## 致谢

## 主要作者

Hillary Baron

## 贡献者

Josh Buker

Marina Bregkou

Ryan Gifford

Sean Heide

Alex Kaluza

John Yeoh

## 平面设计

Claire Lehnert

Stephen Lumpe

## 特别鸣谢

Jessica Mulreany

## 赞助商

谷歌云打造了面向现在和未来的AI、基础建设、开发者、数据、安全和协作的工具，是走向云计算的新通道。谷歌云利用其覆盖全球的基础设施、定制芯片、生成式AI模型、开发平台和基于AI的应用程序提供了一个强大的、完全集成的、优化的AI技术栈来帮助组织进行云计算转型。超过200个国家和地区选择谷歌云作为他们信任的技术合作伙伴。

# 目录

致谢

赞助商

调查创建和方法论

研究目标

关键发现和模式

关键发现1：安全专家对AI的谨慎乐观态度

关键发现2：AI会助力而非取代安全专家

关键发现3：公司管理层和员工对AI持不同的观点

关键发现4：2024年是AI实施之年 - 为变革做好准备

结论

所有调查结果

当前安全状况

网安领域对AI的感知和态度

对AI的行业熟悉度

AI应用的整体规划

AI员工、领导力和培训

网络安全领域的生成式AI计划

人员统计数据

# 调查创建和方法论

云安全联盟（CSA）是一个致力于在云计算和IT技术领域中推广网络安全最佳实践的非营利组织。CSA也教导了云计算和IT行业从业者各种计算机方面的安全问题。云安全联盟的成员主要是云计算、IT和安全领域从业者、企业和专业人士协会。云安全联盟的一个主要目标是调查评估信息安全的主要趋势。这些调查包含了组织们的安全成熟度现状、意见、兴趣、信息安全和技术方面的意向等信息。

谷歌云委托云安全联盟进行调查和报告来更好地理解关于AI方面的行业知识、态度和看法。谷歌云资助了此项目，并和CSA的研究分析人员共同完成调查问卷的设计。云安全联盟于2023年11月在线发布该调查，并收到了来自美洲、亚太地区、欧洲和中东组织的IT和安全专业人士的2486份回复。云安全联盟的研究分析人员对该报告进行了数据分析和解读。

# 研究目标

本次调查的目的主要是更深入地了解：

* 当前安全挑战
* 网安行业对AI的看法
* 对AI的行业熟悉度
* 行业里的AI应用计划
* AI对人员配备和培训的影响

## 关键发现和模式

AI在网安领域的出现标志着数字防御领域变革时代的来临，AI带来了可预见的突破和错综复杂的挑战。AI可能成为强化安全防御、识别新型威胁和实现快速响应的关键工具。然而，将AI集成到网络安全的旅程障碍重重，包括需要减轻社会对军民两用的担忧、弥补技术差距和适度鼓励而非过度依赖自动化系统。深入了解行业专家们对AI在网安领域演进的看法和准备，对于大家引导此项转变和构建弹性的、前瞻性的数字基础建设有着重要作用。

关键发现1：

安全专家对AI的谨慎乐观态度

安全专业人士对AI持谨慎乐观的态度。大部分安全专业人士（63%）相信AI在加强安全度量方面的潜力，特别是提高威胁检测和响应能力。然而，人们对AI潜在的恶意使用也有着敏锐的意识，以下两种看法证实了这点：34%的人认为AI对安全团队更有利，而31%的人认为AI对保护者和攻击者同样有利。

值得注意，有25%的受访者担心AI可能对恶意方更有利，这也表明了他们对潜在的AI使能的高级网络威胁极度关注。

即使更多网络安全专家将AI视作对防御者更有利的工具，而非攻击者的盛宴，仍存在一些对安全领域中使用AI的疑虑。这些担忧主要集中在可能引发意外偏见的数据质量（如，用于模型训练的数据）、AI系统的不透明性（通常被称为‘黑匣子’问题）和管理复杂AI系统的技术/专业知识差距。

这些发现展现了网安社区的一个平衡观点。虽然网络安全专家对AI在加强安全方面持有乐观态度，但也明确意识到其潜在的滥用风险和可能带来的挑战。为确保防御者在快速发展和AI驱动的网安领域中对恶意者保持领先，需要不断进化的安全策略、严格的数据处理、透明的AI模型以及在更新安全协议时持续保持警惕。另外，确保AI系统的安全是一个关键问题，这意味着完整AI技术保护框架的需求。此话题没有在本次调查范围内，但仍是人们最关注的问题。

关键发现2：

AI会助力而非取代安全从业者

AI被视作安全从业者的赋能工具而非替代品。在网络安全现状调查的威胁调查和响应方面，大部分的安全专业人士表示有不同程度的挑战，仅有12%的受访者表示这项任务在他们的组织中没有任何困难。这也确定了AI作为赋能工具的角色。只有很少一部分（12%）的安全专业人士认为AI会完全取代他们的工作角色。30%的人认为AI会帮助他们加强部分安全技能，28%的人认为AI可以全面支持他们的工作，24%的人认为AI可以取代他们大部分的工作角色，这让他们可以脱身去完成其他任务。

这种观点进一步由组织对安全团队实施AI的预期结果所支持。预期结果聚焦在AI加强了安全团队的知识储备（36%），提高了威胁检测效率（26%）和提高生产力（26%），而非减少劳动力（20%）。这与他们的工作角色将会进化而非被取代的观点一致，74%的组织计划在未来五年内组建新的团队来监控AI的安全使用。

尽管受访者非常重视作为AI实施预期效果的团队技能和知识强化，但在最大安全挑战排名时，他们仍将人才排在末尾，而将操劳和威胁检测放在更高的排名。这种差异也许意味着，虽然通过AI增强团队能力是高优先级内容，但安全工作负载管理和威胁识别所面临的工作挑战被视为更紧迫或可能更难以解决的问题。很明显，AI网安领域不仅转型了现有的工作角色，也为新的专业岗位铺平了道路。

然而，有半数的受访者担心对AI的过度依赖，强调在AI驱动安全和人工驱动安全之间的平衡需求。考虑到前文提及的数据质量和AI系统缺少透明度的问题，这个担心尤其相关。

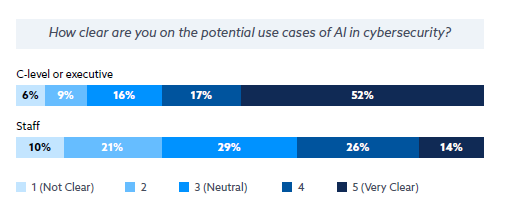
总之，这些发现强调了即使AI会给安全团队带来很大改变，但它主要被视作对安全团队的补充工具而非完全的替代品。AI被设计来帮助弥补困扰行业的技术和知识储备差距，同时人们普遍对过度依赖AI有着合理的担忧。AI集成对网络安全领域的未来有着深远的影响，网络安全领域注定将随着工作角色的改变和新职位的涌现而不断进化。

Page 10

关键发现3：

**企业高管们对人工智能的看法与员工不同**

企业高管和员工的回答凸显了在很多领域内对人工智能知识及其在其组织内使用的脱节。高管对人工智能技术的熟悉程度明显高于其员工。例如，52%的高管表示非常熟悉生成式人工智能(gen AI)，与之形成鲜明对比的是，只有11%的普通员工熟悉生成式人工智能。



*~~图例翻译~~*{

你对人工智能在网络安全中的潜在用例有多清楚?

高管

员工

1不清楚

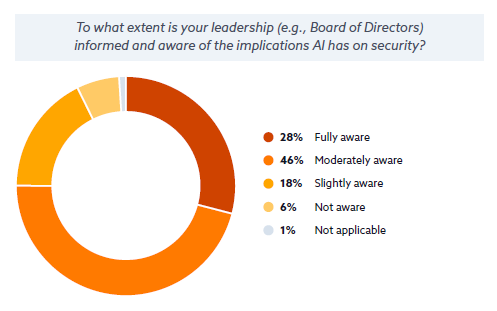
3中等

5非常清楚

}

高管层报告称，高管对人工智能用例有着比员工更清晰的理解，其中，51%的高管表示对此非常清楚，相比而言只有14%的员工表示对此非常清楚。这些差异可能表明高管对人工智能的熟悉程度被高估了，或者他们与员工对人工智能相关知识储备存在非常大的差异。后一种含义得到了行业内普遍看法的认可，即领导层了解并意识到人工智能对安全的影响，74%的人表示他们的领导层完全或适度意识到这一点。这种高度的意识可能是由于组织领导者有浓厚兴趣在其组织内采用人工智能，82%的受访者表示他们的执行领导层和董事会正在推动人工智能的采用。

组织领导者自上而下推动采用人工智能的压力表明，他们可能已经调研了人工智能技术及其用途以及了解人工智能如何使他们的组织受益。然而，值得注意的是该方法可能不完全符合员工的实际准备或理解，可能导致实现层面的挑战，如关键发现2中所述。



*~~图例翻译~~*{

你们的领导层(例如董事会)在多大程度上了解并意识到人工智能对安全的影响?

28%完全清楚

46%基本清楚

18%略微清楚

6%不清楚

1%不适用

}

以上调查可能突出了对采用和实施这种独特和颠覆性技术(例如：提示工程)所面临的困难和所需要的知识的认识缺乏。

Page 11

总的来说，这种模式强调了在网络安全领域实施人工智能对加强沟通、教育和协作方法的关键需求。高管和员工在人工智能技术熟悉程度和对其实施的理解方面存在差距，因此需要制定更具包容性和明智的战略，以应对人工智能在网络安全领域的不断发展。

关键发现4：

**2024年是人工智能实施的一年——准备好迎接变革**

2024年将是人工智能在安全领域应用的革命性一年，超过一半(55%)的组织正在计划实施生成式人工智能解决方案。

组织正在广泛的范围内探索这些技术的各种用例，其中最主要的用例是创建规则 (21%)、模拟攻击 (19%)和监测非合规行为 (19%)。然而，计划用例的分布是相当均匀的，这表明人工智能具有赋能多种应用的潜力。



*~~图例翻译~~*{

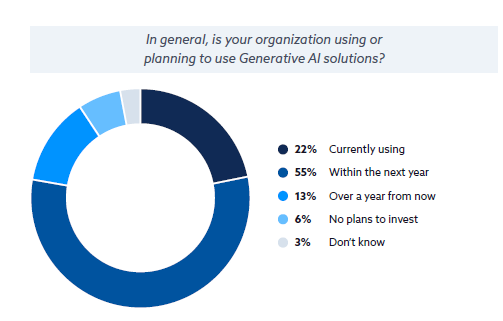
您的组织计划如何将生成式人工智能用于网络安全?(选择前3个用例)?

|  |  |  |
| --- | --- | --- |
| 21%创建规则  19%模拟攻击  19%监测非合规行为  16%网络检测  16%降低误报  15%培训发展和支持  14%异常分类 | 13%自然语言搜索  13%威胁总结  13%数据防泄漏，保护知识产权  11%用户行为分析  10%自动生成报告  10%端点检测  9%事件日志汇总 | 9%取证分析  9%聊天机器人  8%事件总结  8%配置漂移  8%行动/补救建议  7%代码分析 |

}

Page 12

尽管人们对以各种方式实现人工智能感到兴奋和渴望，但仍有重大障碍需要克服。最突出的挑战是技能差距和员工短缺，33%的受访者(尤其是高管)表达了顾虑，这说明该问题的重要性。其他障碍被选择的频率要低得多:资源分配(11%)和对人工智能风险的充分理解(10%)。这些挑战凸显了针对性技能提升、新人才招聘以及用于管理先进人工智能系统的明确战略的必要性。



*~~图例翻译~~*{

总体来说，你的组织正在使用或计划使用生成式人工智能解决方案吗?

22%目前使用

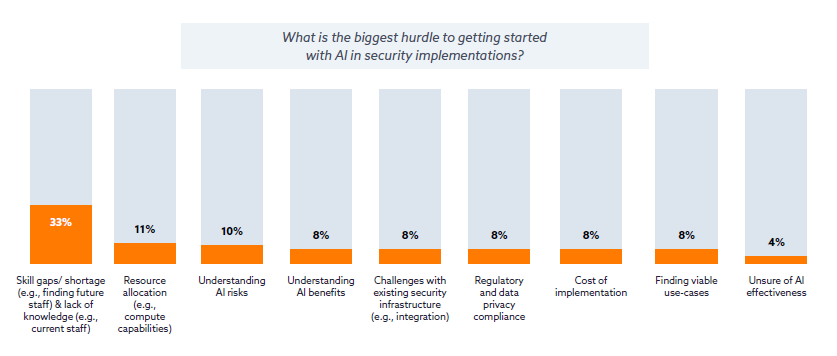
55%在接下来的一年

13%一年多以后

5%没有投资计划

3%不知道

}



*~~图例翻译~~*{

在安全实现中开始使用AI的最大障碍是什么?

33%技能差距/短缺(例如：寻找未来的员工)和知识缺乏(例如：现有员工)

11%资源分配(例如，计算能力)

10%了解人工智能风险

8%了解人工智能收益

8%现有安全基础设施的挑战(例如：集成)

8%法规和数据隐私遵从性

8%实施成本

8%寻找可行的用例

4%不确定人工智能的有效性

}

在人们对人工智能技术日益增长的兴趣和多样化应用的推动下，2024年将是人工智能在网络安全领域的关键一年。推进生成式AI应用的工作得到了董事会和领导层的强烈支持，突显了执行决策在推动组织内部技术进步方面的关键作用。然而，启动人工智能工作的最大挑战——技能差距和员工短缺——强调了需要从战略层面来提升人工智能工作必须的专业知识和资源，以便在网络安全中有效实施人工智能。

Page 13

结论

人工智能在网络安全领域的现状呈现出一个多面的景象，其特点包括谨慎乐观、赋权而非替代、高管和员工之间的理解差异，以及2024年人工智能实施的强劲势头。这种复杂的局面强调，需要一种平衡的、明智的方法来将实现人工智能在网络安全的集成，将战略领导力与全体员工参与、培训相结合，以有效地应对不断演变的网络威胁格局。

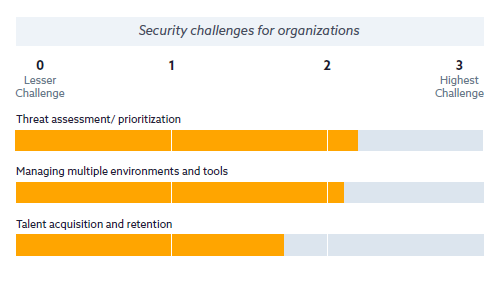
Page 14

全部调查发现

**安全现状**

组织面临的最大安全挑战

组织内的大多数挑战可以分为三个“T”:辛劳(Toil)、威胁(Threat)和人才(Talent)。受访者将这些挑战在其组织内部进行排序，威胁(即：威胁评估和优先级分级)排在首位，紧随其后的是辛劳(例如：管理多个环境和工具)。最后，尽管业内一直关注人才和技能差距，人才在这些挑战中排名最低。



*~~图例翻译~~*{

组织面临的安全挑战

更少挑战 最高挑战

威胁评估和优先级分级

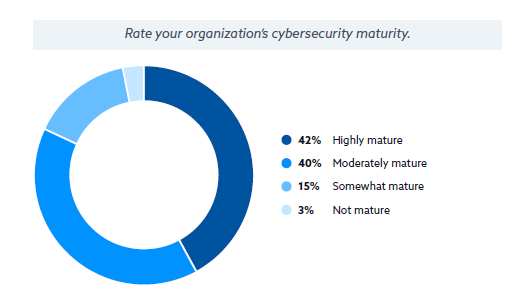
管理多个环境和工具

人才获得与留存

}

组织的网络安全成熟度

企业对自身的网络安全评价很高，42%的企业认为自己高度成熟，另有40%的企业认为自己中度成熟。只有15%的人认为自己有点成熟，3%的人认为自己不成熟。看到这么少的人处于最低的类别当然令人鼓舞，但看到这么多人给他们的组织如此高的评价也令人惊讶。



*~~图例翻译~~*{

对您所在组织的网络安全成熟度进行评分

42%高度成熟

40%中度成熟

15%有点成熟

3%不成熟

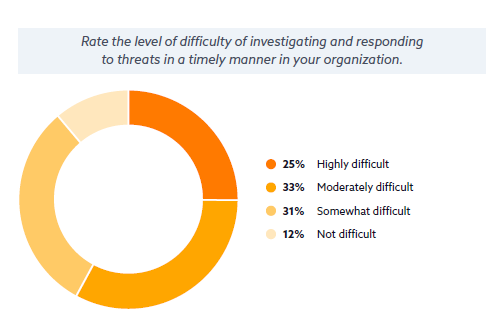
}

也许这是一种准确的反映，但它也可能代表安全专业人员对自己的工作过于自信。下一项发现可能会支持后一个论点。

Page 15

**及时调查和应对威胁的困难程度**

调查和响应威胁对组织构成的困难程度似乎差别很大，但值得注意的是，尽管看到他们的组织相当成熟，但很少有人(12%)表示完成这项任务没有困难；相对平均数量的组织认为这有点困难(31%)或中等困难(33%)；近四分之一的受访者表示，这是一项非常艰巨的任务。也许安全专业人员在评估其成熟度时没有考虑这个指标。它还可能表明，无论您的组织有多成熟，这都是一项艰巨的任务。



*~~图例翻译~~*{

对您所在组织进行及时调查和响应威胁的困难程度进行评分

25%高度困难

33%中度困难

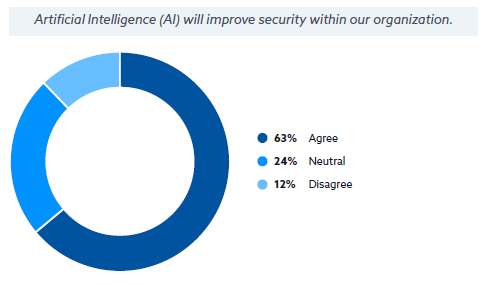
31%有点困难

12%没有困难

}

**对网络安全中人工智能的认知和态度**

关于人工智能作为组织安全增强器的观点



*~~图例翻译~~*{

人工智能(AI)将提高我们组织内部的安全性

63%同意

24%中立

12%不同意

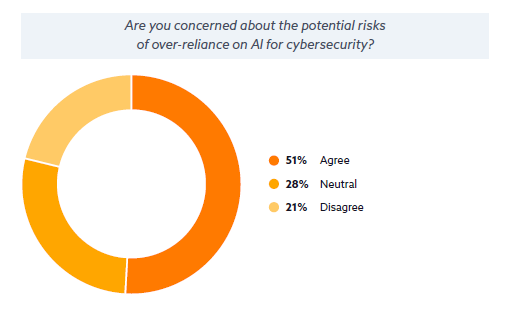
}

安全专业人士对人工智能在提高其组织内部安全性方面的影响持乐观态度。大多数人(63%)认为人工智能将增强安全性，这主要是由于人们对自动化程度提高的期望以及该技术协助安全措施的潜力。然而，有相当一部分受访者(24%)保持中立，可能反映出不确定性或观望态度。这可能是由于人们对跟上人工智能技术的快速发展和日益复杂的步伐的担忧。一个较小但重要的群体(12%)不同意人工智能将提高安全性的观点，这可能是由于担心不法分子利用人工智能或管理这种先进技术会面临挑战。这些不同的反应也可能受到人工智能技术在炒作周期中的当前位置的影响，这表明随着对人工智能在网络安全方面的能力的熟悉和理解的增长，期望和信心水平可能会发生变化。

Page 16

**对网络安全过度依赖人工智能的担忧**

有人对人工智能持怀疑态度。一些安全专业人士看到了过度依赖人工智能来实现网络安全的潜在风险，结果展现出几乎一半受访者持相同观点。大约51%的人认为，人们担心过度依赖人工智能，这反映出人们对从网络安全中去除重要的人为因素持一定程度的怀疑态度。这种担忧可能源于这样一种认识，即人工智能系统虽然先进，但并非万无一失，可能需要人类的监督来监控和解决问题。此外，人们意识到，随着人工智能在网络安全领域的广泛应用，可能会出现不可预见的挑战。值得注意的是，28%的受访者保持中立，这表明对人工智能的利益和风险持不确定或平衡的看法。与此同时，21%的人不同意这种担忧，这可能表明对人工智能的可靠性有信心，或者相信现有的保障措施和反应机制足以解决潜在的人工智能缺陷。这种意见分歧凸显了将人工智能整合到网络安全中的复杂性，需要在技术进步与保留关键的人类判断和监督之间取得平衡。



*~~图例翻译~~*{

你是否担心在网络安全方面过度依赖人工智能的潜在风险?

51%同意

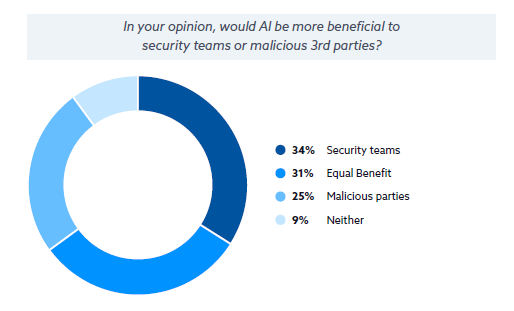
28%中立

21%不同意

}

人工智能给安全带来的利益和风险

安全专业人士对谁将从人工智能中获益更多持谨慎和潜在微妙的观点:安全专业人士或者恶意方。约34%的受访者认为，人工智能将主要使安全团队受益，这表明人们对人工智能在加强网络安全防御方面的作用普遍持乐观态度。然而，接近31%的受访者认为人工智能为安全团队和恶意行为者提供了同等的好处，这突显了人们对人工智能技术在网络安全中的双重用途的认识。25%的人认为人工智能可能对恶意方更有利，如果人工智能被恶意使用，将带来潜在的威胁。



*~~图例翻译~~*{

在你看来，人工智能是对安全团队更有利，还是对恶意第三方更有利?

34%安全团队

31%对等收益

28%恶意第三方

9%双方都不是

}

一小部分人(9%)认为它对安全团队和恶意第三方都没有明显的好处，或者现在下结论还为时过早。这反映了一种潜在的情绪，即考虑到人工智能与网络安全的整合尚处于早期阶段，其全面影响和潜力仍存在许多未知因素。调查结果表明，受访者普遍持谨慎乐观态度，倾向于人工智能对安全团队的帮助稍微多一些，但他们清楚地认识到，如果人工智能工具落入坏人之手或被对手利用，网络那请将面临重大风险。

### Security benefits and risks with AI

### AI 在安全领域的收益和风险

Security professionals have a cautious and potentially nuanced perspective of who will benefit from AI more: security professionals or

*In your opinion, would AI be more beneficial to security teams or malicious 3rd parties?*

malicious parties. About 34% believe that AI will primarily benefit security teams, suggesting a general optimism about AI’s role in bolstering cybersecurity defenses.

|  |  |
| --- | --- |
| **34%** | Security teams |
| **31%** | Equal Benefit |
| **25%** | Malicious parties |
| **9%** | Neither |

However, a closely matched 31% see AI as offering equal benefits to both security

*在您看来，AI 对安全团队还是对第三方恶意行为者更有利？*



|  |  |
| --- | --- |
| **34%** | 对安全团队有利 |
| **31%** | 同样有利 |
| **25%** | 对恶意行为者有利 |
| **9%** | 两者都无受益 |

安全专家在评估 AI 更有利于安全团队还是恶意行为者时，持有一种谨慎且微妙的观点。大约 34% 的人认为 AI 主要有助于安全团队，这反映出他们对 AI 在提升网络安全防护能力方面持乐观态度。

然而，也有 31% 的人认为 AI 对安全团队和恶意行为者的益处相当，

这显示出他们对 AI 技术在网络安全中可能出现是“双刃剑”特性有所警觉。此外，还有 25% 的人认为 AI 可能更有利于恶意方，他们认为如果 AI 被用于恶意目的，可能带来潜在的威胁。

还有一小部分人 (9%) 认为目前无法明确判断 AI 对安全团队还是恶意第三方更有利的情况，或认为现在做出判断还为时尚早。这种看法反映出一个基本观点：由于 AI 融入网络安全领域还处于初步阶段，其全面的影响和潜力仍充满不确定性。调查结果显示出一种谨慎的乐观态度，大多数受访者倾向于认为 AI 会稍微更多地帮助安全团队，但他们也清楚地意识到，如果 AI 工具被不当使用或被敌对势力利用，可能会带来重大风险。

### 在安全领域对 AI 的最大担忧

安全从业者对 AI 在网络安全真实场景中的应用表达了各种担忧，这反映出 AI 集成应用的复杂性和多元性。最主要的忧虑是数据质量，38% 的人提到了非预期偏见的风险，这与对准确性的担忧（24% 的人提及）密切相关。因为 AI 常被视为客观工具，所以这一点非常关键；输入到 AI 系统的数据质量和完整性直接影响到输出的准确性和可靠性。同样地，36% 的人对 AI 系统的不透明性表示担心，他们强调了某些 AI 算法的“黑盒”特性，这使得理解和信任 AI 所做的决策变得更加困难。

其他显著的担忧还包括管理 AI 所需的技能和专业知识（有 33% 的专业人士提到这一点），这显示出他们意识到需要专业的知识来有效地整合和监管 AI 技术。此外，分别有 28% 和 25% 的人关注 [数据投毒](https://spectrum.ieee.org/ai-cybersecurity-data-poisoning) 和 幻觉 ，这与数据泄露或丢失及隐私问题（各有 25% 的提及）密切相关。这些问题虽然相对较少为人所知，但仍被认识到是随着 AI 更广泛使用而可能出现的潜在风险。种种担忧表明，安全专业人员在谨慎考虑 AI 的所有可能影响，他们认识到技术的快速演进意味着当前的次要问题可能变成未来的主要挑战。

*What are your biggest concerns regarding AI in security? (Select up to 3)*

**38%**

**36%**

**33%**

**28%**

**25%**

**25%**

**25%**

**24%**

**21%**

Data quality (e.g., unintended bias)

Lack of transparency

Skills and expertise for managing

Data poisoning Hallucinations Privacy

Data leakage or loss

Accuracy

Misuse

*您最担心的有关 AI 在安全领域的问题有哪些？（最多选择 3 项）*

**38%**

**36%**

**33%**

**28%**

**25%**

**25%**

**25%**

**24%**

**21%**

数据质量(如：非预期偏见)

不透明性

技能和专业知识

数据污染 幻觉 隐私

数据泄露或丢失

准确性

滥用

### Impact of AI on current cybersecurity roles

### AI 对当前网络安全行业岗位的影响

Within the cybersecurity field, professionals widely anticipate that AI will have a significant impact on their

*Please select the option that best reflects your opinion about AI's potential impact on your role. Over the next 5 years, AI will...*

roles over the next five years. This sentiment reflects the disruptive nature of AI in the workplace. A substantial number (58%) perceive AI as a tool that will support and enhance their current roles.

Specifically, 30% believe AI will help enhance certain aspects of their skillset, while 28%

see it as an overall support

 **30%** Help enhance parts of your skillset

|  |  |
| --- | --- |
| **28%** | Support you overall in your current role |
| **24%** | Replace a large part of your role |
| **12%** | Completely replace your role |
| **5%** | Not impact your role |

to their existing functions. This perspective underscores the potential of AI to augment human capabilities, especially in automating manual and routine tasks. Technologies like AI-driven chatbots and analytical tools are expected to streamline operations and increase efficiency, assisting security professionals in more effectively managing their workload. Freeing their time up from more menial tasks to focus on more complex and creative elements of their job role.

在网络安全领域，专业人士广泛预计，在未来五年内，AI 将对他们的工作职责和岗位产生显著影响。这种观点反映了 AI 在职场中的颠覆性。有相当一部分人（58%） 认为 AI 将成为支持和提升他们当前工作职能的工具。

*请选择一个选项，以最佳反映您对 AI 在未来五年对您的岗位可能产生的影响的观点。未来 5 年内，AI 将...*

具体来说，有 30% 的人相信 AI 将有助于提升他们的某些技能，而 28% 的人认为 AI 将全面支持他们现有的工作职责。

 **30%** 帮助增强部分技能



|  |  |
| --- | --- |
| **28%** | 在当前的工作中提供整体支持 |
| **24%** | 替代职责中的大部分 |
| **12%** | 完全取代您的岗位 |
| **5%** | 对您的岗位没有影响 |

这种看法突出了 AI 提高人类能力的可能性，尤其是在将人工执行和日常工作自动化的方面。诸如 AI 驱动的聊天机器人和分析工具等技术有望简化流程并提升效率，从而协助安全专家更加高效地处理工作负载。这样，他们就可以将时间从繁琐的任务中解放出来，转而关注职责中更为复杂和更有创造性的能力。

There’s a notable concern among these professionals about AI’s ability to replace human roles. About 24% foresee AI replacing significant parts of their job, and 12% even predict a complete replacement of their role. This apprehension is more pronounced in aspects of cybersecurity work that are heavily manual or repetitive, where AI’s capabilities for automation are most directly applicable. It’s important to recognize that while AI is seen as a supportive and enhancing tool, its potential to disrupt existing job structures in cybersecurity is also a key consideration. Security professionals are thus faced with the dual challenge of leveraging AI for its benefits while also preparing for the shifts it may bring in the job market, highlighting the importance of adaptability and continuous skill development in this rapidly evolving field.

然而，专业人士对 AI 取代人类职位的能力也表示出显著的担忧。约 24% 的人预计 AI 将取代他们工作的重要部分，还有 12% 的人甚至预测 AI 将完全取代他们的职位。这种担忧在网络安全领域中那些人工执行或重复性工作上明显体现，因为 AI 在这些方面的自动化能力最为直接适用。重要的是，要认识到 AI 虽然被看作是一种支持和增强工具，但其颠覆现有岗位和职能结构的潜在可能性也是网络安全领域需要重视的关键因素。因此，安全专业人员面临的双重挑战是，一方面要利用 AI 带来的好处，另一方面也要为其可能引发的职场变革做好准备，这突显了在这快速发展变化的领域中，适应性和持续技能提升的重要性。

### Confidence in organizations’ skills to execute a security strategy leveraging AI

### 对组织利用 AI 能力实施安全策略的信心

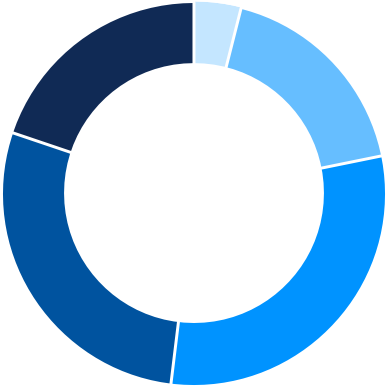
In the cybersecurity sector, there’s a cautiously optimistic view regarding organizations’ readiness to leverage AI. About 48% of professionals express confidence in their organization’s ability to implement AI strategies effectively, with 28% feeling reasonably confident and 20% very confident. This level of assurance is intriguing, considering the nascent stage of AI in this field. It suggests that many professionals might be optimistic about their preparedness or overlook the intricacies of AI integration, a classic scenario of an unknown unknown.

在网络安全行业中，安全从业人员对组织准备利用 AI 的能力持谨慎乐观态度。大约 48% 的专业人员对他们的组织有效地实施 AI 策略的能力表示有信心，其中 28% 的人认为相当有信心，20% 的人非常有信心。考虑到 AI 在该领域还处于初期阶段，这种程度的信心显得尤为引人注意。这种情况表明，许多专业人士可能对他们的准备情况过于乐观，或者忽视了 AI 集成应用的复杂性，这是一个“不知之不知”（对未知情况的未知）的经典示例。

Conversely, a notable 30% remain neutral, indicating either a balanced recognition of their capabilities or uncertainty about the challenges AI might pose.

The remaining 22% show less confidence, including 18% who are somewhat unconfident and 4% who are not confident at all. This spread in confidence levels across the cybersecurity community points to a complex landscape where

*How confident are you about your organization’s skills to execute a strategy for leveraging AI in security?*

 **4%** 1 (Not Confident)

 **18%** 2

 **30%** 3 (Neutral)

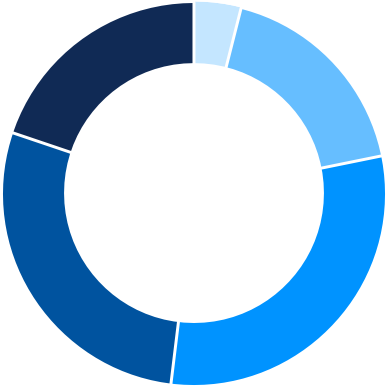
 **28%** 4

 **20%** 5 (Very Confident)

some AI applications are seen as straightforward and readily deployable, while others, more complex and novel, evoke caution and uncertainty.

另一方面，有 30% 的人持中立态度，这可能表明他们对自己的能力有一个平衡的认识，或者对 AI 可能带来的挑战感到不确定性。其余的 22% 对此表示出较低的信心，其中 18% 的人表示有些不自信，4% 的人则完全不自信。网络安全界对信心水平的这种分布揭示了一个复杂的局面：一些 AI 应用被认为是简单直接、容易部署的，而其他更为复杂和新颖的应用则引发了安全从业人员对于 AI 的谨慎和不确定性。

*您对您的组织在安全方面利用 AI 实施策略的能力有多少信心？*

 **4%** 1 （完全不自信)

 **18%** 2

 **30%** 3 （中立态度）

 **28%** 4

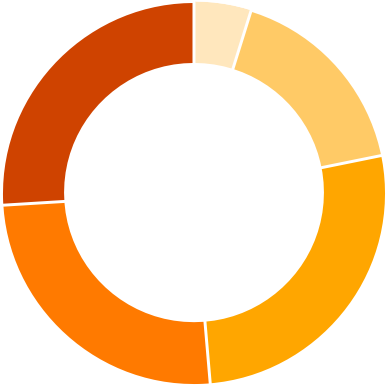
 **20%** 5 （非常自信）

### Confidence in organizations’ skills to execute a security strategy to protect AI systems

### 对组织在保护核心业务或使命中利用AI能力实施安全策略的信心

In assessing confidence levels regarding the execution

*How confident are you about your organization's skills to execute a security strategy for protecting AI used in your core business/mission?*

of a security strategy for protecting AI within core business or mission functions, there is a comparable yet slightly more confident

|  |  |
| --- | --- |
| **4%** | 1 (Not Confident) |
| **17%** | 2 |
| **27%** | 3 (Neutral) |
| **25%** | 4 |
| **26%** | 5 (Very Confident) |

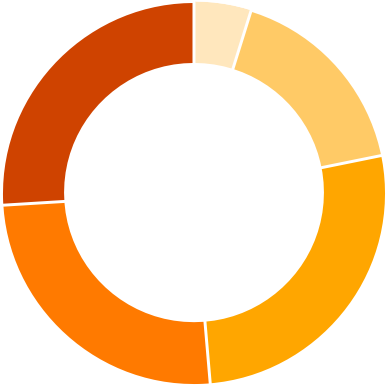
stance among professionals compared to their views on leveraging AI in security.

About 51% of respondents lean towards confidence, with 25% feeling reasonably confident and 26% very confident. This slightly higher

confidence level, particularly in the ‘very confident’ category, is notable. However, it also suggests a potential underestimation of the unique challenges and threats associated with securing AI systems, possibly due to a perception of AI as just another application in the business environment.

On the other hand, 27% of respondents adopt a neutral stance, perhaps reflecting a cautious acknowledgment of the complexities involved or an uncertainty about the emerging threats specific to AI. The lower confidence spectrum includes 17% who are somewhat unconfident and 4% who

are not confident at all. The overall trend indicates that while many professionals are confident in their organization’s ability to protect AI systems, there’s still a significant portion that recognizes the unknowns and potential underestimation of threats.

在评估专业人士对执行保护核心业务或使命中 AI 系统的安全策略的信心水平时，相较于他们对在安全领域利用 AI 的看法，这里表现出了近似但略高于前者的信心。

*您对您的组织在保护核心业务或使命中使用 AI 能力实施安全策略有多少信心？*

|  |  |
| --- | --- |
| **4%** | 1 （完全不自信） |
| **17%** | 2 |
| **27%** | 3 （中立态度） |
| **25%** | 4 |
| **26%** | 5 （非常自信） |

约 51% 的回答者倾向于表示有信心，其中 25% 表示相当自信，26% 表示非常自信。尤其是在“非常自信”这一类别中，这种较高的信心水平值得关注。

然而，这也可能暗示了人们可能低估了保护 AI 系统所面临的独特挑战和威胁，这种低估可能源于将 AI 视为仅仅是业务环境中的一种常规应用的观念。

另一方面，有 27% 的受访者持中立态度，这或许反映了他们对涉及的复杂性持谨慎的态度或对 AI 特有的新兴威胁感到不确定。信心较低的群体中，17% 的人表示有些不自信，4% 的人则完全不自信。整体趋势显示，虽然许多专业人士对他们的组织在保护 AI 系统方面的能力感到自信，但仍有一大部分人意识到了存在的未知因素和可能被低估的威胁。

## Industry Familiarity with AI

## AI 在行业中的成熟度

### Familiarity with AI technologies and systems

### 对 AI 技术和系统的熟悉程度

The survey results regarding familiarity with various AI

*Rate your familiarity with the following AI technologies or systems:*

technologies and systems across the cybersecurity sector show a general trend of moderate to somewhat familiarity. Weighted averages for technologies like Natural Language Processing

(NLP), Generative Artificial Intelligence (gen AI), Deep Learning, Expert Systems, Machine Learning, LLM (Language Models like Gemini or GPT-4), and Robotics fall within a narrow range. This indicates that, generally, if professionals are familiar with one of these technologies, they likely have a comparable understanding of the others.

**0 1**

Not familiar

NLP (Natural Language Processing tools)

GenAI (Generative Artificial Intelligence)

DL (Deep Learning using neural networks)

Expert Systems (Rule-based AI)

ML (Machine Learning)

LLM (Language Models like GP-T3 or GPT-4)

Robotics (AI-driven robots)

**2 3 4**

Highly familiar

Interestingly, there’s a slight inclination towards older,

more established terms like NLP and Deep Learning, which score marginally higher than newer terms like LLM and gen AI. This could suggest a conflation between gen AI and popular tools like ChatGPT, indicating that while such tools are well-known, there may not be a deep understanding of the broader category of gen AI. This surface-level familiarity across various AI technologies might also contribute to the observed overconfidence in implementing AI strategies, as professionals might not fully grasp the complexities of these technologies.

*请对以下 AI 技术或系统的熟悉程度进行评分：*

网络安全行业内对各种 AI 技术和系统的熟悉程度的调查结果显示，总体趋势是从中等到某种程度的熟悉。涉及自然语言处理（NLP）、生成式人工智能（Gen AI）、深度学习、专家系统、机器学习、大语言模型（如 Gemini 或 GPT-4）和机器人技术的加权平均值都在一个较窄的范围内。这表明，在这些技术中，如果专业人士熟悉其中的一种，他们很可能对其他技术也有在一定程度上类似的了解。

**0 1**

非常不熟悉

自然语言处理（NLP）工具

生成式人工智能（GenAI）

深度学习（DL）神经网络

专家系统（基于规则的人工智能）

机器学习（ML）

大语言模型（LLM）如 GPT-3 或 GPT-4

机器人技术（AI 驱动）

**2 3 4**

非常熟悉

有趣的是，调查结果显示，

相较于比较新的术语，如大语言模型（LLM）和生成式人工智能（Gen AI），人们倾向于更为人熟知的成熟技术，如自然语言处理（NLP）和深度学习。这可能暗示了人们将生成式 AI 与 ChatGPT 等流行工具混淆。虽然这些工具广为人知，但对生成式 AI 这一更广泛类别的深入理解可能不足。这种对各种 AI 技术的熟悉度表象也可能是导致在执行 AI 策略时观察到的过度自信的因素之一，因为专业人员可能没有完全理解这些技术的复杂性。

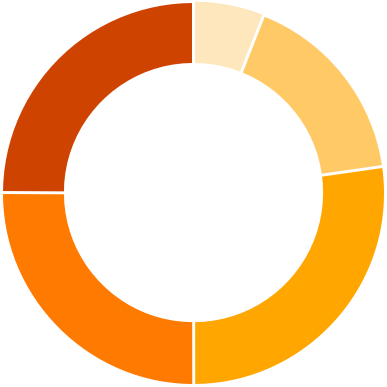
This lack of deep understanding raises questions about the effectiveness of current strategies and the need for further education in these areas. Comparatively, C-level executives report higher

familiarity with all AI categories compared to staff. This discrepancy in familiarity may be due to the pressure from leadership within organizations to explore adoption of AI. It likely requires leadership in the C-suite to familiarize themselves with a wide variety of AI technologies to identify which may provide the greatest benefits to their organizations. This gap in understanding underscores the importance of comprehensive education and training in AI technologies to ensure their effective and secure implementation especially for staff that is responsible for the implementation.

这种对 AI 技术深度理解的缺失，提出了关于目前策略有效性的质疑，并突显了对这些领域进一步教育和培训的必要性。相较于普通员工，首席级别（C级）高管认为他们对所有 AI 类别的熟悉度更高。这种熟悉度的差距可能源于组织内部领导层对探索 AI 应用的推动。首席级别（C级）高管可能需要对各种 AI 技术有广泛的了解，以便识别哪些技术可能为他们的组织或单位带来最大的好处。这种理解上的差异突显了对 AI 技术进行全面教育和培训的重要性，以确保其有效和安全地实施，尤其是对于那些负责实施的员工。

### Clarity of potential AI use cases in cybersecurity

### 网络安全领域中 AI 潜在应用案例的了解程度

The understanding of potential AI use cases in cybersecurity shows a split perspective,

*How clear are you on the potential use cases of AI in cybersecurity?*

with professionals divided on their clarity regarding AI applications. Overall, 50% of respondents feel clear

 **6%** 1 (Not Clear)

 **17%** 2

|  |  |  |
| --- | --- | --- |
| about AI use cases, with 25% | **27%** | 3 (Neutral) |
| somewhat clear and another | **25%** | 4 |
| 25% very clear. However, the | **25%** | 5 (Very Clear) |
| other half of the respondents |  | |
| express less certainty, with |
| 27% neutral, 17% somewhat |
| unclear, and 6% very unclear |
| about AI’s potential roles. |

*How clear are you on the potential use cases of AI in cybersecurity?*

C-level or executive

**52%**

**17%**

**16%**

**9%**

**6%**

Staff

**14%**

**26%**

**29%**

**21%**

**10%**

1 (Not Clear) 2 3 (Neutral) 4 5 (Very Clear)

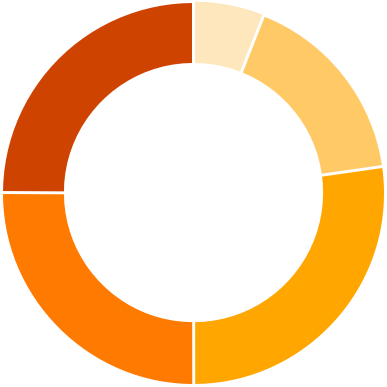
A notable difference emerges when comparing responses from C-level executives

and staff. Among C-level executives, a significant 52% report being very clear on AI use cases in cybersecurity, compared to

only 14% of staff feeling the same. This stark contrast

might suggest that C-level executives have a more aspirational or vision-oriented understanding of AI, focusing on broader goals and potentials, whereas staff, who are typically closer to the practical implementation, might be more aware of the complexities and uncertainties involved. It’s interesting to note that staff usually tend to buy into new technologies like AI earlier than the C-suite, yet in this case, their lower clarity could be influenced by the operational challenges they

foresee. The high level of awareness and clarity among C-level executives aligns with the increasing presence of AI in the news and its growing significance in the corporate zeitgeist.



*您对对 AI 在网络安全中潜在使用案例的了解程度如何？*

|  |  |  |
| --- | --- | --- |
|  | **27%** | 3 （中立） |
| **25%** | 4 |
| **25%** | 5 （非常清楚） |
|  | |

网络安全领域中对潜在 AI 应用案例的理解显示出存在一定的分歧，专业人士在对 AI 应用的了解程度上意见不统一。总体来看，有 50% 的受访者认为对 AI 应用案例有清楚了解，其中 25% 觉得比较清楚，另外 25% 非常清楚。然而，另一半受访者则表现出较低的了解程度，27% 表示中立，17% 觉得不太清楚，6% 认为非常不清楚。

 **6%** 1 （完全不清楚）

 **17%** 2

*您对网络安全中AI潜在应用案例的清晰程度如何？*

首席级别（C级）或高级管理人员

**52%**

**17%**

**16%**

**9%**

**6%**

其他工作人员

**14%**

**26%**

**29%**

**21%**

**10%**

1（完全不清楚） 2 3（中立） 4 5 （非常清楚）

在比较首席级别（C 级）高管和普通员工受访者的反馈时，呈现出一个明显的差异。在首席级别（C 级）高管中，有高达 52% 的人表示对 AI 在网络安全中的应用场景有非常清晰的认识，而只有 14% 的普通员工有同样的感受。

这种鲜明的对比可能说明，首席级别（C 级）高管对 AI 的理解更加具有远见和目标导向，他们关注的是更广泛的目标和潜力；而在普遍情况下，员工因为负责具体的实施工作，可能更清楚其涉及的复杂性和不确定性。有趣的是，虽然员工通常比高层更早接受像 AI 这样的新兴技术，但在这种情况下，他们对 AI 较低的了解程度可能受到预见到的运营挑战影响。首席级别（C 级）高管中的高度意识和清晰理解，与 AI 在新闻中的频繁出现以及在企业文化中逐渐占据的重要地位是相符合的。

### Awareness of AI security frameworks

A significant 88% of security professionals are aware of existing AI security frameworks, such as those based on NIST guidelines in the US. However, it’s crucial to note that awareness does not necessarily equate to usage or deep understanding of these frameworks. Only 12% of respondents report not being aware of any AI security frameworks, highlighting the widespread recognition of these standards in the cybersecurity community yet leaving room for further exploration of their practical application and comprehension.

**88%**

*Are you aware of any existing AI security frameworks?*

## General Plans to Use AI

### Current use of AI products in general

 **69%** Currently using

 **29%** Planning to use

 **2%** Not using and no plans

 **88%** Yes

 **12%** No

The use or planned use of AI products in organizations suggests a few possibilities:

*Does your organization use or plan to use AI products in general?*

AI may be integrated into many products that organizations are using,

but staff might not be fully aware of this integration or may not recognize these as AI-driven products.

Alternatively, it could indicate a gap in understanding or communication within the organization, where C-level

executives believe they are utilizing AI more extensively than their staff are aware, or they might overestimate their actual use of AI technologies. This discrepancy underscores the need for clearer communication and education about AI applications and usage within organizations, ensuring that executives and staff consistently understand how AI is being leveraged in their work environment.

### 对 AI 安全框架的认识

**88%**

*您了解目前有哪些 AI 安全框架吗？*

大部分（88%）的安全专业人士了解现有的 AI 安全框架，如基于美国 NIST 指南的框架。然而值得注意的是，对这些框架的了解并不意味着它们的深入理解和使用。仅有 12% 的调查参与者表示他们不了解任何 AI 安全框架，这表明这些标准在网络安全界得到了广泛的认可，同时也显示出在这些框架的实际应用和深入理解方面还有进一步的探索空间。

### 关于 AI 的总体使用计划

### 目前普遍使用的 AI 产品情况

 **69%** 正在使用

 **29%** 计划使用

 **2%** 没有也不计划使用

 **88%** 了解

 **12%** 不了解

组织中使用或打算使用 AI 产品暗示了几种可能性：AI 可能已经融入了许多组织正在使用的产品中，然而，员工可能并未完全意识到这种集成和融合，或者可能没能认识到这些产品是由 AI 驱动的。

*您的组织目前是否使用或有计划使用 AI 产品？*

另一方面，这也可能暗示组织内部存在理解或沟通的差距，

首席级别（C 级）高管认为他们在使用 AI 的程度上可能超过了员工的认知，或者他们可能高估了实际使用 AI 技术的范围。这种差异突显了组织内部需要更明确的沟通和对 AI 应用及使用的教育和培训，确保高管和员工都能一致地理解 AI 在他们的工作环境中是如何被运用的。

### Security benefits and risks with AI

### AI 在安全领域的收益和风险

Security professionals have a cautious and potentially nuanced perspective of who will benefit from AI more: security professionals or

*In your opinion, would AI be more beneficial to security teams or malicious 3rd parties?*

malicious parties. About 34% believe that AI will primarily benefit security teams, suggesting a general optimism about AI’s role in bolstering cybersecurity defenses.

|  |  |
| --- | --- |
| **34%** | Security teams |
| **31%** | Equal Benefit |
| **25%** | Malicious parties |
| **9%** | Neither |

However, a closely matched 31% see AI as offering equal benefits to both security

*在您看来，AI 对安全团队还是对第三方恶意行为者更有利？*



|  |  |
| --- | --- |
| **34%** | 对安全团队有利 |
| **31%** | 同样有利 |
| **25%** | 对恶意行为者有利 |
| **9%** | 两者都无受益 |

安全专家在评估 AI 更有利于安全团队还是恶意行为者时，持有一种谨慎且微妙的观点。大约 34% 的人认为 AI 主要有助于安全团队，这表明人们对于人工智能在增强网络安全防御方面的作用普遍持乐观态度。

然而，也有 31% 的人认为 AI 对安全团队和恶意行为者的益处相当，

teams and malicious actors, highlighting an awareness of the dual-use nature of AI technologies in cybersecurity. This is further underscored by the 25% who think AI might be more advantageous to malicious parties, acknowledging the potential threat if AI is used with malicious intent.

这显示出人们对 AI 技术在网络安全中可能出现的“双刃剑”特性有所警觉。此外，还有 25% 的人认为 AI 可能更有利于恶意方，他们认为如果 AI 被用于恶意目的，可能带来潜在的威胁。

A smaller segment (9%) feels that it’s neither clearly beneficial to security teams nor malicious 3rd parties, or it’s too early to tell. This reflects an underlying sentiment that, given the early stage of AI’s integration into cybersecurity, there’s still a lot of unknowns about its full impact and potential. The results indicate a cautious optimism where respondents generally lean towards AI helping security teams slightly more, but there’s a clear recognition of the significant risks if AI tools fall into the wrong hands or are exploited by adversaries.

还有一小部分人 (9%) 认为目前无法明确判断 AI 对安全团队还是恶意第三方更有利的情况，或认为现在做出判断还为时尚早。这种看法反映出一个基本观点：由于 AI 融入网络安全领域还处于初步阶段，其全面的影响和潜力仍充满不确定性。以上调查结果显示出一种谨慎的乐观态度，大多数受访者倾向于认为 AI 会稍微更多地帮助安全团队，但人们也清楚地意识到，如果 AI 工具被不当使用或被敌对势力利用，可能会带来重大风险。

### Greatest concerns with AI in security

### 在安全领域对 AI 的最大担忧

Security professionals express a range of concerns regarding the implementation of AI in cybersecurity, reflecting the complexity and multifaceted nature of AI integration. The top concern, cited by 38%, is data quality, specifically the risk of unintended bias, which is closely linked to concerns about accuracy (24%). This connection is significant, as AI is often perceived as an objective tool; thus, the quality and integrity of data fed into AI systems directly influence the accuracy and reliability of their outputs. Similarly, 36% are wary of the lack of transparency in AI systems, highlighting the ‘black box’ nature of some AI algorithms that can make understanding and trust in AI decisions challenging.

安全专家对 AI 在网络安全真实场景中的应用表达了各种担忧，这反映出 整合AI 应用的复杂性和多面性。最主要的忧虑是数据质量，38% 的人提到了预期外偏见的风险，这与对准确性的担忧（24% 的人提及）密切相关。这一点非常关键，因为 AI 常被视为客观工具，而输入到 AI 系统的数据质量和完整性直接影响到输出的准确性和可靠性。同样地，36% 的人对 AI 系统的不透明性表示担心，他们强调了某些 AI 算法的“黑盒”特性，这使得理解和信任 AI 所做的决策变得更加困难。

Other notable concerns include skills and expertise for managing AI, mentioned by 33% of professionals, indicating an awareness of the need for specialized knowledge to effectively integrate and oversee AI technologies. [Data poisoning](https://spectrum.ieee.org/ai-cybersecurity-data-poisoning) and [hallucinations](https://www.ibm.com/topics/ai-hallucinations), concerns for 28% and 25% respectively, are closely related issues, along with data leakage or loss, and privacy concerns, each noted by 25% of respondents. These issues are relatively less understood but nonetheless acknowledged as potential risks that could emerge with more extensive AI usage. The broad range of concerns suggests that security professionals are cautiously considering all possible implications of AI, recognizing that the technology’s rapid evolution means that today’s secondary concerns could become tomorrow’s primary challenges.

其他显著的担忧还包括管理 AI 所需的技能和专业知识（有 33% 的专业人士提到这一点），这显示出他们意识到需要专业的知识来有效地整合和监管 AI 技术。此外，分别有 28% 和 25% 的人关注 [数据污染](https://spectrum.ieee.org/ai-cybersecurity-data-poisoning) 和 幻觉 ，这与数据泄露或丢失及隐私问题（各有 25% 的提及）密切相关。这些问题虽然相对而言更不易被理解，但仍被认为是随着 AI 更广泛使用而可能出现的潜在风险。如此广泛的担忧表明，安全专业人员在谨慎考虑 AI 的所有可能影响，他们认识到技术的快速演进意味着当前的次要问题可能变成未来的主要挑战。

*What are your biggest concerns regarding AI in security? (Select up to 3)*

**38%**

**36%**

**33%**

**28%**

**25%**

**25%**

**25%**

**24%**

**21%**

Data quality (e.g., unintended bias)

Lack of transparency

Skills and expertise for managing

Data poisoning Hallucinations Privacy

Data leakage or loss

Accuracy

Misuse

*您最担心的有关 AI 在安全领域的问题有哪些？（最多选择 3 项）*

**38%**

**36%**

**33%**

**28%**

**25%**

**25%**

**25%**

**24%**

**21%**

数据质量(如：预期外偏见)

不透明性

技能和专业知识

数据污染 幻觉 隐私

数据泄露或丢失

准确性

滥用

### Impact of AI on current cybersecurity roles

### AI 对当前网络安全行业岗位的影响

Within the cybersecurity field, professionals widely anticipate that AI will have a significant impact on their

*Please select the option that best reflects your opinion about AI's potential impact on your role. Over the next 5 years, AI will...*

roles over the next five years. This sentiment reflects the disruptive nature of AI in the workplace. A substantial number (58%) perceive AI as a tool that will support and enhance their current roles.

Specifically, 30% believe AI will help enhance certain aspects of their skillset, while 28%

see it as an overall support

 **30%** Help enhance parts of your skillset

|  |  |
| --- | --- |
| **28%** | Support you overall in your current role |
| **24%** | Replace a large part of your role |
| **12%** | Completely replace your role |
| **5%** | Not impact your role |

to their existing functions. This perspective underscores the potential of AI to augment human capabilities, especially in automating manual and routine tasks. Technologies like AI-driven chatbots and analytical tools are expected to streamline operations and increase efficiency, assisting security professionals in more effectively managing their workload. Freeing their time up from more menial tasks to focus on more complex and creative elements of their job role.

在网络安全领域，专业人士广泛预计，在未来五年内，AI 将对他们的工作职责和岗位产生显著影响。这种观点反映了 AI 在职场中的颠覆性。有相当一部分人（58%） 认为 AI 将成为支持和提升他们当前工作职能的工具。

*请选择一个选项，以最佳反映您对 AI 在未来五年对您的岗位可能产生的影响的观点。未来 5 年内，AI 将...*

具体来说，有 30% 的人相信 AI 将有助于提升他们的某些技能，而 28% 的人认为 AI 将全面支持他们现有的工作职责。

 **30%** 帮助增强部分技能



|  |  |
| --- | --- |
| **28%** | 在当前的工作中提供整体支持 |
| **24%** | 替代职责中的大部分 |
| **12%** | 完全取代您的岗位 |
| **5%** | 对您的岗位没有影响 |

这种看法突出了 AI 提高人类能力的可能性，尤其是在将人工执行和日常工作自动化的方面。诸如 AI 驱动的聊天机器人和分析工具等技术有望简化流程并提升效率，从而协助安全专家更加高效地处理工作。这样，他们就可以将时间从繁琐的任务中解放出来，转而关注职责中更为复杂和更需要创造性的部分。

There’s a notable concern among these professionals about AI’s ability to replace human roles. About 24% foresee AI replacing significant parts of their job, and 12% even predict a complete replacement of their role. This apprehension is more pronounced in aspects of cybersecurity work that are heavily manual or repetitive, where AI’s capabilities for automation are most directly applicable. It’s important to recognize that while AI is seen as a supportive and enhancing tool, its potential to disrupt existing job structures in cybersecurity is also a key consideration. Security professionals are thus faced with the dual challenge of leveraging AI for its benefits while also preparing for the shifts it may bring in the job market, highlighting the importance of adaptability and continuous skill development in this rapidly evolving field.

然而，专业人士对 AI 取代人类职位的能力也表示出明细的担忧。约 24% 的人预计 AI 将取代他们工作的重要部分，还有 12% 的人甚至预测 AI 将完全取代他们的职位。这种担忧更明显的体现在网络安全领域中那些手动的或重复性的工作上，因为 AI 在这些方面的自动化能力最为直接适用。重要的是，要认识到 AI 虽然被看作是一种支持和增强工具，但其颠覆现有岗位和职能结构的潜在可能性也是网络安全领域需要重视的关键因素。因此，安全专业人员面临的双重挑战是，一方面要利用 AI 带来的好处，另一方面也要为其可能引发的职场变革做好准备，这突显了在这快速发展变化的领域中，适应性和持续的技能提升的重要性。

### Confidence in organizations’ skills to execute a security strategy leveraging AI

### 对组织利用 AI 能力实施安全策略的信心

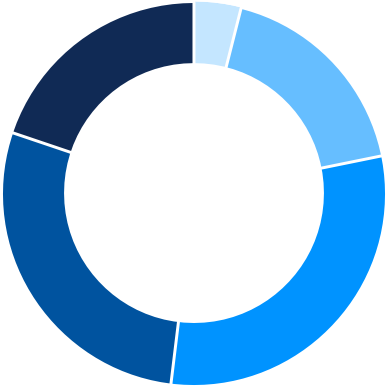
In the cybersecurity sector, there’s a cautiously optimistic view regarding organizations’ readiness to leverage AI. About 48% of professionals express confidence in their organization’s ability to implement AI strategies effectively, with 28% feeling reasonably confident and 20% very confident. This level of assurance is intriguing, considering the nascent stage of AI in this field. It suggests that many professionals might be optimistic about their preparedness or overlook the intricacies of AI integration, a classic scenario of an unknown unknown.

在网络安全行业中，安全从业人员对组织准备利用 AI 的能力持谨慎乐观态度。大约 48% 的专业人员对他们的组织有效地实施 AI 策略的能力表示有信心，其中 28% 的人认为相当有信心，20% 的人非常有信心。考虑到 AI 在该领域还处于初期阶段，这种程度的信心显得尤为引人注意。这种情况表明，许多专业人士可能对他们的准备情况过于乐观，或者忽视了 AI 集成应用的复杂性，这是一个“不知道自己不知道什么”的经典场景。

Conversely, a notable 30% remain neutral, indicating either a balanced recognition of their capabilities or uncertainty about the challenges AI might pose.

The remaining 22% show less confidence, including 18% who are somewhat unconfident and 4% who are not confident at all. This spread in confidence levels across the cybersecurity community points to a complex landscape where

*How confident are you about your organization’s skills to execute a strategy for leveraging AI in security?*

 **4%** 1 (Not Confident)

 **18%** 2

 **30%** 3 (Neutral)

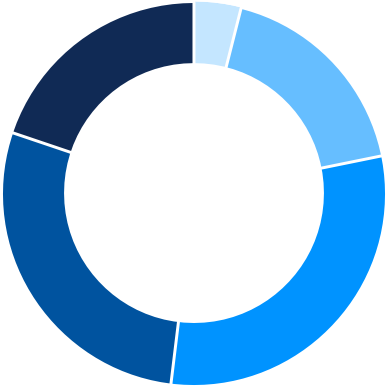
 **28%** 4

 **20%** 5 (Very Confident)

some AI applications are seen as straightforward and readily deployable, while others, more complex and novel, evoke caution and uncertainty.

另一方面，有 30% 的人持中立态度，这可能表明他们对自己的能力有一个平衡的认识，或者对 AI 可能带来的挑战感到不确定性。其余的 22% 对此表示出较低的信心，其中 18% 的人表示有些不自信，4% 的人则完全不自信。网络安全界对信心水平的这种分布揭示了一个复杂的局面：一些 AI 应用被认为是简单直接、容易部署的，而其他更为复杂和新颖的应用则引发了安全从业人员对于 AI 的谨慎和不确定性。

*您对您的组织在安全方面利用 AI 实施策略的能力有多少信心？*

 **4%** 1 （完全不自信)

 **18%** 2

 **30%** 3 （中立态度）

 **28%** 4

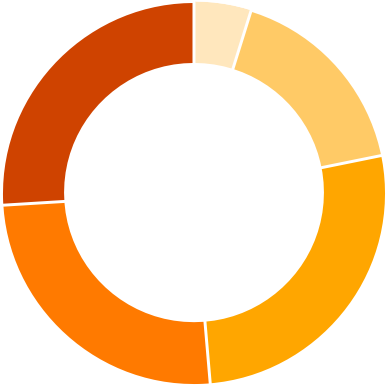
 **20%** 5 （非常自信）

### Confidence in organizations’ skills to execute a security strategy to protect AI systems

### 对组织实施安全策略以保护AI系统的信心

In assessing confidence levels regarding the execution

*How confident are you about your organization's skills to execute a security strategy for protecting AI used in your core business/mission?*

of a security strategy for protecting AI within core business or mission functions, there is a comparable yet slightly more confident

|  |  |
| --- | --- |
| **4%** | 1 (Not Confident) |
| **17%** | 2 |
| **27%** | 3 (Neutral) |
| **25%** | 4 |
| **26%** | 5 (Very Confident) |

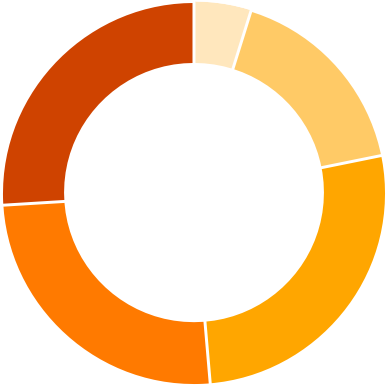
stance among professionals compared to their views on leveraging AI in security.

About 51% of respondents lean towards confidence, with 25% feeling reasonably confident and 26% very confident. This slightly higher

confidence level, particularly in the ‘very confident’ category, is notable. However, it also suggests a potential underestimation of the unique challenges and threats associated with securing AI systems, possibly due to a perception of AI as just another application in the business environment.

On the other hand, 27% of respondents adopt a neutral stance, perhaps reflecting a cautious acknowledgment of the complexities involved or an uncertainty about the emerging threats specific to AI. The lower confidence spectrum includes 17% who are somewhat unconfident and 4% who

are not confident at all. The overall trend indicates that while many professionals are confident in their organization’s ability to protect AI systems, there’s still a significant portion that recognizes the unknowns and potential underestimation of threats.

在评估专业人士对执行保护核心业务或任务中 AI 系统的安全策略的信心水平时，相较于他们对在安全领域利用 AI 的看法，这里表现出了近似但略高于前者的信心。

*您对您的组织实施安全策略以保护在您的核心业务或任务中使用的AI系统的能力有多少信心？*

|  |  |
| --- | --- |
| **4%** | 1 （完全不自信） |
| **17%** | 2 |
| **27%** | 3 （中立态度） |
| **25%** | 4 |
| **26%** | 5 （非常自信） |

约 51% 的回答者倾向于表示有信心，其中 25% 表示相当自信，26% 表示非常自信。尤其是在“非常自信”这一类别中，这种较高的信心水平值得关注。

然而，这也可能暗示了人们可能低估了保护 AI 系统所面临的独特挑战和威胁，这种低估可能源于将 AI 视为仅仅是业务环境中的一种常规应用的观念。

另一方面，有 27% 的受访者持中立态度，这或许反映了他们对涉及的复杂性持谨慎的态度或对 AI 特有的新兴威胁感到不确定。信心较低的群体中，17% 的人表示有些不自信，4% 的人则完全不自信。整体趋势显示，虽然许多专业人士对他们的组织在保护 AI 系统方面的能力感到自信，但仍有一大部分人意识到了存在的未知因素和可能被低估的威胁。

## Industry Familiarity with AI

## AI 在行业中的成熟度

### Familiarity with AI technologies and systems

### 对 AI 技术和系统的熟悉程度

The survey results regarding familiarity with various AI

*Rate your familiarity with the following AI technologies or systems:*

technologies and systems across the cybersecurity sector show a general trend of moderate to somewhat familiarity. Weighted averages for technologies like Natural Language Processing

(NLP), Generative Artificial Intelligence (gen AI), Deep Learning, Expert Systems, Machine Learning, LLM (Language Models like Gemini or GPT-4), and Robotics fall within a narrow range. This indicates that, generally, if professionals are familiar with one of these technologies, they likely have a comparable understanding of the others.

**0 1**

Not familiar

NLP (Natural Language Processing tools)

GenAI (Generative Artificial Intelligence)

DL (Deep Learning using neural networks)

Expert Systems (Rule-based AI)

ML (Machine Learning)

LLM (Language Models like GP-T3 or GPT-4)

Robotics (AI-driven robots)

**2 3 4**

Highly familiar

Interestingly, there’s a slight inclination towards older,

more established terms like NLP and Deep Learning, which score marginally higher than newer terms like LLM and gen AI. This could suggest a conflation between gen AI and popular tools like ChatGPT, indicating that while such tools are well-known, there may not be a deep understanding of the broader category of gen AI. This surface-level familiarity across various AI technologies might also contribute to the observed overconfidence in implementing AI strategies, as professionals might not fully grasp the complexities of these technologies.

*请对以下 AI 技术或系统的熟悉程度进行评分：*

网络安全行业内对各种 AI 技术和系统的熟悉程度的调查结果显示，总体趋势是从中等到某种程度的熟悉。涉及自然语言处理（NLP）、生成式人工智能（Gen AI）、深度学习、专家系统、机器学习、大语言模型（如 Gemini 或 GPT-4）和机器人技术的加权平均值都在一个较窄的范围内。这表明，在这些技术中，如果专业人士熟悉其中的一种，他们很可能对其他技术也有在一定程度上类似的了解。

**0 1**

非常不熟悉

自然语言处理（NLP）工具

生成式人工智能（GenAI）

深度学习（DL）神经网络

专家系统（基于规则的人工智能）

机器学习（ML）

大语言模型（LLM）如 GPT-3 或 GPT-4

机器人技术（AI 驱动）

**2 3 4**

非常熟悉

有趣的是，调查结果显示，

相较于比较新的术语，如大语言模型（LLM）和生成式人工智能（Gen AI），人们倾向于更为人熟知的成熟技术，如自然语言处理（NLP）和深度学习。这可能暗示了人们将生成式 AI 与 ChatGPT 等流行工具混淆。虽然这些工具广为人知，但对生成式 AI 这一更广泛类别的深入理解可能不足。这种对各种 AI 技术的都较熟悉的现象也可能是导致在执行 AI 策略时过度自信的因素之一，因为专业人员可能没有完全理解这些技术的复杂性。

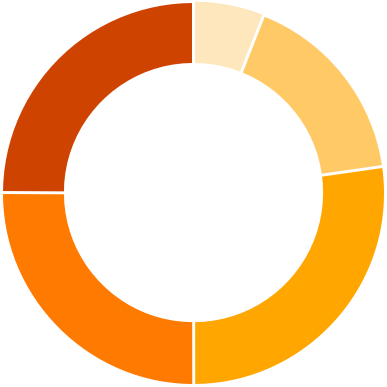
This lack of deep understanding raises questions about the effectiveness of current strategies and the need for further education in these areas. Comparatively, C-level executives report higher

familiarity with all AI categories compared to staff. This discrepancy in familiarity may be due to the pressure from leadership within organizations to explore adoption of AI. It likely requires leadership in the C-suite to familiarize themselves with a wide variety of AI technologies to identify which may provide the greatest benefits to their organizations. This gap in understanding underscores the importance of comprehensive education and training in AI technologies to ensure their effective and secure implementation especially for staff that is responsible for the implementation.

这种对 AI 技术深度理解的缺失，引出了关于目前策略有效性的质疑，并突显了对这些领域进一步教育和培训的必要性。相较于普通员工，首席级别（C级）高管认为他们对所有 AI 类别的熟悉度更高。这种熟悉度的差距可能源于组织内部领导层对探索 AI 应用的推动。首席级别（C级）高管可能需要对各种 AI 技术有广泛的了解，以便识别哪些技术可能为他们的组织或单位带来最大的好处。这种理解上的差异突显了对 AI 技术进行全面教育和培训的重要性，以确保其有效和安全地实施，尤其是对于那些负责具体实现的员工。

### Clarity of potential AI use cases in cybersecurity

### 网络安全领域中 AI 潜在用例的了解程度

The understanding of potential AI use cases in cybersecurity shows a split perspective,

*How clear are you on the potential use cases of AI in cybersecurity?*

with professionals divided on their clarity regarding AI applications. Overall, 50% of respondents feel clear

 **6%** 1 (Not Clear)

 **17%** 2

|  |  |  |
| --- | --- | --- |
| about AI use cases, with 25% | **27%** | 3 (Neutral) |
| somewhat clear and another | **25%** | 4 |
| 25% very clear. However, the | **25%** | 5 (Very Clear) |
| other half of the respondents |  | |
| express less certainty, with |
| 27% neutral, 17% somewhat |
| unclear, and 6% very unclear |
| about AI’s potential roles. |

*How clear are you on the potential use cases of AI in cybersecurity?*

C-level or executive

**52%**

**17%**

**16%**

**9%**

**6%**

Staff

**14%**

**26%**

**29%**

**21%**

**10%**

1 (Not Clear) 2 3 (Neutral) 4 5 (Very Clear)

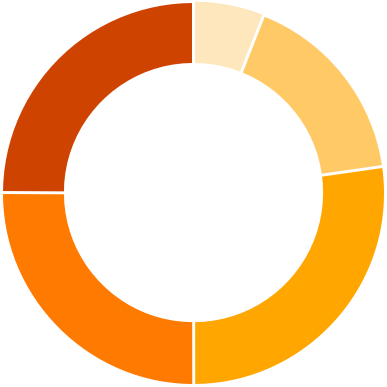
A notable difference emerges when comparing responses from C-level executives

and staff. Among C-level executives, a significant 52% report being very clear on AI use cases in cybersecurity, compared to

only 14% of staff feeling the same. This stark contrast

might suggest that C-level executives have a more aspirational or vision-oriented understanding of AI, focusing on broader goals and potentials, whereas staff, who are typically closer to the practical implementation, might be more aware of the complexities and uncertainties involved. It’s interesting to note that staff usually tend to buy into new technologies like AI earlier than the C-suite, yet in this case, their lower clarity could be influenced by the operational challenges they

foresee. The high level of awareness and clarity among C-level executives aligns with the increasing presence of AI in the news and its growing significance in the corporate zeitgeist.



*您对对 AI 在网络安全中潜在用例的了解程度如何？*

|  |  |  |
| --- | --- | --- |
|  | **27%** | 3 （中立） |
| **25%** | 4 |
| **25%** | 5 （非常清楚） |
|  | |

网络安全领域中对潜在 AI用例的理解显示出存在一定的分歧，专业人士在对 AI 应用的了解程度上意见不统一。总体来看，有 50% 的受访者认为对 AI 对AI的应用场景有清楚了解，其中 25% 觉得比较清楚，另外 25% 非常清楚。然而，另一半受访者则表现出较低的了解程度，27% 表示中立，17% 觉得不太清楚，6% 认为非常不清楚。

 **6%** 1 （完全不清楚）

 **17%** 2

*您对网络安全中AI潜在应用案例的清晰程度如何？*

首席级别（C级）或高级管理人员

**52%**

**17%**

**16%**

**9%**

**6%**

其他工作人员

**14%**

**26%**

**29%**

**21%**

**10%**

1（完全不清楚） 2 3（中立） 4 5 （非常清楚）

在比较首席级别（C 级）高管和普通员工受访者的反馈时，呈现出一个明显的差异。在首席级别（C 级）高管中，有高达 52% 的人表示对 AI 在网络安全中的应用场景有非常清晰的认识，而只有 14% 的普通员工有同样的感受。

这种鲜明的对比可能说明，首席级别（C 级）高管对 AI 的理解更加具有远见和目标导向，他们关注的是更广泛的目标和潜力；而在通常情况下，员工因为负责具体的实施工作，可能更清楚其涉及的复杂性和不确定性。有趣的是，虽然员工通常比高层更早接受像 AI 这样的新兴技术，但在这种情况下，他们对 AI 使用场景的不清楚可能是受到他们预见到的操作上的挑战影响。首席级别（C 级）高管中的高度意识和清晰理解，与 AI 在新闻中的频繁出现以及在企业文化中逐渐占据的重要地位是相符合的。

### Awareness of AI security frameworks

A significant 88% of security professionals are aware of existing AI security frameworks, such as those based on NIST guidelines in the US. However, it’s crucial to note that awareness does not necessarily equate to usage or deep understanding of these frameworks. Only 12% of respondents report not being aware of any AI security frameworks, highlighting the widespread recognition of these standards in the cybersecurity community yet leaving room for further exploration of their practical application and comprehension.

**88%**

*Are you aware of any existing AI security frameworks?*

## General Plans to Use AI

### Current use of AI products in general

 **69%** Currently using

 **29%** Planning to use

 **2%** Not using and no plans

 **88%** Yes

 **12%** No

The use or planned use of AI products in organizations suggests a few possibilities:

*Does your organization use or plan to use AI products in general?*

AI may be integrated into many products that organizations are using,

but staff might not be fully aware of this integration or may not recognize these as AI-driven products.

Alternatively, it could indicate a gap in understanding or communication within the organization, where C-level

executives believe they are utilizing AI more extensively than their staff are aware, or they might overestimate their actual use of AI technologies. This discrepancy underscores the need for clearer communication and education about AI applications and usage within organizations, ensuring that executives and staff consistently understand how AI is being leveraged in their work environment.

### 对 AI 安全框架的认识

**88%**

*您了解目前有哪些 AI 安全框架吗？*

大部分（88%）的安全专业人士了解现有的 AI 安全框架，如基于美国 NIST 指南的框架。然而值得注意的是，对这些框架的了解并不意味着它们的深入理解和使用。仅有 12% 的调查参与者表示他们不了解任何 AI 安全框架，这表明这些标准在网络安全界得到了广泛的认可，同时也显示出在这些框架的实际应用和深入理解方面还有进一步的探索空间。

### 应用AI的计划

### AI 产品的整体使用情况

 **69%** 正在使用

 **29%** 计划使用

 **2%** 没有也不计划使用

 **88%** 了解

 **12%** 不了解

组织中使用或打算使用 AI 产品暗示了几种可能性：AI 可能已经融入了许多组织正在使用的产品中，然而，员工可能并未完全意识到这种集成和融合，或者可能没能认识到这些产品是由 AI 驱动的。

*您的组织目前是否使用或有计划使用 AI 产品？*

另一方面，这也可能暗示组织内部存在理解或沟通的差距，

首席级别（C 级）高管认为他们在使用 AI 的程度上可能超过了员工的认知，或者他们可能高估了实际使用 AI 技术的范围。这种差异突显了组织内部需要更明确的沟通和对 AI 应用及使用的教育和培训，确保高管和员工都能一致地理解 AI 在他们的工作环境中是如何被运用的。

### Evaluation, assessment, or procurement process of AI products or services

**人工智能产品或服务的评估、判定或采购流程**

In assessing the adoption of evaluation, assessment, or procurement processes for GenAI and AI-specific products, survey results show a divide in organizational strategies. Nearly half of the

respondents (47%) rely on their current assessment processes, suggesting a level of adaptability of existing frameworks to AI technologies. However, almost an equal proportion (46%)—comprising those introducing new assessment processes (33%) and those evaluating new processes (13%)— are actively seeking or developing AI-specific evaluation methods. This indicates a recognition of AI’s unique challenges that might not be fully addressed by traditional approaches. The divergence in strategies is more pronounced when considering organization size: larger organizations, particularly those with over 100 employees, predominantly use current processes (87%), while smaller organizations (48%) are more inclined to develop new approaches, highlighting the varying capacities and needs in AI integration across different scales of business operations.

在评估GenAI和人工智能特定产品的评估、判定或采购流程的采用情况时，调查结果显示了组织战略的差异。近一半的受访者（47%）依赖于他们当前的评估流程，这表明现有框架对人工智能技术有一定程度的适应性。然而，几乎同等比例（46%）的人--包括引入新评估流程（33%）和评估新流程（13%）的人，正在积极寻求或开发专门针对人工智能的评估方法。这表明人们认识到人工智能的独特挑战，而传统方法可能无法完全解决这些挑战。在考虑组织规模时，战略上的差异更为明显：较大的组织（特别是员工人数超过100人的组织），主要使用当前流程（87%），而较小的组织（48%）更倾向于开发新方法，这突出了不同业务运营规模中人工智能集成的不同能力和需求。

*Do you have an evaluation, assessment, or procurement process designed for Gen AI or AI-specific products and services?*

*您是否有针对Gen AI或人工智能特定产品和服务设计的评估、判定或采购流程？*

**7%**

**47%**

**33%**

**13%**

无使用政策 使用当前评估流程

引入新的评估流程

评估新流程

### Current and planned use of AI technologies

**当前和计划使用的人工智能技术**

The survey on AI technology usage within organizations reveals diverse adoption patterns across different AI systems. Large Language Models are currently in use by 49% of the respondents, while 35% plan to use them within the next two years, and 14% have no plans for their adoption. This trend of current usage and future planning is similar across other technologies: Deep Learning

is currently used by 41%, with 40% planning future use. Expert Systems are currently at 31% usage, with a notable 51% planning to implement them. Machine Learning and Natural Language

Processing tools show a balanced mix of current usage (39% and 33%, respectively) and future plans (34% and 37%, respectively).

这项关于组织内人工智能技术使用情况的调查揭示了不同人工智能系统的采用不同的模式。49%的受访者目前正在使用大型语言模型，而35%的受访者计划在未来两年内使用，14%的受访者没有采用大型语言模型的计划。当前使用和未来规划的趋势在其他AI技术中也是相似的：深度学习目前有41%的人使用，40%的人规划未来使用。专家系统目前的使用率为31%，其中51%的人计划实施。机器学习和自然语言处理工具显示出当前使用（分别为39%和33%）和未来计划（分别为34%和37%）的平衡。

Interestingly, there seems to be a sense of obligation to keep pace with technological advancements, as indicated by the consistent number of respondents planning to adopt various AI technologies within two years. This could explain why 47% are planning to use Generative AI (GenAI) and 45% are looking at Robotics, despite 21% and 22% respectively having no plans to use these technologies. This highlights a potential trend where organizations feel the need to stay technologically relevant, even if they currently do not see an immediate application for these

AI systems. Additionally, there’s a perceptible discrepancy between C-level executives and staff in their understanding of AI usage within their organizations.

C-level executives tend to report higher current use of these tools, whereas staff members are more inclined to believe that their organizations are planning to adopt these technologies in the next

two years. This difference suggests a gap in awareness or communication about the actual stage of AI integration within their organizations.

*Which of the following AI technologies or systems are you using in your organization? (Select all that apply)*

*您在组织中使用以下哪种人工智能技术或系统？（选择所有适用项）*

LLM (Language Models like GPT-3 or GPT-4) LLM（大语言模型如GPT-3 或者GPT-4）

**3%**

**49%**

**35%**

**14%**

DL (Deep Learning using neural networks) DL（使用神经网络的深度学习）

**4%**

**41%**

**40%**

**14%**

Expert Systems (Rule-based AI) 专家系统（基于规则的AI）

**5%**

**31%**

**51%**

**13%**

ML (Machine Learning) ML（机器学习）

**3%**

**39%**

**34%**

**24%**

NLP (Natural Language Processing tools) NLP(自然语言处理工具)

**21%**

**9%**

**33%**

**37%**

GenAI (Generative Artificial Intelligence) GenAI（生成式AI）

**3%**

**29%**

**47%**

**21%**

Robotics (AI-driven robots) 机器人（人工智能驱动的机器人）

**4%**

**29%**

**45%**

**22%**

没有计划 计划在2年内使用 当前使用 不知道

有趣的是，人们似乎对于跟上技术的步伐有一种责任感，正如计划在两年内采用各种人工智能技术的受访者人数一致。这也可以解释为什么47%的人计划使用生成式AI（GenAI），45%的人正在研究机器人，尽管分别有21%和22%的人没有使用这些技术的计划。这突出了一个潜在的趋势，即组织认为有必要保持技术相关相关性，即使他们目前没有看到这些人工智能系统的直接应用。此外，最高层管理人员和员工对组织内人工智能使用的理解存在明显差异。最高层管理人员倾向于更高地报告这些工具的当前使用率，而工作人员更倾向于相信他们的组织计划在未来两年内采用这些技术。这种差异表明，在组织内部对人工智能整合的实际阶段的认识或沟通存在差距。

### Primary team responsible for AI deployment

**负责AI部署的主要团队**

In the realm of AI deployment in security products, the responsibility predominantly falls on the Security Team and IT Department, with 24% and 21%, respectively taking the lead. This is followed by the Data Science/Analytics team and a Dedicated AI/ML team, handling the task in 16% and 13% of organizations. Interestingly, Senior Management/Leadership and DevOps teams play a

smaller yet significant role, at 9% and 8%, respectively. This distribution highlights a trend where AI deployment is often managed by teams directly involved in technical and security aspects, although cross-functional collaboration and senior leadership also play crucial roles in guiding AI strategies.

在安全产品中的人工智能部署领域，责任主要落在安全团队和IT部门，分别占24%和21%。其次是数据科学/分析团队和专门的人工智能/机器学习团队，分别在16%和13%的组织中处理这项任务。有趣的是，公司高层和DevOps团队所扮演的角色较小但重要，分别占9%和8%。这种分布突出了人工智能部署通常由直接参与技术和安全方面的团队管理的趋势，尽管跨职能协作和公司高层在指导人工智能战略方面也发挥着关键作用。

*Which team is primarily responsible for AI deployment in your organization?*

*哪个团队主要负责您组织中的人工智能部署？*

**1%**

**21%**

**16%**

**13%**

**9%**

**8%**

**6% 3%**

**24%**

### Testing AI capabilities for security

测试AI的安全能力

A high number of security professionals report testing AI capabilities for security in organizations, with 67% affirming that they have

*Have you tested any AI capabilities for security in your organization?*

*您是否测试过组织中的人工智能安全功能？*

tested AI for security purposes specifically. This significant percentage suggests that AI integration into cybersecurity is not just a concept but a practical reality for many. This widespread testing could be attributed to AI functionalities being incorporated into

 **67% 是**

 **27%** 没有，但计划做

 **6% 没有计划**

existing product suites, making it more accessible and easier for organizations to adopt and experiment with or use LLM agents. Furthermore, 27% of respondents are in the planning stages of testing AI capabilities, indicating a growing trend and recognition of AI’s potential in enhancing security measures. On the other hand, a small portion (6%) have no plans to engage with AI for security, possibly due to lack of resources, expertise, or skepticism about AI’s effectiveness in their specific context.

大量安全专业人士报告称，他们在组织中测试了人工智能的安全能力，67%的人证实他们已经专门以安全为目的测试了人工智能。这一显著比例表明，人工智能融入网络安全对许多人来说不仅仅是一个概念，而是一个现实。这种广泛的测试可以归因于人工智能功能被纳入现有的产品套件，使组织更容易采用、试验或使用LLM agent。此外，27%的受访者正处于测试人工智能能力的计划阶段，这表明人工智能在加强安全措施方面的潜力有了越来越大的趋势和认可。另一方面，一小部分人（6%）没有计划在安全领域使用人工智能，这可能是因为缺乏资源、专业知识，或者对人工智能在特定环境中的有效性持怀疑态度。

### Biggest hurdles for implementing AI in security

**在安全领域实施人工智能的最大障碍**

The survey results reveal that the most significant hurdle to implementing AI in security is the skill gaps and shortage of knowledgeable staff, which is highlighted by 33% of respondents. This dual challenge of finding future staff with the necessary skills and enhancing the knowledge of current staff reflects the complex nature of AI in cybersecurity, requiring both specialized cybersecurity knowledge and a continuous understanding of evolving AI technologies. Addressing these skill- related issues is fundamental, as it could potentially alleviate other downstream challenges such as understanding AI risks and benefits, integrating AI with existing security infrastructure, and effectively managing regulatory and data privacy compliance.

调查结果显示，在安全领域实施人工智能的最大障碍是技能差距和缺少有知识的员工，33%的受访者强调了这一点。寻找具备必要技能的未来员工和增强现有员工知识的双重挑战反映了人工智能在网络安全中的复杂性：既需要专业的网络安全知识，又需要对不断发展的人工智能技术有持续的了解。解决这些与技能相关的问题至关重要，因为它可以缓解潜在的其他下游挑战，例如了解人工智能的风险和收益，将人工智能与现有的安全基础设施集成，以及有效地管理监管和数据隐私合规性。

Other notable hurdles include resource allocation (11%), understanding AI risks (10%), and the cost of implementation (8%), among others. Surprisingly, concerns like regulatory and data privacy compliance and the cost of implementation, which are traditionally viewed as significant barriers, are not the foremost concerns in this context. This might indicate an anticipation of long-term cost savings and a focus on current rather than future regulatory scenarios. The responses also show

a general concern across almost all options, indicating that while there is no single overwhelming obstacle, the journey to AI integration in cybersecurity is multifaceted and complex. This widespread concern across various aspects of AI implementation underscores the need for a holistic approach in adopting AI in security, one that addresses skill gaps, resource needs, and regulatory challenges in a balanced manner.

其他值得注意的障碍包括资源分配（11%）、了解人工智能风险（10%）和实施成本（8%）等。令人惊讶的是，传统上被视为重大障碍的监管和数据隐私合规性以及实施成本等问题并不是这种情况下的首要问题。这可能表明对长期成本节约的预期，以及对当前而非未来监管情景的关注。这些回应还显示出几乎所有选项都普遍存在担忧，表明尽管没有单一的压倒性障碍，但人工智能在网络安全的整合过程是多方面且复杂的。这种对人工智能实施各个方面的广泛关注突显了在安全领域采用人工智能的整体方法的必要性，这种方法需要以平衡的方式解决技能差距、资源需求和监管挑战。

*What is the biggest hurdle to getting started with AI in security implementations?*

*在安全实施中开始使用人工智能的最大障碍是什么？*

**33%**

**11%**

**10%**

**8%**

**8%**

**8%**

**8%**

**8%**

**4%**

Skill gaps/ shortage (e.g., finding future staff) & lack of knowledge (e.g., current staff)

技能差距/短缺（例如，寻找未来的员工）和缺乏知识（例如，现有员工）

Resource allocation (e.g., compute capabilities)

资源分配（例如计算能力Understanding AI risks

了解人工智能风险

Understanding AI benefits

了解人工智能的好处

Challenges with existing security infrastructure (e.g., integration)

现有安全基础设施面临的挑战（例如，集成）Regulatory and data privacy compliance

法规和数据隐私合规性

Cost of implementation

实施成本

Finding viable use-cases

寻找可行的用例

Unsure of AI effectiveness

不确定人工智能的有效性

### Desired outcomes from AI implementations

**AI实现的预期结果**

Organizations’ desired outcomes for implementing AI in security teams highlight a strong inclination towards supplementing skills and knowledge gaps, with 36% of respondents identifying this as

a key goal. This aligns with the previously noted challenge of skill gaps and lack of knowledge in AI applications within cybersecurity. This also aligns with the previous finding that AI is expected to support job roles rather than replace them completely. By integrating AI, organizations aim to

uplevel and augment their workforce, addressing these gaps and enhancing their team’s capabilities. This focus on enhancement rather than outright replacement of the workforce is further evidenced by the lower priority given to reducing the workforce (20%), indicating a preference for AI as a tool for empowerment and support.

组织在安全团队中实施人工智能的预期结果强调了弥补技能和知识差距的强烈倾向，36%的受访者将其视为关键目标。这与之前提到的网络安全领域人工智能应用的技能差距和知识缺乏的挑战相一致。这也与之前的发现一致，即人工智能有望成为支持工作的角色，而不是完全取代它们。通过集成人工智能，组织的目标是提升和增加他们的劳动力，解决这些差距并增强他们团队的能力。减少劳动力的优先级较低(20%)进一步证明了这种关注是对增强而不是彻底取代劳动力，这表明人们更倾向于将人工智能作为一种赋权和支持的工具。

Other significant desired outcomes include faster threat detection and improved productivity, each selected by 26% of respondents, as well as enhancing the overall cybersecurity posture, reducing errors and misconfigurations, and accelerating incident response, each at 24%. These goals underscore a desire for AI to bring efficiency and effectiveness to cybersecurity operations. Interestingly, while improved productivity is a key expectation, it is not the dominant outcome, possibly reflecting a nuanced view where the focus is more on quality (such as accurate threat detection and response) rather than quantity of work. However, the fact that a notable portion

of respondents (15% to 20%) also look for AI to reduce workforce, overhead costs, and workload suggests a balanced expectation where AI is seen as a means to optimize and streamline security operations while also enhancing the performance and capabilities of the existing human workforce.

其他重要的期望结果包括更快的威胁检测和提高生产力(26%的受访者选择了这两项)，以及增强整体网络安全态势、减少错误以及错误配置、加速事件响应(24%)。这些目标强调了人工智能为网络安全运营带来效率和有效性的愿望。有趣的是，虽然提高生产力是一个关键的期望，但它并不是主要的结果，这可能反映了一种微妙的观点，即重点更多地放在质量(如准确的威胁检测和响应)上，而不是工作的数量。然而，相当一部分受访者(15%至20%)也希望人工智能能够减少劳动力、管理成本和工作量，这表明了一种平衡的期望，即人工智能被视为优化和简化安全操作的一种手段，同时也能提高现有劳动力的绩效和能力。

*What are your desired outcomes when it comes to implementing AI in your security team?*

*当涉及到在您的安全团队中实施人工智能时，您期望的结果是什么？*

**36%**

**26%**

**26%**

**24%**

**24%**

**24%**

**20%**

**19%**

**17%**

**15%**

Supplemental skills and knowledge gaps (uplevel/ augement workforce)

补充技能和知识差距(提升/增加劳动力)

Faster threat detection

更快的威胁检测

Improved productivity

提高生产力

Improve cybersecurity posture

改善网络安全态势

Reduce errors and misconfigurations

减少错误和错误配置

Faster incident response

更快的事件响应

Reduce workforce

减少劳动力

Improve accuracy of threat analysis

提高威胁分析的准确性

Reduce overhead costs

降低管理费用

Reduce workload

减少工作量

## AI Staff, Leadership, and Training

**人工智能员工、领导和培训**

### Creating a team for governing the secure use of AI

**创建一个团队来管理人工智能的安全使用**

*Are you creating a team to govern the secure use of AI within your organization? (e.g., policy development, AI features/ product procurement, responsible/ ethical use of)*

*您是否正在创建一个团队来管理组织内人工智能的安全使用？（例如，政策制定、人工智能功能/产品采购、负责任/合乎道德的使用）*

A substantial 74% of organizations are planning to create teams dedicated to governing the secure use of AI, emphasizing the serious consideration companies are giving to AI integration. This move towards establishing specialized teams for policy development, AI product procurement, and ensuring responsible and ethical use, signals a clear recognition of AI’s transformative impact

on security roles. Rather than replacing existing functions,

**74% 是**

**20% 否**

**6% 不确定**

AI is leading to the evolution and expansion of organizational roles, requiring new governance structures and expertise. This approach underscores the shift in the security landscape where AI is not merely an additional tool, but a significant factor that necessitates thoughtful integration and management. The fact that only 20% are not forming such teams, and 6% are unsure, further

highlights the widespread acknowledgment across the industry of the need for dedicated oversight and specialized skills to harness AI’s potential effectively and securely.

74%的组织正计划创建专门管理人工智能安全使用的团队，这强调了公司正在认真考虑人工智能的集成。这一举措旨在建立专门团队，负责政策制定、人工智能产品采购，并确保负责任和合乎道德的使用，标志着人们明确认识到人工智能对安全角色的变革性影响。人工智能不是取代现有的功能，而是促使组织角色的演变和扩展，这需要新的治理结构和专业知识。这种方法强调了安全领域的转变，人工智能不仅仅是一个额外的工具，而是一个需要深思熟虑的集成和管理的重要因素。事实上，只有20%的受访者表示没有组建这样的团队，6%的人不确定，这进一步凸显了整个行业普遍认识到，需要专门的监督和专业技能来有效、安全地利用人工智能的潜力。

### Team responsible for securing AI systems

**负责保护AI系统的团队**

*Which team will be responsible for securing AI systems within your organization?*

*哪个团队将负责保护您组织内的人工智能系统？*

The responsibility for securing AI systems within organizations predominantly falls to the Security Team and IT Department, with 29% and 25% respectively taking the lead. These figures mirror the similar distribution seen in AI deployment responsibilities, reflecting a consistent approach where the primary technical teams are entrusted with both implementing and securing AI technologies. This allocation of responsibilities

|  |  |
| --- | --- |
| **29%** | Security Team 安全团队 |
| **25%** | IT Department IT部门 |
| **12%** | The Data Science/ Analytics team  数据科学/分析团队 |
| **10%** | DevOps |
| **10%** | Senior management/ Leadership  高级管理层/领导层 |
| **8%** | Cross-functional team  跨职能团队 |
| **6%** | I’m not sure 我不确定 |

underscores the crucial role these departments play in the effective and safe integration of AI into organizational infrastructures.

在组织内保护人工智能系统的责任主要落在安全团队和IT部门身上，分别有29%和25%。这些数字反映了人工智能部署责任的类似分布，即委托主要技术团队实施和保护人工智能技术。这种职责分配强调了这些部门在人工智能有效、安全地融入组织基础设施方面发挥的关键作用。

### 当前或计划使用与人工智能和网络安全相关的培训项目

The survey indicates a strong inclination towards investing in training programs for staff on AI and cybersecurity within organizations. A notable

*您的组织是否正在实施或计划实施与人工智能和网络安全相关的员工培训计划？*

26% of organizations are already using such training programs, demonstrating a proactive approach to equipping their workforce

|  |  |
| --- | --- |
| **26%** | 当前使用 |
| **50%** | 计划12月内使用 |
| **21%** | 计划使用(没有时间轴) |
| **4%** | 没计划 |

with the necessary skills and knowledge. A significant 50% plan to implement these training programs within

the next 12 months and

21% of organizations have plans to introduce such training, although without a specific timeline. This highlights the widespread recognition of the importance of continuous learning in the rapidly evolving fields of AI and cybersecurity. Only a small fraction (4%) have no plans for such training, suggesting that most organizations are focused on solving the skills and knowledge gaps they’ve previously identified as concerns with AI use. 该调查表明，人们强烈倾向于投资于组织内员工的人工智能和网络安全培训项目。一个值得注意的现象是：26%的组织已经在实施此类培训计划，证明这是一种为员工提供必要的技能和知识的积极方法；有50%的组织计划在接下来的12个月提供；21%的组织尽管没有具体的时间表，但仍有引入此类培训的计划。这凸显了人们对快速发展的人工智能和网络安全领域进行持续学习重要性的共同认识。只有一小部分（4%）组织没有此类培训计划，这表明大多数组织都专注于解决他们之前认为与人工智能使用有关的技能和知识差距。

### 来自高级管理层采用人工智能的压力

*您的高级管理层（如董事会）是否在推动人工智能的采用？*

 **82% 是**

 **12%** 否

 **6% 不确定**

The push for AI adoption from executive leadership, as indicated by 82% of respondents, sheds light on why many C-level executives report higher levels of familiarity with

AI technologies and their applications. This top- down pressure likely stems from a recognition of AI as a competitive advantage

in the modern business landscape. When executive teams, including Boards of

Directors, prioritize AI integration, it creates an organizational culture that values and focuses on AI capabilities, thereby encouraging a deeper understanding and engagement with AI at all levels of the organization. This focus at the top echelons of management not only drives the strategic adoption of AI but also likely influences the reporting of higher familiarity with AI among C-level executives. 关于推动人工智能的采用， 82%的受访者认为，许多首席执行官等高级管理层认为其熟悉人工智能技术及其应用程序。这个自上而下的压力可能源于认为人工智能能够促进组织现代商业竞争中处于优势地位。高级管理团队（包括董事会）会优先考虑人工智能的整合，并为它创造了一种重视和关注人工智能的组织文化，从而鼓励各级组织可以更深入地了解和参与人工智能的活动中，高层管理团队不仅在战略层面关注人工智能领域，他们还将影响C级高管对人工智能的熟悉程度。

### 领导层对人工智能影响安全的认知

There is a tendency among organizational leadership to be more informed and aware of AI’s implications on security than not. Approximately 28% of leaders are reported as

*您的领导层（如董事会）在多大程度上了解和意识到人工智能对安全的影响？*

being fully aware, showing a proactive initiative among a significant portion of upper management to deeply understand AI’s impact

on security. An additional 46% are moderately aware, suggesting that while they have a general understanding,

 28% 完全知情

 46% 适度意识

 18% 稍有察觉

 6% 不知道

there may be gaps in their full comprehension of AI’s complexities and nuances in the security domain. This awareness may be informed by information from security teams and current news, highlighting the importance of continuous and high-level communication within organizations. An interesting point to note is that there is no substantial difference in this awareness between C-level executives and staff, indicating a unified perception of leadership’s awareness. This collective view is a point-in-time measurement and is subject to change as rapidly as the AI and cybersecurity landscape itself evolves. 组织的领导层更加了解人工智能对安全的影响。据报道，大约28%的领导者充分认识到了人工智能对安全的影响，很大一部分高级管理层在团队中表现出积极主动的态度。另外46%的组织则有所了解，这表明他们虽然有总体认识，但在全面理解人工智能在安全领域的复杂性和差别方面可能存在差距。这种认识可能是通过当下新闻或安全团队提供的信息得出的，突出了组织内持续和高层沟通的重要性。值得注意的是，首席执行官和员工在这方面的认识没有实质性差异，表明领导层的认识是一致的。这种集体观点只是在某个时间点的测量，会随着人工智能和网络安全的发展而迅速变化。

**生成式AI的网络安全计划**

### 生成式AI解决方案的当下和计划使用

The anticipation for 2024 as a significant year for the adoption of Generative

*一般来说，您的组织是否正在使用或计划使用生成式AI解决方案？*

AI (GenAI) solutions is evident from the survey results. Currently, 22% of

|  |  |
| --- | --- |
| **22%** | 正在使用 |
| **55%** | 明年内使用 |
| **13%** | 明年以后使用 |
| **6%** | 没有计划 |
| **3%** | 不知道 |

organizations are using GenAI,

but a remarkable 55% plan to adopt these solutions within the next year, signaling a substantial surge in GenAI integration. An additional 13% expect to use GenAI solutions over a year from now, while only 6% have no plans to

invest in this technology. Regardless, the data points to 2024 as a pivotal year, with a significant movement towards embracing GenAI across various organizations. 从调查结果中可以明显看出， 2024年 生成式AI解决方案的预期采用。目前，22%的组织正在使用生成式AI，但55%的组织计划在明年内采用生成式AI解决方案，这标志着生成式AI的大幅增长。另有13%的组织预计在明年后使用生成式AI解决方案，而只有6%的人没有投资这项技术的计划。无论如何，数据表明2024年是关键的一年，各组织都在大力推行生成式AI。

### 生成式AI在网络安全的计划使用

The planned use of GenAI in cybersecurity reflects a broad exploration of potential applications across various organizations. The survey results show a relatively even distribution among the top five use cases, indicating a diverse range of areas where GenAI is expected to make an impact. Rule creation emerges as the leading use case, with 21% of organizations aiming to leverage GenAI to develop more sophisticated security protocols. This is closely followed by attack simulation and compliance violation monitoring, each at 19%, highlighting GenAI’s potential to enhance proactive security measures and regulatory adherence. Additionally, 16% of respondents are looking to use GenAI for network detection, aiming to improve the identification of network threats. Another 16% focus on using GenAI to reduce false positives, underscoring its potential to refine alert accuracy and efficiency. This spread of interest across different use cases suggests that organizations are not only eager to adopt GenAI but are also keen on customizing its applications to meet specific security needs, thereby maximizing its benefits in the evolving landscape of cybersecurity. 生成式AI在网络安全中的计划使用反映了各组织在AI应用的广泛探索。调查结果显示，Top5用例的分布相对均匀，表明生成式AI预计会产生影响的领域多种多样。规则创建成为主要使用用例，21%的组织旨在利用生成式AI开发更复杂的安全规则。紧随其后的是攻击模拟和合规违规监控，各占19%，突显了生成式AI在加强主动安全措施和遵守监管方面的潜力。此外，16%的受访者希望使用生成式AI进行网络检测，旨在改进网络威胁的识别。另有16%的受访者专注于使用生成式AI来减少误报，强调了其提高警报准确性和效率的潜力。这种兴趣在不同用例中的传播表明，组织不仅渴望采用生成式AI，而且热衷于定制其应用程序以满足特定的安全需求，从而在不断发展的网络安全环境中最大限度地提高其效益。

*你的组织计划如何使用生成式AI用于网络安全? (选择Top3 用例)*



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **21%** | 规则创建 | **13%** | 要搜索的资源语言 | **9%** | 取证分析 |
| **19%** | 攻击模拟 | **13%** | 威胁摘要 | **9%** | 聊天机器人 |
| **19%** | 合规违规监控 | **13%** | 数据防泄漏，IP保护 | **8%** | 事件摘要 |
| **16%** | 网络检测 | **11%** | 用户行为分析 | **8%** | 配置漂移 |
| **16%** | 减少误报 | **10%** | 自动生成报告 | **8%** | 行动/消减建议 |
| **15%** | 培训开发和支持 | **10%** | 终端检测 | **7%** | 代码分析 |
| **14%** | 异常分类 | **9%** | 时间日志摘要 |  |  |

### 生成式AI网络安全之旅的现状

The majority of organizations are in the early stages of their GenAI journey in the realm of cybersecurity, with a strong focus on exploration and implementation. Approximately 30% are currently exploring options and use cases, indicating a proactive approach to understanding the potential of GenAI in enhancing their security posture. This phase of exploration is crucial as it lays the groundwork for practical applications. Additionally, 15% are in the testing phase, experimenting with specific use cases to gauge the effectiveness and applicability of GenAI solutions. The implementation phase sees a combined 47% of organizations, with 23% currently implementing solutions and 24% having fully implemented GenAI, suggesting a rapid advancement from theoretical exploration to practical deployment. A negligible 3% are not considering GenAI yet, and an equal 3% maintain a strict no-use policy. These findings reflect a trend towards embracing GenAI in cybersecurity, with most organizations actively engaged in the initial phases of exploring and integrating these innovative solutions. 大多数组织都处于生成式AI网络安全领域之旅的早期阶段，重点关注探索和实施。大约30%的组织目前正在探索选项和用例，这表明他们采取了积极主动的方法来了解生成式AI在增强其安全态势方面的潜力。这一探索阶段至关重要，因为它为实际的应用奠定了基础。此外，15%的组织处于测试阶段，对特定用例进行实验，以评估生成式AI解决方案的有效性和适用性。23%的组织目前正在实施解决方案，24%的组织已完全实施生成式AI，这表明生成式AI从理论探索到实际部署的快速发展。3%的组织还没有考虑生成式AI，同样3%的组织保持严格的禁止使用政策。这些发现反映了在网络安全中采用生成式AI的趋势，大多数组织处在积极参与探索、整合生成式AI创新解决方案的初始阶段。

*你的组织当前在哪些领域使用生成式AI?*

**3%**

**30%**

**15%**

**23%**

**24%**

**3%**

**2%**

尚未考虑t

探索选项和用例

测试用例

实施解决方案中

完全实施

严格禁止使用

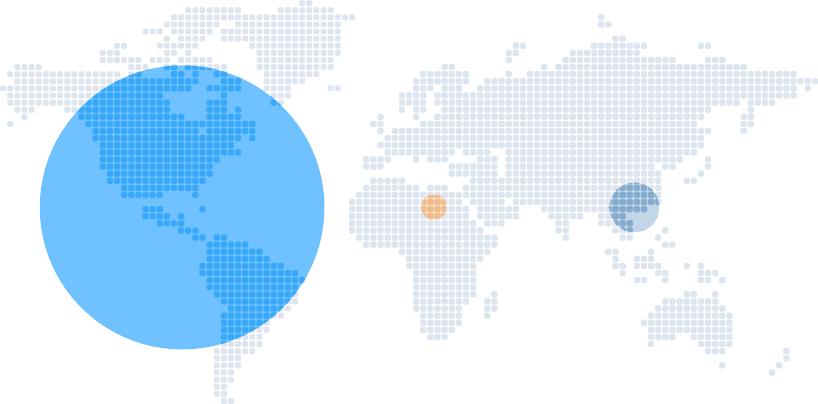
不知道

## 统计

The survey was conducted online by CSA in November 2023 and received 2,486 responses from IT and security professionals from organizations of various sizes across the Americas, APAC and EMEA. 该调查由云安全联盟于2023年11月在线进行，收到了来自美洲、亚太地区和EMEA不同规模组织的IT和安全专业人员的2486份回复

*你所在世界的哪个区域?*

美国



**7%**

**14%**

**79%**

欧洲,中东,非洲 (EMEA)

亚太 (APAC)



*您所在的组织的规模?*



*您在您组织的职位是什么?*

1%



20%

36%

21%

12% 11%



13%

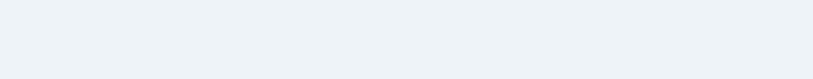
21%

44%

20%

<100 雇员 101-1000 雇员 1001-5000 雇员

5001-10000 雇员 10001+ 雇员



*您所在的企业属于以下哪个主要领域?*

C-层级/执行官 主管 经理 员工 其他

**3% 2%**



**22%**

**7% 6% 6% 5% 5% 5% 4% 4% 4% 4% 4%**

### Security benefits and risks with AI

### AI 在安全领域的收益和风险

Security professionals have a cautious and potentially nuanced perspective of who will benefit from AI more: security professionals or

*In your opinion, would AI be more beneficial to security teams or malicious 3rd parties?*

malicious parties. About 34% believe that AI will primarily benefit security teams, suggesting a general optimism about AI’s role in bolstering cybersecurity defenses.

|  |  |
| --- | --- |
| **34%** | Security teams |
| **31%** | Equal Benefit |
| **25%** | Malicious parties |
| **9%** | Neither |

However, a closely matched 31% see AI as offering equal benefits to both security

*在您看来，AI 对安全团队还是对第三方恶意行为者更有利？*



|  |  |
| --- | --- |
| **34%** | 对安全团队有利 |
| **31%** | 同样有利 |
| **25%** | 对恶意行为者有利 |
| **9%** | 两者都无受益 |

安全专家在评估 AI 更有利于安全团队还是恶意行为者时，持有一种谨慎且微妙的观点。大约 34% 的人认为 AI 主要有助于安全团队，这表明人们对于人工智能在增强网络安全防御方面的作用普遍持乐观态度。

然而，也有 31% 的人认为 AI 对安全团队和恶意行为者的益处相当，

teams and malicious actors, highlighting an awareness of the dual-use nature of AI technologies in cybersecurity. This is further underscored by the 25% who think AI might be more advantageous to malicious parties, acknowledging the potential threat if AI is used with malicious intent.

这显示出人们对 AI 技术在网络安全中可能出现的“双刃剑”特性有所警觉。此外，还有 25% 的人认为 AI 可能更有利于恶意方，他们认为如果 AI 被用于恶意目的，可能带来潜在的威胁。

A smaller segment (9%) feels that it’s neither clearly beneficial to security teams nor malicious 3rd parties, or it’s too early to tell. This reflects an underlying sentiment that, given the early stage of AI’s integration into cybersecurity, there’s still a lot of unknowns about its full impact and potential. The results indicate a cautious optimism where respondents generally lean towards AI helping security teams slightly more, but there’s a clear recognition of the significant risks if AI tools fall into the wrong hands or are exploited by adversaries.

还有一小部分人 (9%) 认为目前无法明确判断 AI 对安全团队还是恶意第三方更有利的情况，或认为现在做出判断还为时尚早。这种看法反映出一个基本观点：由于 AI 融入网络安全领域还处于初步阶段，其全面的影响和潜力仍充满不确定性。以上调查结果显示出一种谨慎的乐观态度，大多数受访者倾向于认为 AI 会稍微更多地帮助安全团队，但人们也清楚地意识到，如果 AI 工具被不当使用或被敌对势力利用，可能会带来重大风险。

### Greatest concerns with AI in security

### 在安全领域对 AI 的最大担忧

Security professionals express a range of concerns regarding the implementation of AI in cybersecurity, reflecting the complexity and multifaceted nature of AI integration. The top concern, cited by 38%, is data quality, specifically the risk of unintended bias, which is closely linked to concerns about accuracy (24%). This connection is significant, as AI is often perceived as an objective tool; thus, the quality and integrity of data fed into AI systems directly influence the accuracy and reliability of their outputs. Similarly, 36% are wary of the lack of transparency in AI systems, highlighting the ‘black box’ nature of some AI algorithms that can make understanding and trust in AI decisions challenging.

安全专家对 AI 在网络安全真实场景中的应用表达了各种担忧，这反映出 整合AI 应用的复杂性和多面性。最主要的忧虑是数据质量，38% 的人提到了预期外偏见的风险，这与对准确性的担忧（24% 的人提及）密切相关。这一点非常关键，因为 AI 常被视为客观工具，而输入到 AI 系统的数据质量和完整性直接影响到输出的准确性和可靠性。同样地，36% 的人对 AI 系统的不透明性表示担心，他们强调了某些 AI 算法的“黑盒”特性，这使得理解和信任 AI 所做的决策变得更加困难。

Other notable concerns include skills and expertise for managing AI, mentioned by 33% of professionals, indicating an awareness of the need for specialized knowledge to effectively integrate and oversee AI technologies. [Data poisoning](https://spectrum.ieee.org/ai-cybersecurity-data-poisoning) and [hallucinations](https://www.ibm.com/topics/ai-hallucinations), concerns for 28% and 25% respectively, are closely related issues, along with data leakage or loss, and privacy concerns, each noted by 25% of respondents. These issues are relatively less understood but nonetheless acknowledged as potential risks that could emerge with more extensive AI usage. The broad range of concerns suggests that security professionals are cautiously considering all possible implications of AI, recognizing that the technology’s rapid evolution means that today’s secondary concerns could become tomorrow’s primary challenges.

其他显著的担忧还包括管理 AI 所需的技能和专业知识（有 33% 的专业人士提到这一点），这显示出他们意识到需要专业的知识来有效地整合和监管 AI 技术。此外，分别有 28% 和 25% 的人关注 [数据污染](https://spectrum.ieee.org/ai-cybersecurity-data-poisoning) 和 幻觉 ，这与数据泄露或丢失及隐私问题（各有 25% 的提及）密切相关。这些问题虽然相对而言更不易被理解，但仍被认为是随着 AI 更广泛使用而可能出现的潜在风险。如此广泛的担忧表明，安全专业人员在谨慎考虑 AI 的所有可能影响，他们认识到技术的快速演进意味着当前的次要问题可能变成未来的主要挑战。

*What are your biggest concerns regarding AI in security? (Select up to 3)*

**38%**

**36%**

**33%**

**28%**

**25%**

**25%**

**25%**

**24%**

**21%**

Data quality (e.g., unintended bias)

Lack of transparency

Skills and expertise for managing

Data poisoning Hallucinations Privacy

Data leakage or loss

Accuracy

Misuse

*您最担心的有关 AI 在安全领域的问题有哪些？（最多选择 3 项）*

**38%**

**36%**

**33%**

**28%**

**25%**

**25%**

**25%**

**24%**

**21%**

数据质量(如：预期外偏见)

不透明性

技能和专业知识

数据污染 幻觉 隐私

数据泄露或丢失

准确性

滥用

### Impact of AI on current cybersecurity roles

### AI 对当前网络安全行业岗位的影响

Within the cybersecurity field, professionals widely anticipate that AI will have a significant impact on their

*Please select the option that best reflects your opinion about AI's potential impact on your role. Over the next 5 years, AI will...*

roles over the next five years. This sentiment reflects the disruptive nature of AI in the workplace. A substantial number (58%) perceive AI as a tool that will support and enhance their current roles.

Specifically, 30% believe AI will help enhance certain aspects of their skillset, while 28%

see it as an overall support

 **30%** Help enhance parts of your skillset

|  |  |
| --- | --- |
| **28%** | Support you overall in your current role |
| **24%** | Replace a large part of your role |
| **12%** | Completely replace your role |
| **5%** | Not impact your role |

to their existing functions. This perspective underscores the potential of AI to augment human capabilities, especially in automating manual and routine tasks. Technologies like AI-driven chatbots and analytical tools are expected to streamline operations and increase efficiency, assisting security professionals in more effectively managing their workload. Freeing their time up from more menial tasks to focus on more complex and creative elements of their job role.

在网络安全领域，专业人士广泛预计，在未来五年内，AI 将对他们的工作职责和岗位产生显著影响。这种观点反映了 AI 在职场中的颠覆性。有相当一部分人（58%） 认为 AI 将成为支持和提升他们当前工作职能的工具。

*请选择一个选项，以最佳反映您对 AI 在未来五年对您的岗位可能产生的影响的观点。未来 5 年内，AI 将...*

具体来说，有 30% 的人相信 AI 将有助于提升他们的某些技能，而 28% 的人认为 AI 将全面支持他们现有的工作职责。

 **30%** 帮助增强部分技能



|  |  |
| --- | --- |
| **28%** | 在当前的工作中提供整体支持 |
| **24%** | 替代职责中的大部分 |
| **12%** | 完全取代您的岗位 |
| **5%** | 对您的岗位没有影响 |

这种看法突出了 AI 提高人类能力的可能性，尤其是在将人工执行和日常工作自动化的方面。诸如 AI 驱动的聊天机器人和分析工具等技术有望简化流程并提升效率，从而协助安全专家更加高效地处理工作。这样，他们就可以将时间从繁琐的任务中解放出来，转而关注职责中更为复杂和更需要创造性的部分。

There’s a notable concern among these professionals about AI’s ability to replace human roles. About 24% foresee AI replacing significant parts of their job, and 12% even predict a complete replacement of their role. This apprehension is more pronounced in aspects of cybersecurity work that are heavily manual or repetitive, where AI’s capabilities for automation are most directly applicable. It’s important to recognize that while AI is seen as a supportive and enhancing tool, its potential to disrupt existing job structures in cybersecurity is also a key consideration. Security professionals are thus faced with the dual challenge of leveraging AI for its benefits while also preparing for the shifts it may bring in the job market, highlighting the importance of adaptability and continuous skill development in this rapidly evolving field.

然而，专业人士对 AI 取代人类职位的能力也表示出明细的担忧。约 24% 的人预计 AI 将取代他们工作的重要部分，还有 12% 的人甚至预测 AI 将完全取代他们的职位。这种担忧更明显的体现在网络安全领域中那些手动的或重复性的工作上，因为 AI 在这些方面的自动化能力最为直接适用。重要的是，要认识到 AI 虽然被看作是一种支持和增强工具，但其颠覆现有岗位和职能结构的潜在可能性也是网络安全领域需要重视的关键因素。因此，安全专业人员面临的双重挑战是，一方面要利用 AI 带来的好处，另一方面也要为其可能引发的职场变革做好准备，这突显了在这快速发展变化的领域中，适应性和持续的技能提升的重要性。

### Confidence in organizations’ skills to execute a security strategy leveraging AI

### 对组织利用 AI 能力实施安全策略的信心

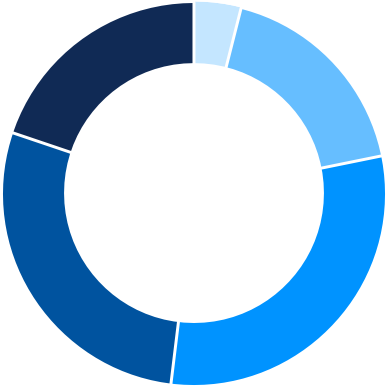
In the cybersecurity sector, there’s a cautiously optimistic view regarding organizations’ readiness to leverage AI. About 48% of professionals express confidence in their organization’s ability to implement AI strategies effectively, with 28% feeling reasonably confident and 20% very confident. This level of assurance is intriguing, considering the nascent stage of AI in this field. It suggests that many professionals might be optimistic about their preparedness or overlook the intricacies of AI integration, a classic scenario of an unknown unknown.

在网络安全行业中，安全从业人员对组织准备利用 AI 的能力持谨慎乐观态度。大约 48% 的专业人员对他们的组织有效地实施 AI 策略的能力表示有信心，其中 28% 的人认为相当有信心，20% 的人非常有信心。考虑到 AI 在该领域还处于初期阶段，这种程度的信心显得尤为引人注意。这种情况表明，许多专业人士可能对他们的准备情况过于乐观，或者忽视了 AI 集成应用的复杂性，这是一个“不知道自己不知道什么”的经典场景。

Conversely, a notable 30% remain neutral, indicating either a balanced recognition of their capabilities or uncertainty about the challenges AI might pose.

The remaining 22% show less confidence, including 18% who are somewhat unconfident and 4% who are not confident at all. This spread in confidence levels across the cybersecurity community points to a complex landscape where

*How confident are you about your organization’s skills to execute a strategy for leveraging AI in security?*

 **4%** 1 (Not Confident)

 **18%** 2

 **30%** 3 (Neutral)

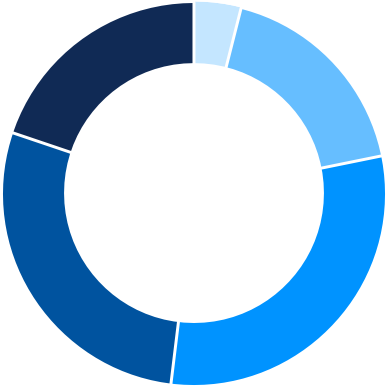
 **28%** 4

 **20%** 5 (Very Confident)

some AI applications are seen as straightforward and readily deployable, while others, more complex and novel, evoke caution and uncertainty.

另一方面，有 30% 的人持中立态度，这可能表明他们对自己的能力有一个平衡的认识，或者对 AI 可能带来的挑战感到不确定性。其余的 22% 对此表示出较低的信心，其中 18% 的人表示有些不自信，4% 的人则完全不自信。网络安全界对信心水平的这种分布揭示了一个复杂的局面：一些 AI 应用被认为是简单直接、容易部署的，而其他更为复杂和新颖的应用则引发了安全从业人员对于 AI 的谨慎和不确定性。

*您对您的组织在安全方面利用 AI 实施策略的能力有多少信心？*

 **4%** 1 （完全不自信)

 **18%** 2

 **30%** 3 （中立态度）

 **28%** 4

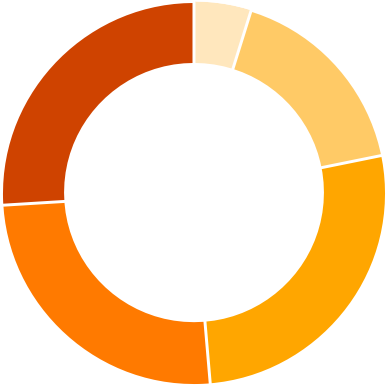
 **20%** 5 （非常自信）

### Confidence in organizations’ skills to execute a security strategy to protect AI systems

### 对组织实施安全策略以保护AI系统的信心

In assessing confidence levels regarding the execution

*How confident are you about your organization's skills to execute a security strategy for protecting AI used in your core business/mission?*

of a security strategy for protecting AI within core business or mission functions, there is a comparable yet slightly more confident

|  |  |
| --- | --- |
| **4%** | 1 (Not Confident) |
| **17%** | 2 |
| **27%** | 3 (Neutral) |
| **25%** | 4 |
| **26%** | 5 (Very Confident) |

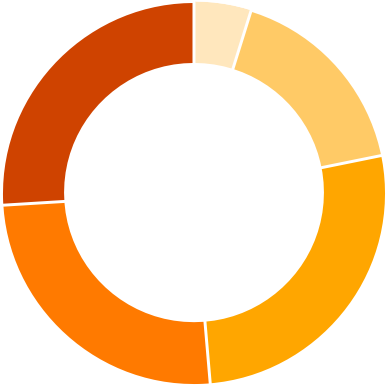
stance among professionals compared to their views on leveraging AI in security.

About 51% of respondents lean towards confidence, with 25% feeling reasonably confident and 26% very confident. This slightly higher

confidence level, particularly in the ‘very confident’ category, is notable. However, it also suggests a potential underestimation of the unique challenges and threats associated with securing AI systems, possibly due to a perception of AI as just another application in the business environment.

On the other hand, 27% of respondents adopt a neutral stance, perhaps reflecting a cautious acknowledgment of the complexities involved or an uncertainty about the emerging threats specific to AI. The lower confidence spectrum includes 17% who are somewhat unconfident and 4% who

are not confident at all. The overall trend indicates that while many professionals are confident in their organization’s ability to protect AI systems, there’s still a significant portion that recognizes the unknowns and potential underestimation of threats.

在评估专业人士对执行保护核心业务或任务中 AI 系统的安全策略的信心水平时，相较于他们对在安全领域利用 AI 的看法，这里表现出了近似但略高于前者的信心。

*您对您的组织实施安全策略以保护在您的核心业务或任务中使用的AI系统的能力有多少信心？*

|  |  |
| --- | --- |
| **4%** | 1 （完全不自信） |
| **17%** | 2 |
| **27%** | 3 （中立态度） |
| **25%** | 4 |
| **26%** | 5 （非常自信） |

约 51% 的回答者倾向于表示有信心，其中 25% 表示相当自信，26% 表示非常自信。尤其是在“非常自信”这一类别中，这种较高的信心水平值得关注。

然而，这也可能暗示了人们可能低估了保护 AI 系统所面临的独特挑战和威胁，这种低估可能源于将 AI 视为仅仅是业务环境中的一种常规应用的观念。

另一方面，有 27% 的受访者持中立态度，这或许反映了他们对涉及的复杂性持谨慎的态度或对 AI 特有的新兴威胁感到不确定。信心较低的群体中，17% 的人表示有些不自信，4% 的人则完全不自信。整体趋势显示，虽然许多专业人士对他们的组织在保护 AI 系统方面的能力感到自信，但仍有一大部分人意识到了存在的未知因素和可能被低估的威胁。

## Industry Familiarity with AI

## AI 在行业中的成熟度

### Familiarity with AI technologies and systems

### 对 AI 技术和系统的熟悉程度

The survey results regarding familiarity with various AI

*Rate your familiarity with the following AI technologies or systems:*

technologies and systems across the cybersecurity sector show a general trend of moderate to somewhat familiarity. Weighted averages for technologies like Natural Language Processing

(NLP), Generative Artificial Intelligence (gen AI), Deep Learning, Expert Systems, Machine Learning, LLM (Language Models like Gemini or GPT-4), and Robotics fall within a narrow range. This indicates that, generally, if professionals are familiar with one of these technologies, they likely have a comparable understanding of the others.

**0 1**

Not familiar

NLP (Natural Language Processing tools)

GenAI (Generative Artificial Intelligence)

DL (Deep Learning using neural networks)

Expert Systems (Rule-based AI)

ML (Machine Learning)

LLM (Language Models like GP-T3 or GPT-4)

Robotics (AI-driven robots)

**2 3 4**

Highly familiar

Interestingly, there’s a slight inclination towards older,

more established terms like NLP and Deep Learning, which score marginally higher than newer terms like LLM and gen AI. This could suggest a conflation between gen AI and popular tools like ChatGPT, indicating that while such tools are well-known, there may not be a deep understanding of the broader category of gen AI. This surface-level familiarity across various AI technologies might also contribute to the observed overconfidence in implementing AI strategies, as professionals might not fully grasp the complexities of these technologies.

*请对以下 AI 技术或系统的熟悉程度进行评分：*

网络安全行业内对各种 AI 技术和系统的熟悉程度的调查结果显示，总体趋势是从中等到某种程度的熟悉。涉及自然语言处理（NLP）、生成式人工智能（Gen AI）、深度学习、专家系统、机器学习、大语言模型（如 Gemini 或 GPT-4）和机器人技术的加权平均值都在一个较窄的范围内。这表明，在这些技术中，如果专业人士熟悉其中的一种，他们很可能对其他技术也有在一定程度上类似的了解。

**0 1**

非常不熟悉

自然语言处理（NLP）工具

生成式人工智能（GenAI）

深度学习（DL）神经网络

专家系统（基于规则的人工智能）

机器学习（ML）

大语言模型（LLM）如 GPT-3 或 GPT-4

机器人技术（AI 驱动）

**2 3 4**

非常熟悉

有趣的是，调查结果显示，

相较于比较新的术语，如大语言模型（LLM）和生成式人工智能（Gen AI），人们倾向于更为人熟知的成熟技术，如自然语言处理（NLP）和深度学习。这可能暗示了人们将生成式 AI 与 ChatGPT 等流行工具混淆。虽然这些工具广为人知，但对生成式 AI 这一更广泛类别的深入理解可能不足。这种对各种 AI 技术的都较熟悉的现象也可能是导致在执行 AI 策略时过度自信的因素之一，因为专业人员可能没有完全理解这些技术的复杂性。

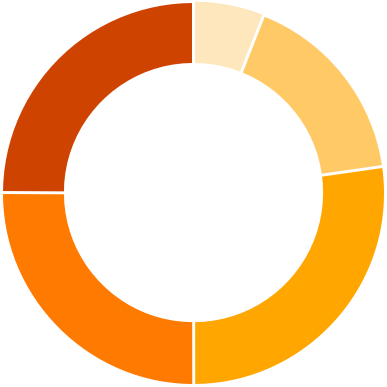
This lack of deep understanding raises questions about the effectiveness of current strategies and the need for further education in these areas. Comparatively, C-level executives report higher

familiarity with all AI categories compared to staff. This discrepancy in familiarity may be due to the pressure from leadership within organizations to explore adoption of AI. It likely requires leadership in the C-suite to familiarize themselves with a wide variety of AI technologies to identify which may provide the greatest benefits to their organizations. This gap in understanding underscores the importance of comprehensive education and training in AI technologies to ensure their effective and secure implementation especially for staff that is responsible for the implementation.

这种对 AI 技术深度理解的缺失，引出了关于目前策略有效性的质疑，并突显了对这些领域进一步教育和培训的必要性。相较于普通员工，首席级别（C级）高管认为他们对所有 AI 类别的熟悉度更高。这种熟悉度的差距可能源于组织内部领导层对探索 AI 应用的推动。首席级别（C级）高管可能需要对各种 AI 技术有广泛的了解，以便识别哪些技术可能为他们的组织或单位带来最大的好处。这种理解上的差异突显了对 AI 技术进行全面教育和培训的重要性，以确保其有效和安全地实施，尤其是对于那些负责具体实现的员工。

### Clarity of potential AI use cases in cybersecurity

### 网络安全领域中 AI 潜在用例的了解程度

The understanding of potential AI use cases in cybersecurity shows a split perspective,

*How clear are you on the potential use cases of AI in cybersecurity?*

with professionals divided on their clarity regarding AI applications. Overall, 50% of respondents feel clear

 **6%** 1 (Not Clear)

 **17%** 2

|  |  |  |
| --- | --- | --- |
| about AI use cases, with 25% | **27%** | 3 (Neutral) |
| somewhat clear and another | **25%** | 4 |
| 25% very clear. However, the | **25%** | 5 (Very Clear) |
| other half of the respondents |  | |
| express less certainty, with |
| 27% neutral, 17% somewhat |
| unclear, and 6% very unclear |
| about AI’s potential roles. |

*How clear are you on the potential use cases of AI in cybersecurity?*

C-level or executive

**52%**

**17%**

**16%**

**9%**

**6%**

Staff

**14%**

**26%**

**29%**

**21%**

**10%**

1 (Not Clear) 2 3 (Neutral) 4 5 (Very Clear)

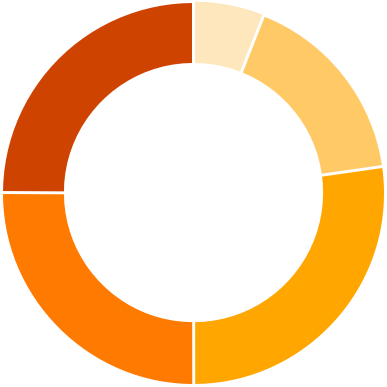
A notable difference emerges when comparing responses from C-level executives

and staff. Among C-level executives, a significant 52% report being very clear on AI use cases in cybersecurity, compared to

only 14% of staff feeling the same. This stark contrast

might suggest that C-level executives have a more aspirational or vision-oriented understanding of AI, focusing on broader goals and potentials, whereas staff, who are typically closer to the practical implementation, might be more aware of the complexities and uncertainties involved. It’s interesting to note that staff usually tend to buy into new technologies like AI earlier than the C-suite, yet in this case, their lower clarity could be influenced by the operational challenges they

foresee. The high level of awareness and clarity among C-level executives aligns with the increasing presence of AI in the news and its growing significance in the corporate zeitgeist.



*您对对 AI 在网络安全中潜在用例的了解程度如何？*

|  |  |  |
| --- | --- | --- |
|  | **27%** | 3 （中立） |
| **25%** | 4 |
| **25%** | 5 （非常清楚） |
|  | |

网络安全领域中对潜在 AI用例的理解显示出存在一定的分歧，专业人士在对 AI 应用的了解程度上意见不统一。总体来看，有 50% 的受访者认为对 AI 对AI的应用场景有清楚了解，其中 25% 觉得比较清楚，另外 25% 非常清楚。然而，另一半受访者则表现出较低的了解程度，27% 表示中立，17% 觉得不太清楚，6% 认为非常不清楚。

 **6%** 1 （完全不清楚）

 **17%** 2

*您对网络安全中AI潜在应用案例的清晰程度如何？*

首席级别（C级）或高级管理人员

**52%**

**17%**

**16%**

**9%**

**6%**

其他工作人员

**14%**

**26%**

**29%**

**21%**

**10%**

1（完全不清楚） 2 3（中立） 4 5 （非常清楚）

在比较首席级别（C 级）高管和普通员工受访者的反馈时，呈现出一个明显的差异。在首席级别（C 级）高管中，有高达 52% 的人表示对 AI 在网络安全中的应用场景有非常清晰的认识，而只有 14% 的普通员工有同样的感受。

这种鲜明的对比可能说明，首席级别（C 级）高管对 AI 的理解更加具有远见和目标导向，他们关注的是更广泛的目标和潜力；而在通常情况下，员工因为负责具体的实施工作，可能更清楚其涉及的复杂性和不确定性。有趣的是，虽然员工通常比高层更早接受像 AI 这样的新兴技术，但在这种情况下，他们对 AI 使用场景的不清楚可能是受到他们预见到的操作上的挑战影响。首席级别（C 级）高管中的高度意识和清晰理解，与 AI 在新闻中的频繁出现以及在企业文化中逐渐占据的重要地位是相符合的。

### Awareness of AI security frameworks

A significant 88% of security professionals are aware of existing AI security frameworks, such as those based on NIST guidelines in the US. However, it’s crucial to note that awareness does not necessarily equate to usage or deep understanding of these frameworks. Only 12% of respondents report not being aware of any AI security frameworks, highlighting the widespread recognition of these standards in the cybersecurity community yet leaving room for further exploration of their practical application and comprehension.

**88%**

*Are you aware of any existing AI security frameworks?*

## General Plans to Use AI

### Current use of AI products in general

 **69%** Currently using

 **29%** Planning to use

 **2%** Not using and no plans

 **88%** Yes

 **12%** No

The use or planned use of AI products in organizations suggests a few possibilities:

*Does your organization use or plan to use AI products in general?*

AI may be integrated into many products that organizations are using,

but staff might not be fully aware of this integration or may not recognize these as AI-driven products.

Alternatively, it could indicate a gap in understanding or communication within the organization, where C-level

executives believe they are utilizing AI more extensively than their staff are aware, or they might overestimate their actual use of AI technologies. This discrepancy underscores the need for clearer communication and education about AI applications and usage within organizations, ensuring that executives and staff consistently understand how AI is being leveraged in their work environment.

### 对 AI 安全框架的认识

**88%**

*您了解目前有哪些 AI 安全框架吗？*

大部分（88%）的安全专业人士了解现有的 AI 安全框架，如基于美国 NIST 指南的框架。然而值得注意的是，对这些框架的了解并不意味着它们的深入理解和使用。仅有 12% 的调查参与者表示他们不了解任何 AI 安全框架，这表明这些标准在网络安全界得到了广泛的认可，同时也显示出在这些框架的实际应用和深入理解方面还有进一步的探索空间。

### 应用AI的计划

### AI 产品的整体使用情况

 **69%** 正在使用

 **29%** 计划使用

 **2%** 没有也不计划使用

 **88%** 了解

 **12%** 不了解

组织中使用或打算使用 AI 产品暗示了几种可能性：AI 可能已经融入了许多组织正在使用的产品中，然而，员工可能并未完全意识到这种集成和融合，或者可能没能认识到这些产品是由 AI 驱动的。

*您的组织目前是否使用或有计划使用 AI 产品？*

另一方面，这也可能暗示组织内部存在理解或沟通的差距，

首席级别（C 级）高管认为他们在使用 AI 的程度上可能超过了员工的认知，或者他们可能高估了实际使用 AI 技术的范围。这种差异突显了组织内部需要更明确的沟通和对 AI 应用及使用的教育和培训，确保高管和员工都能一致地理解 AI 在他们的工作环境中是如何被运用的。

### Evaluation, assessment, or procurement process of AI products or services

**人工智能产品或服务的评估、判定或采购流程**

In assessing the adoption of evaluation, assessment, or procurement processes for GenAI and AI-specific products, survey results show a divide in organizational strategies. Nearly half of the

respondents (47%) rely on their current assessment processes, suggesting a level of adaptability of existing frameworks to AI technologies. However, almost an equal proportion (46%)—comprising those introducing new assessment processes (33%) and those evaluating new processes (13%)— are actively seeking or developing AI-specific evaluation methods. This indicates a recognition of AI’s unique challenges that might not be fully addressed by traditional approaches. The divergence in strategies is more pronounced when considering organization size: larger organizations, particularly those with over 100 employees, predominantly use current processes (87%), while smaller organizations (48%) are more inclined to develop new approaches, highlighting the varying capacities and needs in AI integration across different scales of business operations.

在评估GenAI和人工智能特定产品的评估、判定或采购流程的采用情况时，调查结果显示了组织战略的差异。近一半的受访者（47%）依赖于他们当前的评估流程，这表明现有框架对人工智能技术有一定程度的适应性。然而，几乎同等比例（46%）的人--包括引入新评估流程（33%）和评估新流程（13%）的人，正在积极寻求或开发专门针对人工智能的评估方法。这表明人们认识到人工智能的独特挑战，而传统方法可能无法完全解决这些挑战。在考虑组织规模时，战略上的差异更为明显：较大的组织（特别是员工人数超过100人的组织），主要使用当前流程（87%），而较小的组织（48%）更倾向于开发新方法，这突出了不同业务运营规模中人工智能集成的不同能力和需求。

*Do you have an evaluation, assessment, or procurement process designed for Gen AI or AI-specific products and services?*

*您是否有针对Gen AI或人工智能特定产品和服务设计的评估、判定或采购流程？*

**7%**

**47%**

**33%**

**13%**

无使用政策 使用当前评估流程

引入新的评估流程

评估新流程

### Current and planned use of AI technologies

**当前和计划使用的人工智能技术**

The survey on AI technology usage within organizations reveals diverse adoption patterns across different AI systems. Large Language Models are currently in use by 49% of the respondents, while 35% plan to use them within the next two years, and 14% have no plans for their adoption. This trend of current usage and future planning is similar across other technologies: Deep Learning

is currently used by 41%, with 40% planning future use. Expert Systems are currently at 31% usage, with a notable 51% planning to implement them. Machine Learning and Natural Language

Processing tools show a balanced mix of current usage (39% and 33%, respectively) and future plans (34% and 37%, respectively).

这项关于组织内人工智能技术使用情况的调查揭示了不同人工智能系统的采用不同的模式。49%的受访者目前正在使用大型语言模型，而35%的受访者计划在未来两年内使用，14%的受访者没有采用大型语言模型的计划。当前使用和未来规划的趋势在其他AI技术中也是相似的：深度学习目前有41%的人使用，40%的人规划未来使用。专家系统目前的使用率为31%，其中51%的人计划实施。机器学习和自然语言处理工具显示出当前使用（分别为39%和33%）和未来计划（分别为34%和37%）的平衡。

Interestingly, there seems to be a sense of obligation to keep pace with technological advancements, as indicated by the consistent number of respondents planning to adopt various AI technologies within two years. This could explain why 47% are planning to use Generative AI (GenAI) and 45% are looking at Robotics, despite 21% and 22% respectively having no plans to use these technologies. This highlights a potential trend where organizations feel the need to stay technologically relevant, even if they currently do not see an immediate application for these

AI systems. Additionally, there’s a perceptible discrepancy between C-level executives and staff in their understanding of AI usage within their organizations.

C-level executives tend to report higher current use of these tools, whereas staff members are more inclined to believe that their organizations are planning to adopt these technologies in the next

two years. This difference suggests a gap in awareness or communication about the actual stage of AI integration within their organizations.

*Which of the following AI technologies or systems are you using in your organization? (Select all that apply)*

*您在组织中使用以下哪种人工智能技术或系统？（选择所有适用项）*

LLM (Language Models like GPT-3 or GPT-4) LLM（大语言模型如GPT-3 或者GPT-4）

**3%**

**49%**

**35%**

**14%**

DL (Deep Learning using neural networks) DL（使用神经网络的深度学习）

**4%**

**41%**

**40%**

**14%**

Expert Systems (Rule-based AI) 专家系统（基于规则的AI）

**5%**

**31%**

**51%**

**13%**

ML (Machine Learning) ML（机器学习）

**3%**

**39%**

**34%**

**24%**

NLP (Natural Language Processing tools) NLP(自然语言处理工具)

**21%**

**9%**

**33%**

**37%**

GenAI (Generative Artificial Intelligence) GenAI（生成式AI）

**3%**

**29%**

**47%**

**21%**

Robotics (AI-driven robots) 机器人（人工智能驱动的机器人）

**4%**

**29%**

**45%**

**22%**

没有计划 计划在2年内使用 当前使用 不知道

有趣的是，人们似乎对于跟上技术的步伐有一种责任感，正如计划在两年内采用各种人工智能技术的受访者人数一致。这也可以解释为什么47%的人计划使用生成式AI（GenAI），45%的人正在研究机器人，尽管分别有21%和22%的人没有使用这些技术的计划。这突出了一个潜在的趋势，即组织认为有必要保持技术相关相关性，即使他们目前没有看到这些人工智能系统的直接应用。此外，最高层管理人员和员工对组织内人工智能使用的理解存在明显差异。最高层管理人员倾向于更高地报告这些工具的当前使用率，而工作人员更倾向于相信他们的组织计划在未来两年内采用这些技术。这种差异表明，在组织内部对人工智能整合的实际阶段的认识或沟通存在差距。

### Primary team responsible for AI deployment

**负责AI部署的主要团队**

In the realm of AI deployment in security products, the responsibility predominantly falls on the Security Team and IT Department, with 24% and 21%, respectively taking the lead. This is followed by the Data Science/Analytics team and a Dedicated AI/ML team, handling the task in 16% and 13% of organizations. Interestingly, Senior Management/Leadership and DevOps teams play a

smaller yet significant role, at 9% and 8%, respectively. This distribution highlights a trend where AI deployment is often managed by teams directly involved in technical and security aspects, although cross-functional collaboration and senior leadership also play crucial roles in guiding AI strategies.

在安全产品中的人工智能部署领域，责任主要落在安全团队和IT部门，分别占24%和21%。其次是数据科学/分析团队和专门的人工智能/机器学习团队，分别在16%和13%的组织中处理这项任务。有趣的是，公司高层和DevOps团队所扮演的角色较小但重要，分别占9%和8%。这种分布突出了人工智能部署通常由直接参与技术和安全方面的团队管理的趋势，尽管跨职能协作和公司高层在指导人工智能战略方面也发挥着关键作用。

*Which team is primarily responsible for AI deployment in your organization?*

*哪个团队主要负责您组织中的人工智能部署？*

**1%**

**21%**

**16%**

**13%**

**9%**

**8%**

**6% 3%**

**24%**

### Testing AI capabilities for security

测试AI的安全能力

A high number of security professionals report testing AI capabilities for security in organizations, with 67% affirming that they have

*Have you tested any AI capabilities for security in your organization?*

*您是否测试过组织中的人工智能安全功能？*

tested AI for security purposes specifically. This significant percentage suggests that AI integration into cybersecurity is not just a concept but a practical reality for many. This widespread testing could be attributed to AI functionalities being incorporated into

 **67% 是**

 **27%** 没有，但计划做

 **6% 没有计划**

existing product suites, making it more accessible and easier for organizations to adopt and experiment with or use LLM agents. Furthermore, 27% of respondents are in the planning stages of testing AI capabilities, indicating a growing trend and recognition of AI’s potential in enhancing security measures. On the other hand, a small portion (6%) have no plans to engage with AI for security, possibly due to lack of resources, expertise, or skepticism about AI’s effectiveness in their specific context.

大量安全专业人士报告称，他们在组织中测试了人工智能的安全能力，67%的人证实他们已经专门以安全为目的测试了人工智能。这一显著比例表明，人工智能融入网络安全对许多人来说不仅仅是一个概念，而是一个现实。这种广泛的测试可以归因于人工智能功能被纳入现有的产品套件，使组织更容易采用、试验或使用LLM agent。此外，27%的受访者正处于测试人工智能能力的计划阶段，这表明人工智能在加强安全措施方面的潜力有了越来越大的趋势和认可。另一方面，一小部分人（6%）没有计划在安全领域使用人工智能，这可能是因为缺乏资源、专业知识，或者对人工智能在特定环境中的有效性持怀疑态度。

### Biggest hurdles for implementing AI in security

**在安全领域实施人工智能的最大障碍**

The survey results reveal that the most significant hurdle to implementing AI in security is the skill gaps and shortage of knowledgeable staff, which is highlighted by 33% of respondents. This dual challenge of finding future staff with the necessary skills and enhancing the knowledge of current staff reflects the complex nature of AI in cybersecurity, requiring both specialized cybersecurity knowledge and a continuous understanding of evolving AI technologies. Addressing these skill- related issues is fundamental, as it could potentially alleviate other downstream challenges such as understanding AI risks and benefits, integrating AI with existing security infrastructure, and effectively managing regulatory and data privacy compliance.

调查结果显示，在安全领域实施人工智能的最大障碍是技能差距和缺少有知识的员工，33%的受访者强调了这一点。寻找具备必要技能的未来员工和增强现有员工知识的双重挑战反映了人工智能在网络安全中的复杂性：既需要专业的网络安全知识，又需要对不断发展的人工智能技术有持续的了解。解决这些与技能相关的问题至关重要，因为它可以缓解潜在的其他下游挑战，例如了解人工智能的风险和收益，将人工智能与现有的安全基础设施集成，以及有效地管理监管和数据隐私合规性。

Other notable hurdles include resource allocation (11%), understanding AI risks (10%), and the cost of implementation (8%), among others. Surprisingly, concerns like regulatory and data privacy compliance and the cost of implementation, which are traditionally viewed as significant barriers, are not the foremost concerns in this context. This might indicate an anticipation of long-term cost savings and a focus on current rather than future regulatory scenarios. The responses also show

a general concern across almost all options, indicating that while there is no single overwhelming obstacle, the journey to AI integration in cybersecurity is multifaceted and complex. This widespread concern across various aspects of AI implementation underscores the need for a holistic approach in adopting AI in security, one that addresses skill gaps, resource needs, and regulatory challenges in a balanced manner.

其他值得注意的障碍包括资源分配（11%）、了解人工智能风险（10%）和实施成本（8%）等。令人惊讶的是，传统上被视为重大障碍的监管和数据隐私合规性以及实施成本等问题并不是这种情况下的首要问题。这可能表明对长期成本节约的预期，以及对当前而非未来监管情景的关注。这些回应还显示出几乎所有选项都普遍存在担忧，表明尽管没有单一的压倒性障碍，但人工智能在网络安全的整合过程是多方面且复杂的。这种对人工智能实施各个方面的广泛关注突显了在安全领域采用人工智能的整体方法的必要性，这种方法需要以平衡的方式解决技能差距、资源需求和监管挑战。

*What is the biggest hurdle to getting started with AI in security implementations?*

*在安全实施中开始使用人工智能的最大障碍是什么？*

**33%**

**11%**

**10%**

**8%**

**8%**

**8%**

**8%**

**8%**

**4%**

Skill gaps/ shortage (e.g., finding future staff) & lack of knowledge (e.g., current staff)

技能差距/短缺（例如，寻找未来的员工）和缺乏知识（例如，现有员工）

Resource allocation (e.g., compute capabilities)

资源分配（例如计算能力Understanding AI risks

了解人工智能风险

Understanding AI benefits

了解人工智能的好处

Challenges with existing security infrastructure (e.g., integration)

现有安全基础设施面临的挑战（例如，集成）Regulatory and data privacy compliance

法规和数据隐私合规性

Cost of implementation

实施成本

Finding viable use-cases

寻找可行的用例

Unsure of AI effectiveness

不确定人工智能的有效性

### Desired outcomes from AI implementations

**AI实现的预期结果**

Organizations’ desired outcomes for implementing AI in security teams highlight a strong inclination towards supplementing skills and knowledge gaps, with 36% of respondents identifying this as

a key goal. This aligns with the previously noted challenge of skill gaps and lack of knowledge in AI applications within cybersecurity. This also aligns with the previous finding that AI is expected to support job roles rather than replace them completely. By integrating AI, organizations aim to

uplevel and augment their workforce, addressing these gaps and enhancing their team’s capabilities. This focus on enhancement rather than outright replacement of the workforce is further evidenced by the lower priority given to reducing the workforce (20%), indicating a preference for AI as a tool for empowerment and support.

组织在安全团队中实施人工智能的预期结果强调了弥补技能和知识差距的强烈倾向，36%的受访者将其视为关键目标。这与之前提到的网络安全领域人工智能应用的技能差距和知识缺乏的挑战相一致。这也与之前的发现一致，即人工智能有望成为支持工作的角色，而不是完全取代它们。通过集成人工智能，组织的目标是提升和增加他们的劳动力，解决这些差距并增强他们团队的能力。减少劳动力的优先级较低(20%)进一步证明了这种关注是对增强而不是彻底取代劳动力，这表明人们更倾向于将人工智能作为一种赋权和支持的工具。

Other significant desired outcomes include faster threat detection and improved productivity, each selected by 26% of respondents, as well as enhancing the overall cybersecurity posture, reducing errors and misconfigurations, and accelerating incident response, each at 24%. These goals underscore a desire for AI to bring efficiency and effectiveness to cybersecurity operations. Interestingly, while improved productivity is a key expectation, it is not the dominant outcome, possibly reflecting a nuanced view where the focus is more on quality (such as accurate threat detection and response) rather than quantity of work. However, the fact that a notable portion

of respondents (15% to 20%) also look for AI to reduce workforce, overhead costs, and workload suggests a balanced expectation where AI is seen as a means to optimize and streamline security operations while also enhancing the performance and capabilities of the existing human workforce.

其他重要的期望结果包括更快的威胁检测和提高生产力(26%的受访者选择了这两项)，以及增强整体网络安全态势、减少错误以及错误配置、加速事件响应(24%)。这些目标强调了人工智能为网络安全运营带来效率和有效性的愿望。有趣的是，虽然提高生产力是一个关键的期望，但它并不是主要的结果，这可能反映了一种微妙的观点，即重点更多地放在质量(如准确的威胁检测和响应)上，而不是工作的数量。然而，相当一部分受访者(15%至20%)也希望人工智能能够减少劳动力、管理成本和工作量，这表明了一种平衡的期望，即人工智能被视为优化和简化安全操作的一种手段，同时也能提高现有劳动力的绩效和能力。

*What are your desired outcomes when it comes to implementing AI in your security team?*

*当涉及到在您的安全团队中实施人工智能时，您期望的结果是什么？*

**36%**

**26%**

**26%**

**24%**

**24%**

**24%**

**20%**

**19%**

**17%**

**15%**

Supplemental skills and knowledge gaps (uplevel/ augement workforce)

补充技能和知识差距(提升/增加劳动力)

Faster threat detection

更快的威胁检测

Improved productivity

提高生产力

Improve cybersecurity posture

改善网络安全态势

Reduce errors and misconfigurations

减少错误和错误配置

Faster incident response

更快的事件响应

Reduce workforce

减少劳动力

Improve accuracy of threat analysis

提高威胁分析的准确性

Reduce overhead costs

降低管理费用

Reduce workload

减少工作量

## AI Staff, Leadership, and Training

**人工智能员工、领导和培训**

### Creating a team for governing the secure use of AI

**创建一个团队来管理人工智能的安全使用**

*Are you creating a team to govern the secure use of AI within your organization? (e.g., policy development, AI features/ product procurement, responsible/ ethical use of)*

*您是否正在创建一个团队来管理组织内人工智能的安全使用？（例如，政策制定、人工智能功能/产品采购、负责任/合乎道德的使用）*

A substantial 74% of organizations are planning to create teams dedicated to governing the secure use of AI, emphasizing the serious consideration companies are giving to AI integration. This move towards establishing specialized teams for policy development, AI product procurement, and ensuring responsible and ethical use, signals a clear recognition of AI’s transformative impact

on security roles. Rather than replacing existing functions,

**74% 是**

**20% 否**

**6% 不确定**

AI is leading to the evolution and expansion of organizational roles, requiring new governance structures and expertise. This approach underscores the shift in the security landscape where AI is not merely an additional tool, but a significant factor that necessitates thoughtful integration and management. The fact that only 20% are not forming such teams, and 6% are unsure, further

highlights the widespread acknowledgment across the industry of the need for dedicated oversight and specialized skills to harness AI’s potential effectively and securely.

74%的组织正计划创建专门管理人工智能安全使用的团队，这强调了公司正在认真考虑人工智能的集成。这一举措旨在建立专门团队，负责政策制定、人工智能产品采购，并确保负责任和合乎道德的使用，标志着人们明确认识到人工智能对安全角色的变革性影响。人工智能不是取代现有的功能，而是促使组织角色的演变和扩展，这需要新的治理结构和专业知识。这种方法强调了安全领域的转变，人工智能不仅仅是一个额外的工具，而是一个需要深思熟虑的集成和管理的重要因素。事实上，只有20%的受访者表示没有组建这样的团队，6%的人不确定，这进一步凸显了整个行业普遍认识到，需要专门的监督和专业技能来有效、安全地利用人工智能的潜力。

### Team responsible for securing AI systems

**负责保护AI系统的团队**

*Which team will be responsible for securing AI systems within your organization?*

*哪个团队将负责保护您组织内的人工智能系统？*

The responsibility for securing AI systems within organizations predominantly falls to the Security Team and IT Department, with 29% and 25% respectively taking the lead. These figures mirror the similar distribution seen in AI deployment responsibilities, reflecting a consistent approach where the primary technical teams are entrusted with both implementing and securing AI technologies. This allocation of responsibilities

|  |  |
| --- | --- |
| **29%** | Security Team 安全团队 |
| **25%** | IT Department IT部门 |
| **12%** | The Data Science/ Analytics team  数据科学/分析团队 |
| **10%** | DevOps |
| **10%** | Senior management/ Leadership  高级管理层/领导层 |
| **8%** | Cross-functional team  跨职能团队 |
| **6%** | I’m not sure 我不确定 |

underscores the crucial role these departments play in the effective and safe integration of AI into organizational infrastructures.

在组织内保护人工智能系统的责任主要落在安全团队和IT部门身上，分别有29%和25%。这些数字反映了人工智能部署责任的类似分布，即委托主要技术团队实施和保护人工智能技术。这种职责分配强调了这些部门在人工智能有效、安全地融入组织基础设施方面发挥的关键作用。

### 当前或计划使用与人工智能和网络安全相关的培训项目

The survey indicates a strong inclination towards investing in training programs for staff on AI and cybersecurity within organizations. A notable

*您的组织是否正在实施或计划实施与人工智能和网络安全相关的员工培训计划？*

26% of organizations are already using such training programs, demonstrating a proactive approach to equipping their workforce

|  |  |
| --- | --- |
| **26%** | 当前使用 |
| **50%** | 计划12月内使用 |
| **21%** | 计划使用(没有时间轴) |
| **4%** | 没计划 |

with the necessary skills and knowledge. A significant 50% plan to implement these training programs within

the next 12 months and

21% of organizations have plans to introduce such training, although without a specific timeline. This highlights the widespread recognition of the importance of continuous learning in the rapidly evolving fields of AI and cybersecurity. Only a small fraction (4%) have no plans for such training, suggesting that most organizations are focused on solving the skills and knowledge gaps they’ve previously identified as concerns with AI use. 该调查表明，人们强烈倾向于投资于组织内员工的人工智能和网络安全培训项目。一个值得注意的现象是：26%的组织已经在实施此类培训计划，证明这是一种为员工提供必要的技能和知识的积极方法；有50%的组织计划在接下来的12个月提供；21%的组织尽管没有具体的时间表，但仍有引入此类培训的计划。这凸显了人们对快速发展的人工智能和网络安全领域进行持续学习重要性的共同认识。只有一小部分（4%）组织没有此类培训计划，这表明大多数组织都专注于解决他们之前认为与人工智能使用有关的技能和知识差距。

### 来自高级管理层采用人工智能的压力

*您的高级管理层（如董事会）是否在推动人工智能的采用？*

 **82% 是**

 **12%** 否

 **6% 不确定**

The push for AI adoption from executive leadership, as indicated by 82% of respondents, sheds light on why many C-level executives report higher levels of familiarity with

AI technologies and their applications. This top- down pressure likely stems from a recognition of AI as a competitive advantage

in the modern business landscape. When executive teams, including Boards of

Directors, prioritize AI integration, it creates an organizational culture that values and focuses on AI capabilities, thereby encouraging a deeper understanding and engagement with AI at all levels of the organization. This focus at the top echelons of management not only drives the strategic adoption of AI but also likely influences the reporting of higher familiarity with AI among C-level executives. 关于推动人工智能的采用， 82%的受访者认为，许多首席执行官等高级管理层认为其熟悉人工智能技术及其应用程序。这个自上而下的压力可能源于认为人工智能能够促进组织现代商业竞争中处于优势地位。高级管理团队（包括董事会）会优先考虑人工智能的整合，并为它创造了一种重视和关注人工智能的组织文化，从而鼓励各级组织可以更深入地了解和参与人工智能的活动中，高层管理团队不仅在战略层面关注人工智能领域，他们还将影响C级高管对人工智能的熟悉程度。

### 领导层对人工智能影响安全的认知

There is a tendency among organizational leadership to be more informed and aware of AI’s implications on security than not. Approximately 28% of leaders are reported as

*您的领导层（如董事会）在多大程度上了解和意识到人工智能对安全的影响？*

being fully aware, showing a proactive initiative among a significant portion of upper management to deeply understand AI’s impact

on security. An additional 46% are moderately aware, suggesting that while they have a general understanding,

 28% 完全知情

 46% 适度意识

 18% 稍有察觉

 6% 不知道

there may be gaps in their full comprehension of AI’s complexities and nuances in the security domain. This awareness may be informed by information from security teams and current news, highlighting the importance of continuous and high-level communication within organizations. An interesting point to note is that there is no substantial difference in this awareness between C-level executives and staff, indicating a unified perception of leadership’s awareness. This collective view is a point-in-time measurement and is subject to change as rapidly as the AI and cybersecurity landscape itself evolves. 组织的领导层更加了解人工智能对安全的影响。据报道，大约28%的领导者充分认识到了人工智能对安全的影响，很大一部分高级管理层在团队中表现出积极主动的态度。另外46%的组织则有所了解，这表明他们虽然有总体认识，但在全面理解人工智能在安全领域的复杂性和差别方面可能存在差距。这种认识可能是通过当下新闻或安全团队提供的信息得出的，突出了组织内持续和高层沟通的重要性。值得注意的是，首席执行官和员工在这方面的认识没有实质性差异，表明领导层的认识是一致的。这种集体观点只是在某个时间点的测量，会随着人工智能和网络安全的发展而迅速变化。

**生成式AI的网络安全计划**

### 生成式AI解决方案的当下和计划使用

The anticipation for 2024 as a significant year for the adoption of Generative

*一般来说，您的组织是否正在使用或计划使用生成式AI解决方案？*

AI (GenAI) solutions is evident from the survey results. Currently, 22% of

|  |  |
| --- | --- |
| **22%** | 正在使用 |
| **55%** | 明年内使用 |
| **13%** | 明年以后使用 |
| **6%** | 没有计划 |
| **3%** | 不知道 |

organizations are using GenAI,

but a remarkable 55% plan to adopt these solutions within the next year, signaling a substantial surge in GenAI integration. An additional 13% expect to use GenAI solutions over a year from now, while only 6% have no plans to

invest in this technology. Regardless, the data points to 2024 as a pivotal year, with a significant movement towards embracing GenAI across various organizations. 从调查结果中可以明显看出， 2024年 生成式AI解决方案的预期采用。目前，22%的组织正在使用生成式AI，但55%的组织计划在明年内采用生成式AI解决方案，这标志着生成式AI的大幅增长。另有13%的组织预计在明年后使用生成式AI解决方案，而只有6%的人没有投资这项技术的计划。无论如何，数据表明2024年是关键的一年，各组织都在大力推行生成式AI。

### 生成式AI在网络安全的计划使用

The planned use of GenAI in cybersecurity reflects a broad exploration of potential applications across various organizations. The survey results show a relatively even distribution among the top five use cases, indicating a diverse range of areas where GenAI is expected to make an impact. Rule creation emerges as the leading use case, with 21% of organizations aiming to leverage GenAI to develop more sophisticated security protocols. This is closely followed by attack simulation and compliance violation monitoring, each at 19%, highlighting GenAI’s potential to enhance proactive security measures and regulatory adherence. Additionally, 16% of respondents are looking to use GenAI for network detection, aiming to improve the identification of network threats. Another 16% focus on using GenAI to reduce false positives, underscoring its potential to refine alert accuracy and efficiency. This spread of interest across different use cases suggests that organizations are not only eager to adopt GenAI but are also keen on customizing its applications to meet specific security needs, thereby maximizing its benefits in the evolving landscape of cybersecurity. 生成式AI在网络安全中的计划使用反映了各组织在AI应用的广泛探索。调查结果显示，Top5用例的分布相对均匀，表明生成式AI预计会产生影响的领域多种多样。规则创建成为主要使用用例，21%的组织旨在利用生成式AI开发更复杂的安全规则。紧随其后的是攻击模拟和合规违规监控，各占19%，突显了生成式AI在加强主动安全措施和遵守监管方面的潜力。此外，16%的受访者希望使用生成式AI进行网络检测，旨在改进网络威胁的识别。另有16%的受访者专注于使用生成式AI来减少误报，强调了其提高警报准确性和效率的潜力。这种兴趣在不同用例中的传播表明，组织不仅渴望采用生成式AI，而且热衷于定制其应用程序以满足特定的安全需求，从而在不断发展的网络安全环境中最大限度地提高其效益。

*你的组织计划如何使用生成式AI用于网络安全? (选择Top3 用例)*



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **21%** | 规则创建 | **13%** | 要搜索的资源语言 | **9%** | 取证分析 |
| **19%** | 攻击模拟 | **13%** | 威胁摘要 | **9%** | 聊天机器人 |
| **19%** | 合规违规监控 | **13%** | 数据防泄漏，IP保护 | **8%** | 事件摘要 |
| **16%** | 网络检测 | **11%** | 用户行为分析 | **8%** | 配置漂移 |
| **16%** | 减少误报 | **10%** | 自动生成报告 | **8%** | 行动/消减建议 |
| **15%** | 培训开发和支持 | **10%** | 终端检测 | **7%** | 代码分析 |
| **14%** | 异常分类 | **9%** | 时间日志摘要 |  |  |

### 生成式AI网络安全之旅的现状

The majority of organizations are in the early stages of their GenAI journey in the realm of cybersecurity, with a strong focus on exploration and implementation. Approximately 30% are currently exploring options and use cases, indicating a proactive approach to understanding the potential of GenAI in enhancing their security posture. This phase of exploration is crucial as it lays the groundwork for practical applications. Additionally, 15% are in the testing phase, experimenting with specific use cases to gauge the effectiveness and applicability of GenAI solutions. The implementation phase sees a combined 47% of organizations, with 23% currently implementing solutions and 24% having fully implemented GenAI, suggesting a rapid advancement from theoretical exploration to practical deployment. A negligible 3% are not considering GenAI yet, and an equal 3% maintain a strict no-use policy. These findings reflect a trend towards embracing GenAI in cybersecurity, with most organizations actively engaged in the initial phases of exploring and integrating these innovative solutions. 大多数组织都处于生成式AI网络安全领域之旅的早期阶段，重点关注探索和实施。大约30%的组织目前正在探索选项和用例，这表明他们采取了积极主动的方法来了解生成式AI在增强其安全态势方面的潜力。这一探索阶段至关重要，因为它为实际的应用奠定了基础。此外，15%的组织处于测试阶段，对特定用例进行实验，以评估生成式AI解决方案的有效性和适用性。23%的组织目前正在实施解决方案，24%的组织已完全实施生成式AI，这表明生成式AI从理论探索到实际部署的快速发展。3%的组织还没有考虑生成式AI，同样3%的组织保持严格的禁止使用政策。这些发现反映了在网络安全中采用生成式AI的趋势，大多数组织处在积极参与探索、整合生成式AI创新解决方案的初始阶段。

*你的组织当前在哪些领域使用生成式AI?*

**3%**

**30%**

**15%**

**23%**

**24%**

**3%**

**2%**

尚未考虑t

探索选项和用例

测试用例

实施解决方案中

完全实施

严格禁止使用

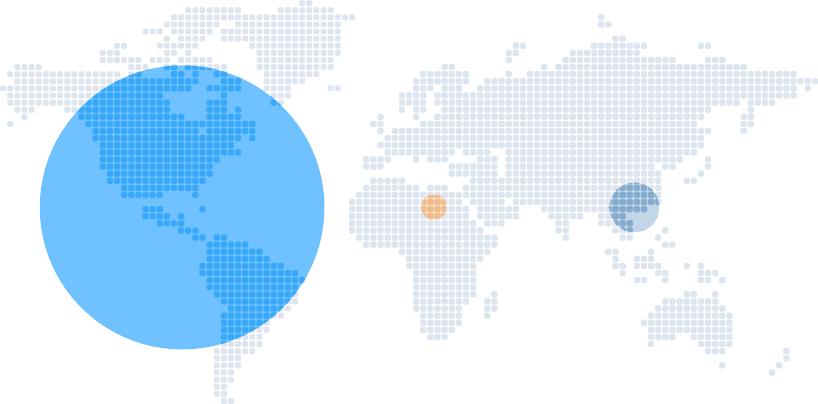
不知道

## 统计

The survey was conducted online by CSA in November 2023 and received 2,486 responses from IT and security professionals from organizations of various sizes across the Americas, APAC and EMEA. 该调查由云安全联盟于2023年11月在线进行，收到了来自美洲、亚太地区和EMEA不同规模组织的IT和安全专业人员的2486份回复

*你所在世界的哪个区域?*

美国



**7%**

**14%**

**79%**

欧洲,中东,非洲 (EMEA)

亚太 (APAC)



*您所在的组织的规模?*



*您在您组织的职位是什么?*

1%



20%

36%

21%

12% 11%



13%

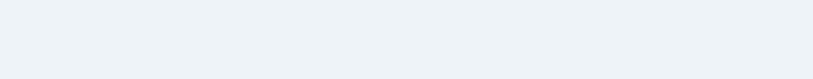
21%

44%

20%

<100 雇员 101-1000 雇员 1001-5000 雇员

5001-10000 雇员 10001+ 雇员



*您所在的企业属于以下哪个主要领域?*

C-层级/执行官 主管 经理 员工 其他

**3% 2%**



**22%**

**7% 6% 6% 5% 5% 5% 4% 4% 4% 4% 4%**