CISM、CGEIT、CIPM、CISSP、FGIA、GAICD、NACD.DC

澳大利亚证券和投资委员会首席信息安全官, 澳大利亚

Stephen Gilfus

NACD.DC

哈佛大学认证公司董事, 美国

Niel Harper

CISA、CRISC、CDPSE、CISSP、NACD.DC

德国

Gabriela Hernández-Cardoso

NACD.DC

GE 墨西哥前总裁兼首席执行官, 墨西哥

Jason Lau

CISA、CISM、CGEIT、CRISC、CDPSE、AAIA、AAISM、CEH、CIPM、CIPP/E、CIPT、CISSP、FIP、HCISPP、SM IEEE

Crypto.com 全球首席信息安全官, 新加坡

Maureen O'Connell

NACD.DC

Scholastic Corporation 前执行副总裁兼首席财务官, 美国

Erik Prusch

ISACA 首席执行官, 美国

Tim Sattler

CISA、CISM、CGEIT、CRISC、CDPSE、CCSP、CISSP、ISO 27000 LI/LA、NACD.DC

Jungheinrich AG 企业信息安全副总裁兼首席信息安全官, 德国

Asaf Weisberg

CISA、CISM、CGEIT、CRISC、CSX-P、CDPSE

introSight Ltd. 创始人兼首席执行官, 以色列

John De Santis

ISACA 董事会主席, 2023-2026 年美国

Pamela Nigro

ISACA 董事会主席, 2022-2023 年

CISA、CGEIT、CRISC、CDPSE、CRMA Medecision 高级副总裁兼安全官, 美国

Tracey Dedrick

ISACA 董事会主席, 2020-2021 年

First Bancorp Puerto Rico 董事兼风险委员会主席; Hudson City Bancorp 前首席风险官, 美国

关于 ISACA

ISACA (www.isaca.org) 致力于支持全球技术人才队伍，共同增进对技术的信任。55 年来，ISACA 为其由 19.5 万余名会员组成的全球社区提供知识、专业认证、培训和人脉网络，助力会员在信息安全、治理、鉴证、风险管理、数据隐私和新兴技术等领域实现职业发展。ISACA 在超过 195 个国家设有分支机构，包括全球 230 多个分会，并针对会员职业生涯的各个阶段提供相应资源，帮助他们在快速变化的数字环境中不断发展、推动可信创新，共同构建更加安全的数字世界。ISACA 还通过 ISACA 基金会拓展 IT 和教育领域的职业发展路径，为培养下一代技术专业人才创造更多机会。

关于 Wolters Kluwer TeamMate

Wolters Kluwer TeamMate 提供专为治理、风险与合规 (GRC) 及审计打造的解决方案，帮助审计、风险、合规和控制团队更加自信、精准地开展工作。凭借灵活且可配置的解决方案，TeamMate 能够适应团队当前的工作方式，并可无缝扩展，以满足其未来不断变化的需求。TeamMate 业务遍及全球，并拥有深厚的本地专业知识，可随时随地为组织提供支持。通过整合鉴证、风险和合规等领域的数据，TeamMate 为管理层提供互联互通的实时风险视图，从而强化决策能力，推动企业实现更具韧性的经营绩效。

免责声明

ISACA 设计并编制了《2026 年网络安全现状：全球劳动力、资源与网络安全运营更新报告》（以下简称“本作品”），主要供专业人士学习和参考之用。ISACA 无法保证使用本作品就一定能够实现成功的结果。本作品不应被视为包含所有适用的信息、程序和测试，不排除在其它信息、程序和测试的合理指导下获得同样结果的可能。在确定任何具体信息、程序或测试的适宜性时，专业人员应就具体的情况（特定的系统或信息技术环境）做出自己专业性的判断。

保留权利

© 2026 ISACA。版权所有。

《2026 年网络安全现状：全球劳动力、资源与网络安全运营更新报告》



1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

电话: +1.847.660.5505

传真: +1.847.253.1755

支持: support.isaca.org

网站: www.isaca.org

加入 ISACA 在线论坛:

<https://engage.isaca.org/onlineforums>

X: www.x.com/ISACANews

领英:

www.linkedin.com/company/isaca

脸书:

www.facebook.com/ISACAGlobal

Instagram:

www.instagram.com/isacanews/