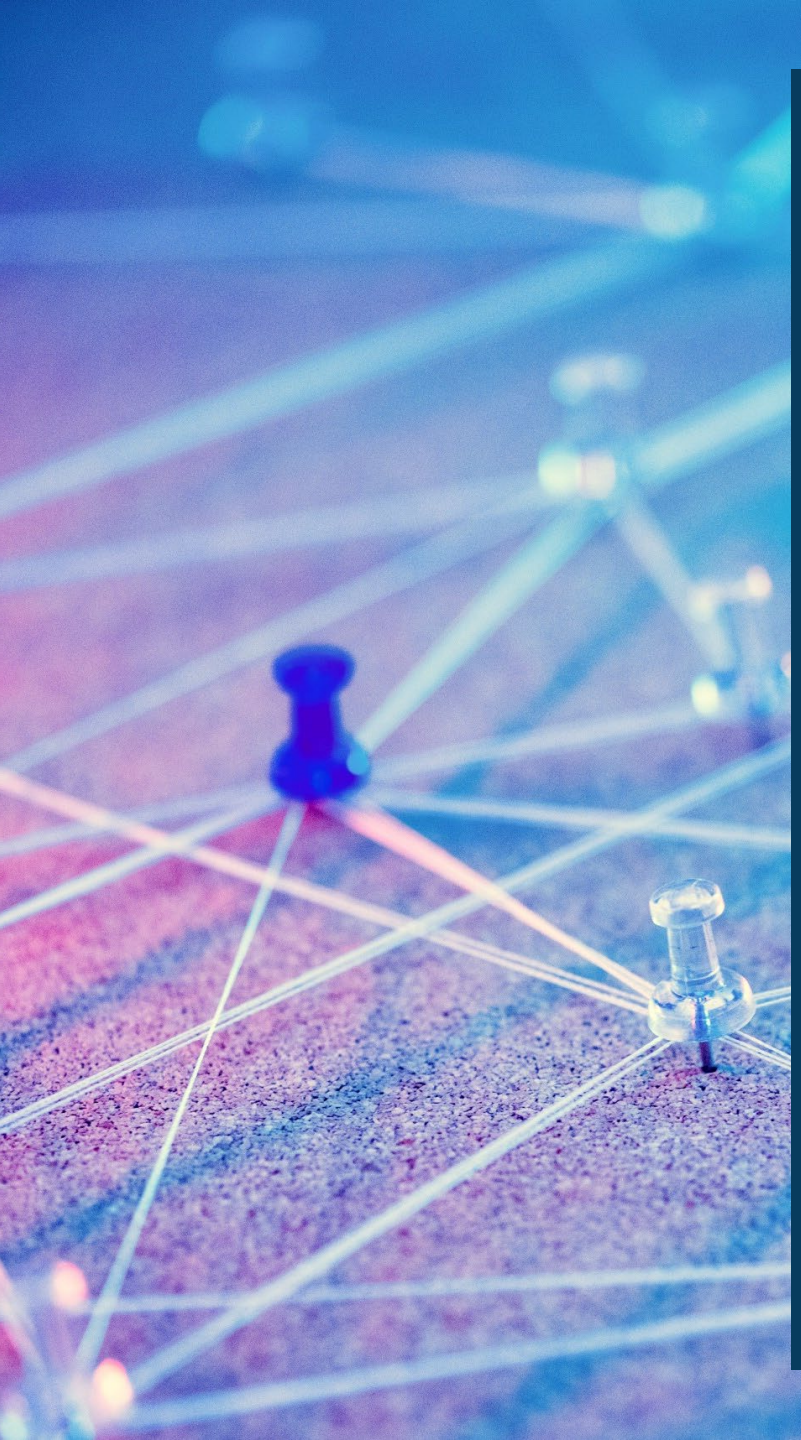
(CS)²AI

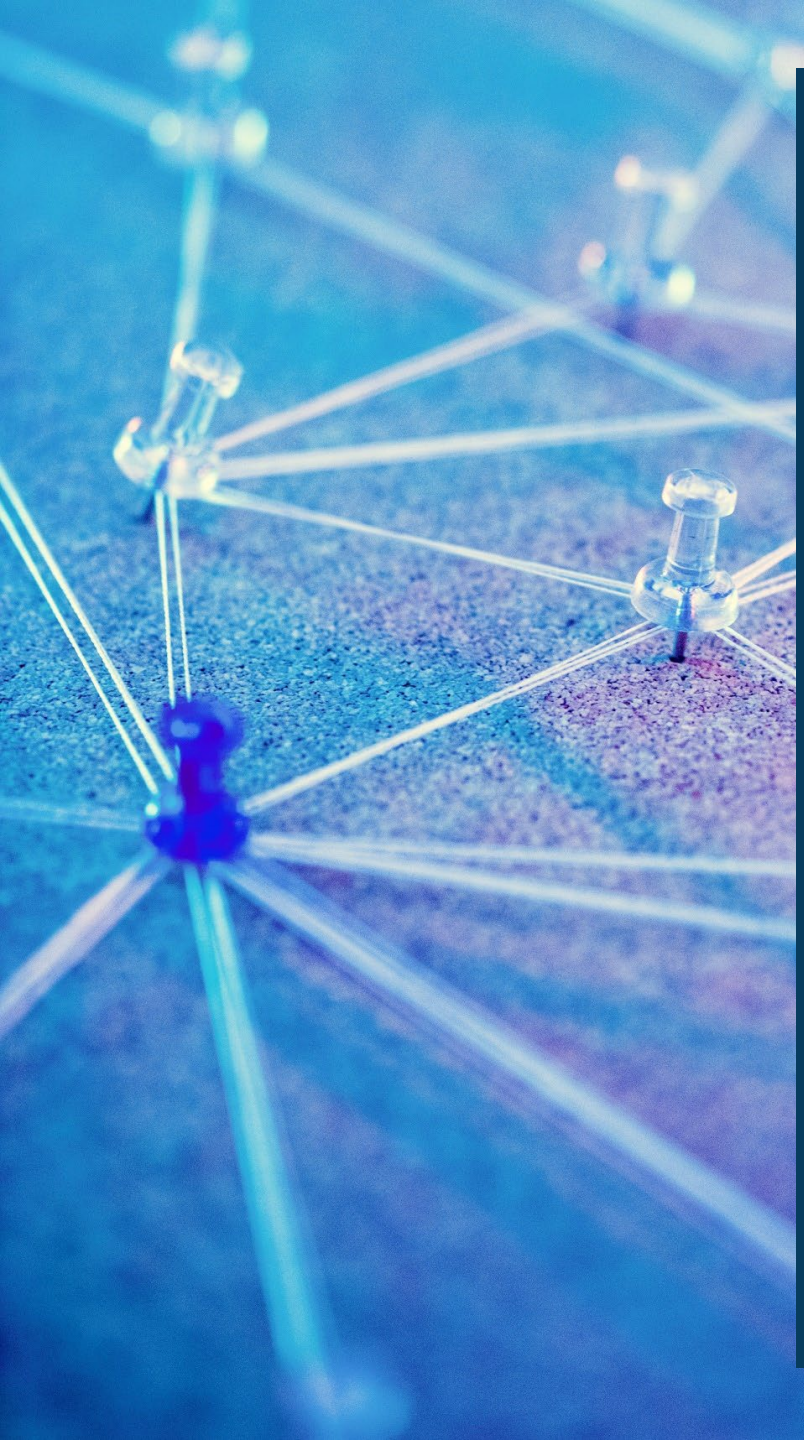
KPMG
毕马威

(CS)²AI-KPMG 控制系统网络安全年度报告

2024



目录



目录

主席致辞

尊敬的业界同仁：

在新年到来之际，回顾我们在控制系统安全领域取得的进展以及我们继续面临的挑战至关重要。

即使作为一个百分之百的乐观主义者，在去年数以百次与他人交谈中仍然可以感受到，想要取得真正的进展还有很长的路要走。有一点始终没改变的，就是我们面前还有大量的工作要做，来确保能够实现现代生活方式的安全系统。

我很自豪地发布第三版(CS)²AI-KPMG控制系统网络安全年度报告，这份报告不仅凝结着我们分析师和研究人员的心血，也离不开所有报告指导委员和同仁的辛勤付出。

今年的报告基于630多名行业成员的调查结果和(CS)²AI全球会员的代表性样本（目前约有3,4000名社区成员）而形成，其中包括关于控制系统安全事件、攻击模式和应对方面的经验，以及将资源集中于保护关键系统和资产所面临的问题。

2024年的报告阐明了控制系统安全行业的几个关键趋势和挑战。虽然网络攻击的增加令人担忧，但各组织在网络安全预算方面也更加充裕，专注于预防，并认识到供应链攻击的威胁。报告中强调的一个重要问题是网络安全领域的技术工人短缺。

随着网络威胁的兴起，对网络安全专业人员的需求从未如此之高。

调查报告中的受访者增加了招聘合格人员的难度，报告强调各组织需要投资发展现有员工的网络安全技能并对其进行培训。

每年都有越来越多的参与者为我们的年度报告付出努力。我们必须向报告发起人毕马威国际表示最大的感谢，感谢他们几年前使我们能够启动这个项目，并感谢他们在项目制作方面继续支持和合作。

Waterfall安全解决方案和Fortinet自我们的第一版报告以来一直与我们合作，并提供资源和专业知识。我们还要感谢所有其他合作伙伴，他们的支持和指导每年都有助于使这成为一个宝贵的决策支持工具（见附录D）。当然，我们也不能忽略那些主动加入年度报告指导委员会的所有成员（见附录B）。

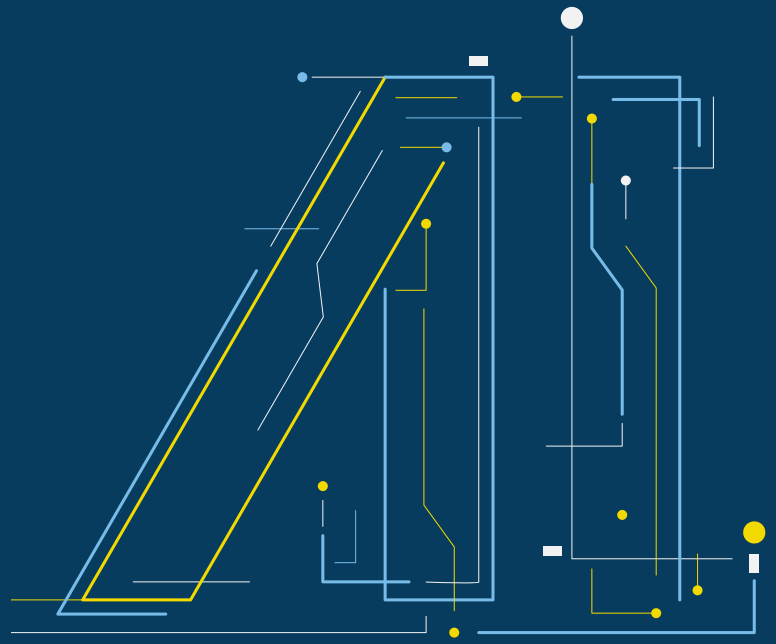
我们的共同目标是，本报告能够为业界同事提供基于经验的有价值见解，成为辅助日常做出许多艰难决定的工具。重要的是，要利用本报告的结论做出明智的决策，并优先考虑能为控制系统安全支出提供最佳投资回报率的领域。我们将一如既往地支持我们的社区，努力确保系统安全，使现代生活方式成为可能。

Derek R. Harp

德里克·哈普

(CS)²AI创始人兼董事长

年度报告冠名赞助商前言



瓦尔特·里西

毕马威国际全球OT网络安全负责人，
毕马威阿根廷咨询业务主管合伙人

巴勃罗·阿尔马达

毕马威国际全球OT网络安全副主管，
毕马威阿根廷OT网络安全主管合伙人

虽然运营技术（OT）网络安全已经在大多数行业首席信息安全官（CISO）的议程上占据了一席之地，但在许多情况下，它仍然是更广泛的网络安全领域中一个孤立的问题。尽管近年来许多公司取得了重大进展，但该领域仍在不断走向成熟和整合。今年(CS)²AI和毕马威国际合作的结果揭示了我们取得的进展和面临的持续挑战。

关于成熟度，近一半（49%）的受访组织运营仍处于较低的成熟度（第1级或第2级），即只拥有解决问题和基本管理的能力。虽然建立OT网络安全项目的必要性不再是一个新颖的概念，尽管市场上已有成熟的技术解决方案，但调查结果发现成熟度仍没有大幅提升。可能阻碍进步的一个显著因素是技术资源的稀缺，这也是该领域多年来一直在努力应对的一个众所周知的挑战。

尽管存在这些挑战和相对渐进的发展步伐，但我们与行业高管的讨论表明，我们对OT网络安全相关风险的认识有所提高。尽管在过去几年里，这可能是一次艰难的推销，但与高层管理人员的网络安全对话越来越多地围绕着OT网络安全作为焦点。这意味着对学科的关键重要性有了更高层次的理解和认识。正如所料，高管们也更愿意参与以OT网络安全为中心的危机模拟和桌面演习。

我们相信，毕马威国际和(CS)²AI之间的年度合作在提高高管层的意识方面发挥着关键作用。通过对全球从业者和领导者所提供的真实案例进行分析，我们的调查为该领域的全球演变提供了一个公正的视角。它有助于做出明智的投资决策，并突出了人们对这一领域日益增长的兴趣。我们相信，我们的联合报告为OT网络安全从业人员和领导者以及更广泛的执行社区提供了宝贵的资源。在第三版报告中，我们重申，我们将致力于对该领域全球领导人所认为的围绕OT网络安全的主要挑战提供公正的展望。

我们诚邀读者深入了解本年度报告的见解，希望我们的年度工作能让您在这一领域做出更明智的决策和投资，无论您是领导者、执行者还是实践者。我们认为，OT 网络安全是一个持续的旅程，没有真正的终点。本调查与网络安全本身一样，是这一永恒旅程中不可或缺的一部分，致力于年复一年地为这一关键领域提供更好的见解。

执行摘要

主要调查结果

- 几乎一半的响应组织（49%）仍然没有ICS/OT网络安全计划，或者只有基本的网络安全计划，缺乏既定的计划、程序或能力改进过程。
- 不同组织级别的受访者在分配额外酌处权资金方面的优先事项大相径庭，这就提出了他们的动机是否一致以及他们的目标为何不同的问题。
- 对控制系统网络活动的全面监控正在增加，在过去一年中增加了80%。
- 我们评估了来自企业网络、互联网、云以及集成商/供应商的许多控制系统组件（PLC、IED、RTU、HMI、服务器、工作站和Historian）的可访问性。在这一领域，拥有高成熟度项目的组织和拥有低成熟度项目的组织之间通常没有什么区别。事实上，高成熟度组织中的组件通常比低成熟度组织中的组件更容易访问。
- 有关高成熟度和低成熟度的定义，请参见第8页。

本报告是一系列年度出版物中的最新一份，这些出版物来自国际控制系统网络安全协会（又称(CS)²AI），其拥有近3,4000名成员的社区和数十个战略联盟伙伴的研究。在(CS)²AI创始人兼董事长Derek Harp和联合创始人兼总裁Bengt Gregory-Brown领导的数十年网络安全调查开发、研究和分析的基础上，(CS)²AI团队邀请我们的全球成员和我们扩展社区中的数千名其他人参加。

通过询问关键问题，了解他们在运营、保护和维护运营技术（OT）系统和资产的第一线的经验，这些系统和资产耗资数百万至数十亿美元的资本支出，对持续收入产生同等或更多的影响，并影响全世界个人的日常生活和企业的业务运营。其中超过630人对我们的初步调查做出了回应，更多人参与了我们通过正在进行的(CS)²教育计划开展的额外数据收集工作。

该数据池以匿名方式提交，以确保排除可能影响参与者反应的考虑因素，从而深入了解负责控制系统运营和资产的个人和组织的真实经验，超出本报告的预设范围。

我们希望我们选择的细节能为读者提供所需的决策支持工具。

调查目标与方法

本报告使用总体术语“控制系统”(CS)和“运营技术”（OT）来指代管理、监控和/或控制物理设备和过程的任何/所有系统。因此，CS、(CS)和OT应理解为包括工业控制系统（ICS）、数据采集与监视控制系统（SCADA）、过程控制系统（PCS）、过程控制域（PCD）、建筑/设施控制、自动化和管理系统（BACS/BAMS/FRCS…）、联网医疗设备等。

同样，“$(CS)^2$”是泛指控制系统网络安全领域、专业、项目和人员。

$(CS)^2$AI-KPMG控制系统网络安全年度报告系列于2019年推出，旨在为世界各地参与控制系统资产和运营安全工作的各方（无论是终端用户还是供应商、高管、经理还是运营团队）提供信息丰富的决策工具。

本报告由以下实体共同完成：

- $(CS)^2$AI：作为项目发起人，$(CS)^2$AI在项目规划、领导和实施中发挥着主要作用，包括数据收集、分析和编写本报告。
- 毕马威国际：作为产权报告发起人，毕马威提供了主要资金和组织资源支持，以增强$(CS)^2$AI自身的能力。
- 其他赞助商：非冠名赞助商Fortinet、Waterfall Security Solutions 和 Opscura提供了额外的资金和其他资源。（见附录D：报告发起人。）

根据上述目标，$(CS)^2$AI和我们的赞助商向在该领域工作的CS/OT网络安全社区成员分发了在线调查，收集了CS事件、活动和技术的关键数据，以及组织如何应对不断变化的威胁的详细信息[1]。

$(CS)^2$AI邀请其相关成员、已知的OT安全捍卫者和研究人员参与，通过直接邀请和各种广播媒体渠道分发调查，并在为CS网络安全工作人员服务的网站上进行推广，目的是收集尽可能广泛的样本。受访者通过确认他们目前或最近参与$(CS)^2$领域而自我选择。他们包括所有组织层面的专业人员：网络安全专家和事务专家（SME），以及其工作包括但不仅限于安全和保护控制系统的人员。

能够将我们的参与者解析为不同的群体，并比较他们在这些群体关联中的投入，这是从这个年度研究项目中获得见解的关键。虽然我们认为调查参与者$(CS)^2$AI计划的成熟度是最重要的维度，但我们也考虑了他们的组织级别、地区以及他们与$(CS)^2$资产（供应商、用户、所有者或运营商）的关系。当然，我们也进行了纵向分析，当我们发现有趣的趋势时，我们也分享这些趋势。

[1] 威胁范围：对CS/OT行动和资产的所有可能威胁的总和。威胁是动态的，随着漏洞的发现和针对漏洞利用的保护措施的制定而不断变化。

(CS)²项目

衡量受访组织的(CS)²计划成熟度是我们年度分析的关键，它为评估受访组织提供的许多其他数据提供了衡量标准。与其他组织相比，拥有更加成熟计划[2]的组织在哪些方面做得更不同或更频繁？如果我们发现这些组织的回答之间存在明显差异，我们会提请读者注意。我们要求每位参与者从以下描述中选择最适合其组织情况的一项。

控制系统网络安全计划成熟度

第5级	第4级	第3级	第2级	第1级
网络安全流程通过现有流程的反馈不断改进，并适应更好地满足组织需求。 执行流程的人员具有足够的技能和知识。优化、自动化、集成、可预测。 主动防御、威胁情报、事件管理。	网络安全计划利用数据收集和分析来改善其结果。 活动以文件化的组织指令为指导，政策包括特定标准和/或指南的合规要求。 负责控制系统安全职责的人员受过培训并具备经验。计划是管理的，主动的，跟踪指标，部分自动化。 主动防御、安全信息和事件管理（SIEM）、异常和漏洞检测。	网络安全根据文件化的流程和程序进行生产和工作。确定并参与关键利益相关者。提供足够的资源来支持这一过程（人员、资金和工具）。已经确定了指导实施的标准和/或指导方针。 被动防御。	在网络安全实施中遵循基本的项目管理实践；成功仍然需要关键人物，但知识体系正在发展。执行最佳实践，但可能是临时的。 被动防御。	救火状态。网络安全程序是无组织和无记录的，不是在“程序”中组织的。成功取决于个人的努力；是不可重复或可扩展的，因为没有充分定义和记录流程。 被动防御。

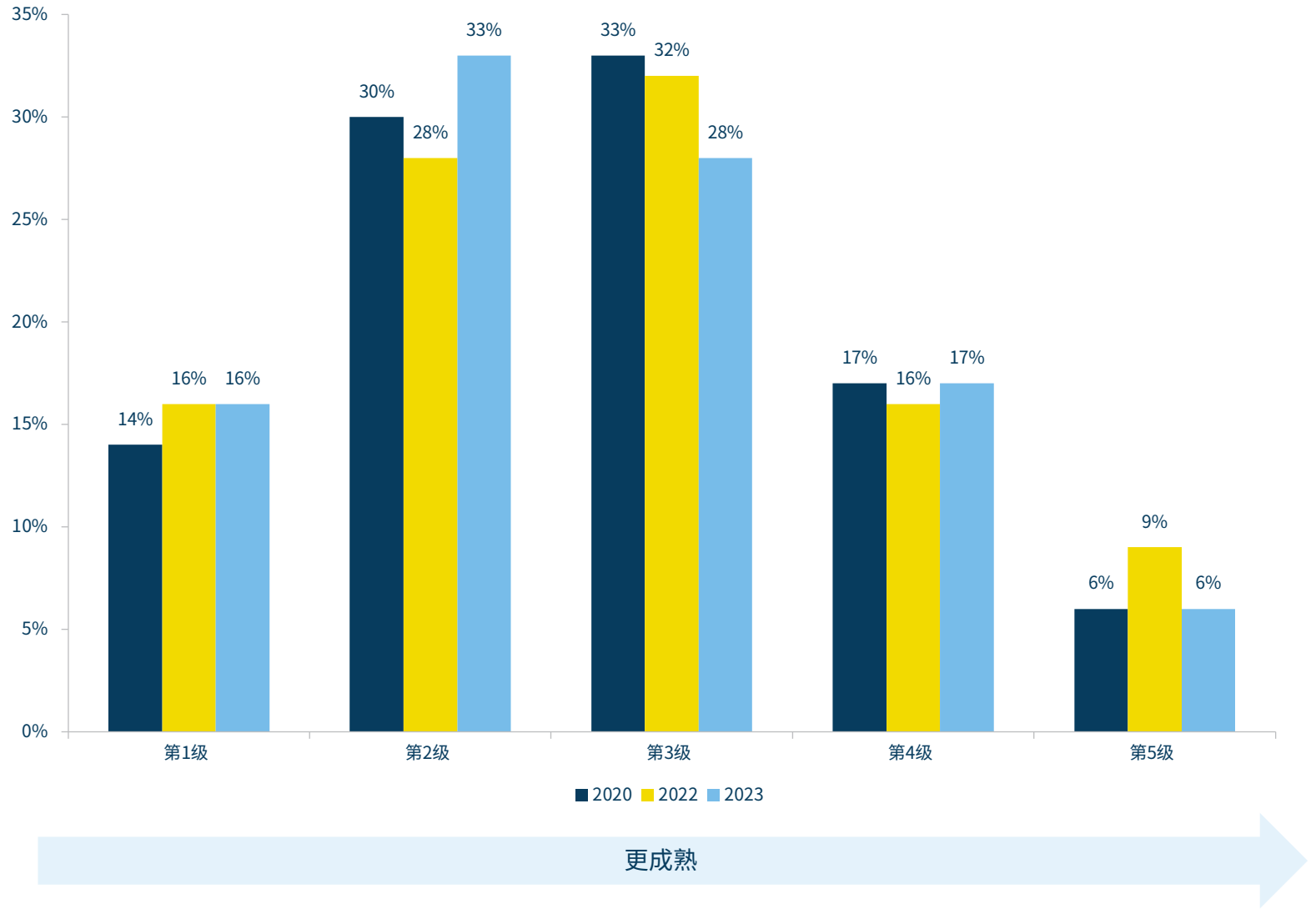
2. 高成熟度组包括所有自评为第4级或第5级的受访者；低成熟度组指被识别为第1级或第2级的受访者。

(CS)²项目成熟度——纵向分析

每个排名的参与者数量都有所变化（值得注意的是，第2级组织的数量在今年有所增加），但我们发现，多年来高成熟度和低成熟度组织的规模变化不大。

参与者继续对他们自己的(CS)²项目进行评分。我们的团队认为这有利于自我评价有效性。我们在分析高成熟度（第4级和第5级）和低成熟度（第1级和第2级）组之间的对比和相似性时广泛使用了这一点，并以此作为划分建议的基础。

以下哪一项最能描述您的控制系统网络安全程序？

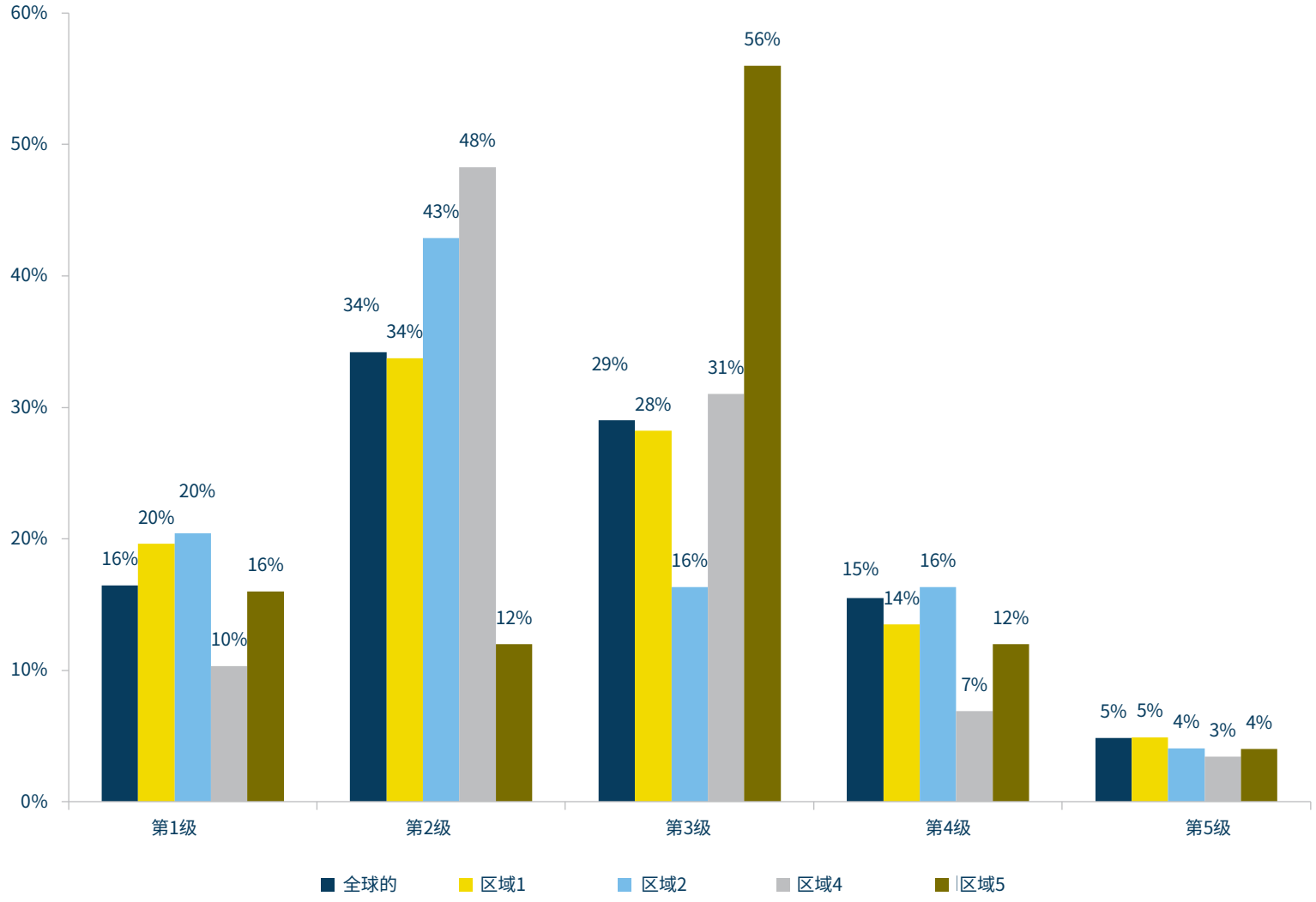


客户(CS)²项目成熟度 —— 地区³

世界各地的顾问（供应商、服务提供商、集成商）对其客户(CS)²项目的成熟度看法不一。不同地区对成熟度有不同的看法。区域2的自评得分较低，63%在第1级和第2级，区域4的有近一半（48%）处于第2级，而区域5有超过一半的组织（56%）处于第3级。区域3、6和7缺乏足够的参与，无法纳入本分析（见脚注3）。

3. (CS)²AI将组织划分成七个区域。
1) 北美；
2) 欧洲（中部、西部、北部和南部）；
3) 欧亚大陆；
4) 印度太平洋；
5) 中东-北非；
6) 南部非洲；
7) 拉丁美洲-加勒比

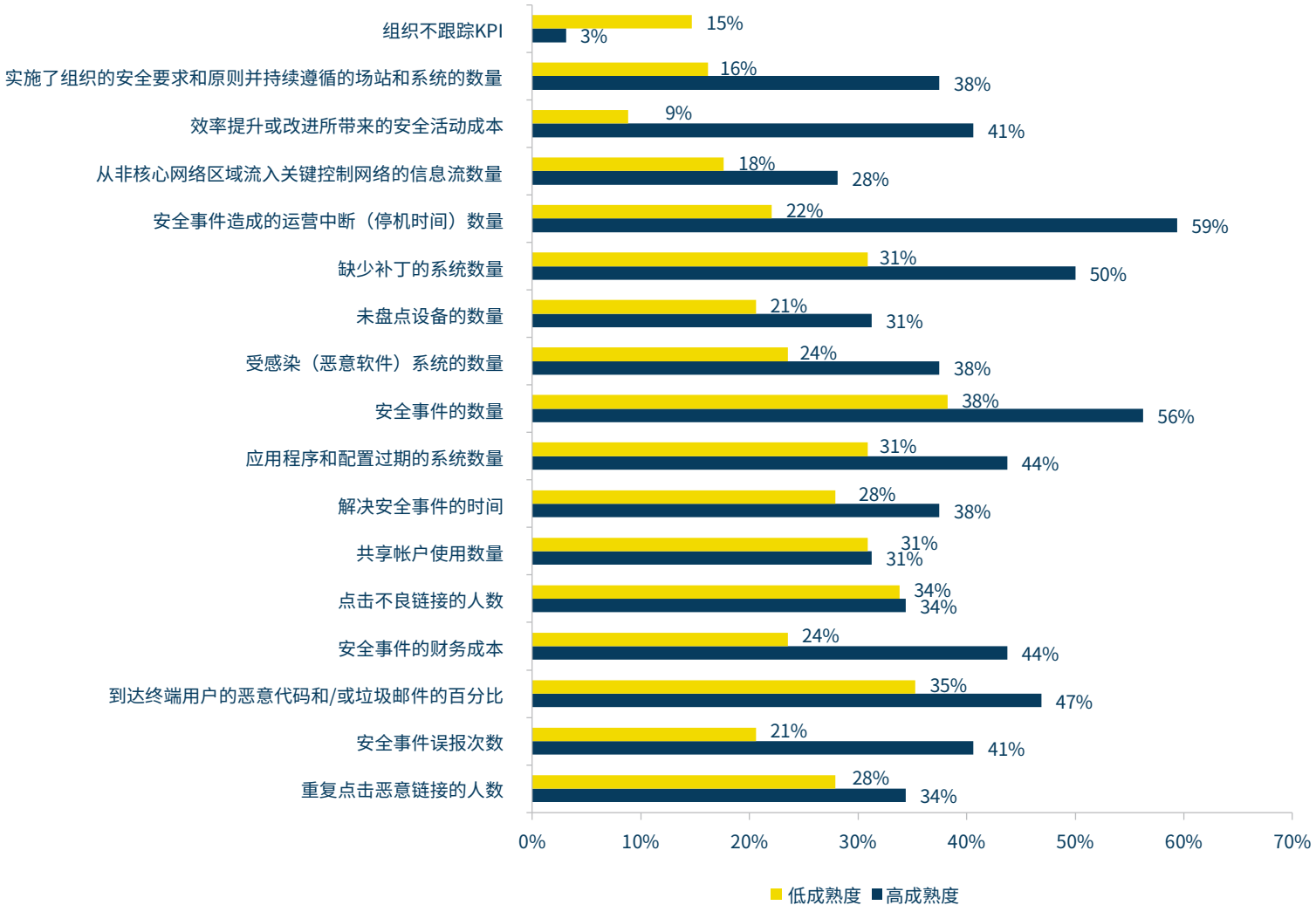
以下哪一项最能描述您的控制系统网络安全程序?



(CS)²关键绩效指标（KPI）——高成熟度vs低成熟度

尽管更多成熟项目对某些关键绩效指标(KPI)的跟踪力度更大并不令人惊讶（例如，作为任何项目随时间推移不断改进的核心活动，效率提升或改进所带来的安全活动成本增加至近五倍的差距：低成熟度的 8%对高成熟度的40%，这是符合预期的），我们认为如此多的项目对于绩效的跟踪力度之低是令人担忧的。今年，我们的低成熟度受访者大约是高成熟度受访者的两倍，尽管85.3%的受访者跟踪了一些KPI，但大多数人只跟踪了少数KPI。我们强烈建议这些组织扩大其衡量标准，以更好地了解其安全计划工作的有效性。

组织监控的典型(CS)²KPI

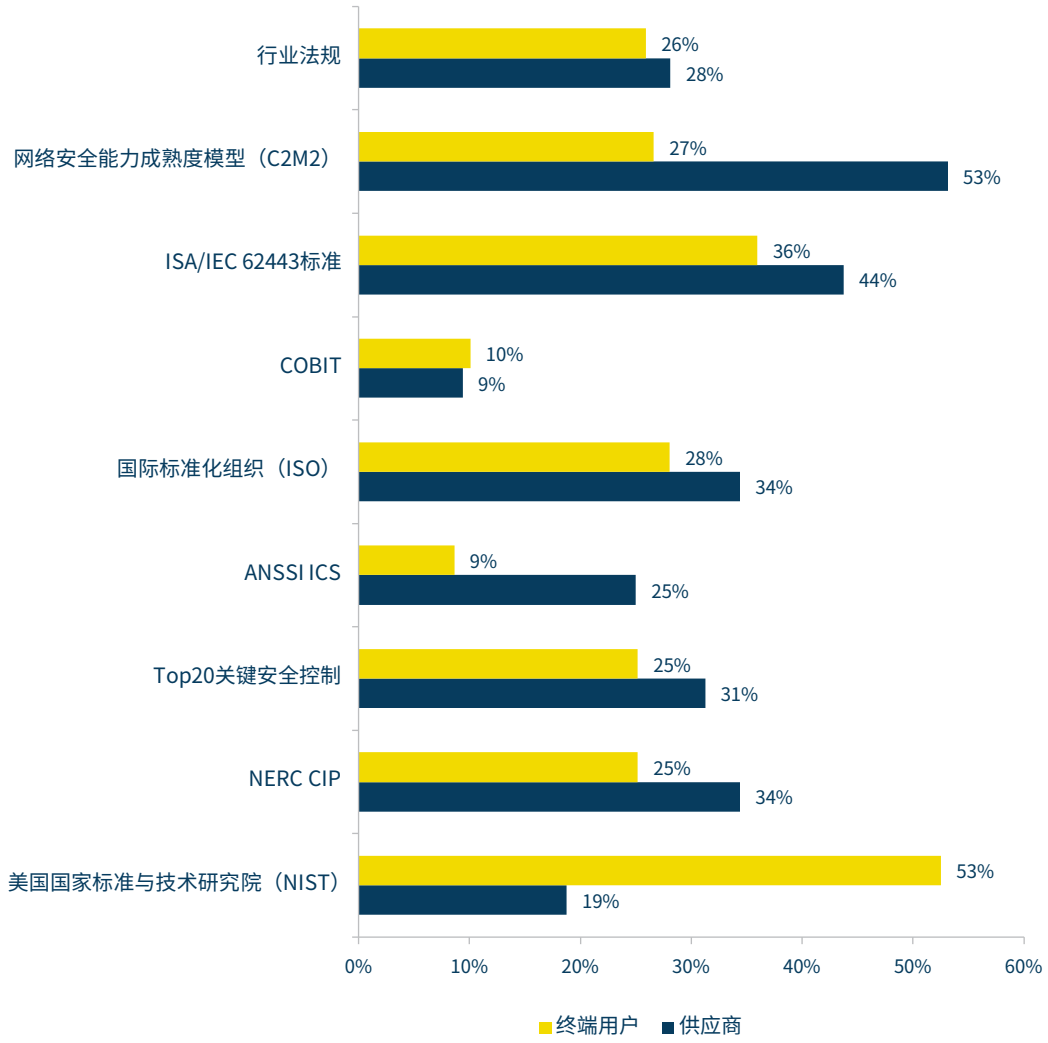


使用的安全成熟度框架——终端用户 vs 供应商

比较不同群体的观点有其不利之处，但我们认为，将这两个群体的观点并列看待是有用的，因为他们都对控制系统的安全负有责任。我们在这里看到，虽然C2M2和NIST是最突出的，但前者适用于供应商，后者适用于终端用户。报告的使用情况终端用户的C2M2与去年的总体数据（2022年-C2M2 26.3%）有效匹配，但该报告没有区分终端用户和供应商。

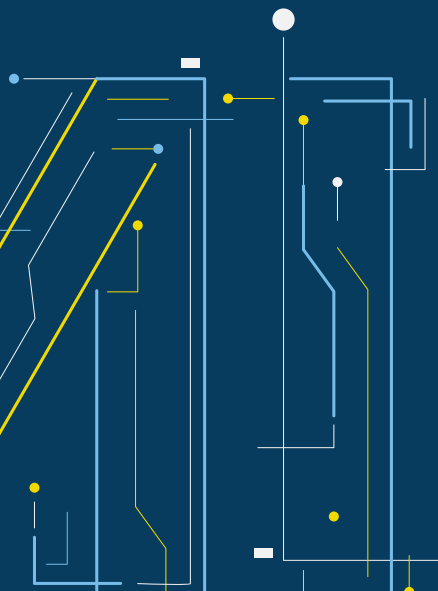
在我们的最新一轮调查中，供应商分别做出回应，并报告使用C2M2的频率几乎是原来的两倍（终端用户C2M2 26.6%vs供应商C2M2 53.1%）。NIST的使用率似乎变化不大，去年所有参与者的反馈结果为45.7%（2022年），本次调研两个群体的平均值也基本落在这个范围内。

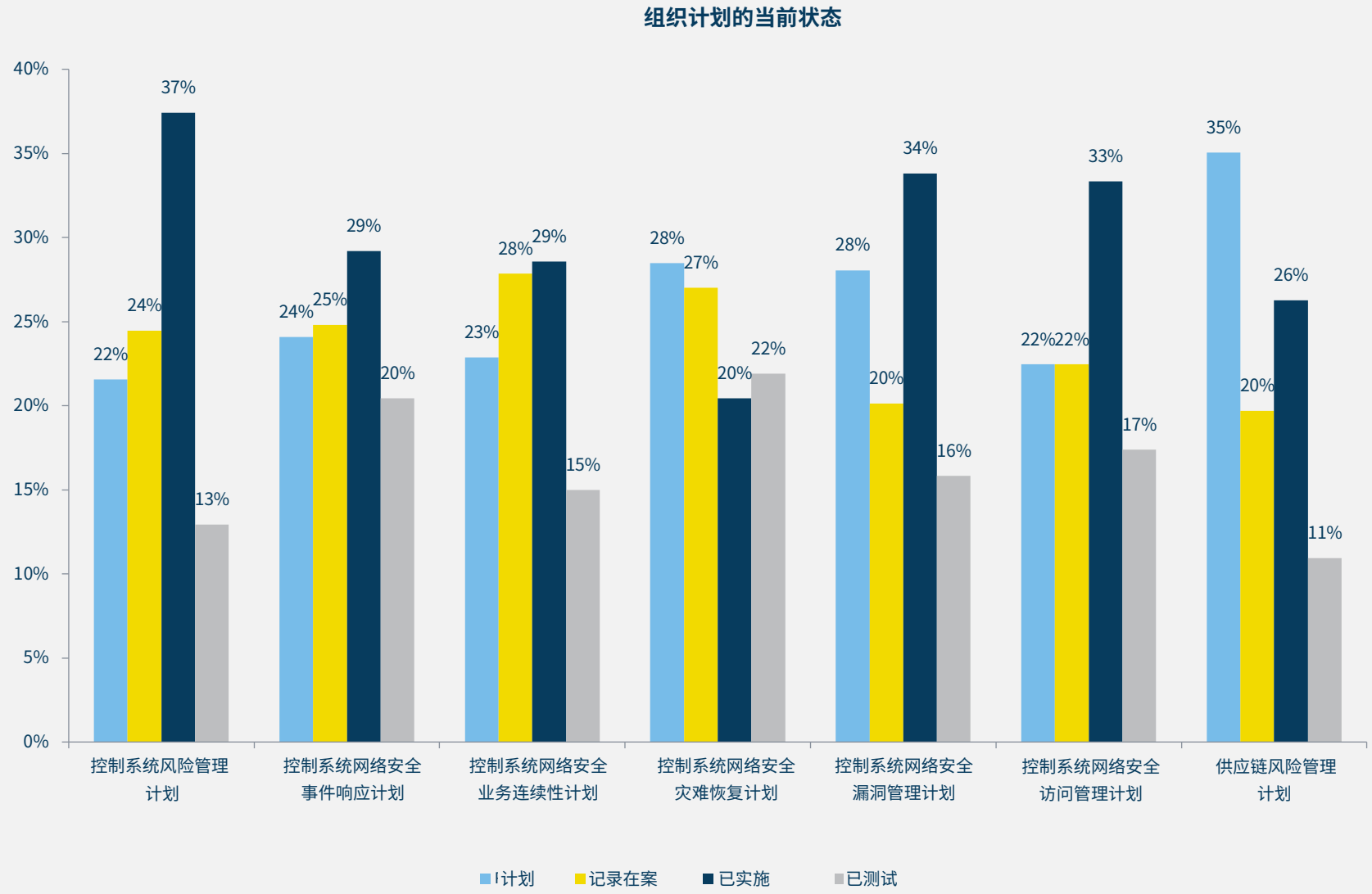
控制系统安全团队使用的框架



组织计划
—— 终端用户

我们团队认为，每个有控制系统安全(CS)[2]责任的组织都应全面管理其风险，制定文档化的实施和测试计划及程序，以减少事故发生，并最大限度降低对公司、员工和客户的影响。随着全面实施计划和测试成为黄金标准，大量受访公司仅拥有文档化的计划和记录，但在程序上并未做好这些计划所针对的事件发生后的应对准备。





(CS)²服务
—— 终端用户

组织应该到哪里去寻求保护其控制系统安全(CS)²资产、人员和运营所需的帮助?

根据我们的受访者反馈，他们会从各个渠道获取帮助。内部IT安全资源（56.2%）作为多数反馈表明，大多数组织的OT网络安全由IT部门推动， 并且可能IT安全方法和技术正在这些环境中应用。

许多首席信息安全官（CISO）对运营技术（OT）安全项目感到畏惧，因为对工厂网络安全的‘治愈’比‘疾病’本身还要糟糕。我曾经是CISO，所以我理解这种情况。OT需要生产优先，而IT则优先考虑安全性而不是停机时间。

我们在与恶意行为者的斗争中节节败退，很大程度上是因为无所作为。使用传统的IT工具来保护运营技术（OT）十分昂贵，不仅因为咨询、规划和设备的成本，更重要的是因为大量的停机时间。

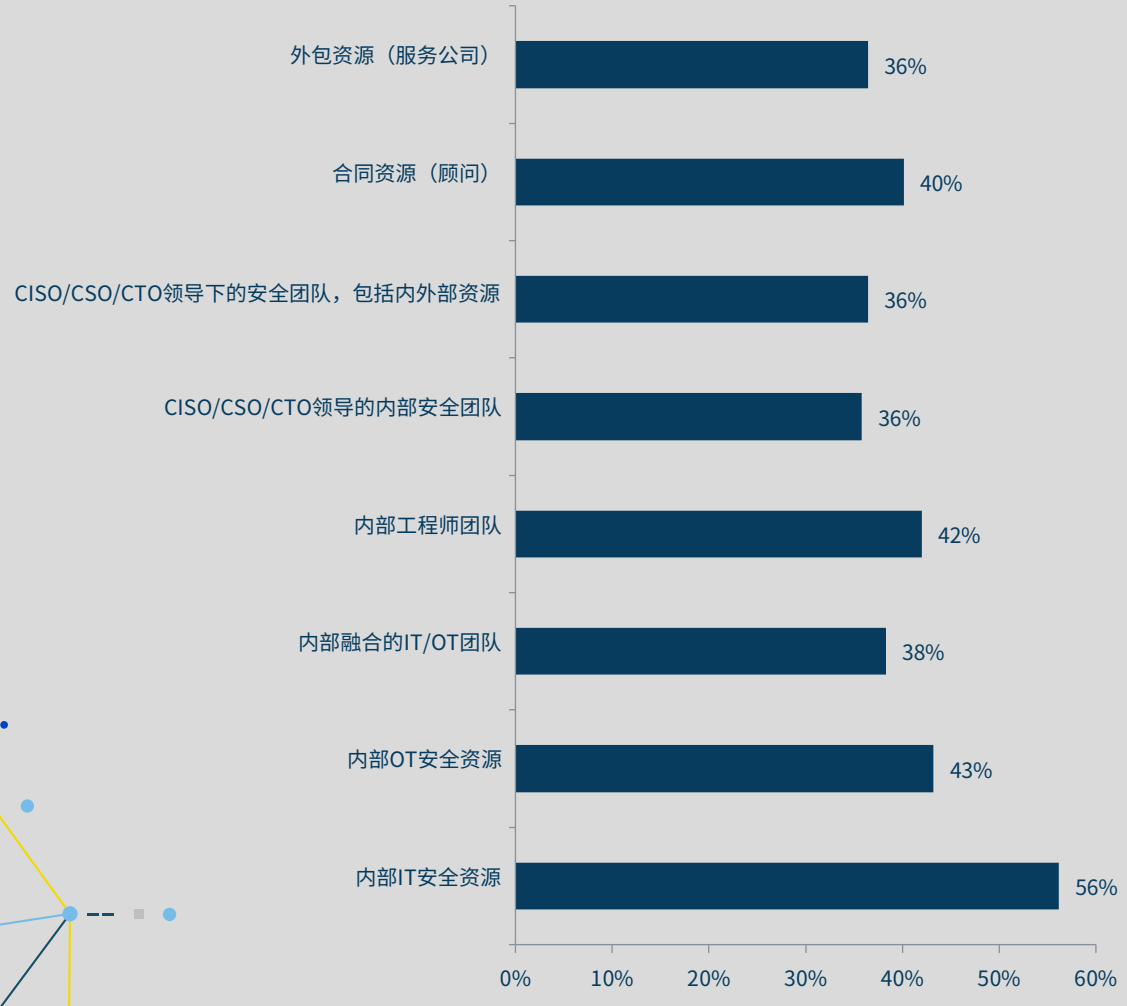
运营者必须做出痛苦的决定，重新配置他们的网络，替换仍在使用但已过寿命的资产，并部署安全团队——所有这些都需要关闭他们的工厂数天甚至数周。我们正在迫使他们做出不推进其运营产线和设施网络安全的艰难决定。在许多情况下，停机损失比整个安全项目本身成本还要昂贵。

让我们合作，使得保护和维护我们的工厂和设施的时间成本更低，更加经济，最重要的是，减少甚至消除停机时间。

通过合作，我们可以消除传统IT的障碍，共同保障全球的基础设施安全。

Brian Brammeier
Opscura首席执行官

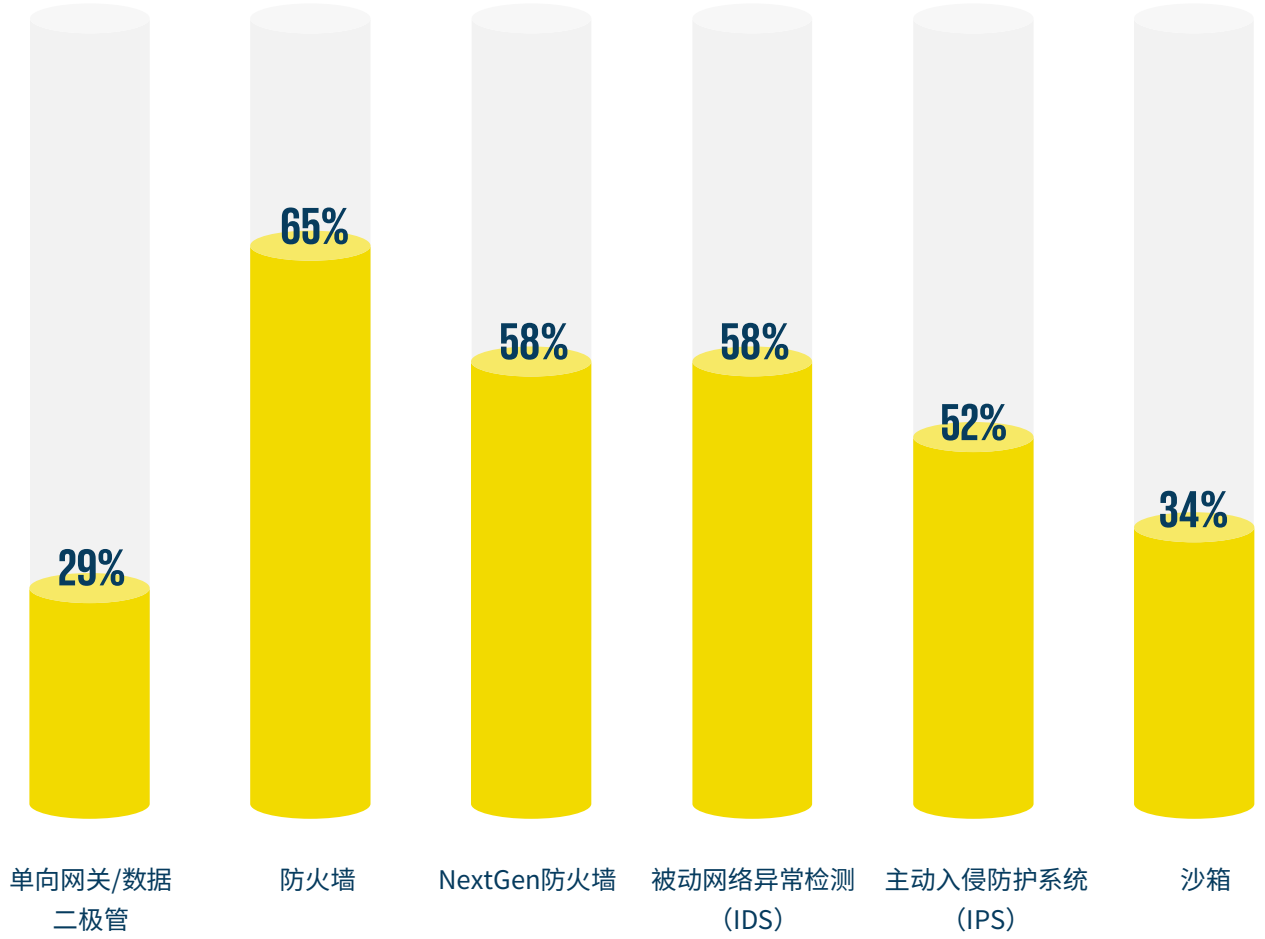
各组织使用的控制系统安全服务的来源



(CS)²技术
—— 终端用户

并不是所有技术都适合所有环境的需求和要求。尽管如此，我们认为那些拥有和/或运营工业控制系统(ICS)/运营技术(OT)资产的组织表示他们拥有被动网络异常检测（58%入侵检测系统（IDS））的情况下，通过实施主动入侵防御系统（IPS）将会大有裨益。NextGen防火墙同样具有广泛的适用性，应该保护更多ICS环境免受来自企业或其他外部网络的威胁。单向网关/数据二极管由于主要在最高安全环境（如核电站）中使用而被认为复杂且昂贵，但我们最近看到这些因素有所减弱，预计未来会有更多部署。

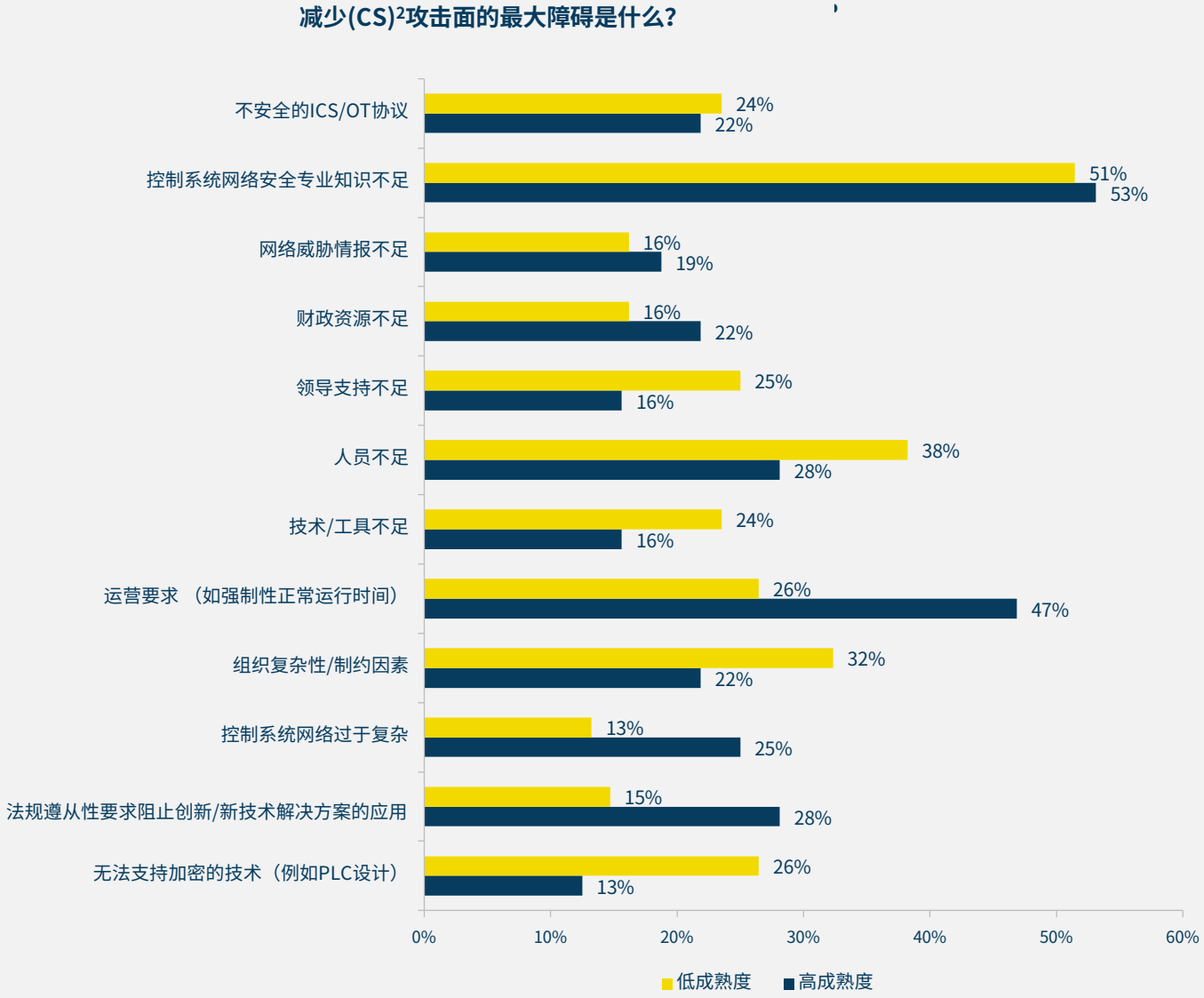
组织用于保护控制系统资产免受网络威胁的安全技术



减少(CS)²攻击面的障碍

(CS)²障碍
—— 高成熟度vs低成熟度

我们每年都会比较不同群体之间的情况和观点，在这里，我们通过受访组织的控制系统网络安全项目的相对成熟度（高成熟度 vs 低成熟度）来分析他们认为的最大障碍，以确定哪些方法有效，哪些无效，以及随着组织在提高安全性方面的进展，情况会如何变化。如右图，我们看到一些障碍被广泛认同，例如：控制系统网络安全专业知识不足（低成熟度51.5%，高成熟度 53.1%）和不安全的ICS/运营技术（OT）协议（低成熟度23.5% vs 高成熟度21.9%），而其他障碍则存在较大差异，例如：无法支持加密的技术（低成熟度26.5% vs 高成熟度12.5%）和领导支持不足（低成熟度25.0% vs 高成熟度15.6%）。这些表明，更成熟的项目已经克服了一些较不成熟的项目仍在努力应对的障碍。

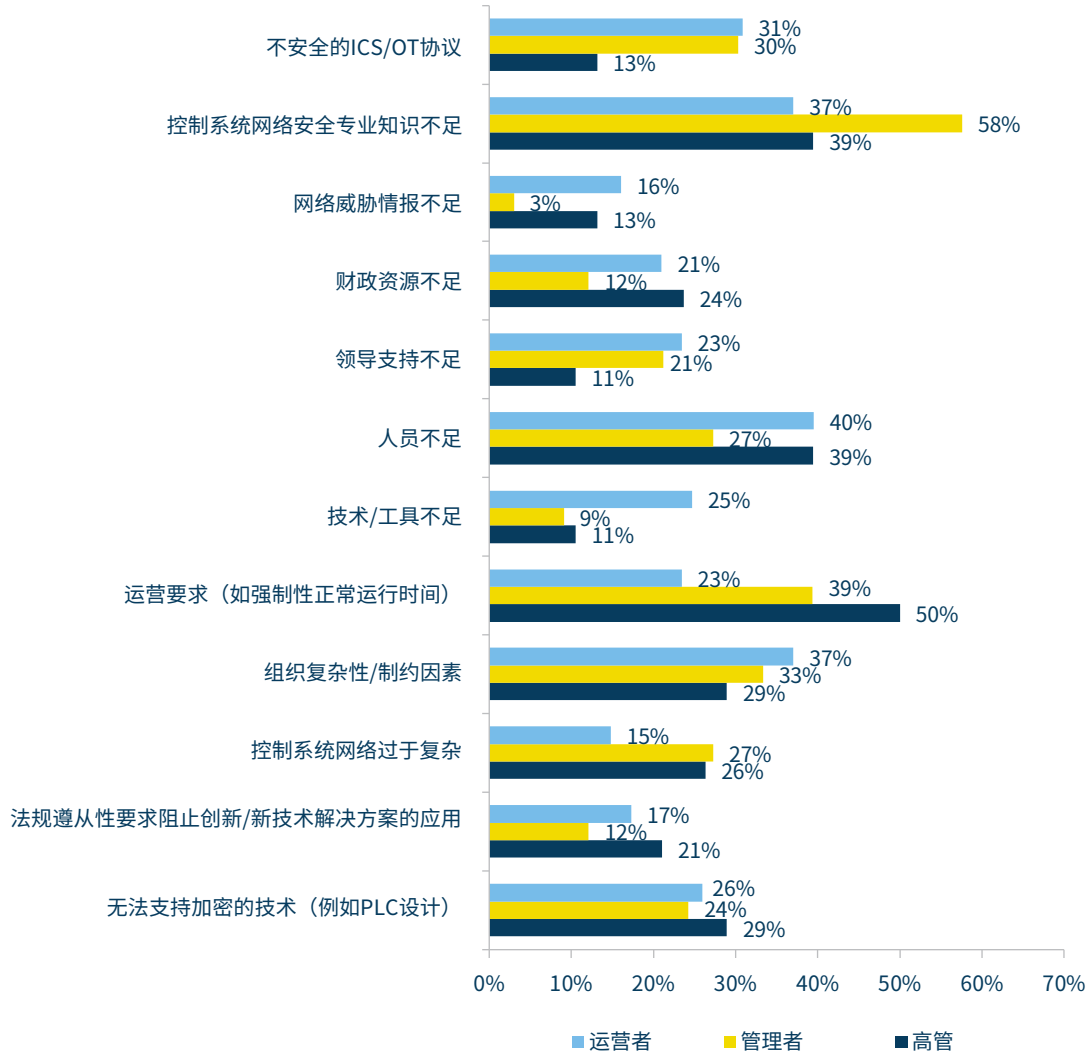


(CS)²障碍——组织层面[4]

任何一个人都不太可能全面了解和掌握现代控制系统环境的所有细节，个人观点的差异不可避免地会导致对需要完成的工作的看法不同。在这里，我们看到高管一致认为运营要求（50.0%）、人员不足（39.5%）和控制系统安全专业知识不足（39.5%）是最大的障碍，这与运营者部分一致（该群体认为最大的障碍是人员不足39.5%和控制系统安全专业知识不足37.0%），但运营者（Ops）认为运营要求不是主要障碍（在操作人员列表中排第六，23.5%）。管理层经常与一方或双方意见不一致，这突显了当我们支持他们解决问题时，了解终端用户在其组织中的角色的重要性。

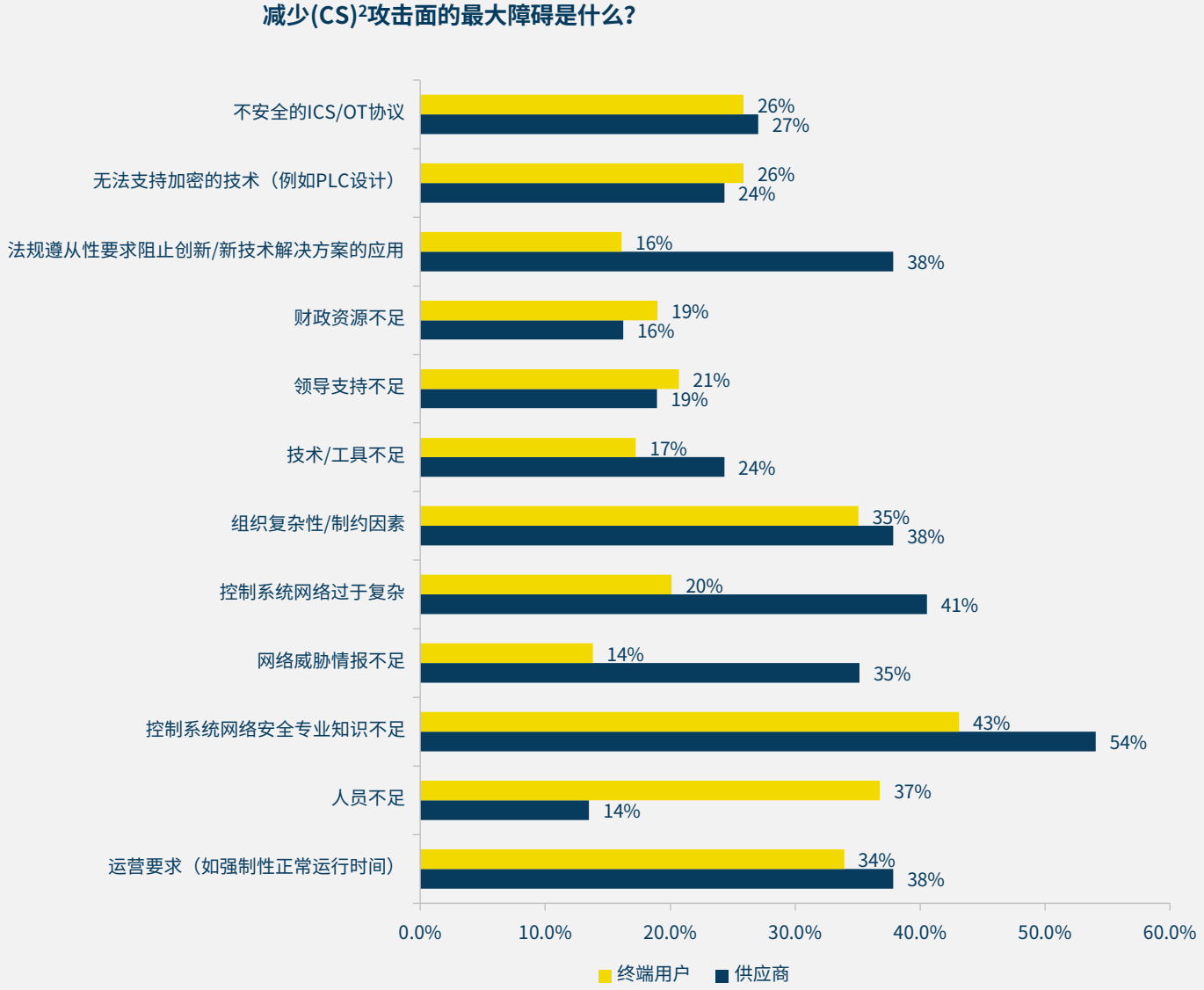
4. 在我们的调查中，回答每个问题的参与者人数各不相同。有时，这会导致参与者的特定子集不足以进行有效的统计分析。在根据其组织不同级别的参与对我们的数据进行细分的情况下，我们收到的领导层受访者太少，无法将他们包括在一些图表中。

减少(CS)²攻击面的最大障碍是什么？



(CS)²障碍
——终端用户vs供应商

我们的团队发现，终端用户和供应商受访者在观点上的许多差异都很有趣。这些是否源于其控制系统的所有权/操作与OT（运营技术）资产的生产/监控、可供其使用的不同资源、不同的财政责任或某些因素的组合？值得注意的是，供应商将法规遵从性要求、过于复杂的控制系统网络和网络威胁情报不足确定为最大障碍，其比例是终端用户的两到三倍。终端用户反馈中唯一与之比例相似的是他们对人员不足的看法（终端用户36.8%，供应商13.5%）。我们建议供应商注意终端用户客户确定的最大障碍，以便最好地帮助他们克服这些障碍。



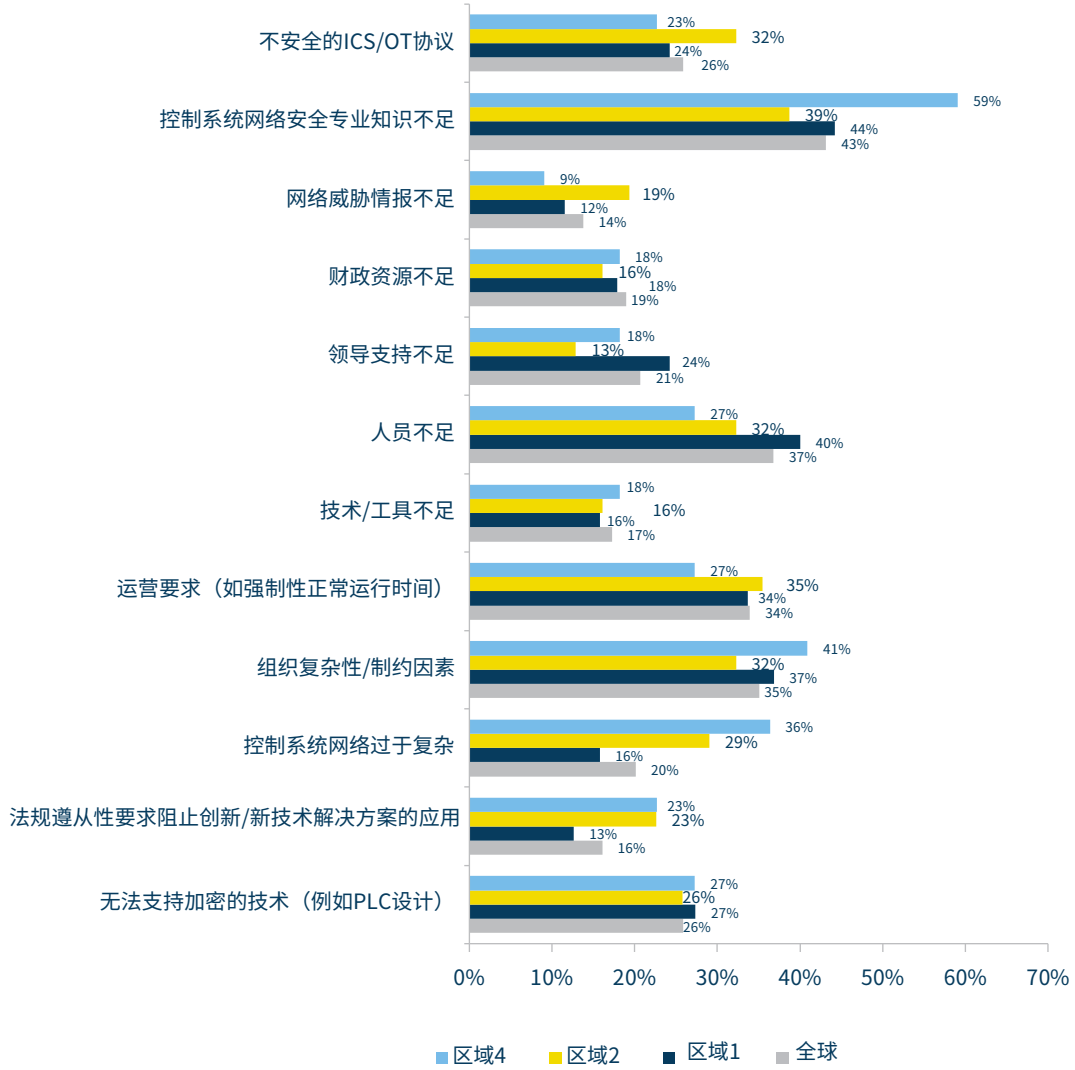
(CS)²障碍
—— 区域分析[5] [6]

最后，对于安全障碍的分析，我们对来自全球不同区域的受访者之间的差异进行了研究。由于全球控制系统主要建立在通用技术之上，我们预计无论地理位置如何，对这个问题的回答会有一定程度的一致性。事实上，这张图表显示的差异比本报告中的许多其他图表要少。一个显著的区别是，区域4（亚太区域）将控制系统网络安全专业知识不足（59.1%）作为主要问题，其比例比区域2、区域1或全球高出15个百分点。区域2（欧洲、中部、西部和北部）和区域4（亚太区域）的受访者也比世界其他区域更关心过于复杂的控制系统网络（区域2 29.0%，区域4 36.4%，全球20.1%）。

5. 正如我们对参与者组织层面的反应进行的分析一样，一些地区缺乏足够的代表样例来进行有效的分析。下表仅显示了有足够参与的区域，以及全球（所有答复者）以供比较。

6. (CS)²AI将组织划分成七个区域 。1） 北美；2） 欧洲（中部、西部、北部和南部）；3） 欧亚大陆；4） 印度太平洋；5） 中东-北非；6） 南部非洲；7） 拉丁美洲-加勒比

减少(CS)²攻击面的最大障碍是什么?




SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

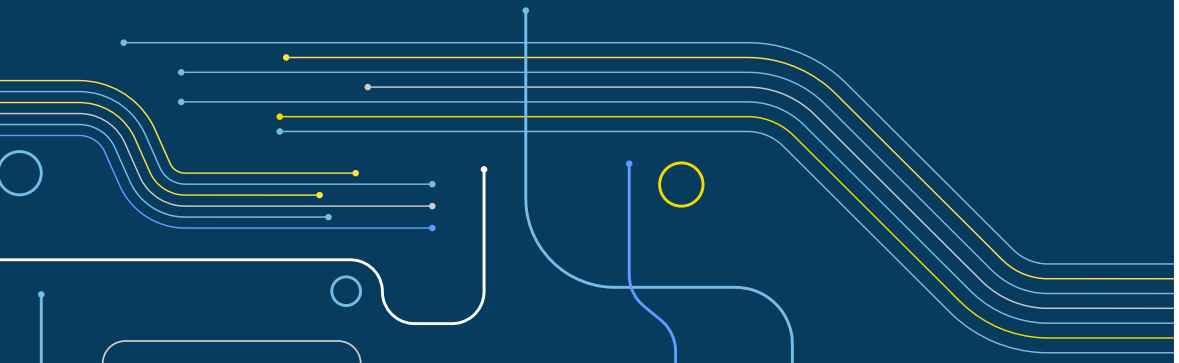
(CS)²支出和预算

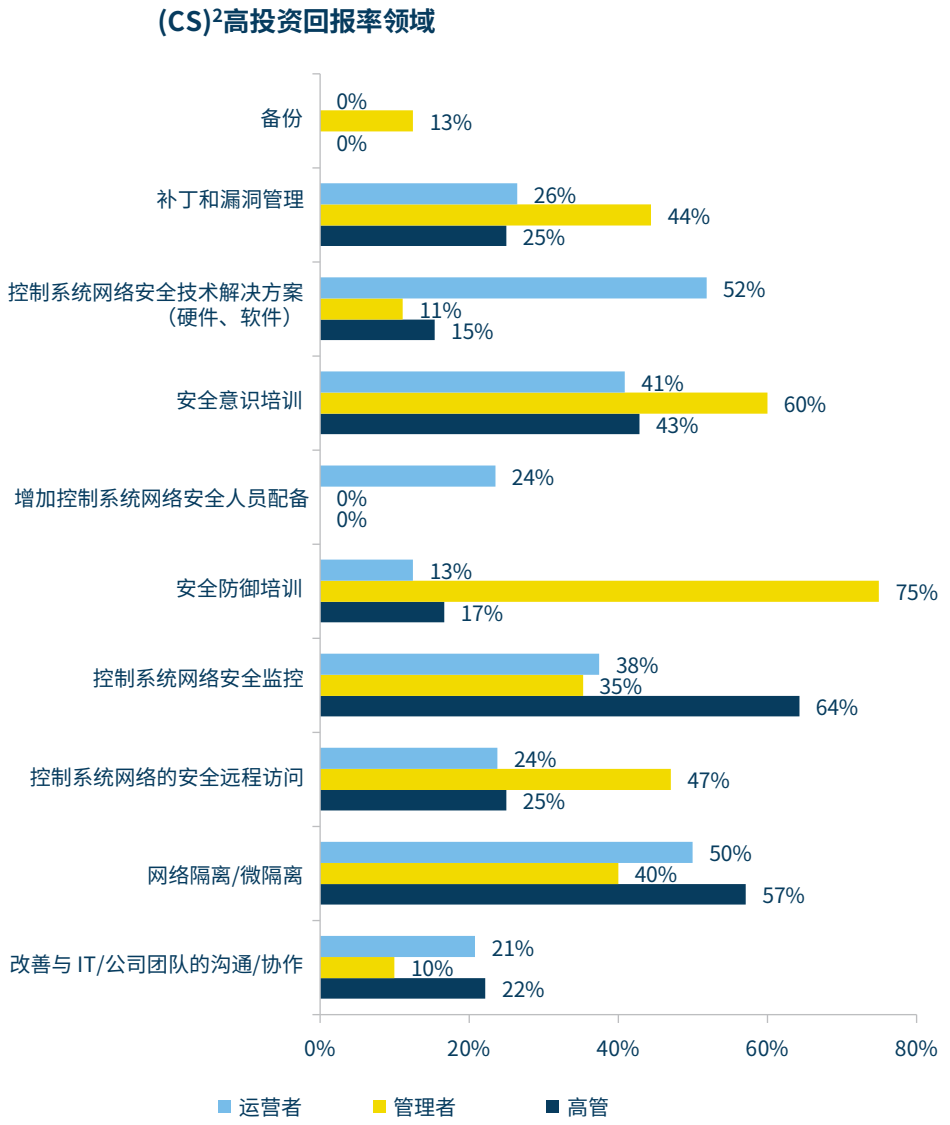
(CS)²高投资回报率领域——组织级别[7]

(CS)² AI “团队和我们的许多演讲者都熟悉如何获得高管对安全需求支持的问题，尤其是需要进行影响分析的细分项目；在某些情况下，甚至还需要进行大量的网络架构重建工作，当然我们很高兴地看到，大多数参与的高管（57.1%）认识到在他们的组织中实施网络架构重建的高投资回报率，这对安全性和弹性都是至关重要的。我们甚至看到他们对(CS)²监控(64.3%)的支持更加积极，多年来，专家们一直认为可见性是任何安全改进计划的第一步。另一方面，受访管理者发现培训的投资回报率最高，无论是安全意识方面(60.0%)还是安全防御方面(75%)。

我们的团队认为有必要提请注意以下事实：尽管有 27% 至 39% 的参与者认为 “人员不足”（参见图表(CS)² 障碍-组织层面）是他们改善其(CS)² 状况的最大障碍，但没有一位高管或管理参与者将增加控制系统网络安全人员配备视为高投资回报率（两组均为 0%）。

7. 领导层受访者反馈太少，未纳入本分析。





(CS)²高投资回报率领域
—— 高成熟度vs低成熟度

与他们对需要克服的安全障碍的看法相比，就在(CS)²支出中识别最高投资回报率（ROI）的安全计划领域上，他们有更多的共识。有一些明显的异常值需要注意，特别是低成熟度的强调改善与IT/公司团队的沟通/协作（低成熟度16.7%，高成熟度0%）和而高成熟度的更强调备份[8]（低成熟度0%，高成熟度50%）。

这说明最成熟的项目已经整合了团队，并实施了可靠的备份系统和程序。

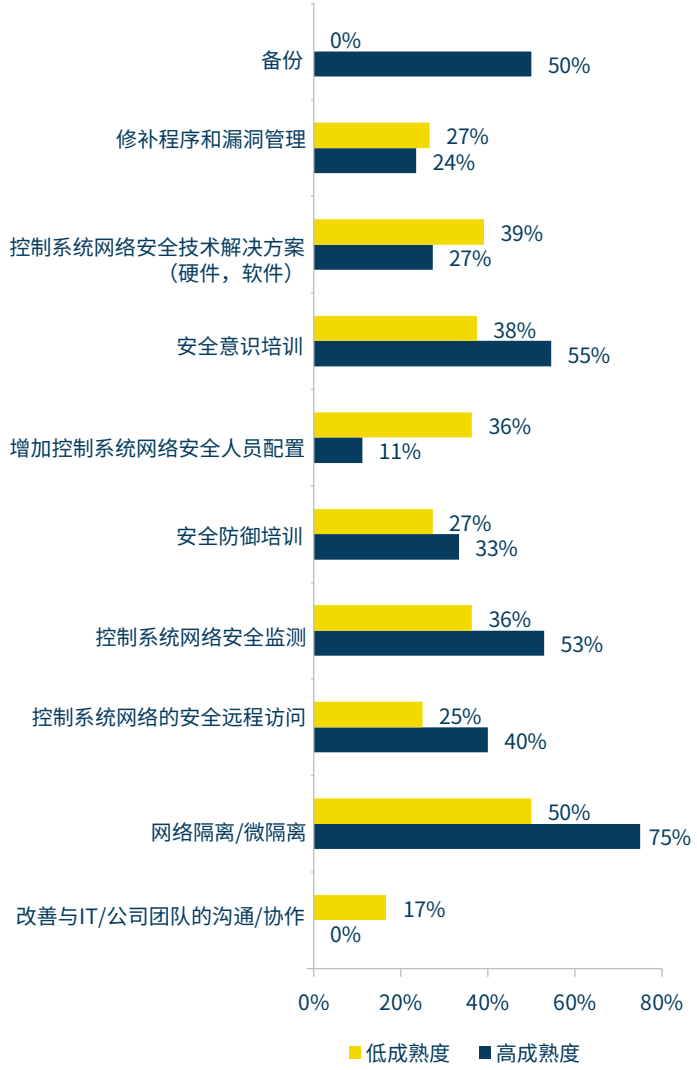
所有小组都一致认为，网络隔离/微隔离的投资回报率最高，这与多年来的研究和建议是一致的，即实施网络隔离/微隔离既能提高整体安全性，又能减少网络事件的影响。

8. 可能表明，在最近勒索软件攻击上升期间，更成熟的程序经历了这种情况。

50%的受访者认为网络隔离是网络安全计划投资回报率的首要领域。网络工程的最新想法是，在重要边界部署任何一种工程级网络隔离方法都是最有收益的。重要边界包括IT/OT接口、任何OT/互联网接口以及网络之间的任何其他连接，这些边界的漏洞导致的最差情况后果差异巨大。攻击树分析结果表明，在这样的边界上进行工程级隔离可以将关键网络的攻击面减少3个数量级。

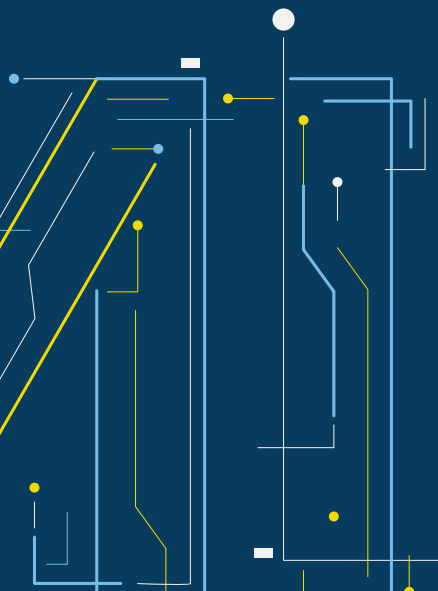
Andrew Ginter
Waterfall Security Solutions
工业安全副总裁

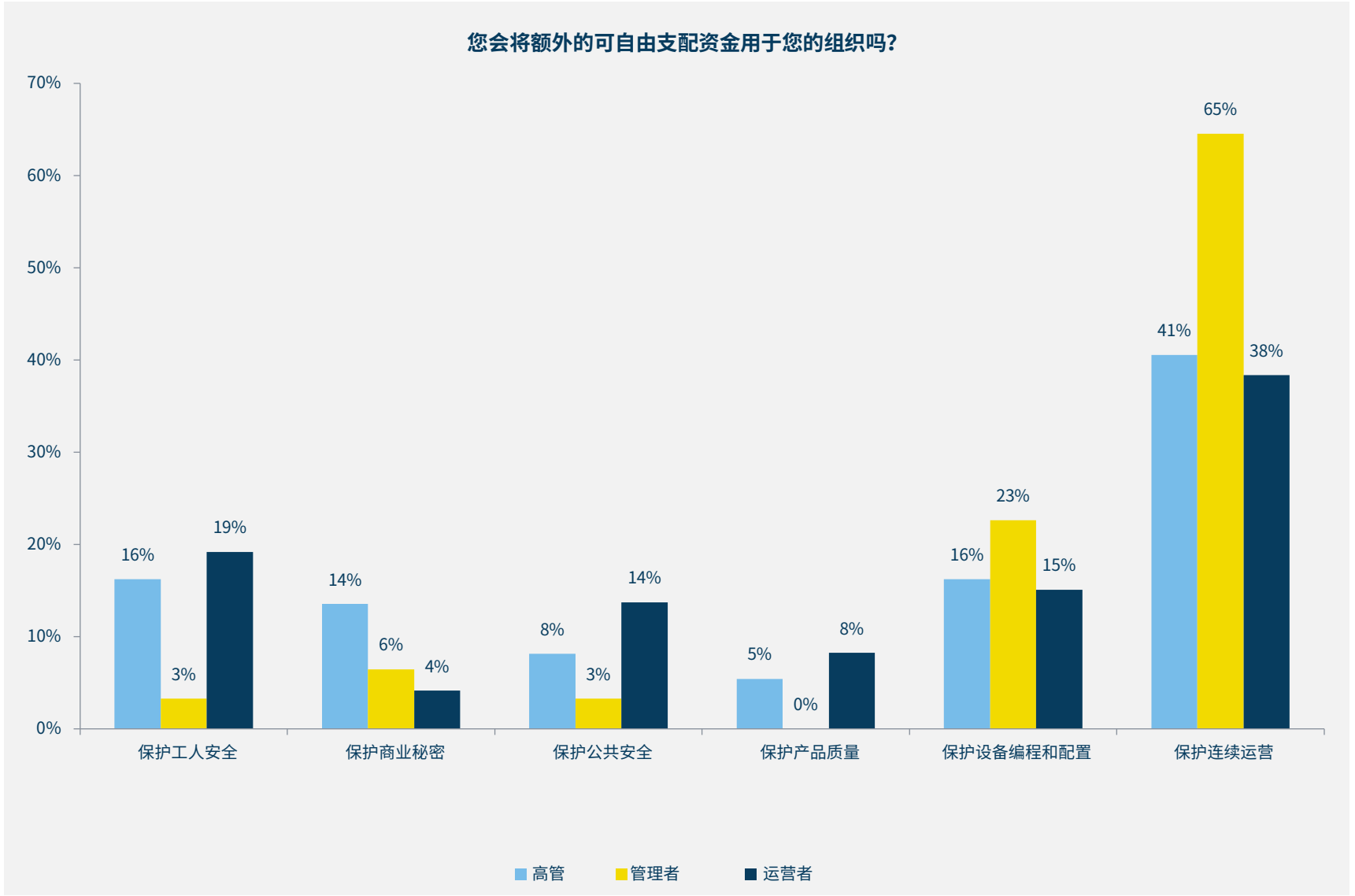
(CS)²高投资回报率领域（高成熟度与低成熟度）



支出优先级
——组织层面

今年的一个新情况是，我们的团队发现参与者的回答很有趣，除了一些普遍共识（例如各级将保护连续运营确定为他们支出额外资金的首要目标）之外，差异确实很突出。请注意，管理层的参与者对保护公共安全和保护工人安全的重视程度很低（两者均为3.2%），对保护产品质量的重视程度也很低。鉴于这些差异，鼓励组织就调整业务优先级进行讨论。

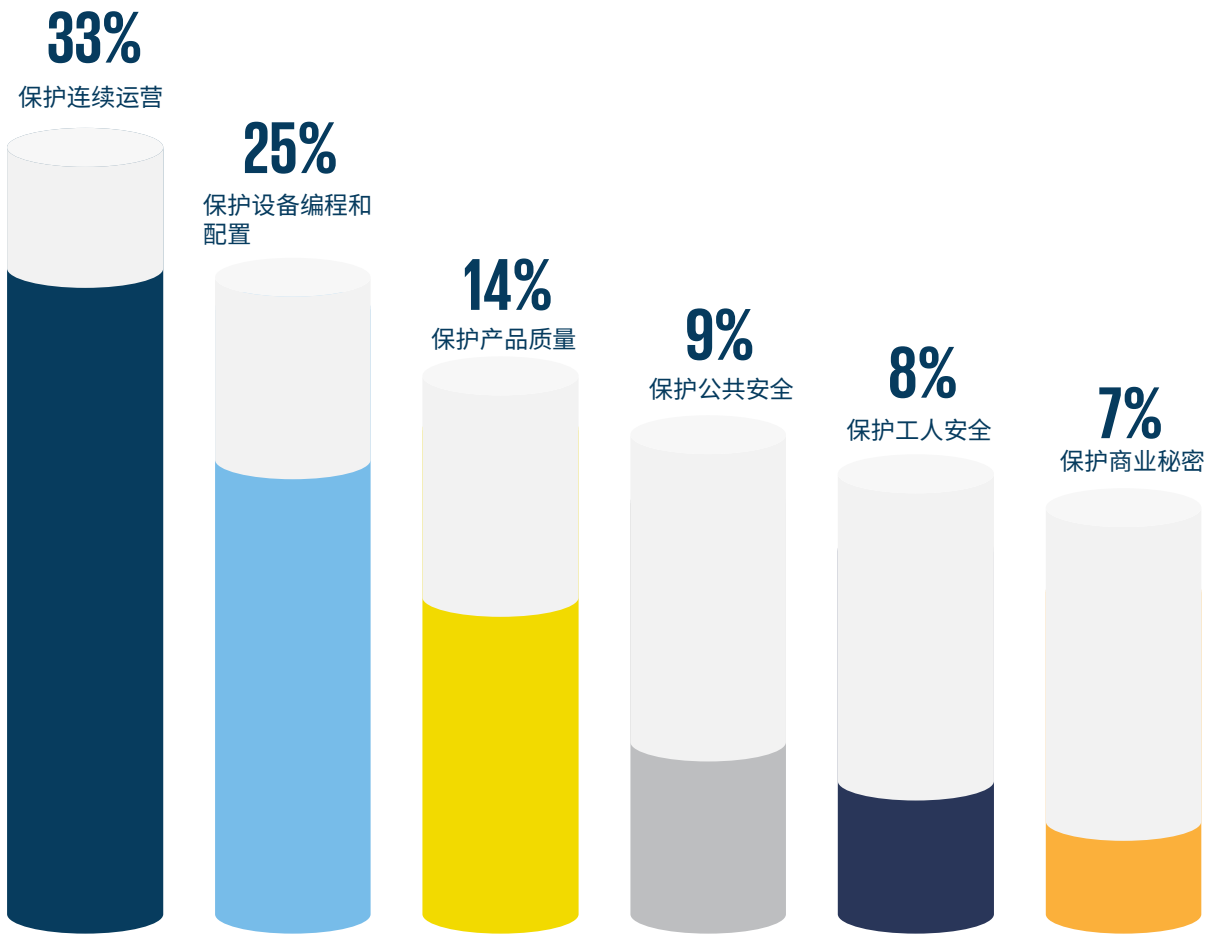




供应商对客户预算的指导——供应商

许多资产所有者或运营商依赖其信任的供应商提供的安全事务专家建议，因此我们今年研究了供应商关于资源分配的建议。将此图表与上一图表进行比较，我们发现最重要的仍然是保护连续运营。

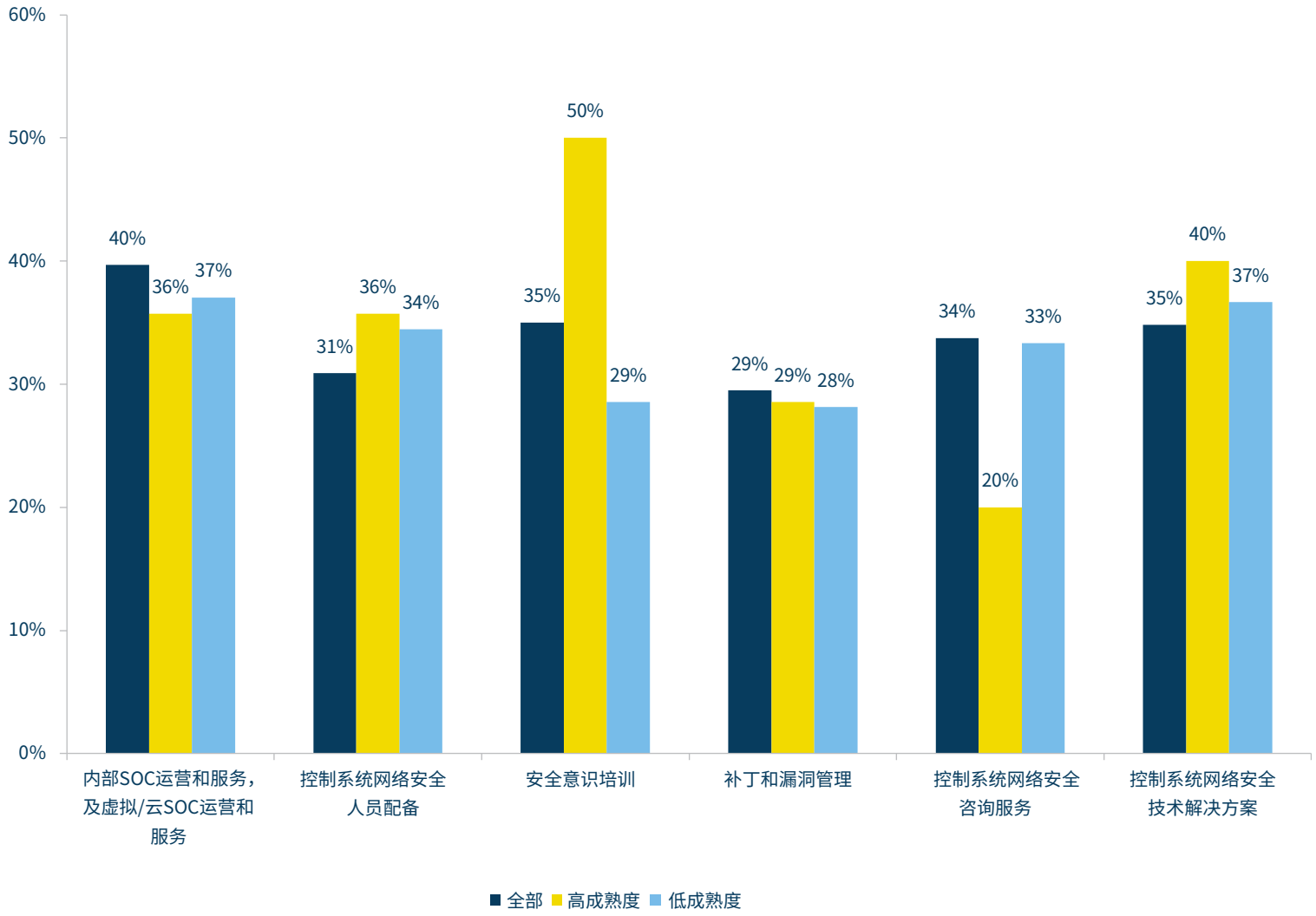
您会建议您的大多数客户在未来一年将更多的资源投入到哪里？



(CS)²高支出
——高成熟度vs低成熟度vs全部

为了便于比较，我们在这些表格中包含了所有参与者的回复。这使我们能够表明，高成熟度组在安全意识培训上的支出显著增加（高成熟度50.0%，低成熟度28.6%，全部35.0%），以及他们中很少有人专注于控制系统网络安全咨询服务（高成熟度20.0%，低成熟度33.3%，全部33.8%）。

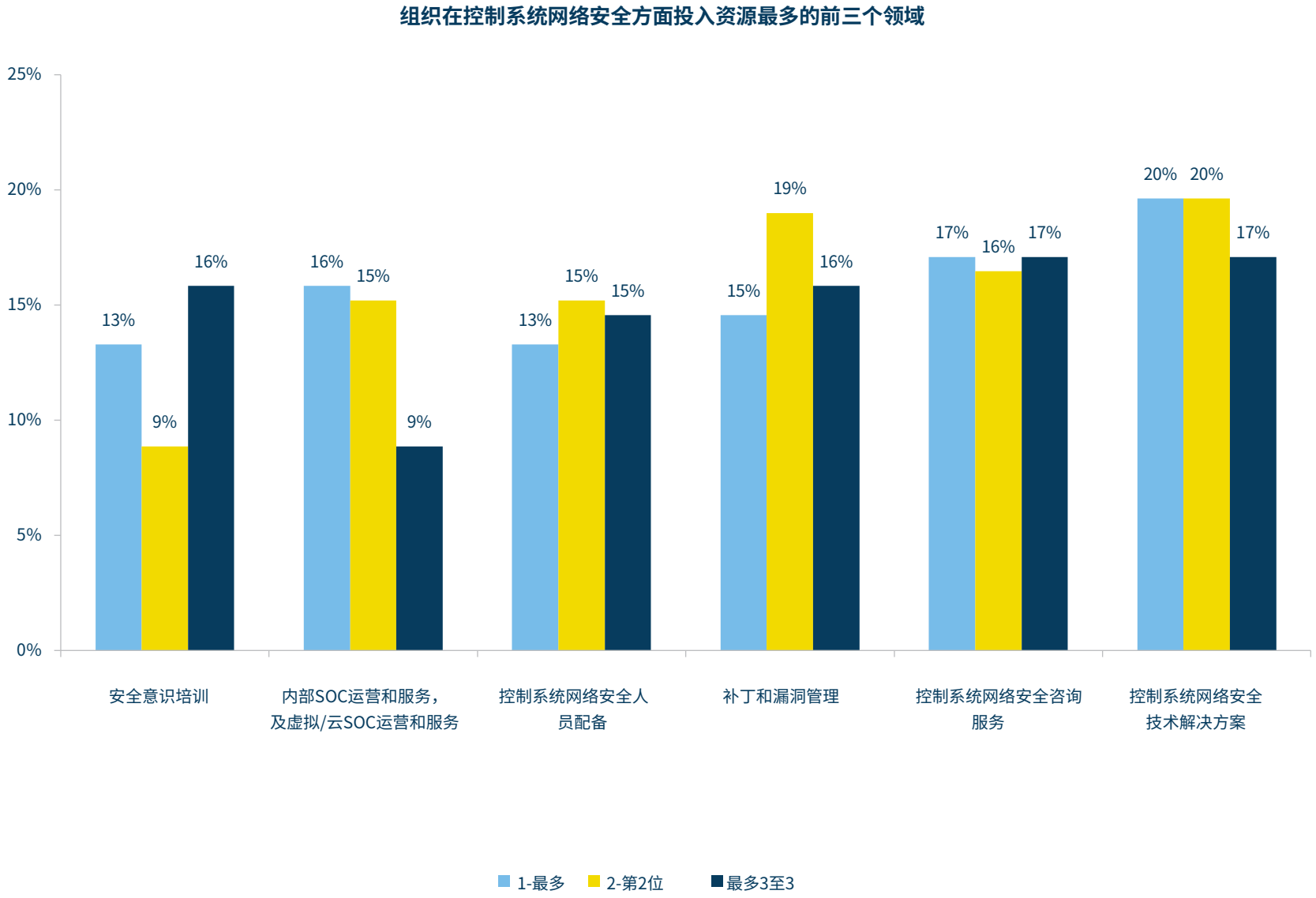
(CS)²高支出区域（高成熟度vs低成熟度vs全部）



(CS)²高支出——终端用户

除了高成熟度和低成熟度集团的最高支出之外，我们还要求终端用户识别其组织投入资源的前三领域，以进一步了解(CS)²预算优先事项。

安全技术和安全咨询服务在预算中占有最大份额（分别为56.3%和50.6%）。我们的团队认为值得调查的是，对控制系统网络安全人员相对较低的投资是否是导致该领域员工持续供不应求的一个因素。



(CS)²预算变化——纵向分析

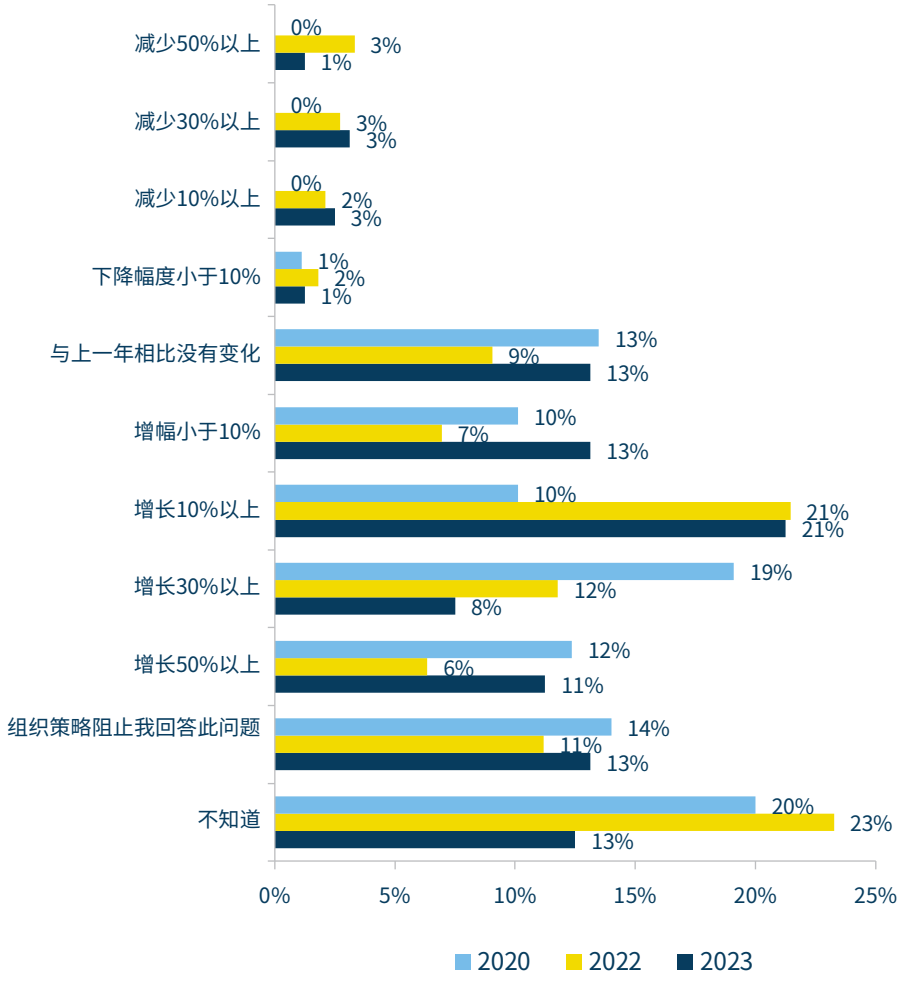
绝大多数组织继续增加其(CS)²的预算（53%），这一响应率在几年内徘徊在接近中点（2022年为47%，2020年为52%）。低增长群体呈现出稳步增长的模式，即(CS)²预算增长低于30%的群体，从2020年的20%上升到今年的34%。增长率较高的群体，即增长率超过30%的群体，相应地从2020年受访者的31%下降到现在的19%。我们的分析团队成员指出，(CS)²供应商/解决方案提供商行业出现了某些放缓，这可能是对竞争加剧或市场需求过大的反应。

持续致力于增加同比支出表明，各组织正在更好地了解其运营所处的威胁环境以及所面临的一定程度的风险。最近的控制系统网络安全事件头条提高了人们对当前网络风险和防止类似事件发生的必要行动的认识。

Brad Raiford

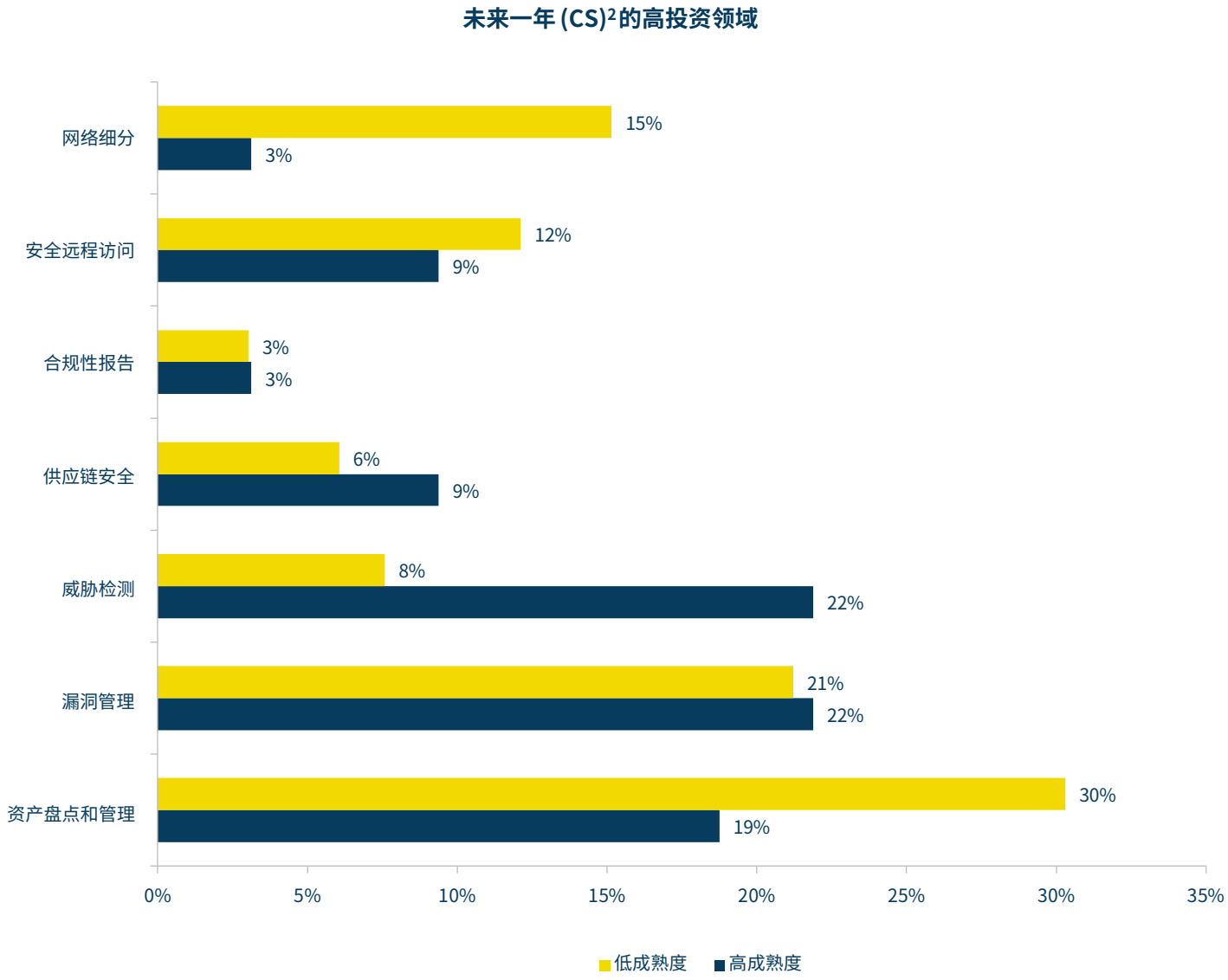
毕马威美国物联网和运营技术网络服务总监

组织的控制系统安全预算近几年同比估算



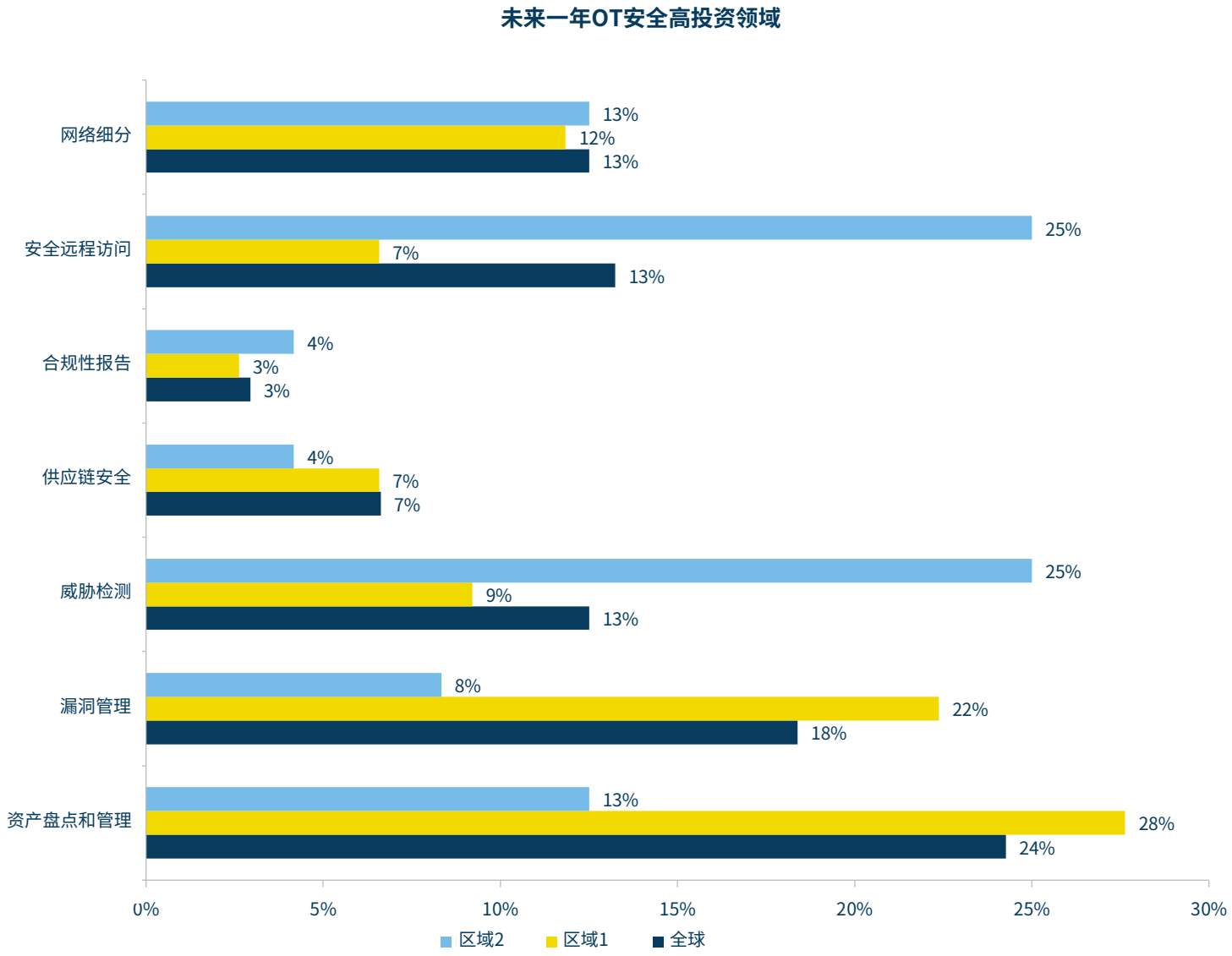
(CS)²投资计划
——高成熟度vs低成熟度

虽然对网络隔离的价值有强烈认同（请参见(CS)²高投资回报率领域图表），但我们认为值得注意的是，很少有组织计划将未来安全支出集中在该领域。可能的解释是，高成熟度的组织可能已经对其网络进行了显著划分，因此他们现在的支出（3%）远低于低成熟度组织（15%）。他们在资产盘点和管理与威胁检测方面支出计划差异的背后可能也有类似的因素。



(CS)²投资计划——地区

区域3-7[9]对此问题的回答不足以进行独立分析，但区域1和区域2的受访者的计划却有很大差异。区域2的参与者目前专注于安全远程访问和威胁检测[10]（两者各占25%），而他们的北美同行似乎认为漏洞管理与资产盘点和管理更为紧迫（分别为18.4%和24.3%）。在我们的分析中提出的一种可能性是，地区2的组织已经解决了这些管理问题，而地区1的组织尚未达到这一程度。



9. (CS)²AI将组织划分为七个区域。1）北美；2）欧洲（中部、西部、北部和南部）；3）欧亚大陆；4）印度太平洋；5）中东-北非；6）南部非洲；7） 拉丁美洲-加勒比

10. 其中一个可能的因素是，欧洲的监管机构（包括国家和国际监管机构）一直在推进/发布立法，要求在多个行业和基础设施部门进行威胁检测。

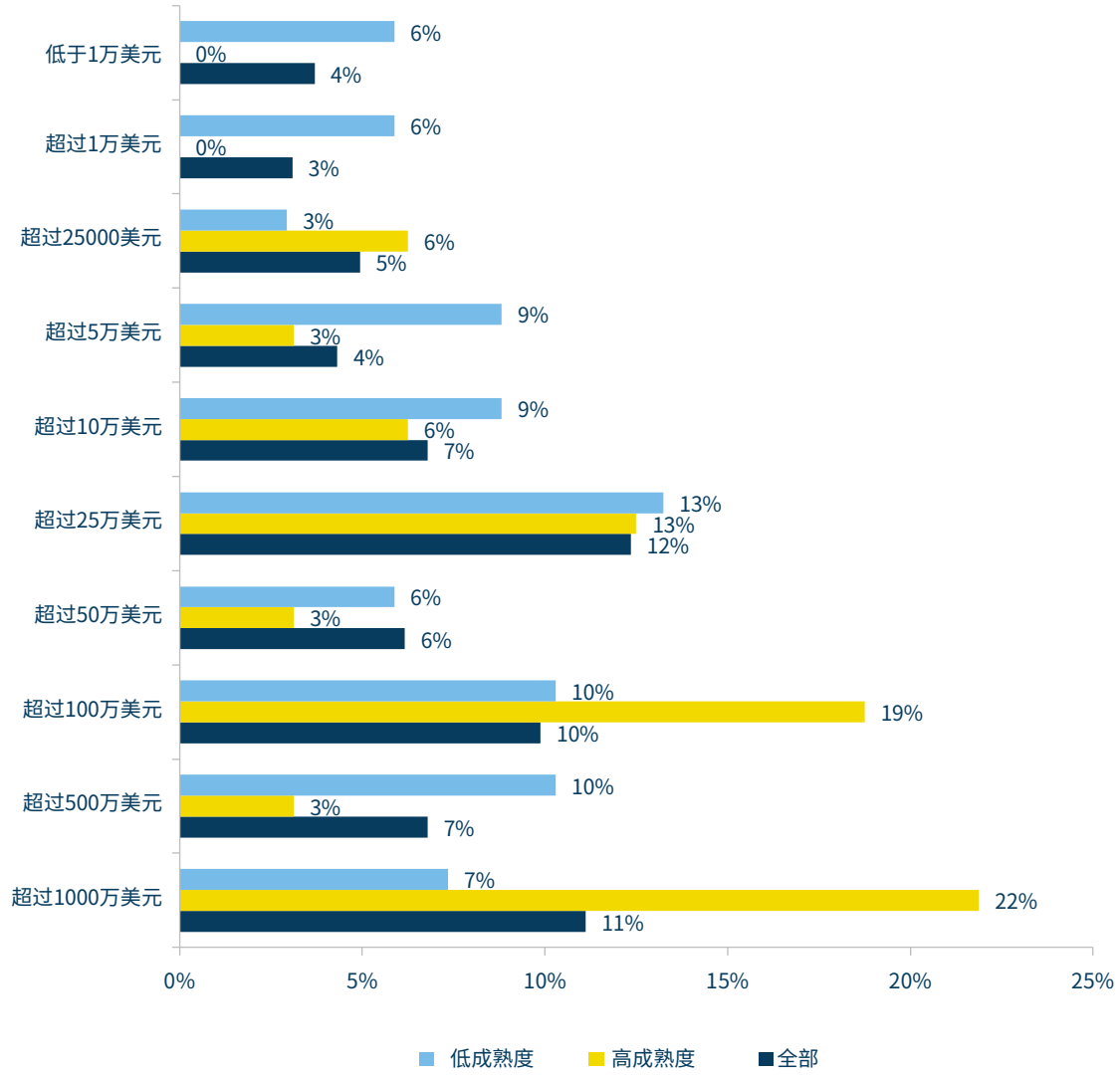
(CS)²预算情况
——高成熟度vs低成熟度

我们已经看到，高成熟度组织往往拥有最高的控制系统网络安全预算。一种理论认为，大型组织（即拥有更多资源的组织）通常比小型组织在安全之旅中走得更远。虽然我们认识到，分配足够资源来提高安全性的小公司面临的财务挑战往往更大，但我们也希望指出，同样的财政限制可能意味着它们抵御和恢复破坏性网络事件影响的能力较弱。网络攻击导致他们的运营长时间关闭的威胁对他们来说可能更为现实，他们的风险管理过程需要考虑到这一点。

这种相关性也突显了针对(CS)² 领域的需求，需要考虑通过缩减预算的解决方案和服务从而更好地为较小的客户服务。

Rod Locke
Fortinet产品管理总监

上一财年各组织的(CS)²预算规划总计



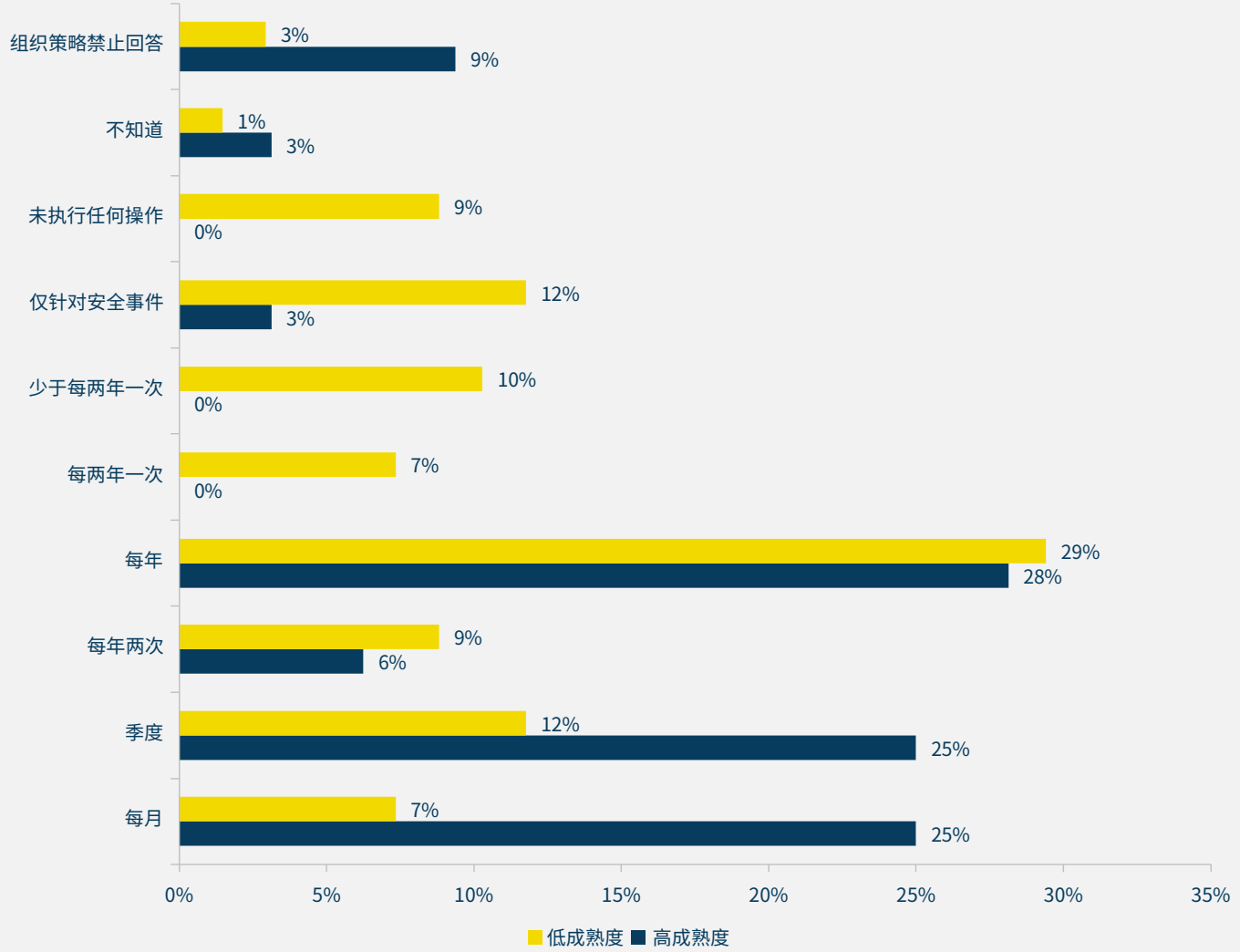

SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

(CS)²评估

(CS)²评估频率
——高成熟度vs低成熟度

不同成熟度水平的项目之间最明显的差异之一是其控制系统网络安全评估的频率。高成熟度项目中有一半至少每季度进行一次评估，而低成熟度项目中有一半以上每年或更低频进行一次评估。9%的低成熟度项目没有进行过安全评估，这本身就说明了问题。

各组织(CS)²评估的频率（低成熟度与高成熟度）

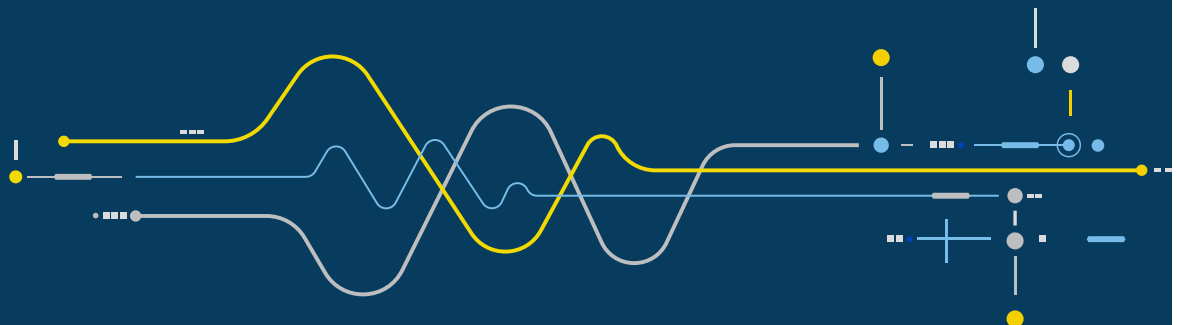


(CS)²评估频率 —— 终端用户vs供应商

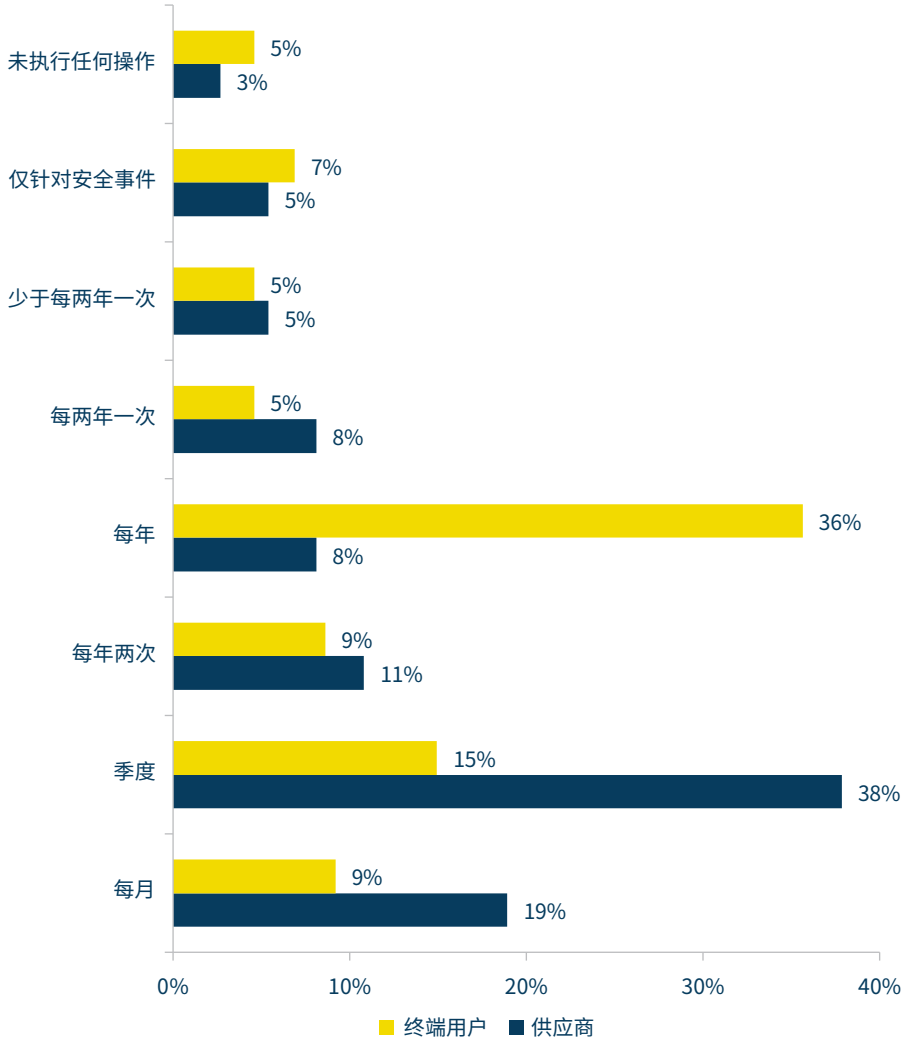
供应商对其安全承担着与最终用户不同的责任，因为他们不仅必须保护自己，还必须保护他们的客户，而客户通常会授予特权访问权限以进行持续的监控、维护和更新。我们的团队很高兴看到供应商如此频繁地进行(CS)²评估，超过三分之二（67.6%）的供应商每年至少进行两次评估。他们在最终用户供应链中的地位使他们成为攻击者非常有价值的目标[11]。终端用户组织这样做的频率较低，评估中最大的单一群体（35.6%）仅每年进行一次评估，的确不那么令人鼓舞。

技术、特权人员、攻击方法和能力都在不断发生变化，即使使用IPS/IDS（入侵预防/检测系统），一些受害者也只能在评估活动中发现恶意分子访问了他们的网络。更频繁的评估可以大大减少这种停留时间，从而减少各种潜在的危害。我们建议所有组织，包括终端用户和供应商，至少每季度评估一次其(CS)²网络和资产。

11. 请参阅许多报道2021年太阳风供应链攻击事件的文章中的任何一篇。



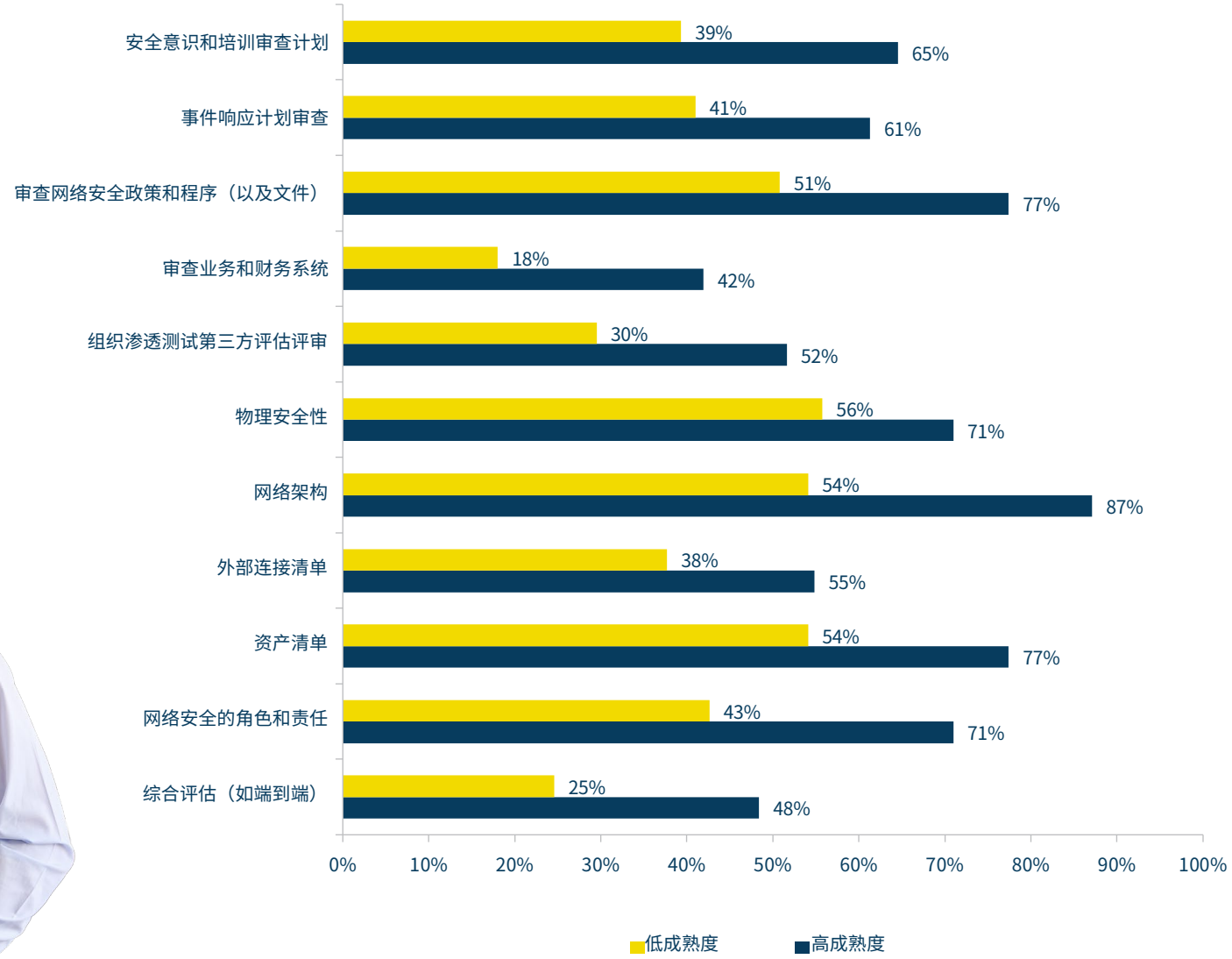
各组织进行(CS)²评估的频率



(CS)²评估内容——高成熟度vs低成熟度

与安全评估频率同等重要的是评估的彻底性，如本表所示， 高成熟度项目在我们使用的每个指标上都比低成熟度项目进行了更完整的评估，几乎在每个类别中都至少进行了50%的评估。

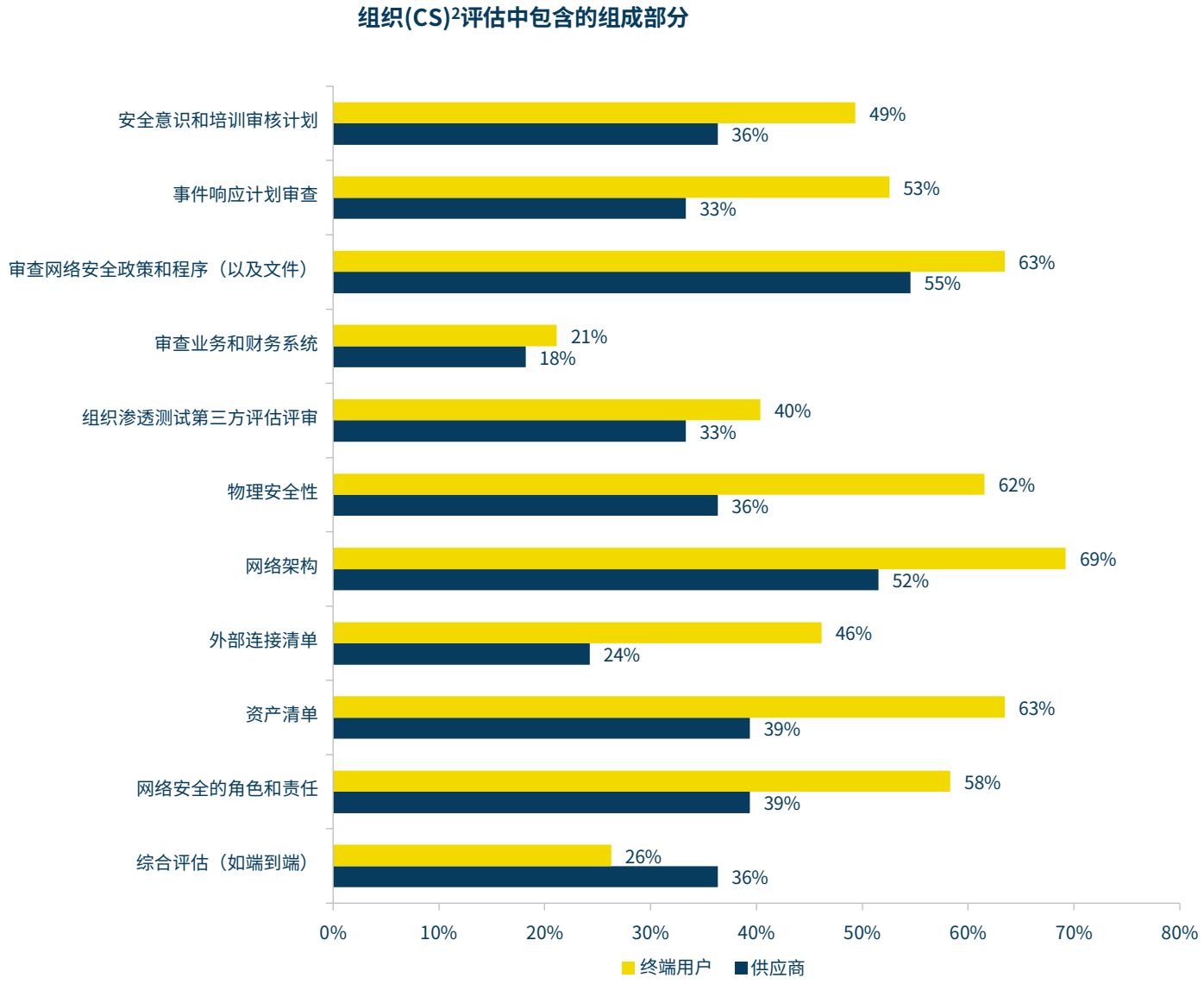
组织(CS)²评估的组成分布



(CS)²评估内容——终端用户和供应商

一个有趣的发现是，除了综合评估（终端用户26%，供应商36%）之外，终端用户似乎比供应商执行了更多的安全检查。这表明，虽然终端用户的评估包括多个重要活动（终端用户：物理安全62%、网络架构69%、资产清单63%等）但通常不如供应商或供应商客户的评估完整。终端用户可能缺乏所需的端到端的可见性，另外就是，供应商通常处于供应链中部，其必须考虑自身供应链和应用程序的安全性，以及他们为客户提供的服务的安全性。

该图表中列出的每一项都解决了一个防止入侵者沿其杀伤链前进的关键点（或在过程中捕获他们）。我们建议制定包括所有这些组成部分的计划，每个计划都有明确的评估和补救周期。



(CS)²评估响应——高成熟度vs低成熟度

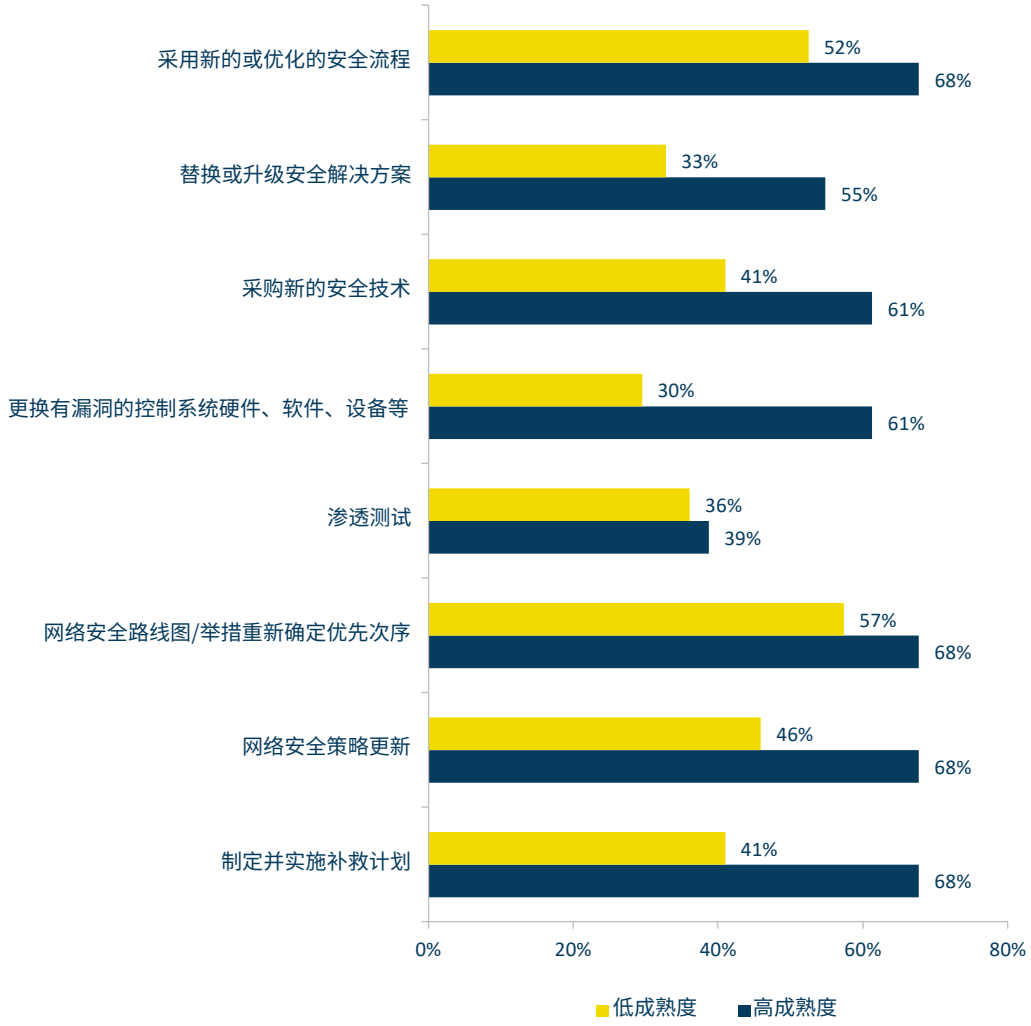
为了完成组织(CS)²评估因素的三位一体，我们调查了他们在分析后采取的行动。再次，我们看到高成熟度项目在每项指标上都比低成熟度项目更频繁地跟进评估结果。尤其是他们在制定和实施补救计划（低成熟度41.0% vs 高成熟度67.7%）和更换有漏洞的控制系统硬件、软件、设备等（低成熟度29.5% vs 高成熟度61.3%）这两方面。

尽管在网络安全基本措施（如网络隔离、培训和漏洞修补）上的投资是防止工业网络的潜在漏洞的关键，但要阻止有高度动机且技艺精湛的攻击者访问网络将非常困难。从网络事件中快速恢复的能力对于最大限度地减少对运营或向消费者供应电力或水等基础服务的中断至关重要。

应审查常规备份和恢复评估，以提高关键或工业系统的网络弹性。

Eddie Toh
毕马威新加坡合伙人兼毕马威亚太区鉴证技术主管

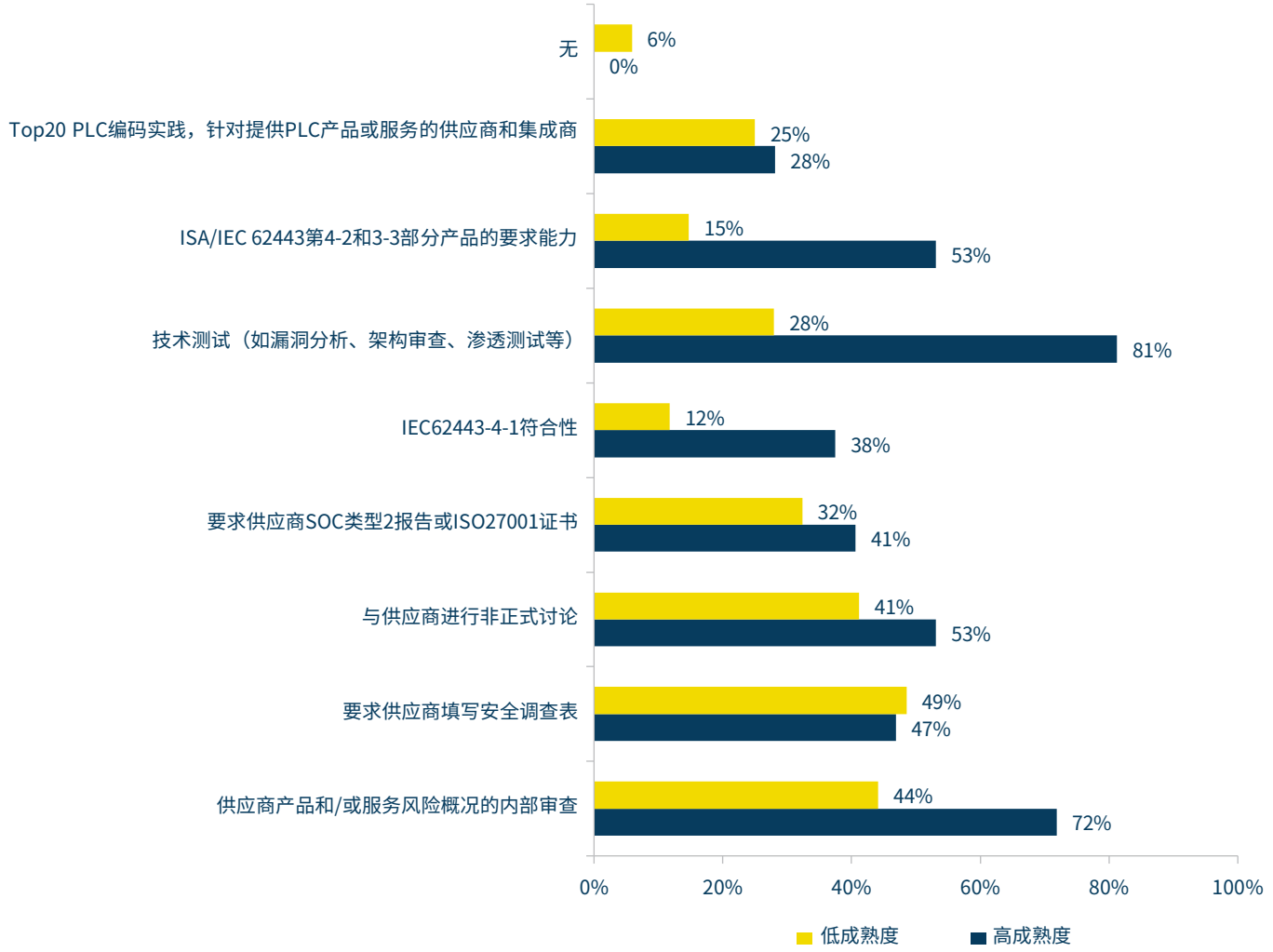
针对各组织在过去12个月内完成的(CS)²评估结果而开展或计划开展的活动



获取前的(CS)²风险评估
——高成熟度vs低成熟度

对新设备和/或软件的风险评估与周期性安全评估不同，必须单独考虑。正如我们看到具有高成熟度的(CS)²项目的组织更频繁地进行总体安全评估一样，我们注意到，他们更有可能进行几乎所有类型的获取前风险评估（安全问卷除外）。对于我们的许多受访者来说，美国监管活动的增加可能是影响合规性的一个因素，但我们认为高成熟度的技术测试率很高（低成熟度为27.9%，高成熟度为81.3%），因为它只提供快照，是对定期安全评估的正向的补充。

组织在获取控制系统产品或服务之前进行的风险评估（高成熟度与低成熟度）

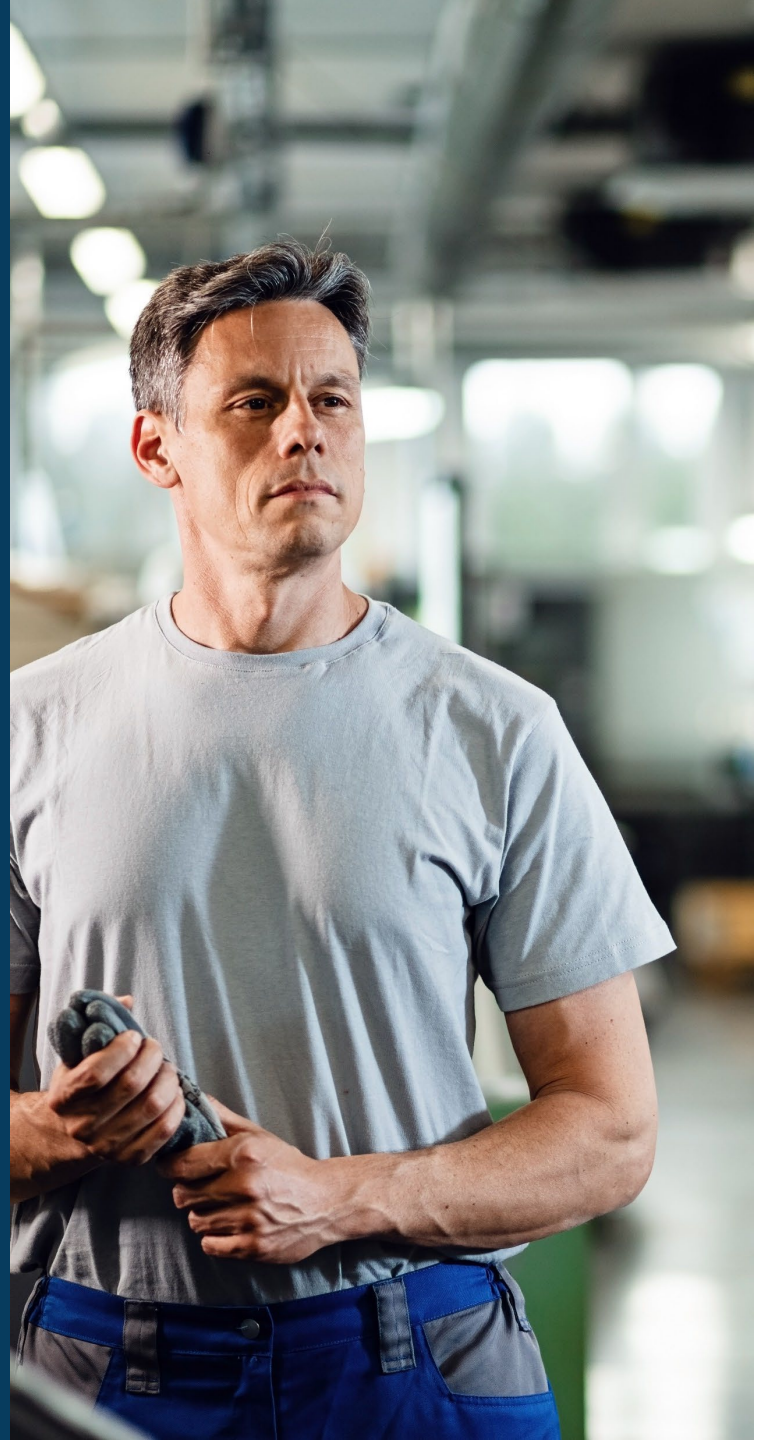



SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

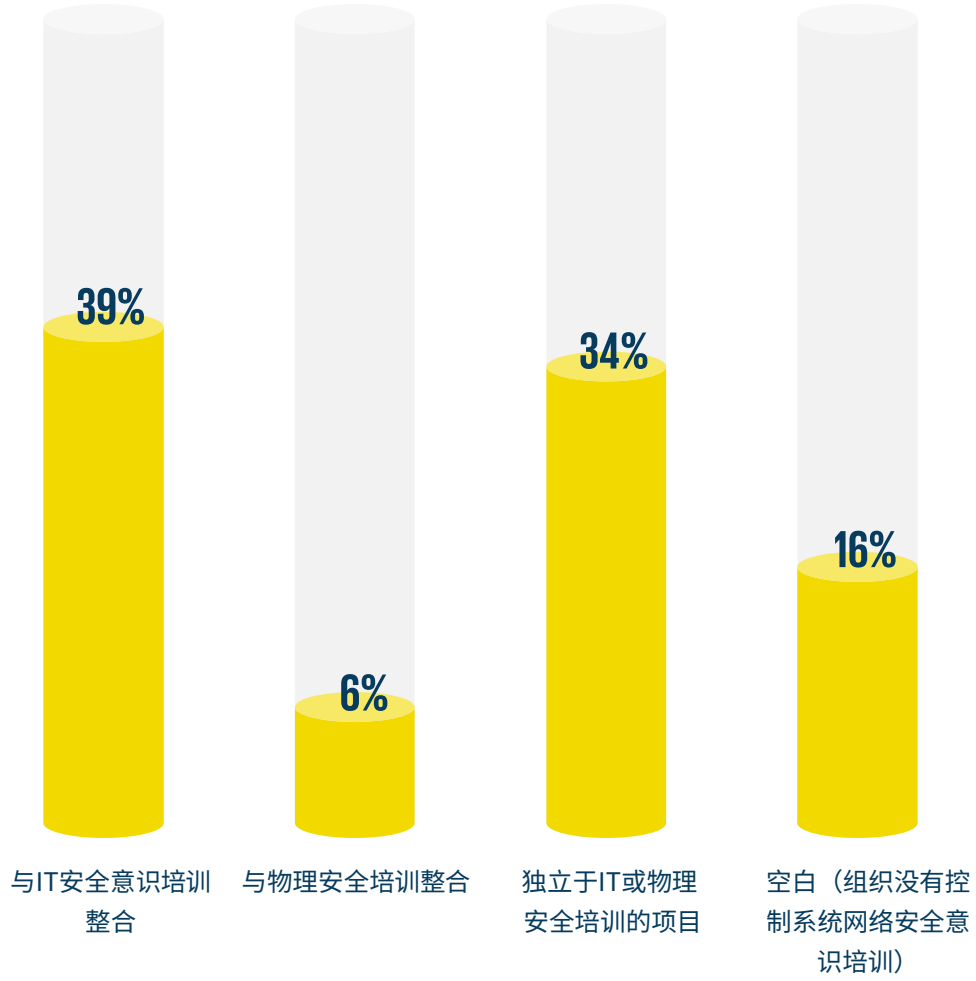
安全培训

(CS)²意识培训整合——终端用户

这里明显的问题是，许多终端用户组织缺乏任何(CS)²意识培训（16.1%空白）。无论是由IT部门或风险管理计划所驱动、或是完全由运营或其他设计部门负责，以实现并保持对(CS)²威胁、攻击方法、漏洞和程序的高度认识，对于管理任何ICS/OT运营环境中的固有风险都至关重要。我们强烈建议每个负责资产/运营的组织实施此类计划。



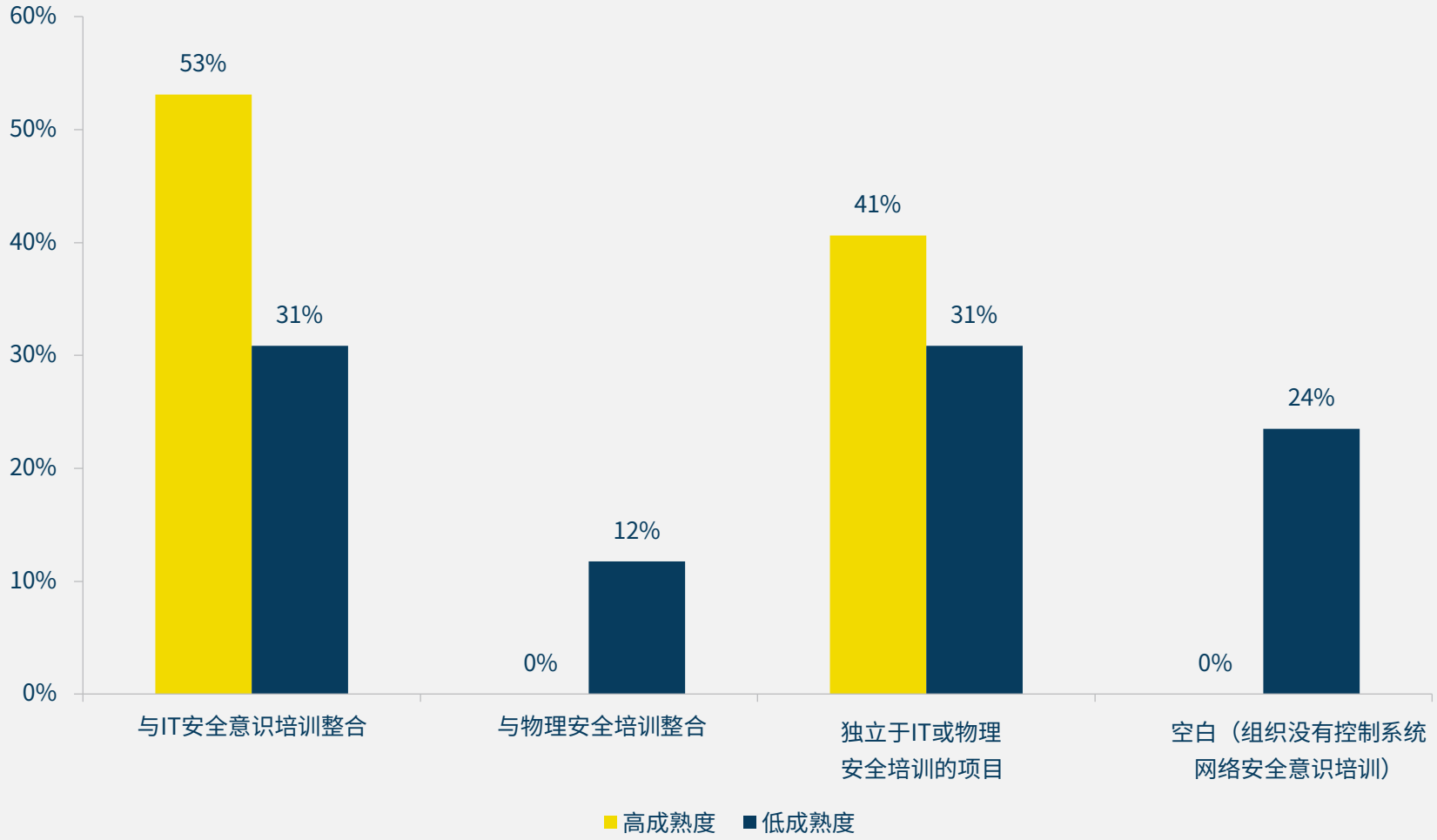
组织的控制系统安全意识培训现状



(CS)²意识培训整合
——高成熟度vs低成熟度

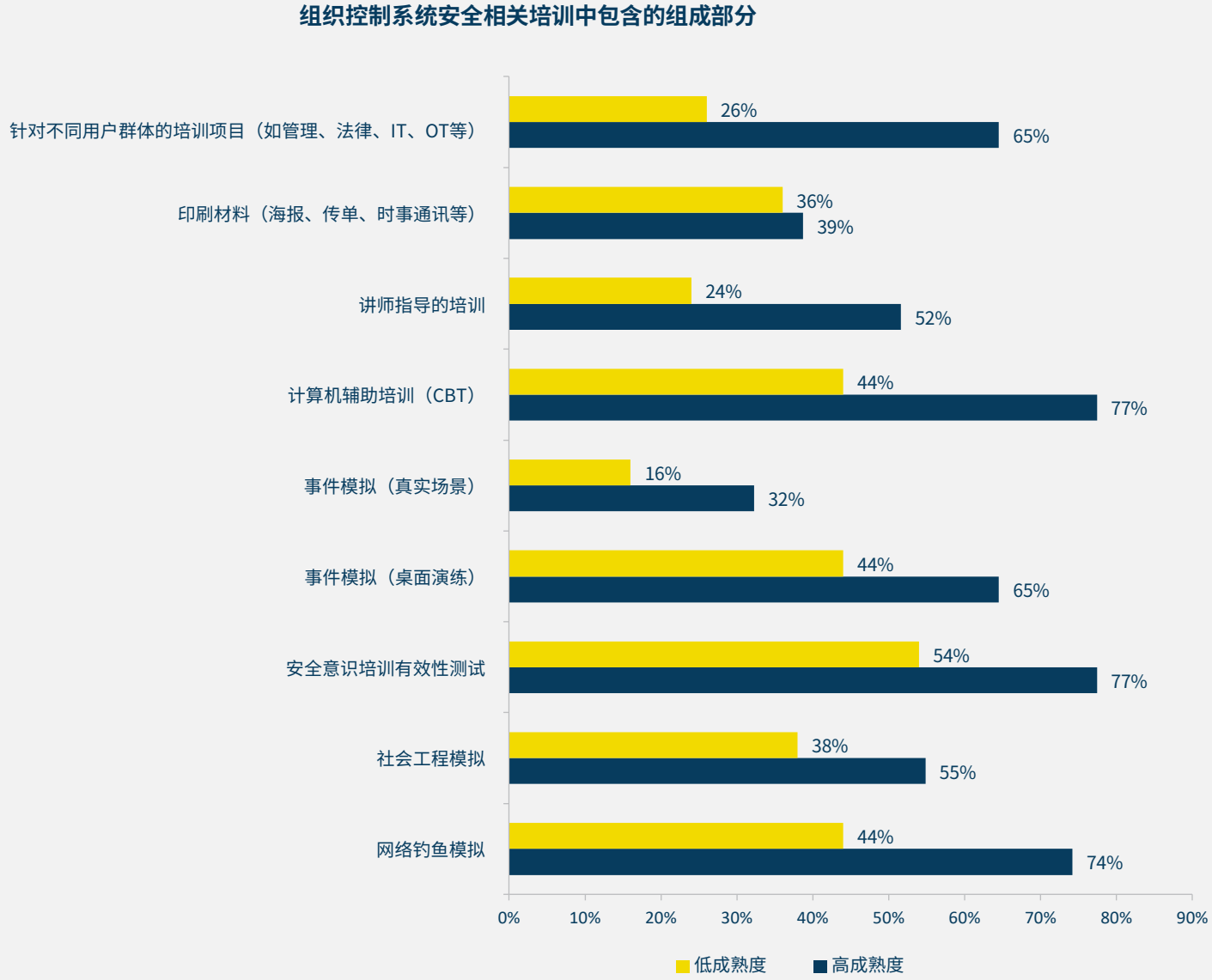
按成熟度级别分组的数据显示，只有(CS)²安全计划处于低成熟度的组织缺乏相关的意识培训（存在空白的，低成熟度24%，高成熟度0%），而高成熟度组织的大多数同事都接受了整合IT安全和控制系统安全的网络安全意识培训。

组织的控制系统安全意识培训现状



(CS)²培训内容
——高成熟度vs低成熟度

尽管我们在对各种安全项目成熟度级别的描述中没有包括安全培训，但从该图表中可以清楚地看出，高成熟度组织在确保训练有素的员工队伍方面投入了更多。这两组人甚至彼此接近的唯一组成部分是使用印刷材料，这通常被认为不如其他任何一组培训内容有效。事实上，在模拟（任何）和讲师指导培训等最有效的领域，我们看到了一些最大差异。更多地使用安全意识培训有效性测试（高成熟度77%，低成熟度54%）能够使这些公司专注于最有效的方法，并不断改进其培训项目。




SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558BKLSPPP166161

(CS)²网络

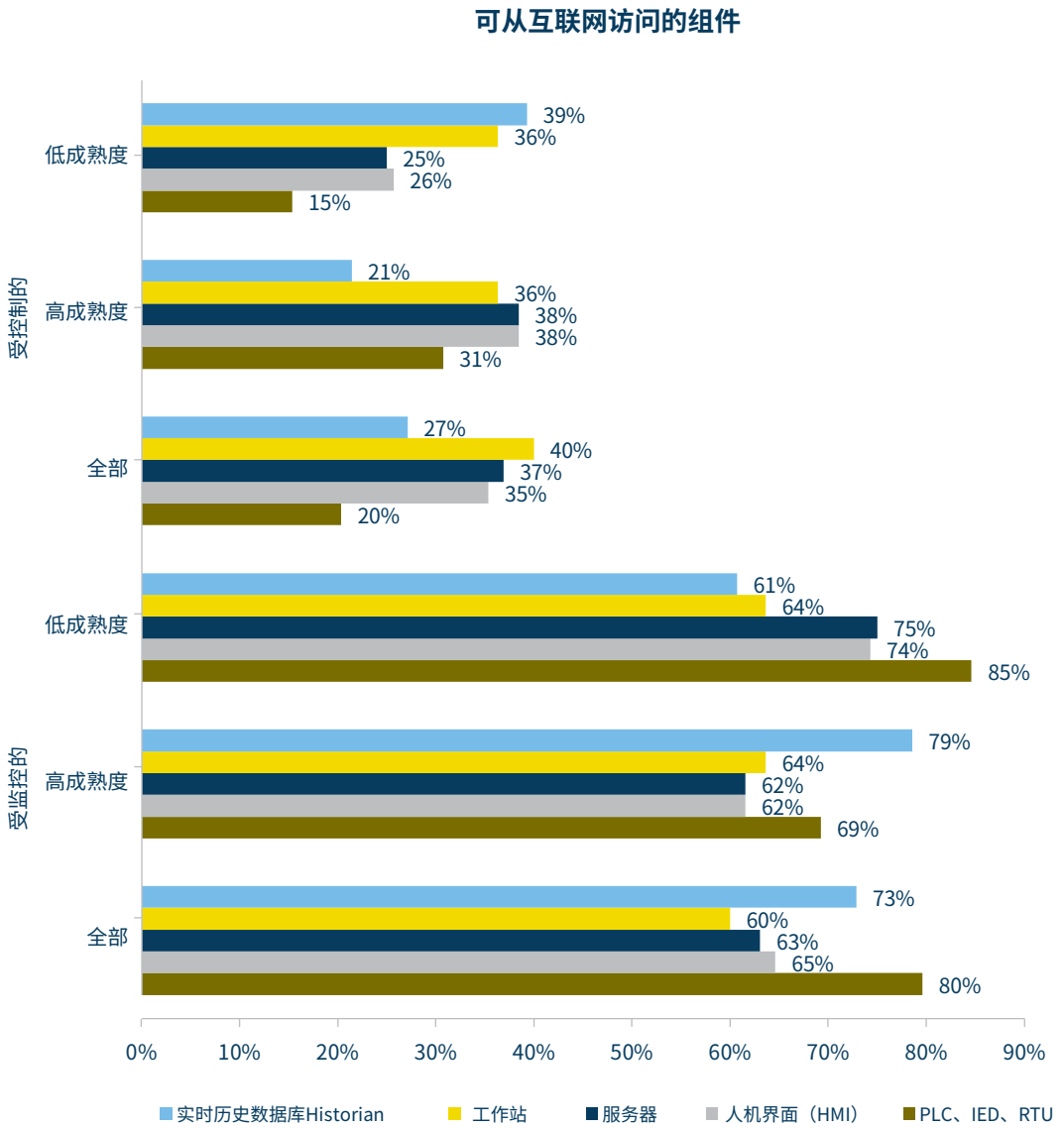
控制系统组件的可访问性

总的来说，这张图表和后续图表令人十分担忧。控制系统中有这么多元素可以从互联网进行访问，甚至被控制（低成熟度组织15%的PLC和39%的实时历史数据库），这表明攻击者拥有非常大的攻击面，并且对这些公司可能造成巨大的影响。

我们的一些专家贡献者指出，必须牢记这些“可访问”确实揭示了对可访问性控制和措施的问题。这些系统可能是具有对互联网开放的端口（例如HMI登录窗口），具有从互联网远程访问的功能（例如VPN或者RDP），或可以通过暴露在互联网上的另一台机器（例如跳板机）访问，或在跳板机可访问的网络上访问。评估其风险级别时，必须考虑其可访问性的具体细节和防护控制措施。

我们确实感到奇怪的是，在高成熟度组织中，如此多的组件可以通过互联网进行频繁控制，就像在低成熟度组织中一样。事实上，在高成熟度的组织中，服务器、HMI和PLC/IED/RTU更经常以这种方式访问[12]。以下图表继续显示了这种模式，显示了来自业务网络、供应商/集成商和云的组件可访问性。

12. 更成熟的群体对网络隔离的高投资回报率（75%，请参见高投资回报率图表——高成熟度 vs 低成熟度）可能会对此处产生影响。

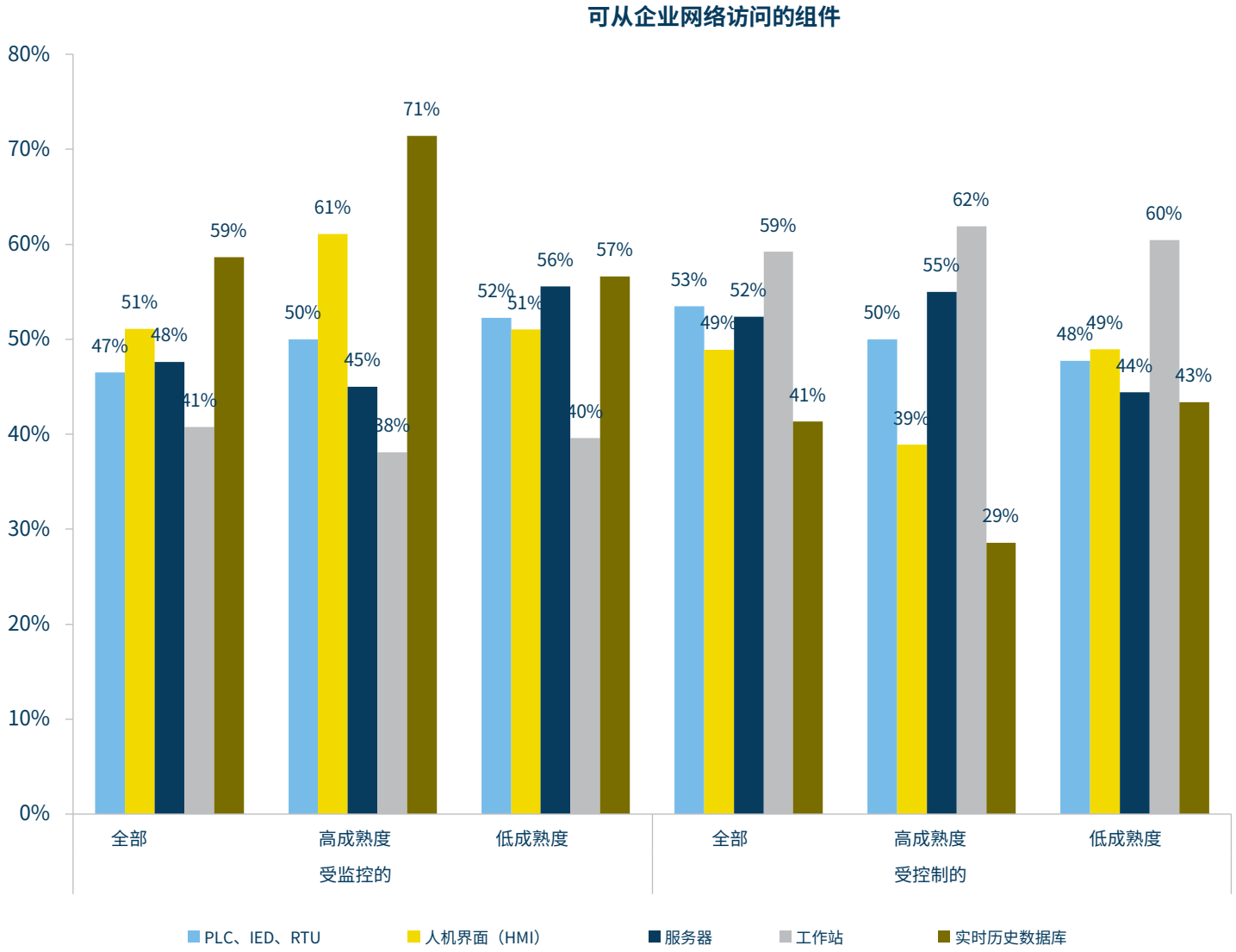


控制系统组件的可访问性（续）

这些反馈表明，如今控制系统的外部访问很普遍，包括来自企业网络、供应商和云的访问。由于IT/OT的融合日益增强，组织必须将控制系统安全视为其整体安全计划的一部分，而不是一个单独的领域。这既适用于安全管理程序（根据IEC 62443和ISO 27001等标准），也适用于用以保护和监控这些系统的控制措施。

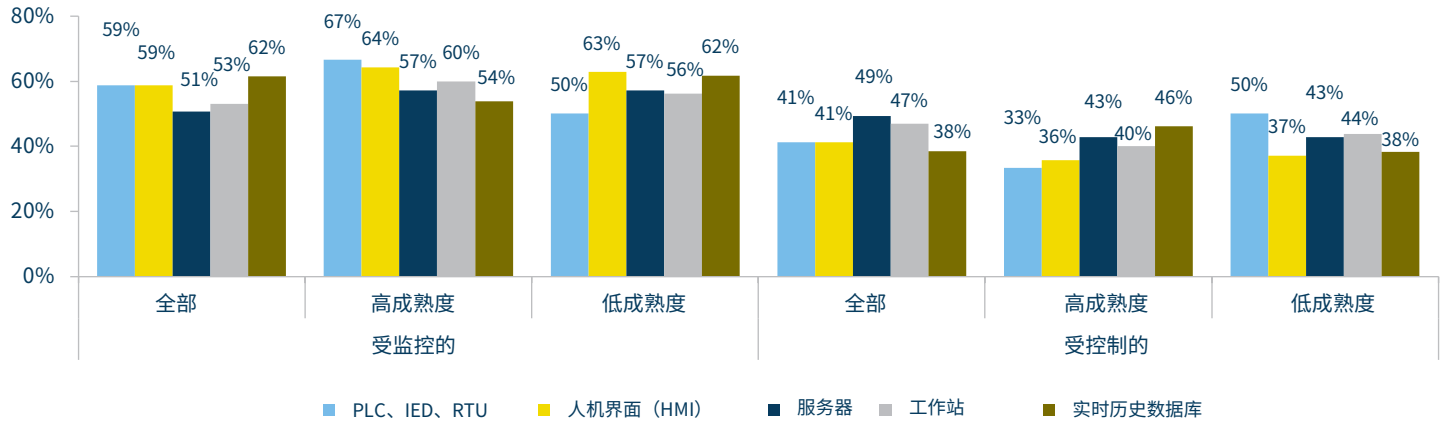
在Fortinet的《2023年运营技术和网络安全状况报告》中，受访者表示，OT安全是几乎所有组织（95%）首席信息安全官职责的一部分。IT/OT融合的现实也反映在组织对威胁格局的看法中——绝大多数组织（77%）认为勒索软件比OT环境的其他威胁更令人担忧。

Rod Locke
Fortinet产品管理总监

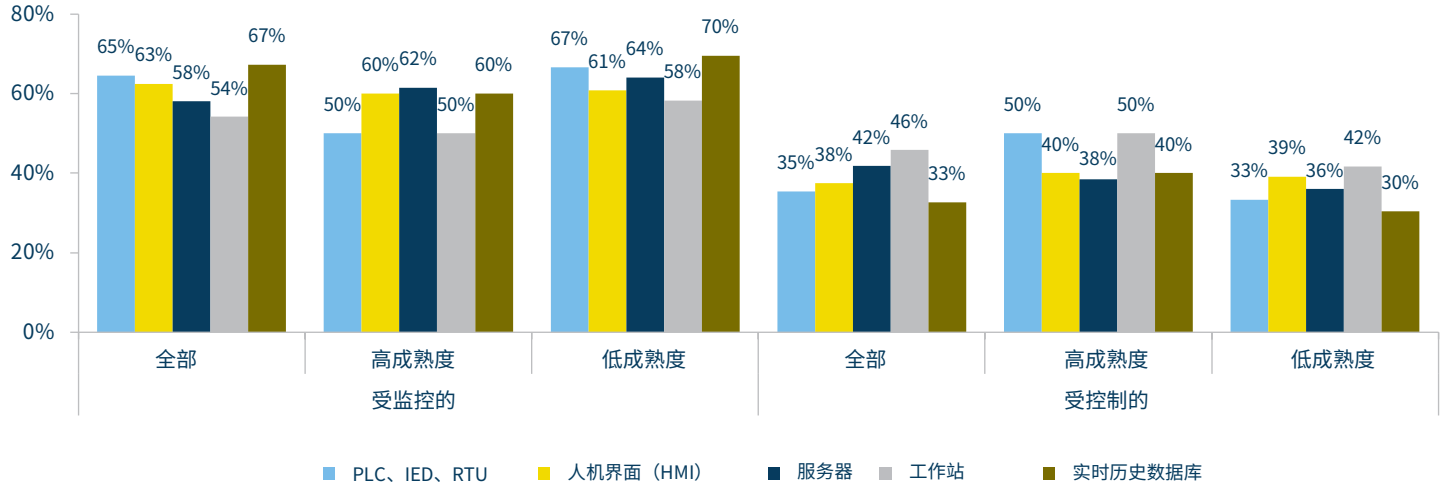


控制系统组件的可访问性（续）

供应商/集成商可远程访问的组件

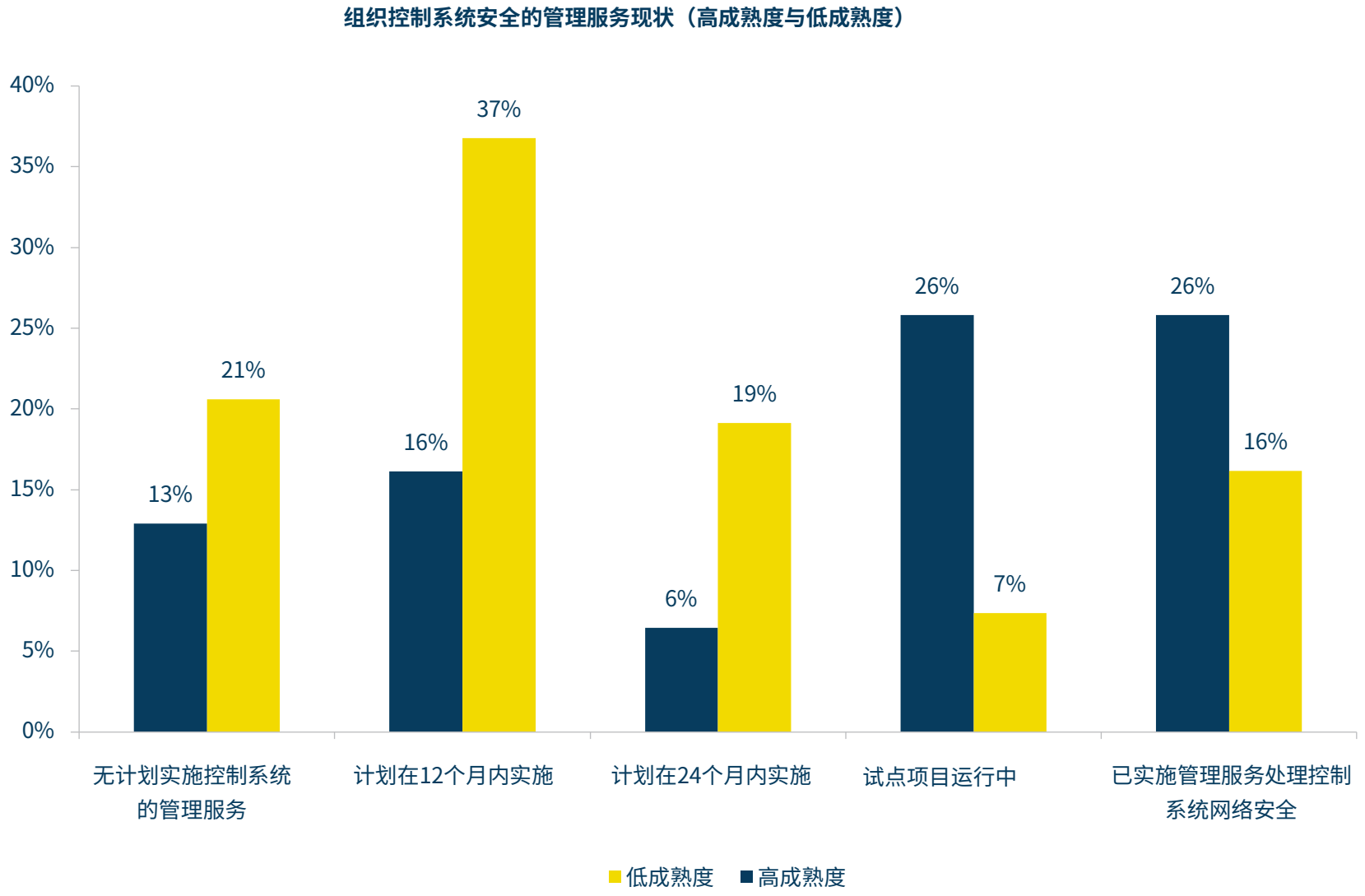


可从云访问的组件



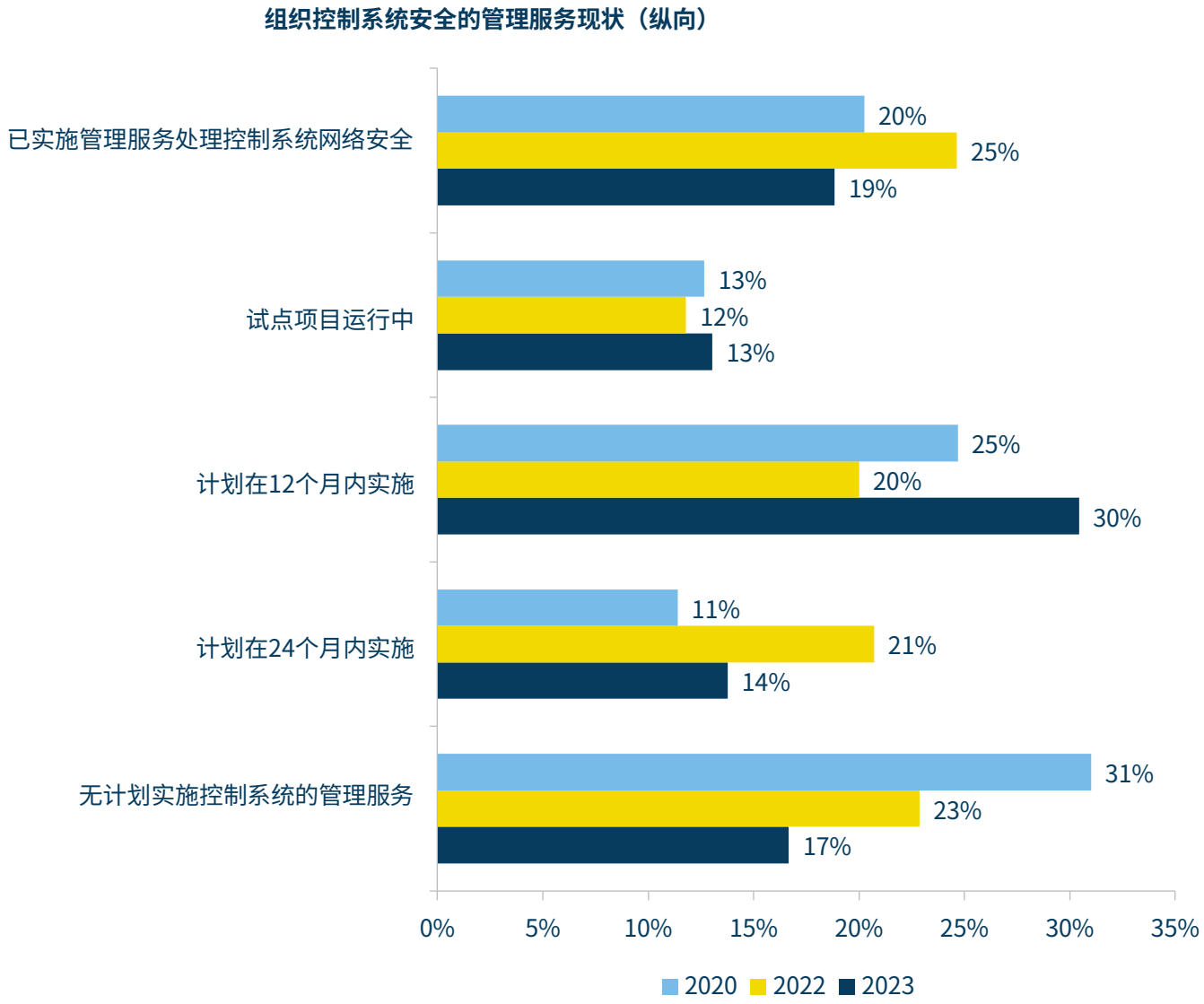
(CS)²管理服务现状
——高成熟度vs低成熟度

今年的参与者再次表示，高成熟度组织更有可能已经拥有管理服务来处理其网络安全（高成熟度25.8%，低成熟度16%），或正在通过试点管理服务项目来处理网络安全（高成熟度25.6%，低成熟度7%）。



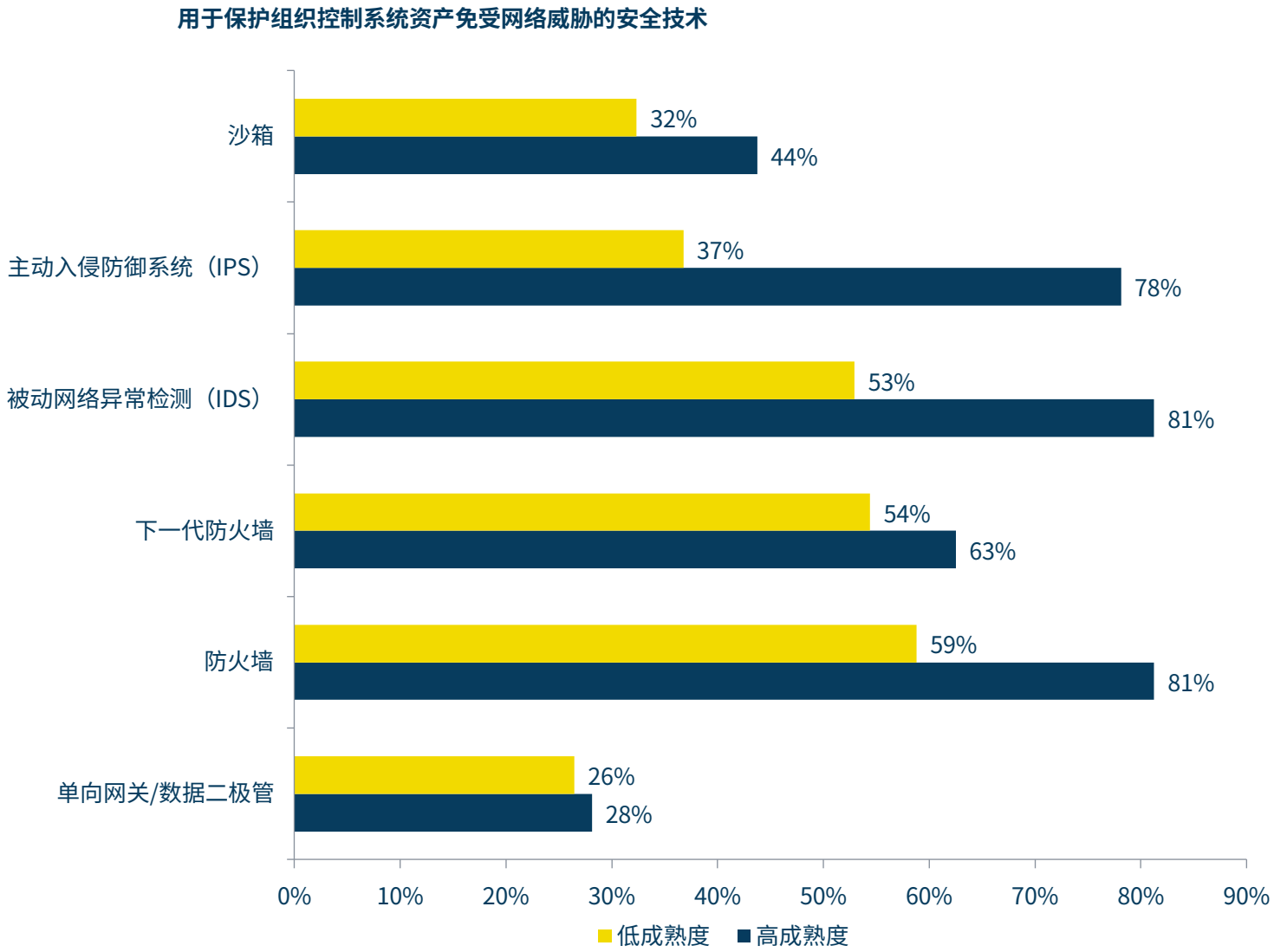
(CS)²管理服务的使用——纵向分析

转向使用(CS)²管理服务符合我们多年来向读者的建议。内部资源的培训和教育有着无可争议的意义，但这些都是长期（短期内可能不太确定）的投资。长期以来，(CS)²劳动力中知识渊博、经验丰富的从业者供应一直不足以满足快速变化的技术、实践和控制系统设备日益增长的超连接性的需求。这不可避免地为不断扩大的(CS)²服务市场提供了动力。我们建议那些拥有足够资源的公司既要推行内部资源开发计划，又要利用外部专业知识来满足保护其资产和运营的迫切需求。我们认为，这是改善其组织长期前景的最佳方法。



(CS)²技术现状
——高成熟度vs低成熟度

除了高成熟度组织比低成熟度组更频繁地使用每种安全技术的总体趋势外，主动入侵防御系统（高成熟度78.1%，低成熟度36.8%）和被动网络异常检测（高成熟度81.3%，低成熟度52.8%）的使用之间的巨大差异也说明，高成熟度公司更有可能在较短的时间内识别和阻止入侵企图，从而减少对其系统的潜在影响。



(CS)²网络监控——纵向分析

对我们的控制系统网络的可见性对于保护这些网络和连接的资产至关重要。尽管OT文化历来抵制将网络监控技术引入其环境（可以理解的是，由于这样做会导致一些运营中断）。但是，监控工具和技术不断成熟和改进，人们对其风险收益比的接受度也在提高。令人鼓舞的是，实施(CS)²网络监控并计划加强的组织同比在增长，从几年前的0到今天的17.9%。未计划实施任何网络活动监控的组织占比首次降至百分比个位数（9%）。结果表明，未来组织将继续部署和加强网络活动监控。

2022年未计划实施监测的组织数量曾激增（19%），最初这被认为是许多组织已进入“全面监控”状态的迹象；但今年的结果对这一点产生了质疑。我们将继续探索这个谜题。

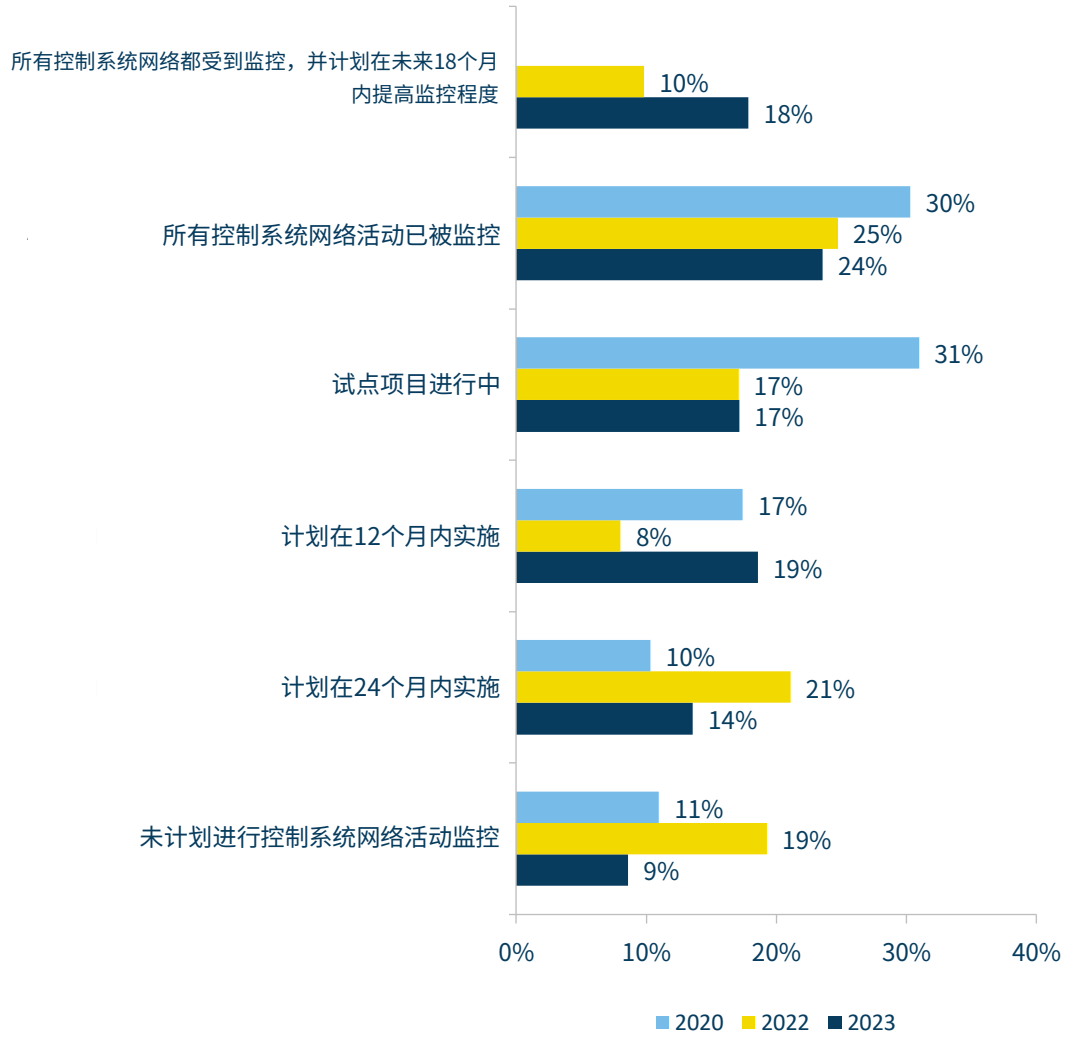
随着运营技术的现代化，当OT系统越来越多地连接到IT系统时，攻击面会继续扩大。威胁行为者将继续应用精密的“战术、技术和程序”，并利用其来攻击任何薄弱环节以破坏这些系统。例如，鉴于其功能性，Pipedream是威胁行为者在破坏工业系统方面的能力和日益复杂的一个体现。

为了检测恶意活动并及时应对此类事件，必须对OT、IT、IIOT网络保持可见性并持续监控。

Eddie Toh

毕马威新加坡合伙人
毕马威亚太区法政技术主管

组织控制系统网络活动监控的现状



(CS)²可见性——终端用户

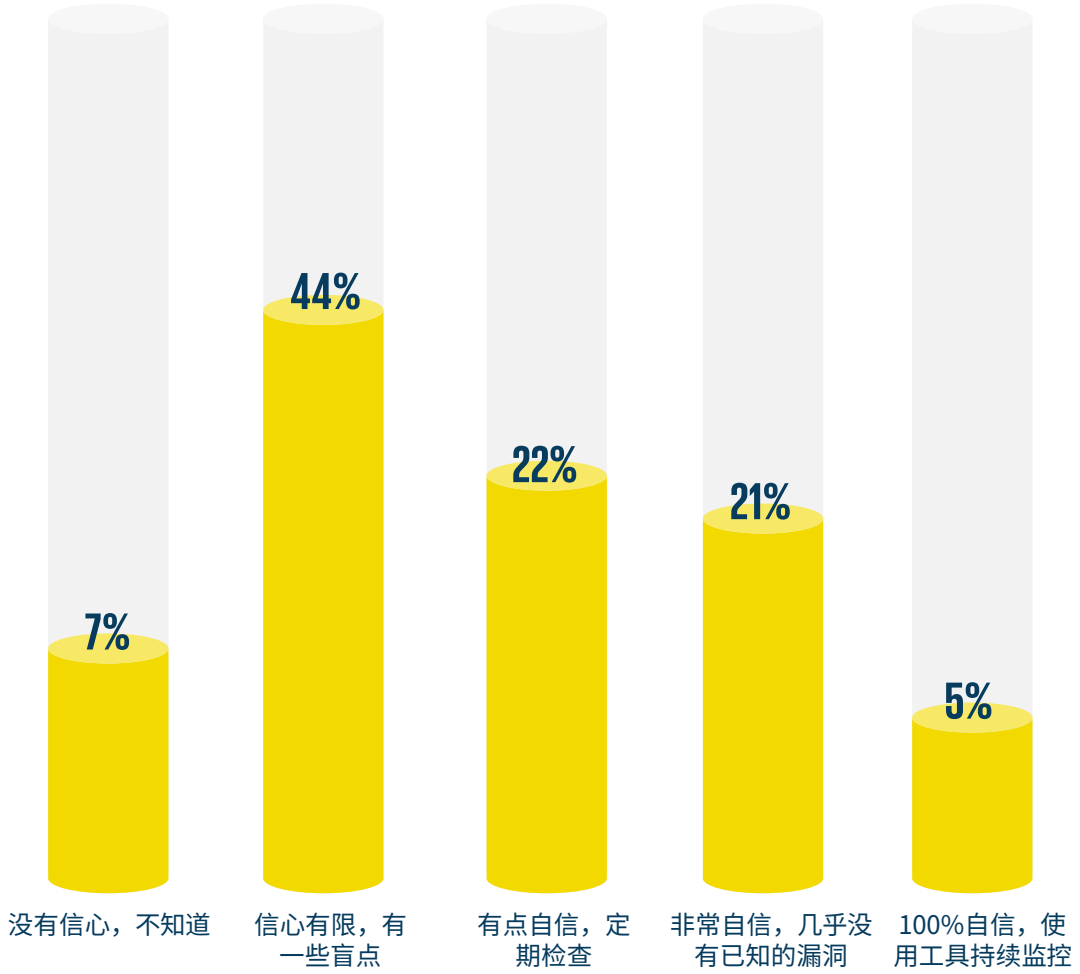
我们的团队认为，我们最大的终端用户受访者群体（信心有限，有一些盲点43.7%）的信心水平相当现实。控制系统网络的可见性一直是一个问题，直到最近几年，具备这一重要能力的工具才得到普及。我们建议我们的读者，如果尚未实施的，利用这些工具来解决盲点，并为您的(CS)²守卫者提供履行职责所需的基本知识。

离线网络建模是以非侵入方式提供全面网络可见性的最快、最有效的方法。它有助于准确了解我们致力于保护的网络环境，而不会中断运营。通过分析离线环境中的网络配置、拓扑和安全策略，我们可以深入了解关键的通信路径和覆盖缺口，否则这些路径和缺口可能会在实时网络分析会话中被隐藏。这种方法在快速识别和解决缺乏可见性的区域的同时，保持了网络的完整性和性能，从而增强网络对潜在网络威胁的防御。

Robin Berthier

Network Perception
首席执行官兼联合创始人

组织对网络上设备、用户和应用程序可见性的信心水平



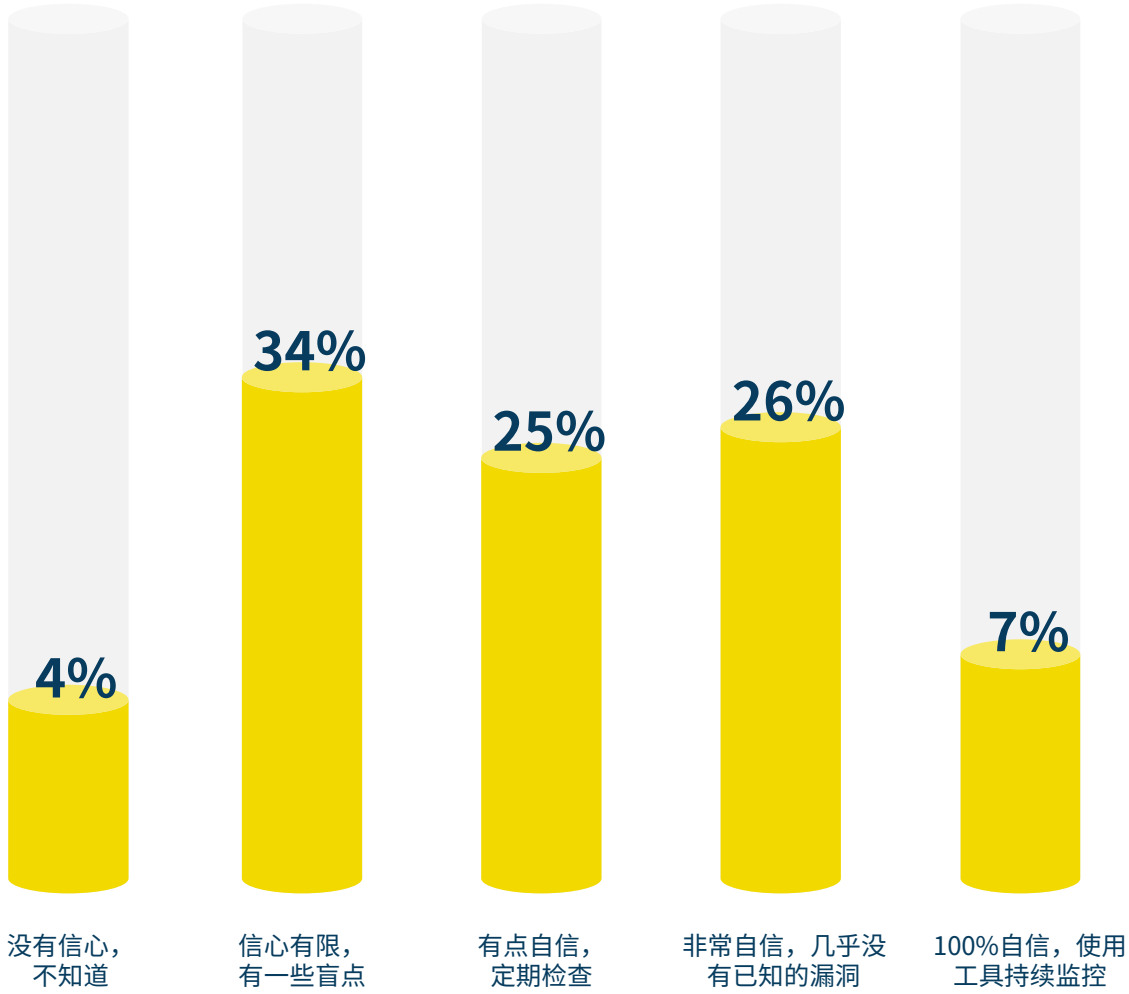

SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558RKLSPPP166161

$(CS)^2$事件

(CS)²攻击响应——终端用户

我们的团队很高兴看到资产所有者或运营商（最终用户）对网络攻击事件响应流程的信心水平，58%的人至少有点自信，其中大多数人非常或100%自信。这比他们对网络的可见性的信心更足（参照上页图表）

组织对网络攻击事件响应流程的信心水平



(CS)²事件近况——纵向分析

尽管在过去一年中，经历50件以上(CS)²事件的受访者略有上升（从上次报告的5.2%上升到现在的5.8%），但更突出的结果是，回答“无”的受访者大幅上升（2022年14.8%对比2023年25.4%），而回答“26-50”的受访者则有所下降（2022年19.4%对2023年10.1%）。希望这体现了持续的保护和复原努力的结果，而不是无视或错误反馈。

网络攻击预计只会增加——这是工业生产数字化的不利方面。不仅组织内部的接口数量，而且与外部合作伙伴的接口数量都在不断提升。不幸的是，这增加了攻击的媒介。

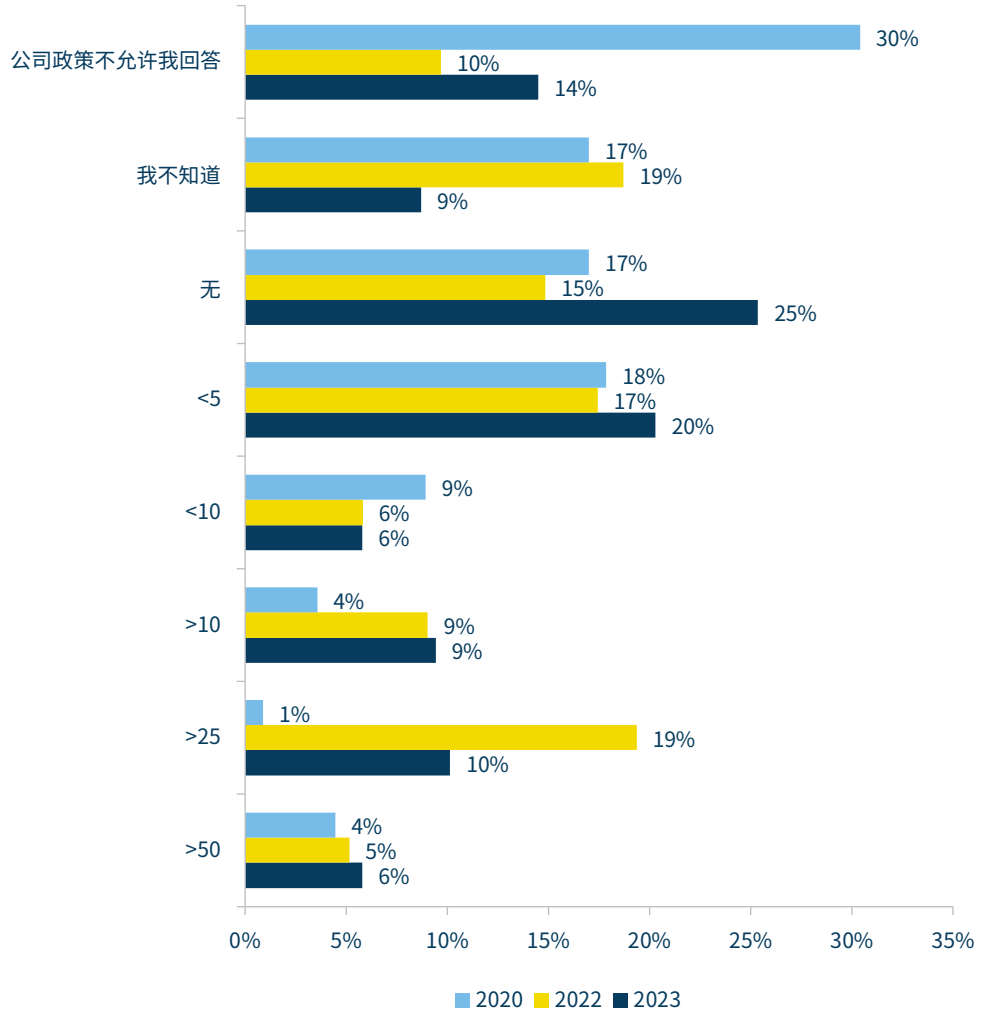
因此，有优先级且重点突出的方案对于保护生产系统和流程非常重要。一套健全的OT安全方案不仅包括技术方面，还包括安全流程、治理和人为因素。

预防、检测和防御的关键是在于与时俱进。因为OT网络安全具有两个关键特征：变化和发展快。

Marko Vogel

毕马威德国OT网络安全合伙人

过去12个月内组织发生的控制系统网络安全事件估算数量



客户(CS)²事件攻击媒介——区域[13]

电子邮件（全球35%）和受感染的用户帐户（全球31%）是今年的前两大攻击媒介，可能存在重复计算，刚好把受感染的移动介质从第二位挤了下来，尽管后者出现的频率更高了（去年24%，今年26%）。地区5（中东和北非地区）的供应商更新漏洞事件（36%）比其他任何地区都高70%以上，同时遭受被入侵的公司网站的水平与地区4（亚太地区）几乎相当（分别为28%和31%）。区域4的Wi-Fi入侵（24%）和被感染或入侵的移动设备或手机（28%）最为突出，这两个数值都远远高于其他。

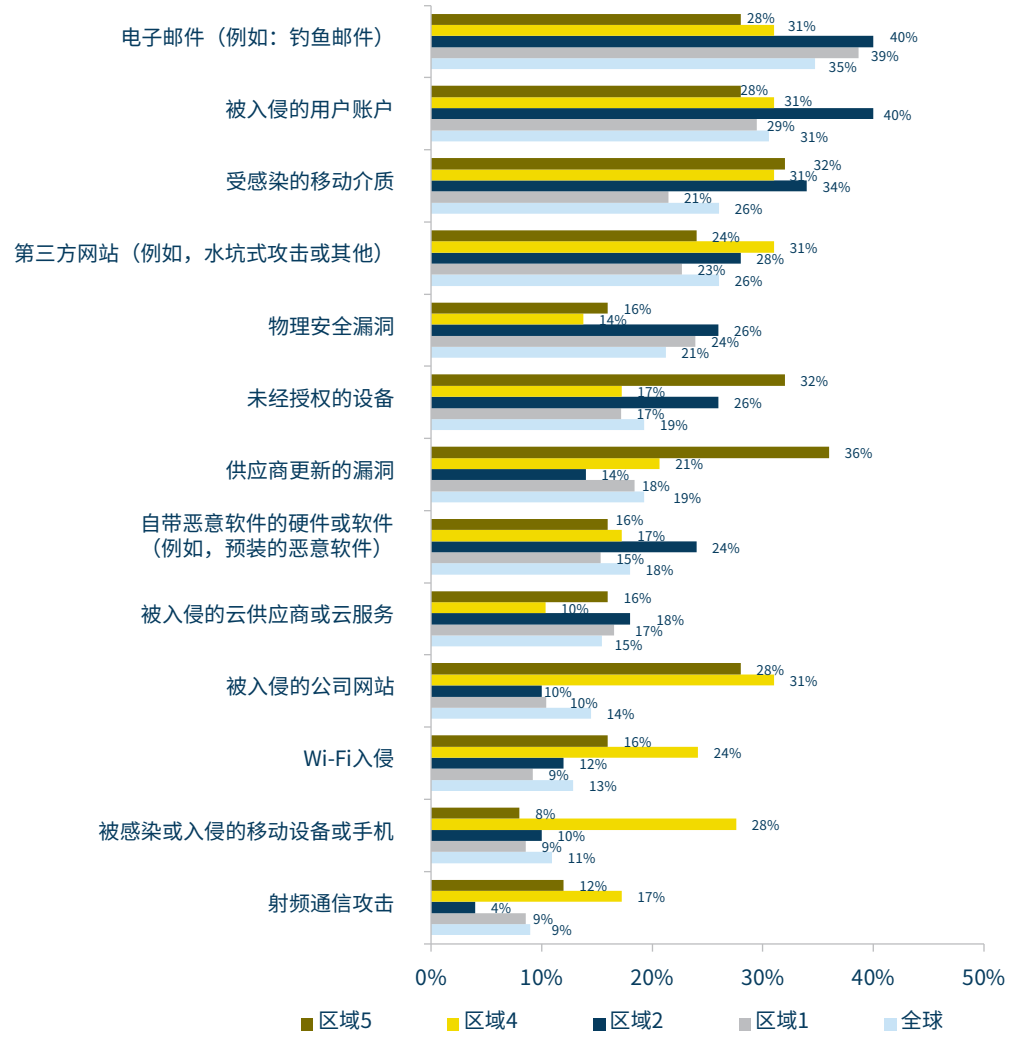
在许多组织中，由于各种不可抗拒的原因，IT安全成熟度态势远优于OT安全态势。然而，组织通过应用IT/OT网络安全融合，可以有很大机会提升OT安全态势，提高安全运营效率，并提升业务创新。这将有助于组织拥有统一的安全态势，减少攻击面，使IIoT能够促进数字化转型并支持先进技术，从而改善企业众多决策。

Hossain Alshedoki

毕马威沙特阿拉伯自然资源行业网络安全与隐私主管

13. (CS)²AI将组织划分成七个区域 。1） 北美；2）欧洲（中部、西部、北部和南部）；3） 欧亚大陆；4） 印度太平洋；5） 中东-北非；6） 南部非洲；7） 拉丁美洲-加勒比。

客户反馈的过去12个月(CS)²事件的攻击媒介



(CS)²事件影响——纵向分析

这些年我们编写报告中，这个问题也在变化，我们增加了答案的选项，以提高分析数据（和调查结果）的价值，因此有几项2020年是没有应答结果的。

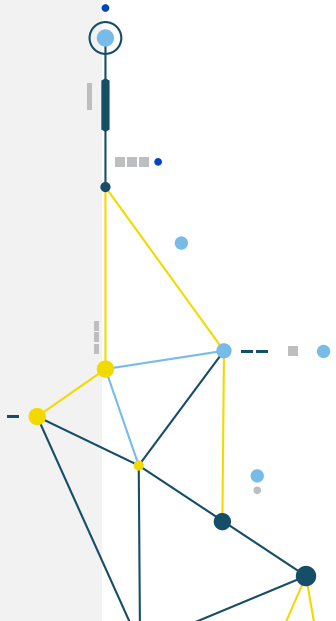
从这些数据中可以得出关键结论，即因运营中断、生命损失、产品损失导致的财务损失同比上升。回顾之前提到的对连续运营的重视（见图表：自由支配资金分配优先级（24页），供应商对客户预算的指导（25 页））。

过去几年关于生命损失的调查结果一直都是一个疑问。人们认为造成人员死亡的恶意网络攻击一定会成为头版新闻。即使事件发生在企业或政府压制此类报道的地区，也很难理解为什么在过去的两次调查中，5-6% 的受访者都报告了因 “网络事件 ” 造成的生命损失，而媒体却连一起事件都没有报道过。我们的受访者包括防护医院和保健中心等的工作者，这些地方的系统中断可能直接或间接导致死亡，但没有太多的受访者解释这一结果。这些“事件”是否真的是由被蓄意攻击所混淆的计算机产生的错误或疏忽？

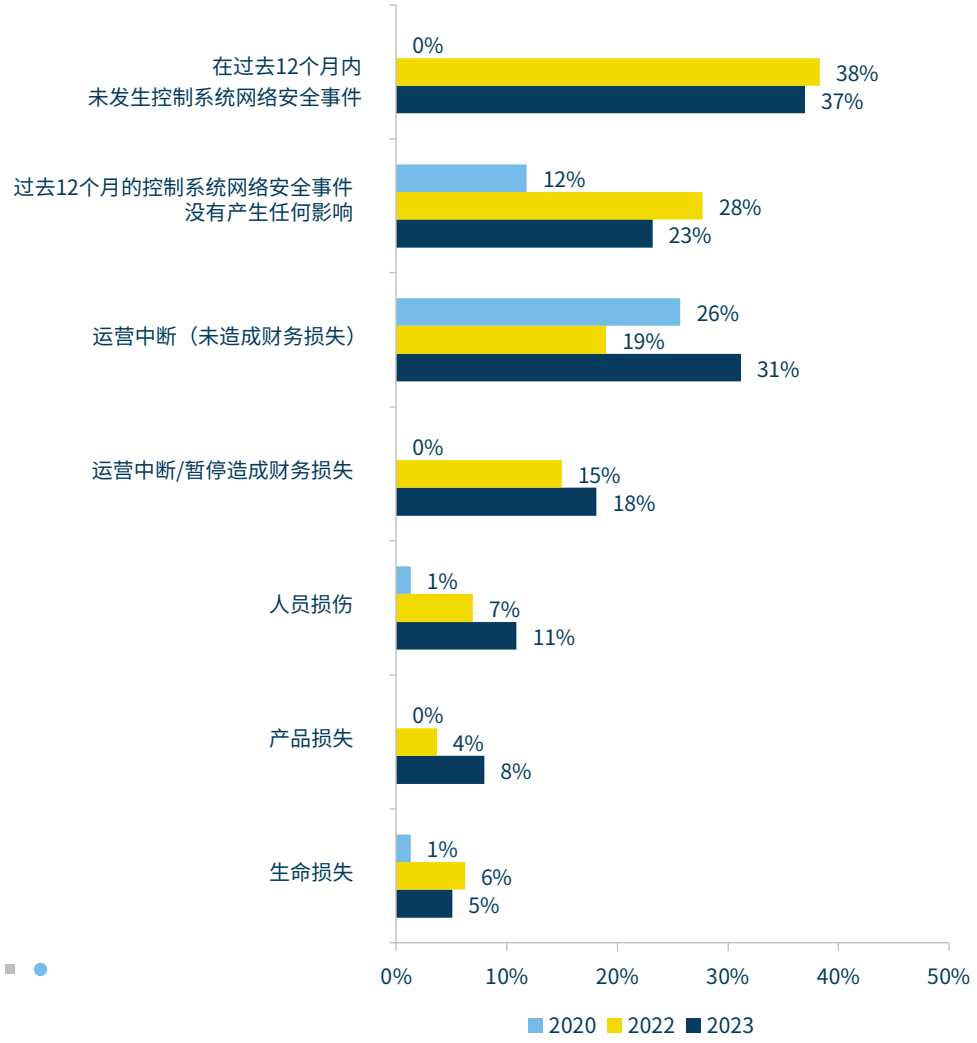
(CS)²入侵调查数据显示，安全事件导致运营中断加剧，这些中断导致更严重的后果。Fortinet的《2023年运营技术和网络安全状况报告》也发现了类似的比率，49%的组织在运营环境中受到了一些影响。报告还显示，成熟度较高的组织经历的网络入侵较少，对运营的影响较小。这些组织也更有可能将OT网络安全态势作为一个重要因素纳入与执行领导层和董事会共享的风险报告中。

Rod Locke

Fortinet产品管理总监



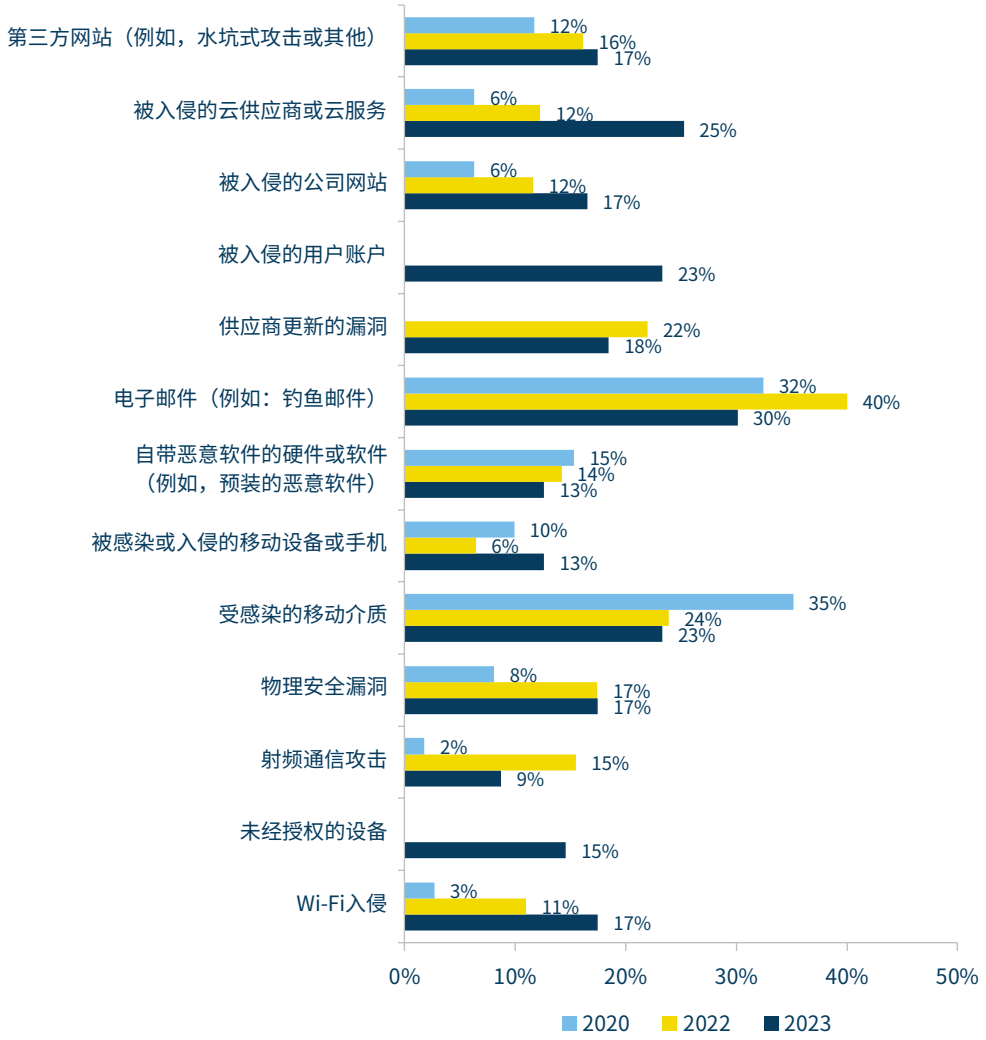
过去12个月内控制系统安全事件对组织造成的影响



近期(CS)²攻击媒介——纵向分析

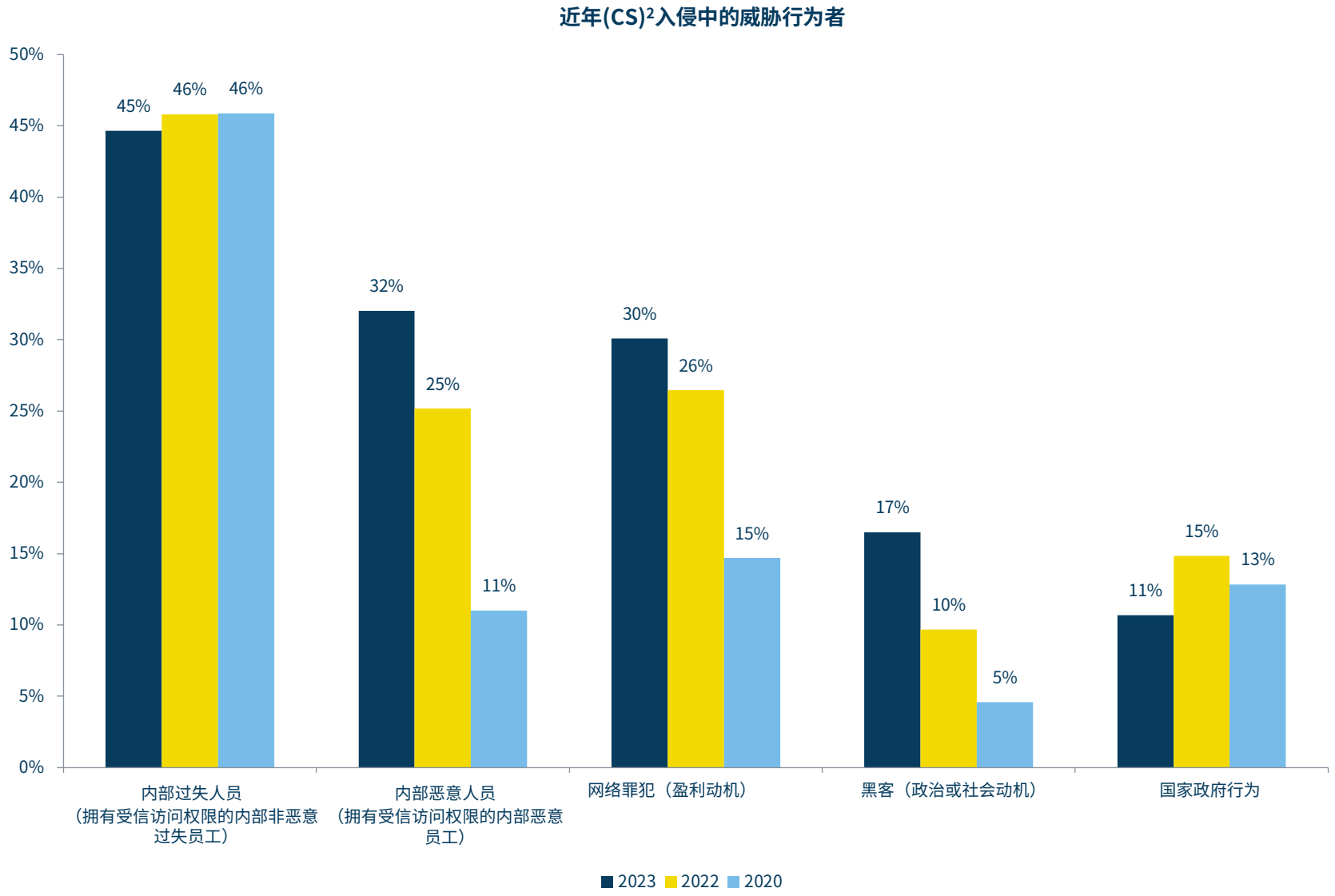
前面我们已经考虑了区域差异的特定攻击媒介的发生率。这里我们探索同比趋势发现了几个明显的增长模式。尤其值得关注的是，被入侵的云供应商或云服务（2020 年为 6%，2023 年为 25%）、Wi-Fi入侵（2020 年为 3%，2023 年为 18%）和被入侵的公司网站（2020 年为 6%，2023 年为 17%）的反馈持续增加，这页支持了威胁研究报告的观点，即攻击者正在从网络钓鱼扩展到目标攻击面的其他部分。云和Wi-Fi至少部分归因于近年来这些解决方案在(CS)²环境中的使用增加。需要注意的是，被入侵的用户帐户和未经授权的设备是今年的新选项，因此在2020-2022年的数据中未出现；自2022年添加了供应商更新的漏洞。

过去12个月内组织内发生的(CS)²事件中被利用的攻击媒介



(CS)²威胁行为者——纵向分析

相较国家政府行为和内部过失人员（后者仍是被提及最多的）的平稳比例，黑客、网络犯罪和恶意内部人员的报告数据每年都有所增加，这一点值得注意。我们没有发现任何重大的区域差异。媒体报道和国家情报机构都显示认为，近年来以盈利为动机的网络犯罪活动急剧增加，这与我们的调查结果一致。另一方面，来自内部恶意人员的(CS)²入侵活动兴起并没有引起公众的注意。这可能是社会日益分裂和紧张局势加剧的衍生结果。




SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG125588KLSPPP166161

供应商指引

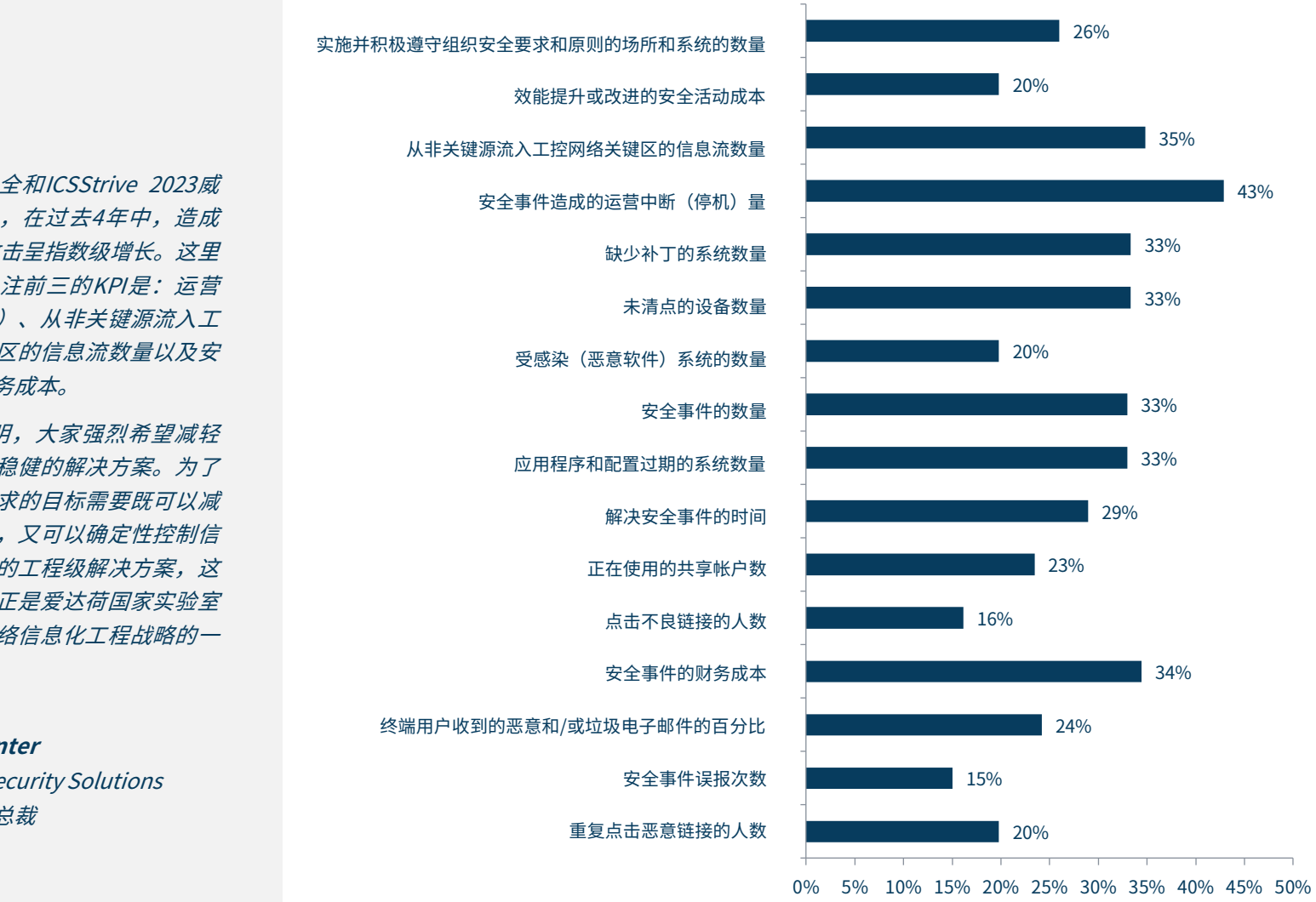
客户KPI关注指引
——供应商

Waterfall安全和ICSStrive 2023威胁报告显示，在过去4年中，造成OT后果的攻击呈指数级增长。这里我们看到关注前三的KPI是：运营中断（停机）、从非关键源流入工控网络关键区的信息流数量以及安全事件的财务成本。

这些KPI表明，大家强烈希望减轻后果并部署稳健的解决方案。为了达成这些追求的目标需要既可以减轻物理后果，又可以确定性控制信息流的强大的工程级解决方案，这些解决方案正是爱达荷国家实验室领导的新网络信息化工程战略的一部分。

Andrew Ginter
Waterfall Security Solutions
工业安全副总裁

未来一年客户关注的安全计划KPI

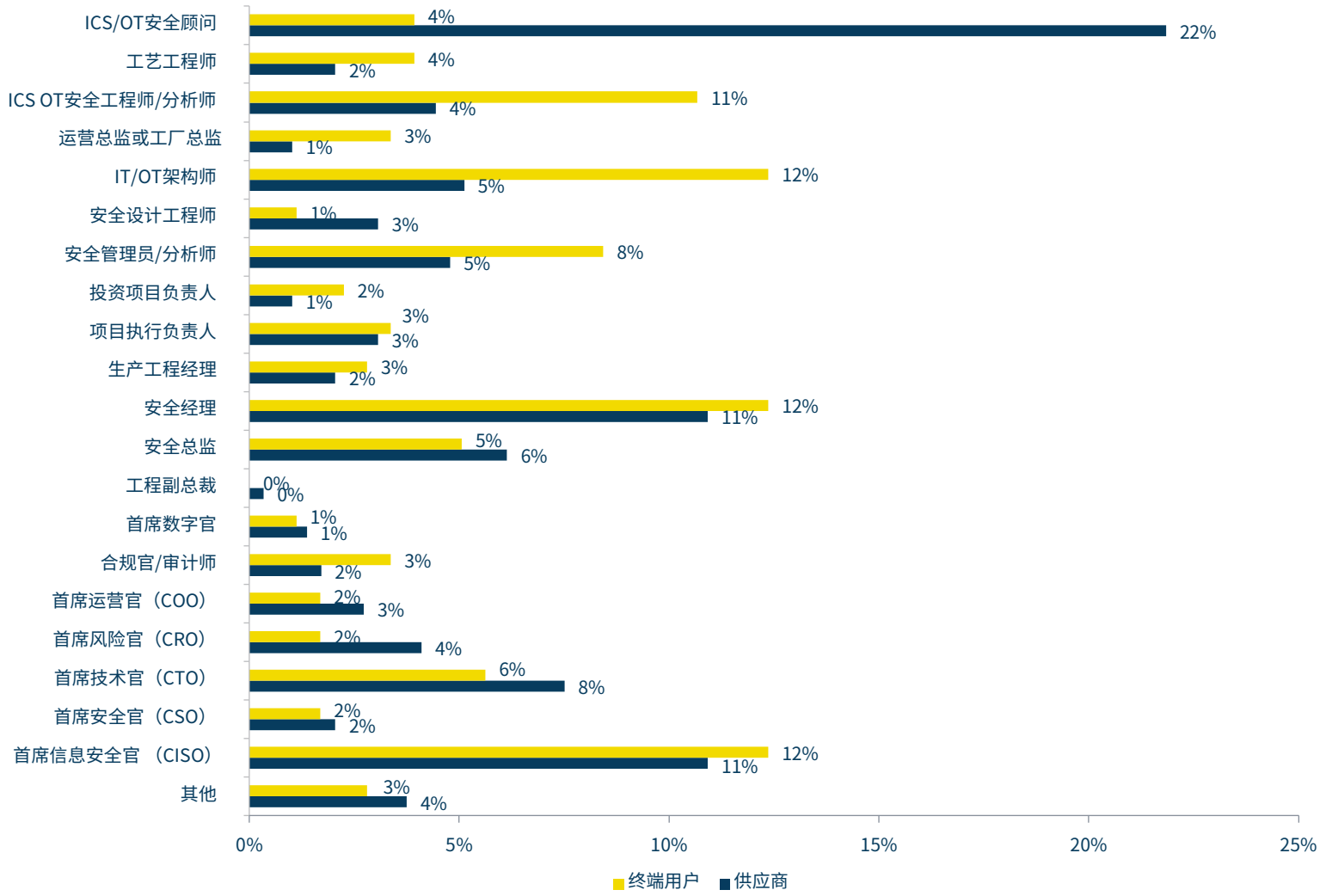



SERVER ROOM ASSISTANT
12-8976-3457-567
1 ACCESS CATEGORY
FG12558RKLSPPP166161

附录A：受访者组成

受访者职位
——终端用户和供应商

与控制系统安全相关工作有关的受访者职位分布

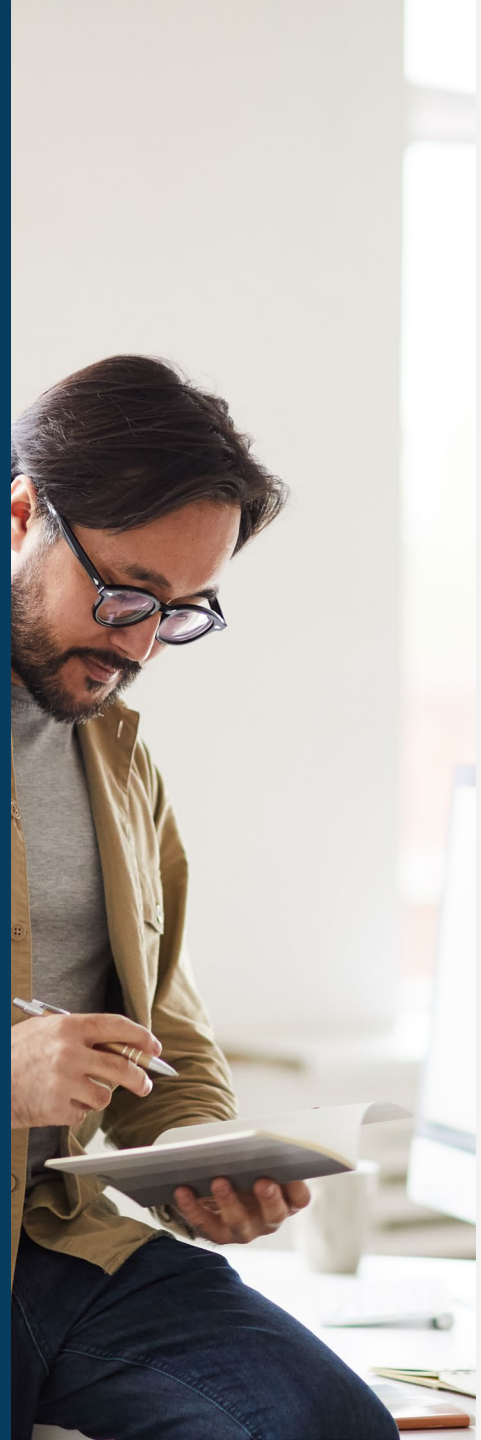


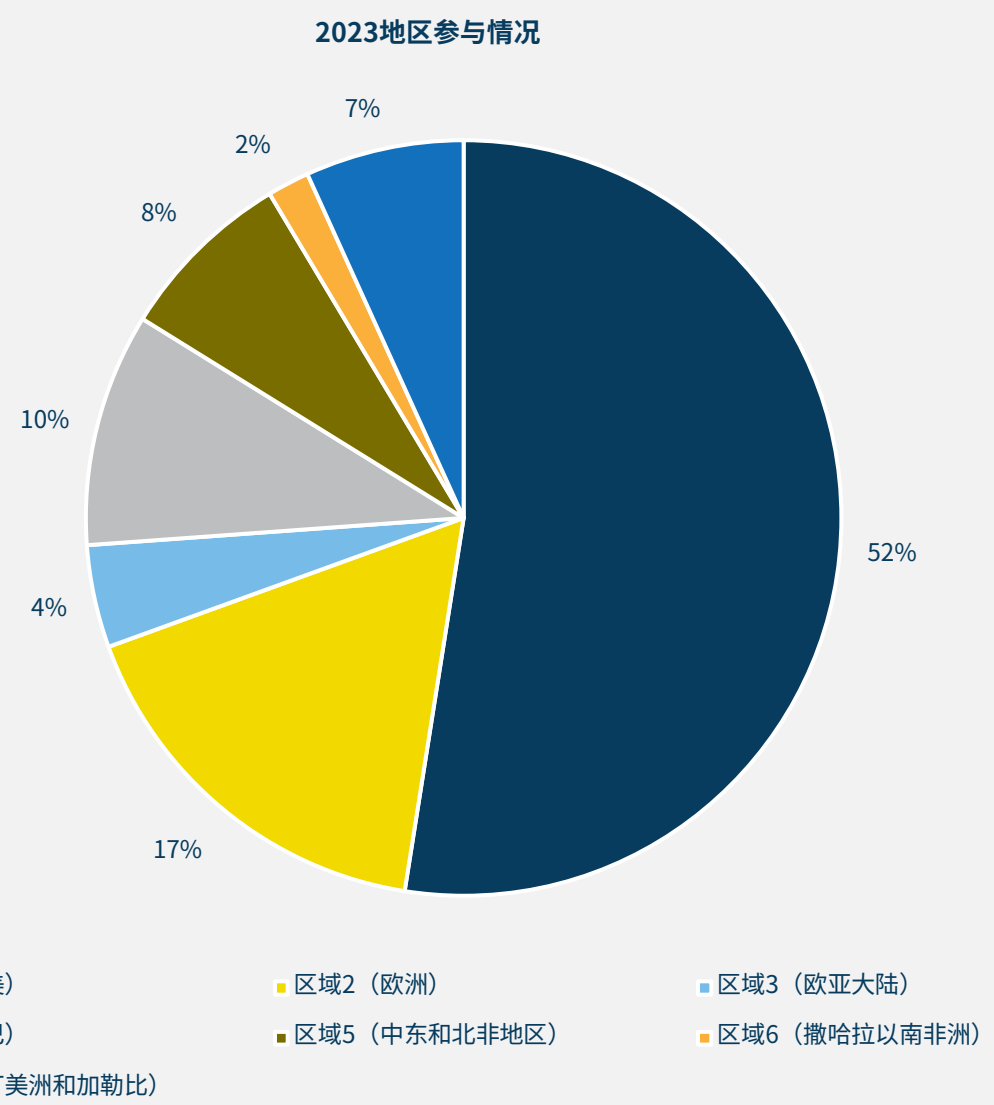
受访者区域分布

(CS)²AI将组织划分成七个区域：

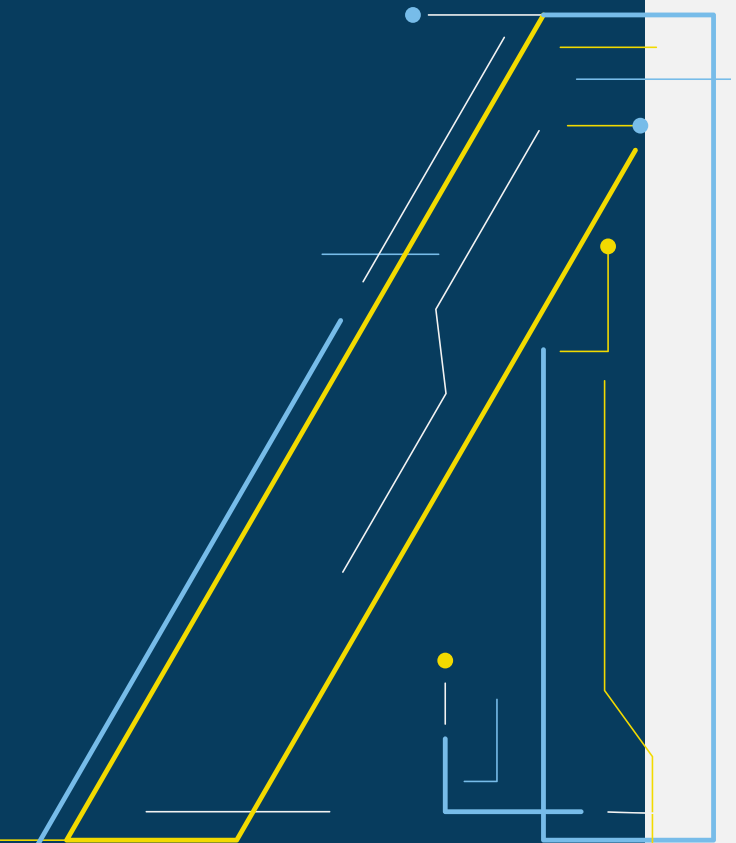
1. 北美；
2. 欧洲（中部、西部、北部和南部）；
3. 欧亚大陆；
4. 印度太平洋；
5. 中东-北非；
6. 南部非洲；
7. 拉丁美洲-加勒比

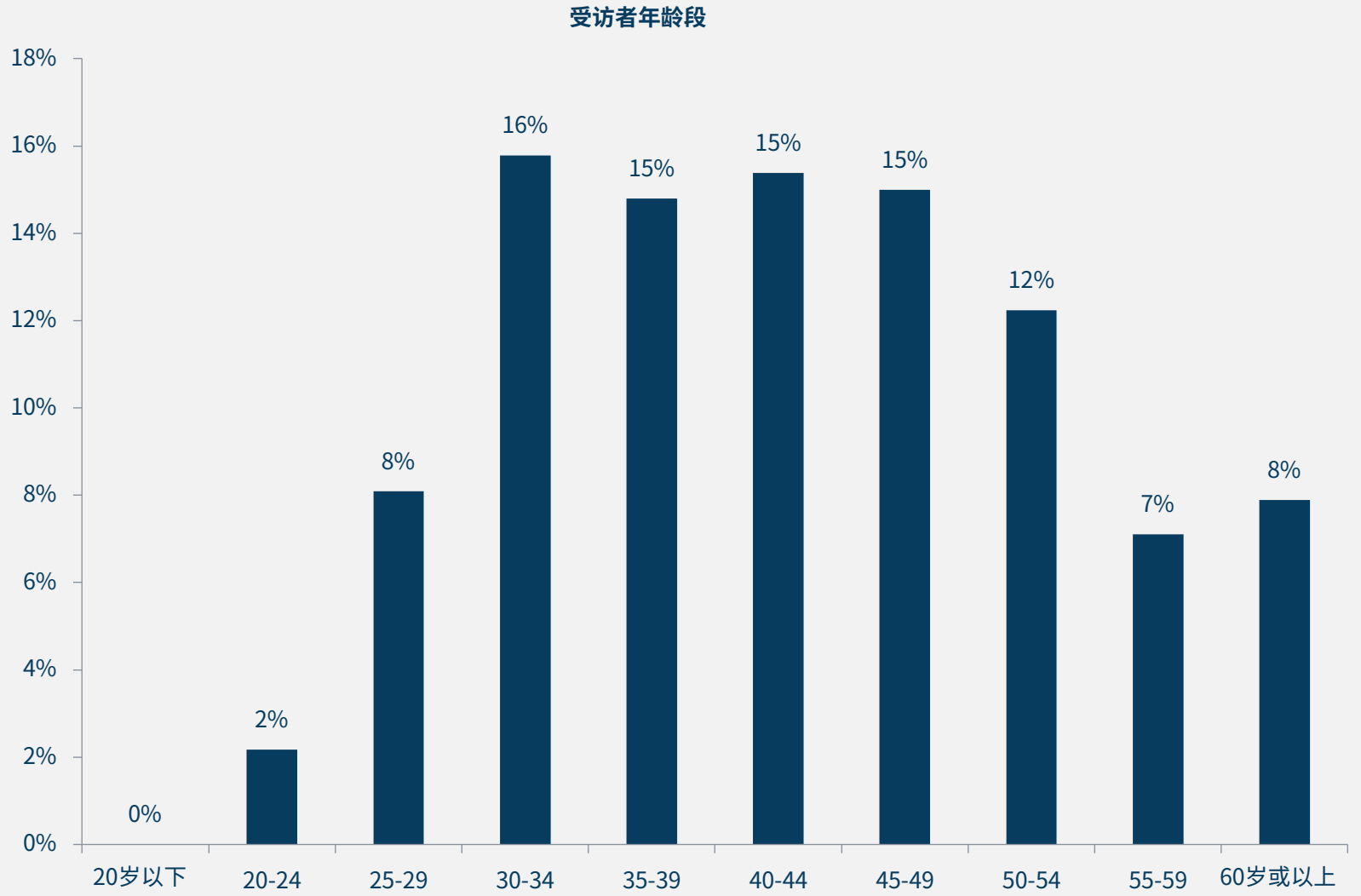
今年，第2、5和7地区的代表人数有所增加。我们的持续目标是增加所有地区的参与度，以获得充分的数据，进行统计分析，并希望接触到更多(CS)²信息的消费者，无论是一线从业人员、经理、高管还是学生。





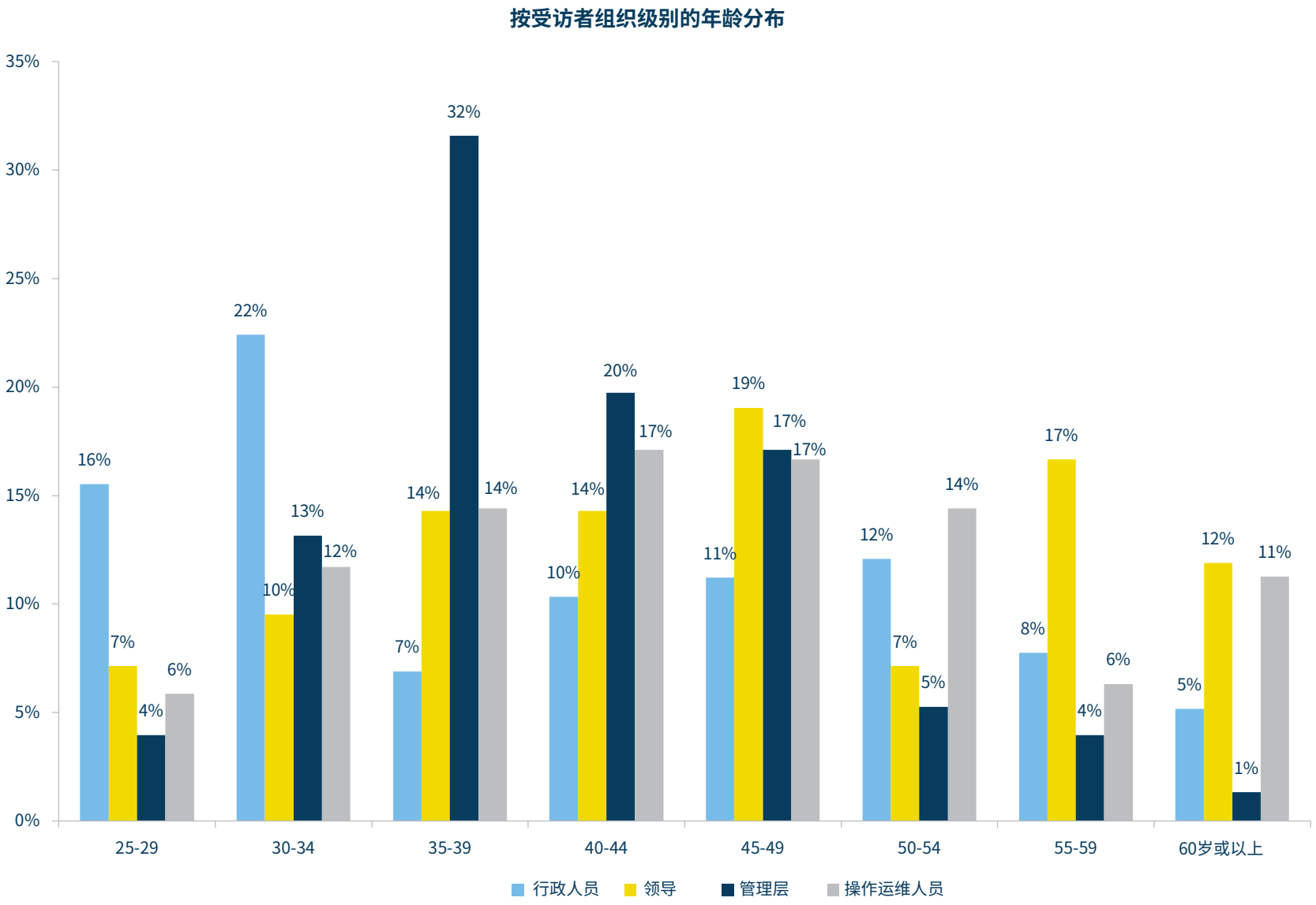
受访者年龄分布




受访者年龄段
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
0%
2%
8%
16%
15%
15%
15%
12%
7%
8%
20岁以下
20-24
25-29
30-34
35-39
40-44
45-49
50-54
55-59
60岁或以上

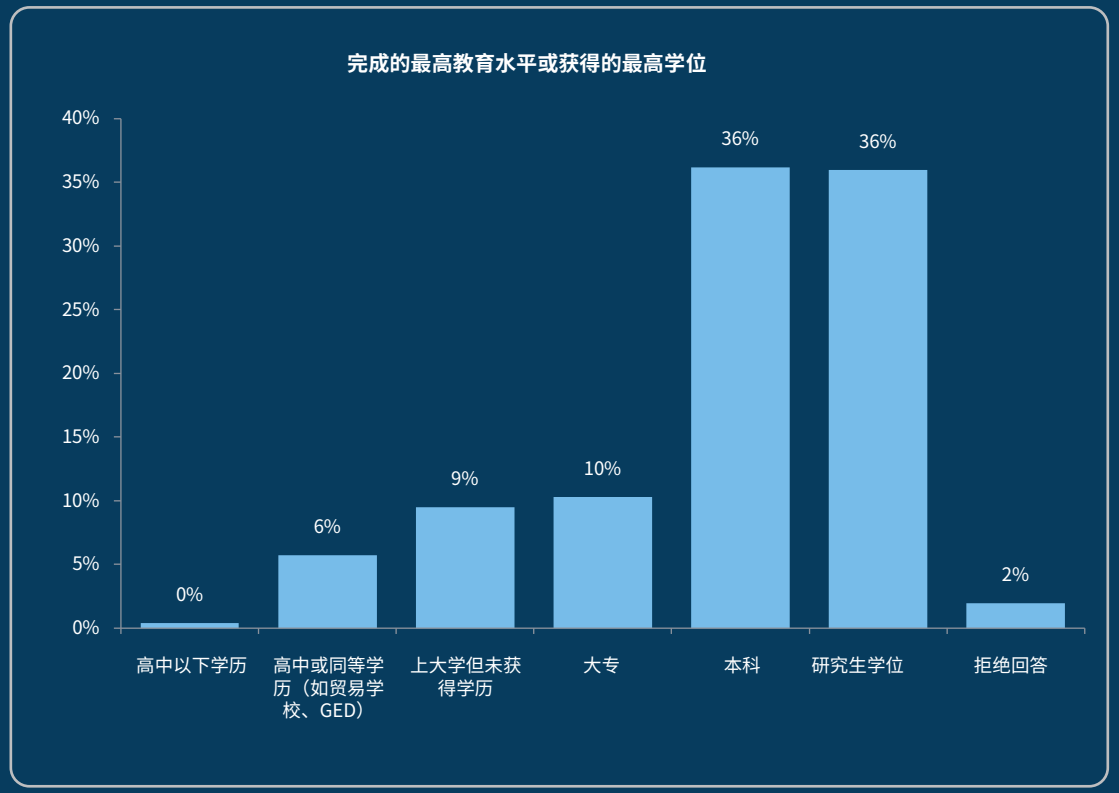
按受访者组织级别的年龄分布

绝大多数受访者（N>60%）的年龄段是30-50岁。我们倾向于将重点放在运营团队上，因为他们最直接地与资产/系统打交道，是技术知识和专业技能的重要储备库，当他们退休时，这些知识和专业技能也会随之留下。保持代际储备，同时与时俱进，对于维护和改进我们控制系统的保护工作至关重要。因此，处于职业生涯中早期的群体，即那些向更资深人员学习的群体，能够有如此多的代表，是一件好事。



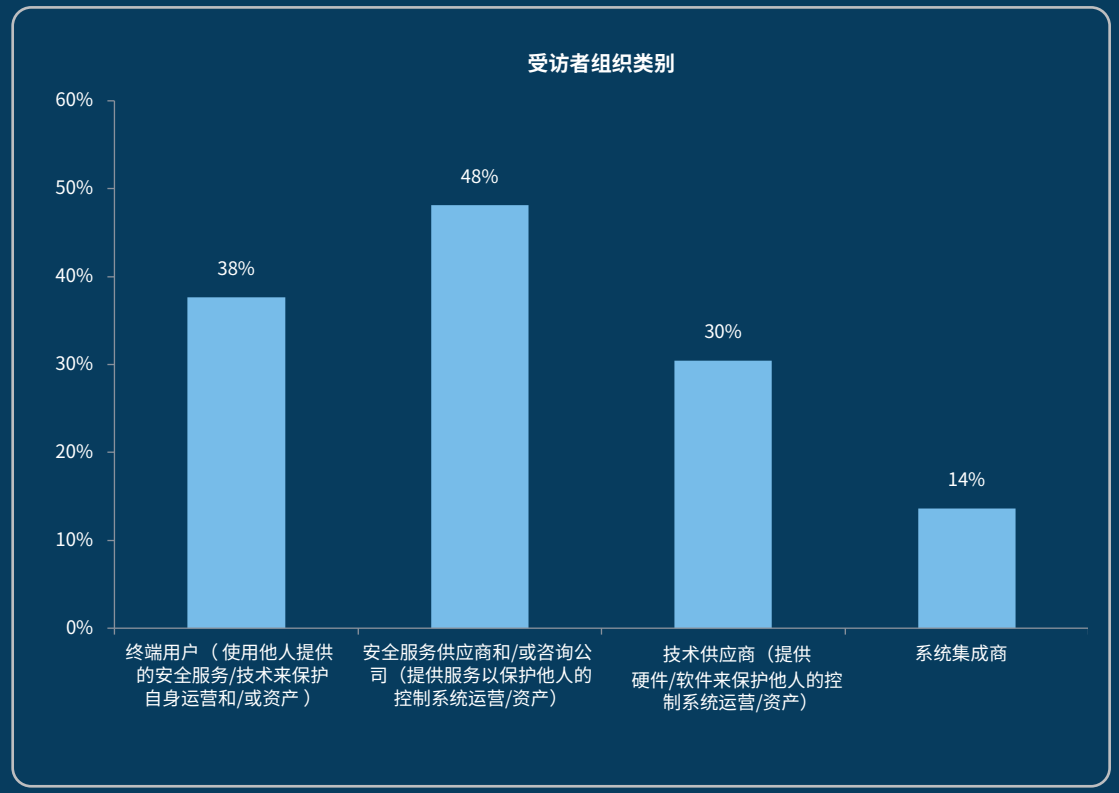
受访者教育水平

参与者的教育情况与前几年非常相似。



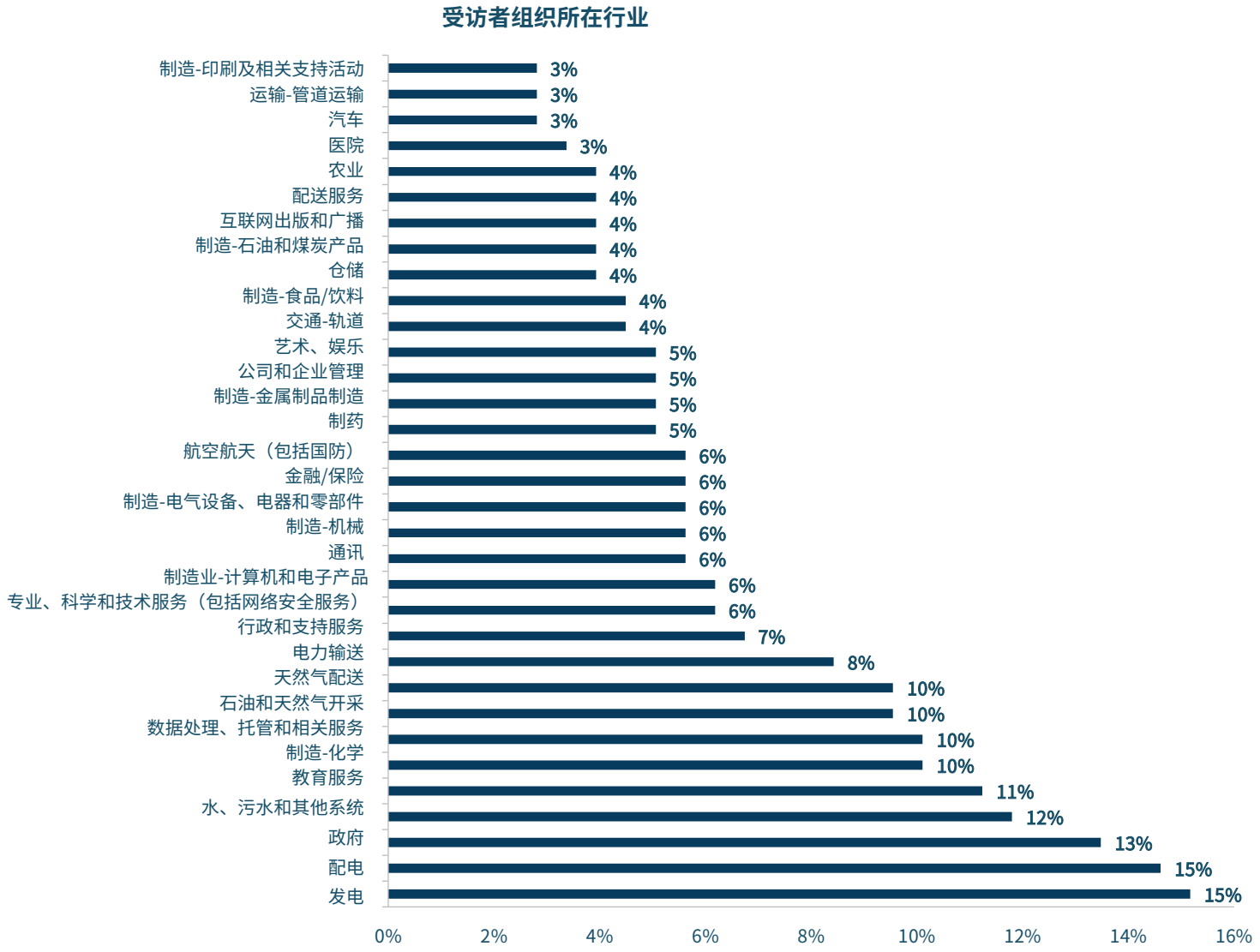
受访者所在公司类别

最终用户和技术供应商之间的百分比差异几乎相等（欧盟下降了10个百分点，技术供应商上涨了7个百分点）。系统集成商是今年的一个新类别。所有适用类别都会做统计，因此比例总和远超过100%。当然，今年还有一个“其他”类别，收到了5%的回复。



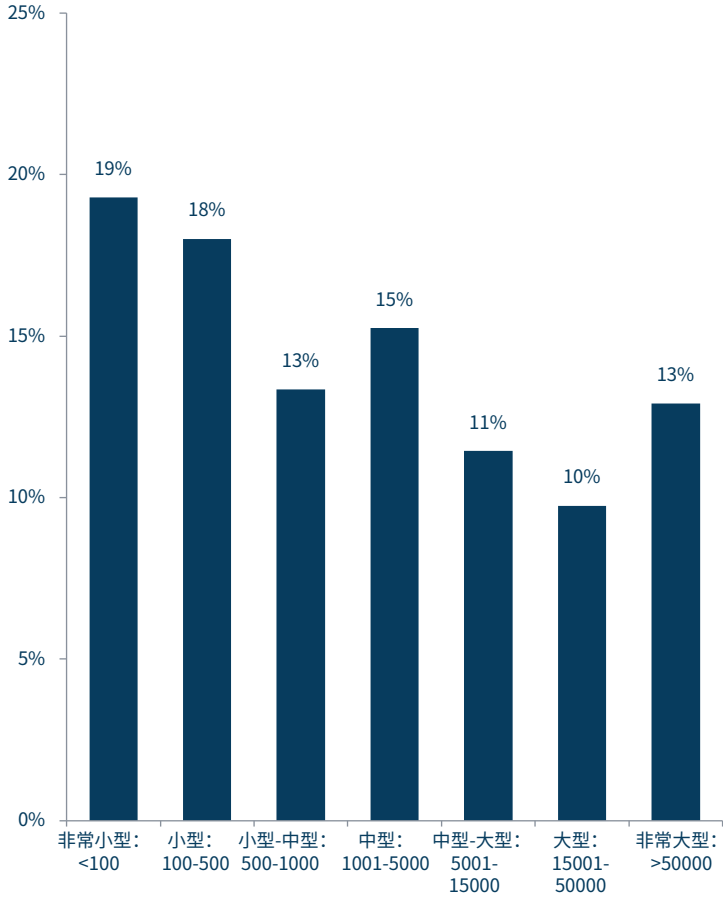
受访者所在行业（仅限终端用户）

组织从哪里可以找到保护其(CS)²资产、人员和运营所需的援助？根据我们的受访者的说法，他们无处不在。内部IT安全资源（56.2%）的突出响应表明，OT网络安全是由大多数组织的IT团队推动的，随之而来的是IT安全方法和技术可能被应用于这些环境。



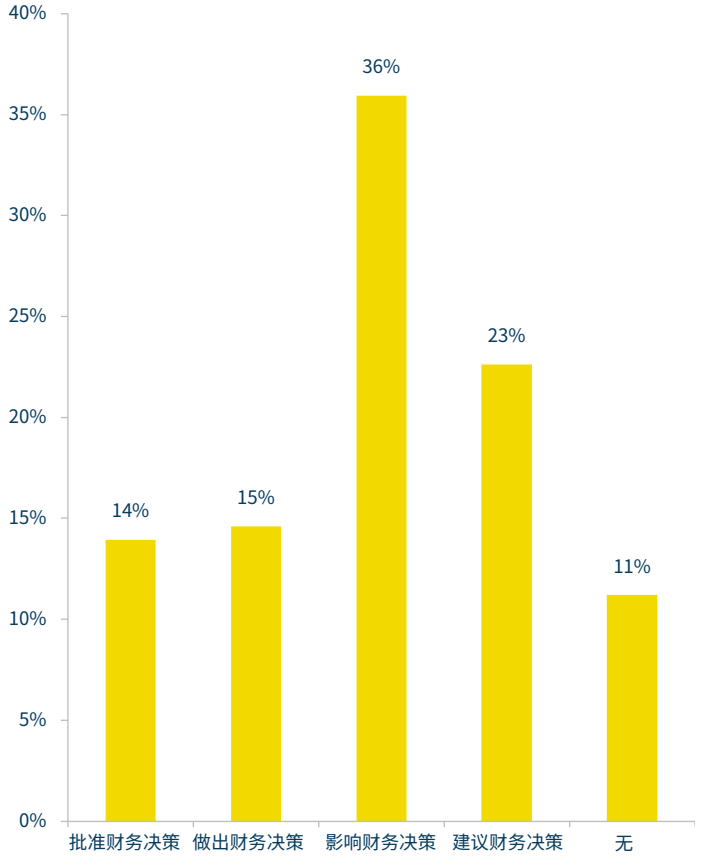
受访者组织规模

组织劳动力规模的适当估算



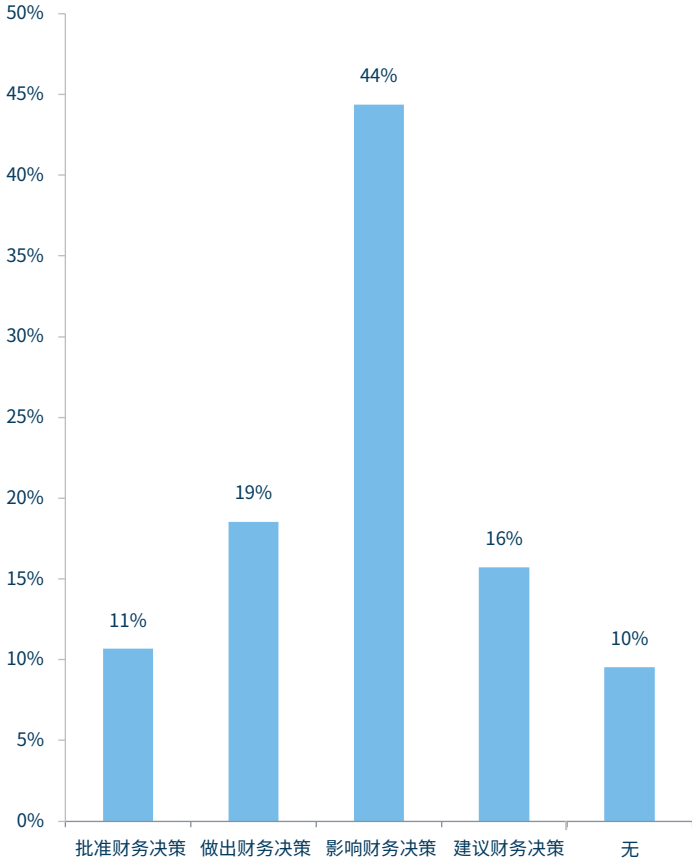
受访者决策角色

在控制系统安全相关支出决策中角色

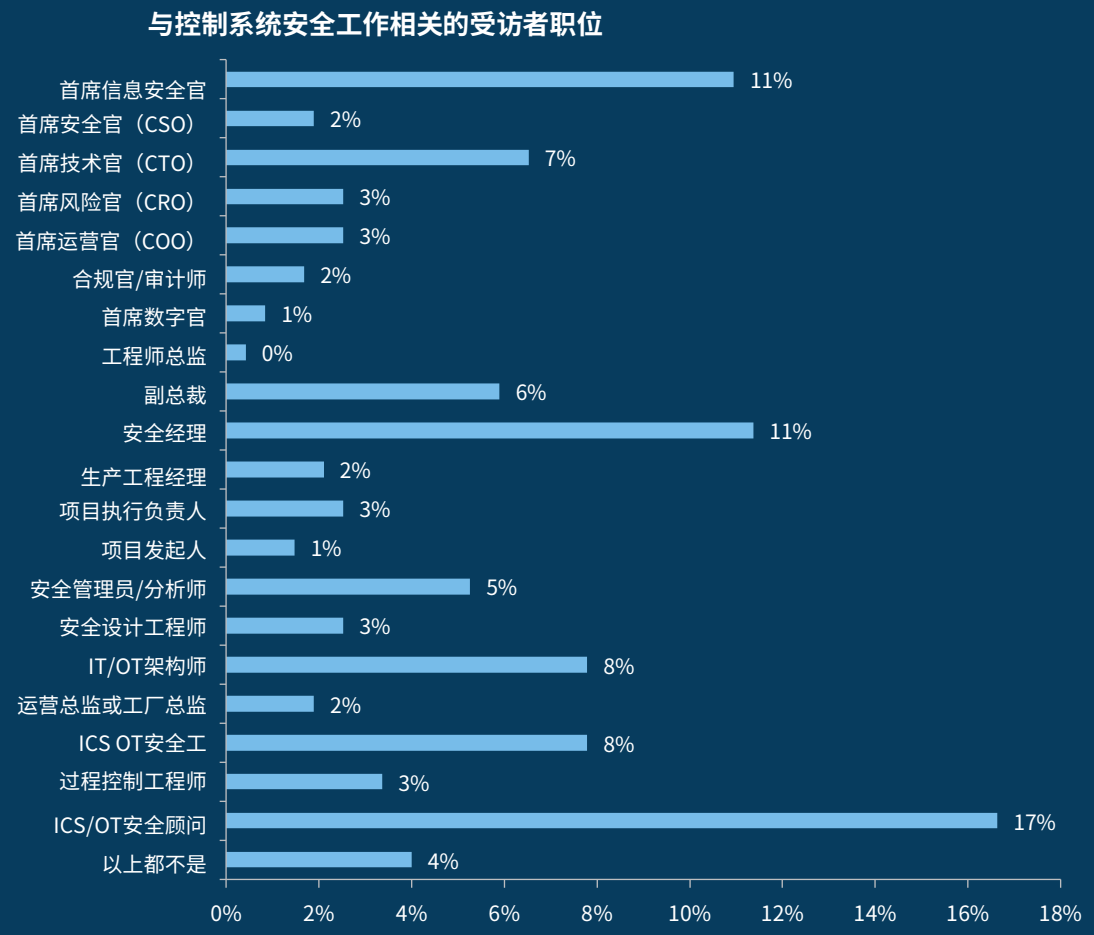


受访者决策角色——仅限终端用户

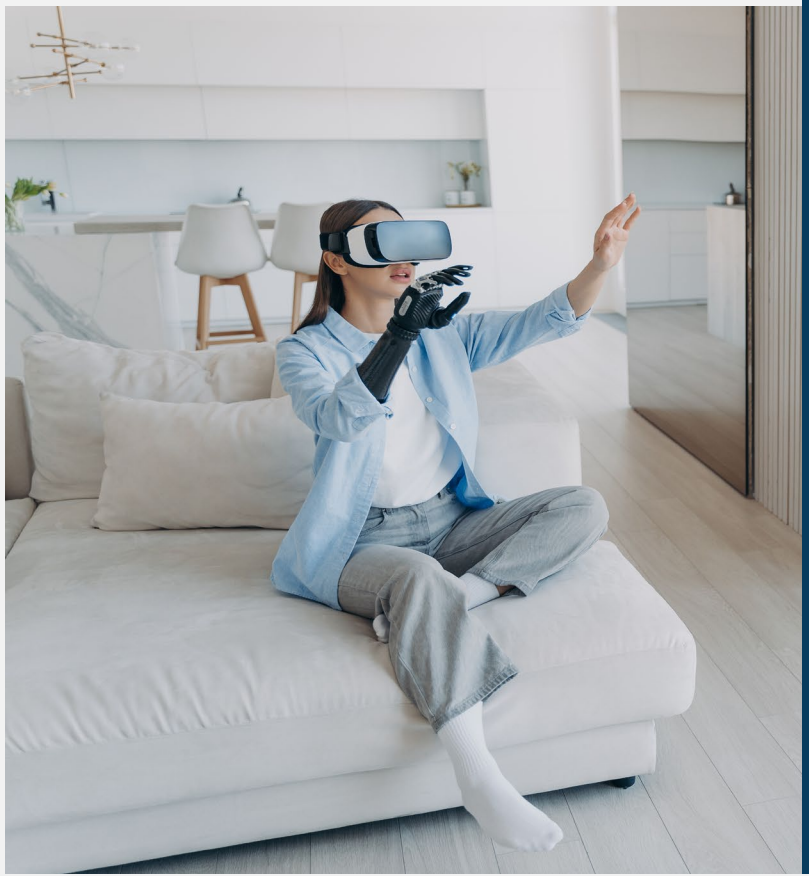
参与控制系统安全相关支出决策的人员角色（仅限终端用户）

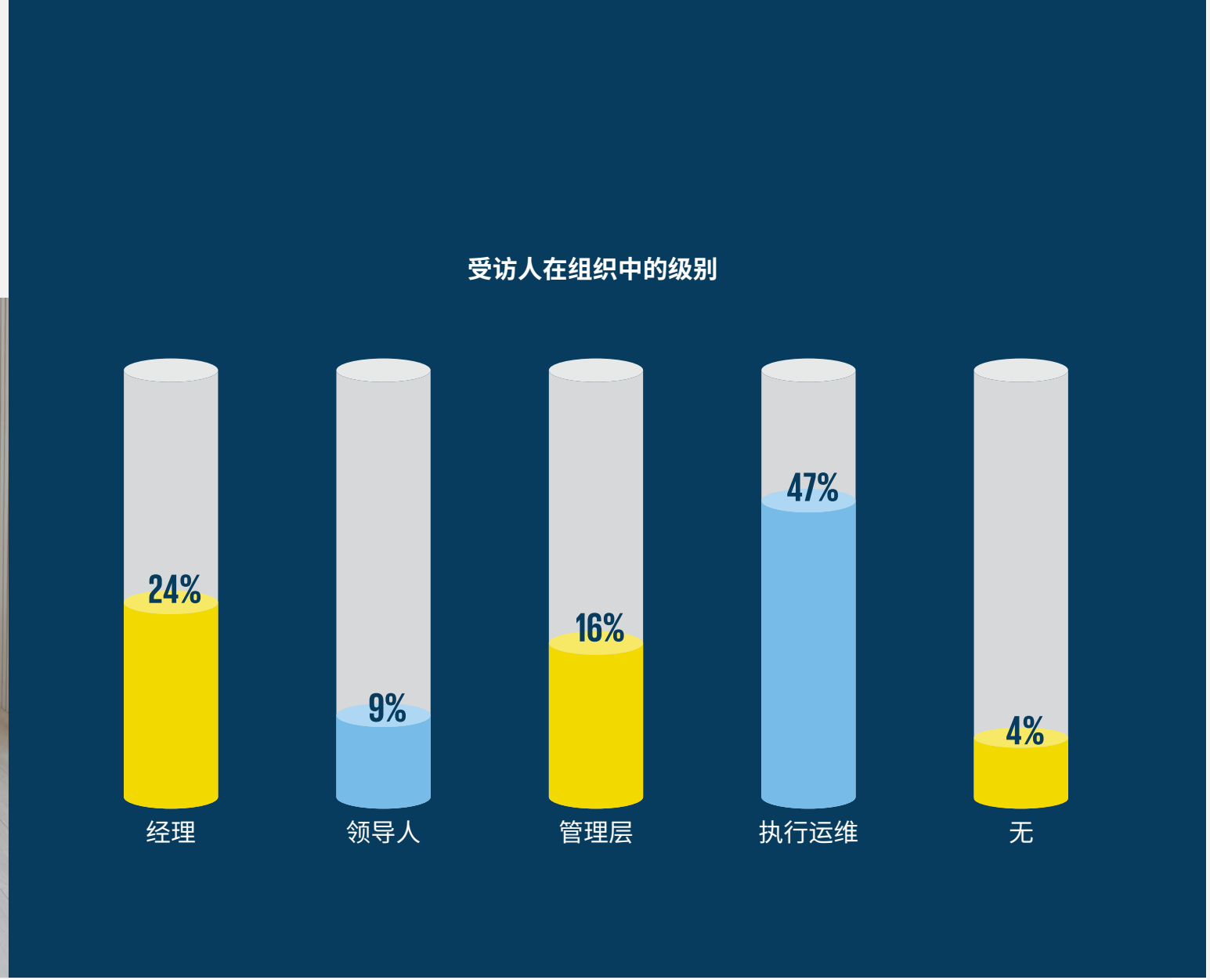


受访者的职务和组织级别



受访者的职务和组织级别（续）





附录B：
年度报告指导委员会及撰稿人

德里克·哈普

(CS)²AI创始人兼主席

年度调查与报告主席、联合作者

derek.harp@cs²ai.org

本特·格利高里-布朗

(CS)²AI联合创始人兼总裁

年度调查与报告总监、首席设计师和分析师、联合作者

bengt.gregory-brown@cs²ai

瓦尔特·里西

(CS)²AI战略联盟合作伙伴联络员

调查设计和报告分析团队

全球OT网络安全负责人

毕马威国际全球OT网络安全负责人，毕马威阿根廷咨询业务主管合伙人

wrisi@kpmg.com.ar

安德鲁·金特

调查设计和报告分析小组

(CS)²AI创始研究员

瀑布式安全解决方案工业安全副总裁

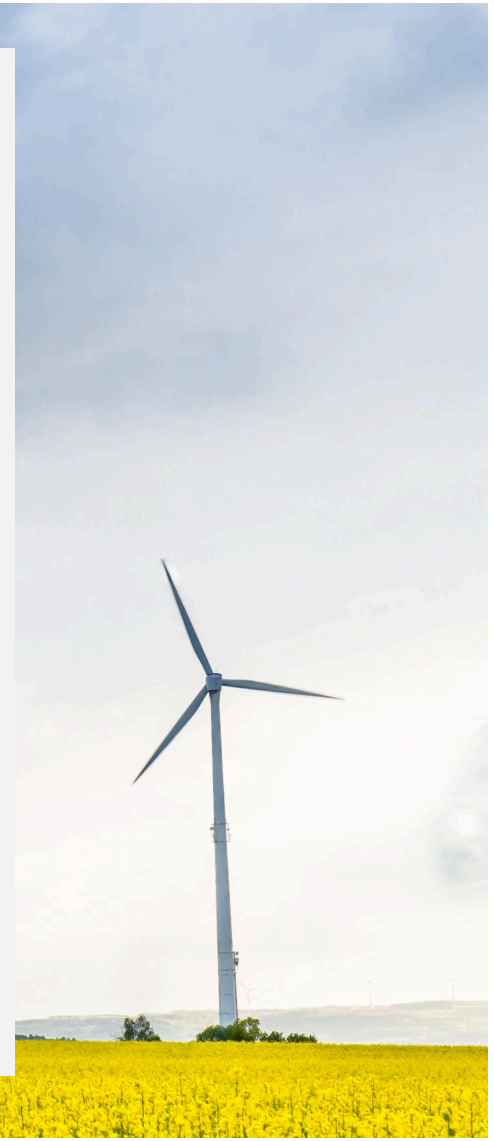
作者兼讲师

andrew.ginter@waterfall-security.com

我们要感谢以下人员为本报告的分析、设计和其他工作所做的贡献

Ana Girdner - Cognite 安全副总裁
Brent Huston - MicroSolved 首席执行官
Daryl Haegley - 美国国防部控制系统网络弹性技术总监
Mark Bristow - CIPIC MITRE董事
Michael Chipley - PMC集团总裁
Rees Machtemes - Waterfall安全解决方案工业安全总监
Rod Locke - Fortinet集团产品管理总监
Steve Mustard - National Automation总裁兼首席执行官
Vivek Ponnada - Nozomi Networks技术解决方案总监

Anish Mitra - 毕马威印度总监
Hossain Alshedoki – 毕马威沙特阿拉伯总监
Jayne Goble - 毕马威英国总监
Craig Morris - 毕马威澳大利亚总监
Joshua Turner - 毕马威日本顾问
Brad Raiford - 毕马威美国总监
Pablo Almada - 毕马威阿根廷合伙人
Thomas Gronenwald - 毕马威德国高级经理
Marko Vogel - 毕马威德国合伙人
Eddie Toh - 毕马威新加坡合伙人
Sarah Puzewicz - 毕马威德国高级助理
Valentin Steinforth – 毕马威德国网络安全顾问



附录C：关于(CS)²AI

愿景

通过促进控制系统网络安全对等网络和发展，加强全球关键基础设施。

使命

一个支持对等组织并支持其基层努力的国际组织。

目标

- 专业网络
- 社区外联
- 全球联盟
- 领导机会
- 专业发展

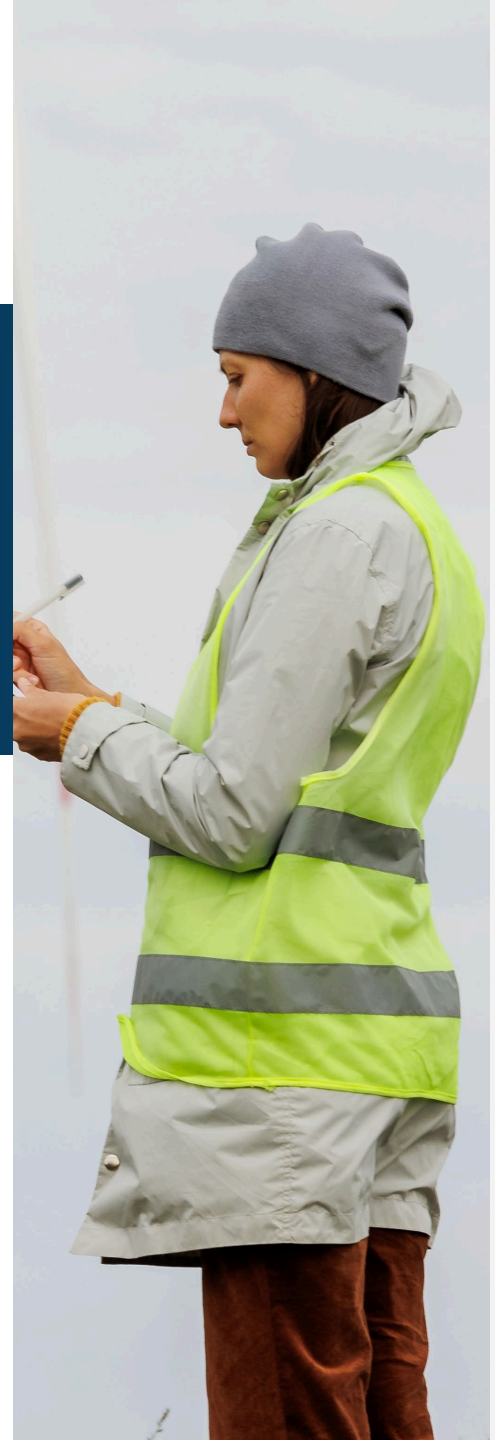
(CS)²AI是一个快速发展的全球非营利协会，在全球拥有3,4000名会员。全球首屈一指的非营利劳动力发展组织，支持负责确保控制系统安全的各级专业人员。我们为会员提供帮助会员的平台，促进有意义的同行交流，继续进行专业教育，并以各种方式直接支持网络安全专业发展。

https://www.cs2ai.org

全球范围内的点对点网络

作为(CS)²AI的成员，您加入了一个由控制系统网络安全从业人员组成的全球社区，他们有动力在这个高度关键和重要的领域改善和发展个人和专业。(CS)²AI提供了一个场所，用于点对点连接、与领先的行业专家进行小组互动、分享经验、挑战和最佳实践，以及开发和发展所需的资源。探索越来越多的独家(CS)²AI会员机会，旨在帮助您在职业生涯中达到更高的水平。

如果您还不是国际控制系统网络安全协会的活跃成员，我们邀请您今天就参与进来，加入我们的会员互助活动。我们的协会有很多方式可以作为全球成员、发言人、教师、导师、合作伙伴、贡献者、委员会成员、(CS)²AI Fellow或研究参与者做出贡献。



附录D：报告发起人

一级赞助商

KPMG

三级赞助商

Fortinet
Waterfall 安全解决方案

五级赞助商

Opscura
Network Perception

六级赞助商

Bridewell

联系我们

毕马威

张令琪
网络安全和数据保护咨询服务主管合伙人
毕马威中国
电话：+86 (21) 2212 3637
邮箱：richard.zhang@kpmg.com

郝长伟
网络安全和数据保护咨询服务合伙人
毕马威中国
电话：+86 (10) 8508 5498
邮箱：danny.hao@kpmg.com

黄芃芃
网络安全和数据保护咨询服务合伙人
毕马威中国
电话：+86 (21) 2212 2355
邮箱：quin.huang@kpmg.com

周文韬
网络安全和数据保护咨询服务合伙人
毕马威中国
电话：+86 (21) 2212 3149
邮箱：kevin.wt.zhou@kpmg.com

李振
网络安全和数据保护咨询服务总监
毕马威中国
电话：+86 (21) 8508 5397
邮箱：jz.li@kpmg.com

邬敏华
网络安全和数据保护咨询服务总监
毕马威中国
电话：+86 (21) 2212 3180
邮箱：fm.wu@kpmg.com

宋智佳
网络安全和数据保护咨询服务总监
毕马威中国
电话：+86 (21) 2212 3306
邮箱：jason.song@kpmg.com

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：https://home.kpmg/cn/zh/home/about/offices.html