Rockwell Automation

2022 年调查结果

关键基础设施网络安全就绪度：避免“大停摆”

目录

引言

关键基础设施领域正面临一场网络安全“完美风暴”。与日俱增的安全漏洞、新增和现有网络安全缺口、不断扩大的攻击面以及日益加剧的全球威胁令运营技术 (OT) 组织倍感压力。

资源充足、手段老练的威胁主体（如勒索软件团伙和民族国家黑客）都将关键基础设施组织列为目标。2021 年，受访的关键基础设施组织中有 83% 表示他们经历过网络安全攻击[1]。随着攻击不断升级，关键基础设施的弱点仍未得到缓解，“大停摆”（一场牵连甚广的大规模灾难）越来越可能成为现实。关键基础设施组织不能再坐以待毙。

为了解关键基础设施网络安全的现状，以及剖析各组织的就绪度和最佳实践，罗克韦尔自动化委托 ISMG 调查了多个关键基础设施行业的 IT 和网络安全领导者。报告中载列了我们的调查结果以及经验教训和建议。

根据 NIST 网络安全框架结构（识别、保护、检测、响应和恢复），我们将报告分为五个核心主题。罗克韦尔自动化还将该框架用作评估和加强关键基础设施网络安全的基本路线图。

[1]Skybox Security（通过雅虎财经）：2021 网络安全研究显示，83% 的关键基础设施组织遭受过攻击，2021 年 11 月 11 日

执行摘要

意图造成严重破坏或获得快速投资回报的威胁主体发现关键基础设施组织是一个极具吸引力的目标。比如，勒索团伙就经常将公用事业、能源、石油和天然气公司作为攻击目标。他们在所有领域中最有可能支付赎金[2]，因为承担不起任何停摆风险。

IT 和 OT 环境的复杂性也使这些组织更难恢复，停摆的危害可能非常大，包括设备停机、财务损失以及对公共安全和福祉造成的威胁。

ISMG 调查显示，关键基础设施组织正朝着正确的方向发展。他们正在采取措施来改善网络安全就绪度和弹性。但调查也显示，面对紧迫的网络安全挑战，他们的进展过于缓慢。许多组织都在努力克服各种障碍，如预算和人才短缺、管理缺乏优先级排序，以及在关于如何改善防御体系方面缺乏真知灼见。

大多数组织尚未实施资产清单评估、网络分段和威胁监测等基本步骤，或者在这些方面明显落后。因此，关键基础设施中仍普遍存在漏洞。

业务和安全领导力方面的主要发现包括：

1. **关键基础设施组织仍然极易受到网络攻击。**调查发现，在资产清单监控、远程访问管理、补丁管理、端点安全、网络分段、事件响应与恢复规划、供应链安全评估以及员工安全意识等高优先级领域存在重大防范缺口。例如，在受访组织中，资产清单审计频率的达标率不到 20%。只有 1/3 的组织实施有效的 OT 补丁管理实践。而且，持续威胁检测方面尚属空白，60% 的组织缺乏实时威胁检测措施。机械制造行业尤其突出，只有 37% 的受访组织表示在所有问题上都采取了应对措施。令人震惊的是，剩下 63% 的组织毫无准备，灾难性后果的到来只是时间问题。
2. **弥合防范缺口必须成为当务之急。**最近公开的攻击事件表明，网络攻击会造成高昂的停机成本，并且不仅会导致运营瘫痪，还会扰乱日常生活。水、食品、石油和天然气、医疗和运输等具有公共安全影响风险的行业的 OT（运营技术）ICS（工业控制系统）网络所面临的攻击数量和强度不断增加，而关键基础设施组织的行动速度不够快，无法降低这些风险。例如，目前只有 56% 的受访组织能够分析、控制和缓解即将到来的威胁。
3. **预算不足也会增加风险并阻碍进程。**安全负责人指出，缺乏资金阻碍了他们应用已知风险降低工具和流程（如资产清单评估和补丁管理）的能力。鉴于网络攻击的威胁趋势和潜在危害，各组织必须认识到，不作为（或行动太慢）的代价可能会严重影响正常运行时间，破坏系统防御，并最终影响最终客户、经济乃至国家安全。
4. **组织缺乏高瞻远瞩。**美国政府正在重点聚焦网络安全，特别是在地缘政治风险上升之际。为帮助弥合缺口，联邦政府计划为关键基础设施组织提供 10 亿美元网络安全拨款，但只有不到 30% 的受访组织部署了网络安全计划来帮助识别关键网络安全缺口和支持撰写拨款申请书。
5. **关键基础设施组织必须迅速行动起来。**基于这些发现，罗克韦尔自动化的网络安全专业人员建议实施以下核心步骤：
   - 执行准确的风险和漏洞评估，找出最薄弱的环节。
   - 根据评估结果制定网络安全计划。
   - 通过 IDMZ（工业非军事隔离区）和防火墙分割和加固网络。
   - 实施威胁监控。
   - 准备事件响应计划并进行演练。

调查统计数据

调查于 2022 年 1 月开展，共收到 122 份回复。ISMG 向高级工业安全负责人（其职务从 CISO 和安全负责人到工厂工程师和业务经理不等）征求了答案。CISO 和安全总监或负责人是最大的两个群体，占比分别达到近 25% 和 19%。

受访组织所代表的行业涵盖近 20 个 OT 垂直行业，其中 57% 代表包括石油和天然气、能源、化工、供水/废水处理垂直领域在内的关键基础设施组织。单一垂直领域的制造业组织的回复数量最多，达到 18%。

[2] Sophos，“2021 年勒索软件现状”，2021 年 4 月

第 1 部分

识别和评估风险

近年来，关键基础设施安全愈加复杂。威胁主体正在投入大量资源，企图了解新的互联关键基础设施系统及网络运行方式，并找出可以被他们利用的弱点。但是，关键基础设施运营商在获取所需可见性方面始终落后，也就很难识别风险和确定防御策略优先级。

为了避免发生“大停摆”，关键基础设施组织需要立即采取紧急措施，了解风险并弥合防范缺口。

资产清单评估

资产清单审计是风险评估中至关重要的第一步。这也是组织在获得正确见解和正确报告频率方面举步维艰的领域。正如一家受访组织所分享的：“资产盘点真的很难保持。虚拟机可以在不经意间建立和移除，治理团队甚至都不知道它存在过。”

在参与调查的组织中，既有资产清单评估的最常见频率不到每季度一次，只有近 30% 的受访组织达到此频率。这样的节奏在三个关键行业（机械制造行业；医疗保健、公共卫生和应急服务行业；以及制药和化学品行业）中也是最常见的。

总体来说，45% 的组织每季度监测一次资产清单，不到 1/5 的组织每天进行一次审计，这是罗克韦尔自动化建议的最低频率。

这一步为何至关重要？

每台未知设备都会在您的网络中形成一个脆弱的突破口。放在几年前，每季度甚至每月评估一次可能就已经足够。而现在，随着攻击速度的提高，在大多数情况下，每日检查已必不可少，一些受访组织表示，他们正在努力向实时评估过渡，这一点在合适的网络设计和监控工具到位的情况下是可以实现的。

我们还发现，组织对既有资产清单评估的认识存在脱节现象。受访的 C 级高管（如 CIO、CEO、COO）很可能认为评估执行频率可以达到每小时一次、每天一次或每周一次。但是，更了解安全运营日常情况的技术人员（例如，安全负责人、IT 总监和架构师或工程师）却不那么乐观，他们一致表示最多只有每月一次、每季度一次，甚至更少。

建议

自动资产盘点可以预防或阻止因缺乏可见性而导致的攻击。有多种自动工具和服务可用于简化 IT 和 OT 的资产清单评估流程，只要执行频率在您的风险容忍能力阈值范围内即可。关键基础设施组织对大众的影响超乎想象，而实时资产盘点对他们而言是一种谨慎策略，可以提供完整的网络资产可见性。

业务关键系统

我们的调查发现，只有 56% 的组织能够识别业务关键系统并设立其优先级，表明了这是一项紧迫任务（图 1）。此外，根据罗克韦尔自动化经验，一些组织低估了其业务关键系统保护措施的有效性。调查评论也反映出了些许不明确性，一家受访组织指出，其已经用强大的安全软件解决了这一问题。

事实上，部署通用的网络安全控制方法可能无法为高度关键系统提供所需的保护级别。最高关键度的运营和业务系统通常必须通过额外的网络分段、身份与访问控制（如多重认证及相关措施）来加强。首先确定关键度及其优先级，这样可以确保妥善应用附加安全策略逐个系统地解决风险。

零信任是所有行业中应用越来越多的安全最佳实践。它还受到了美国联邦政府的重视，要求关键基础设施组织予以实施，确保在识别业务关键系统这一步骤中发挥作用。

零信任并不是一种“孤注一掷”的安全模型，它可以从多个角度实施并逐渐应用，甚至可以细分为更小的步骤。这一渐进过程的关键一步是确定对组织最重要的事项并设定优先级，从而生成洞察，将零信任控制置于最需要的位置。

是否识别了
业务关键系统及其优先级？

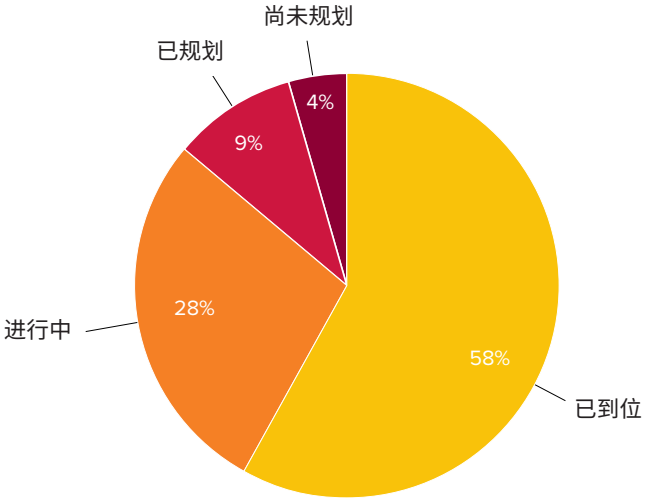


图 1

建议

借鉴零信任战略，检查组织的所有 DAAS 元素（数据、资产、应用程序和服务），并根据关键度确定每个元素的优先级。这些都是组织的“保护面”，每一个都按照优先顺序应用了正确的网络安全控制措施。

在关键基础设施中，ICS 和生产线应用程序与数据可能都属于典型的业务关键系统。咨询您的业务、运营、IT 和安全团队，如果这些系统因为勒索软件攻击被锁定，会有什么后果；什么样的系统能够改善生产运营、数据安全性或完整性、通信、供应链连续性，或者仅仅是向客户提供服务的能力 —— 解答这些问题能够帮助您进行优先级排序。

第 2 部分

保护和实施保障措施

数字化转型、流程数字化和物联网技术以及由此产生的 OT 和 IT 融合提高了关键基础设施的效率和可靠性，使供应商能够更好地为公众服务，并提高服务效率。

虽然这方面的发展是积极的，却也让关键基础设施组织面临新的威胁和漏洞，因为传感器和设备、远程工作者、第三方 API 和未采取保护措施的可编程逻辑控制器、网关、执行器以及许多其他组件使得企业资产更易于暴露在互联网中。

OT 系统的安全控制与 IT 实践不同，因为许多 OT 组件通常连基本的保护措施都没有。传统生产控制系统甚至无法进行修补，就算可以，也无法达到 IT 系统的正常修补速度，况且工厂车间还有其他现实问题。

此外，OT 安全越来越多地被归入 CISO 的职责范围，但许多 CISO 并不完全理解 OT 管理以及物联网安全的含义。另一方面，工厂的工程设计负责人必须确保正常运行时间，不能轻易长时间关闭 OT 网络以修补安全漏洞，尤其是在业务繁忙期。

或许这就是调查结果（目前只有 28% 的受访组织拥有 IT/OT 融合安全路线图，另有 35% 表示这一步骤正在进行中）背后的原因。关键基础设施组织应以机械制造业为榜样，在该行业中，84% 的受访组织表示已经实现了 IT/OT 融合或已将其纳入路线图。显然，其他领域要迎头赶上还有很大的距离。

尽管如此，融合进程仍将继续。为了创建稳健的融合路线图，IT 和 OT 领导层需要一起探索真正的联合规划过程。罗克韦尔自动化通常建议客户留出一整周时间，让经验丰富的过程先驱人士引导两支团队确定所有安全要素、障碍和要求。在进行重要决策时，这种方法可以帮助您赢得所有相关利益者的支持。

有些客户还创建了网络安全卓越中心 (COE)，让 IT、OT 和业务利益相关者群体持续合作以创建工作系统，并在出现新问题时一起进行故障排除。

安全远程访问

威胁主体会利用任何能够在组织内部立足的手段。随着全球疫情推动行业向纯远程办公或混合办公的转变，以及人员整体流动性的加剧，安全措施不够充分的远程访问极易成为攻击目标。

远程访问系统往往使用过时的安防策略，通常只通过密码提供保护，并没有部署多重身份验证 (MFA) 功能。在公用事业、石油/天然气开采和采矿领域，登陆凭据是最经常被泄露的数据类型[3]，而暗网上拥有大量被盗和被泄露的凭据，这使得黑帽黑客很容易破解远程访问系统。因此，尽管 69% 的受访组织报告说已经部署了安全远程访问，但在能否提供足够的远程访问保护方面，调查结果可能具有误导性。

就这一点而言，新冠疫情带来的不仅仅是挑战，还有良机。一家受访组织指出，混合办公模式不利于巩固强化远程访问，而另一家受访组织则表示，在新冠疫情期间已经成为标准的“任意地点办公模式”迫使组织加强了关注。

建议

可靠的身份识别和访问管理 (IAM) 计划有利于零信任策略的实施。通过 IAM，可以知道谁在请求访问、要访问哪些应用程序和数据、从何处访问、使用什么设备访问以及在何时访问，同时还能对其他经批准的行为规范进行控制。这样一来，您就可以实施监控以及执行访问策略和控制了。集成 MFA 的 IAM 解决方案可以显著降低密码泄露威胁。

工业非军事隔离区 (IDMZ)

利用 IDMZ 在 ICS 与 OT 系统和 IT 之间采取“物理隔离”是网络网络安全设计的基线，有助于确保威胁主体在获得 IT 系统的访问权限时不会横向移动到 OT 网络和控制器，反之亦然。根据调查结果，约 50% 的组织已经在 OT 架构中部署 IDMZ，另有 25% 的组织正在开展此项工作（图 2）。

医疗保健、公共卫生领域和应急服务行业尤其落后，38% 的受访组织尚未规划 IDMZ，而就所有行业而言，这一比例为 16.5%。这些发现与罗克韦尔自动化在更广泛市场中见证的事实一致。

在网络安全领域，有 IDMZ 物理隔离不代表可以万事大吉，特别是在 OT 系统和物联网设备可以通过 IT 网络直接连接互联网之后。必须采取更多措施来构建强有力的安全防线。

在 OT 安全架构中实施工业非军事隔离区 (IDMZ) 方面进展如何？

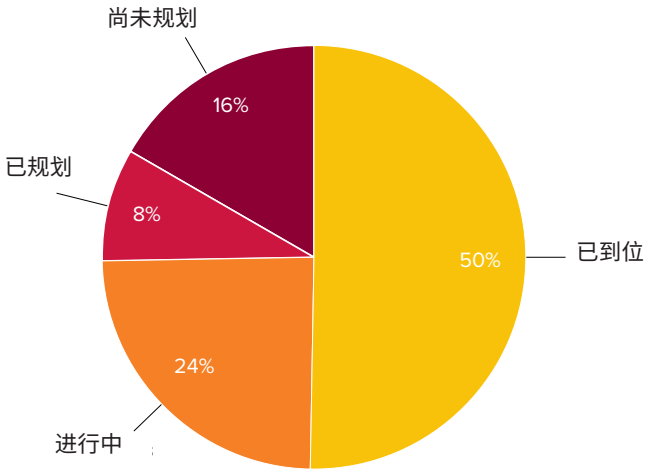


图 2

建议

要打造安全稳固的架构，需要将 IDMZ 作为基本最佳实践来实施。将 IT 和 OT 网络及资产彼此隔离，可以确保威胁主体无法在两个系统之间横向移动。但请记住，现代关键基础设施的安全架构中应纳入多层防御，这一点对于业务关键保护面以及所有联网资产尤为重要。

[3] Verizon，“2021 数据泄露调查报告”，2021 年 5 月

补丁管理

OT 修补工作是一块难啃的骨头。调查证实了该领域存在的常见问题：补丁管理要么不被视为重要实践，要么缺乏资金支持，要么过于复杂以致难以实施。在受访组织中，只有 37% 实施了有效的 OT 补丁管理，13% 甚至还没有规划修补方法（图 3）。

在机械制造业垂直领域，42% 的受访组织不具备有效的补丁管理方法，甚至没有开展这一步骤。美国和英国/爱尔兰的制造业以及中东和亚太地区的金融业取得的进展高于其他行业。

鉴于已知漏洞的严重性级别和潜藏的恶意软件风险，这些发现足以让所有行业感到恐慌。

许多 OT 系统因为功能有限和/或传统结构不支持嵌入安全组件等原因而无法正常进行修补。而且，当您拥有数十或数百台网络服务器时，每次修补工作还可能占用一整天时间，而停机成本又非常高昂，因此工厂运营商历来抗拒 IT 修补方法。

实现有效的 OT 补丁管理方面进展如何？

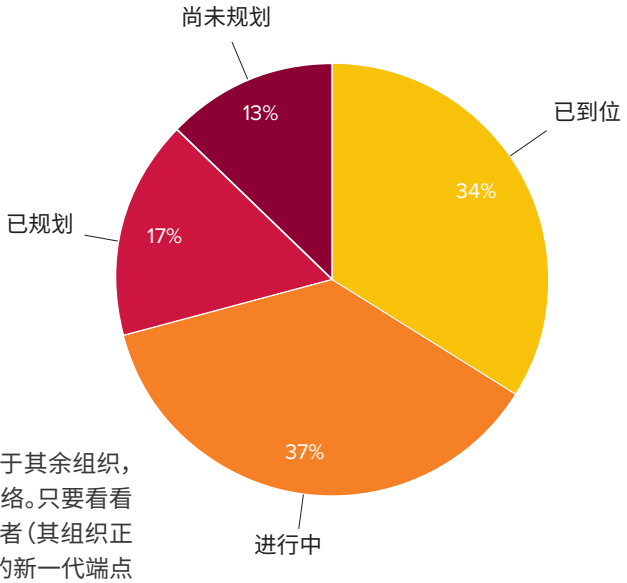


图 3

其他安全防范缺口

- **可移动介质。**一半以上的组织实施了行之有效的可移动介质安防程序。对于其余组织，任何人都可以随时携带数据外出，或者进入工作场所并将恶意软件植入网络。只要看看有关斯诺登和曼宁的业内案例，就不难理解其中蕴含的风险了。一位受访者（其组织正在进行一次修补工作）提出了一种不错的方法："配置能够拒绝 U 盘访问的新一代端点检测和响应 (EDR) 工具。"
- **网络分段。**在类似案例中，只有 49% 的组织实施了分段或微分段策略来保护业务关键系统。这是许多政府政策所要求的基本最佳实践，也是零信任策略的核心组成部分。鉴于零信任方法的效力，关键基础设施供应商可能需要给予更多授权才能有效分割网络。
- **员工意识。**69% 的组织实施了员工安全培训与测试计划。亚太地区和中东的金融与银行业在这方面处于领先地位，而美国的旅游和运输业则完全不提供培训。近 1/3 的组织总体来说没有实施安全培训，而这恰恰是一项强烈推荐的 NIST 框架最佳实践。意识培训是一种行之有效的保护措施，可以预防和阻止始于网络钓鱼的攻击（86% 的已确认泄露事件都属于这种）。无论培训计划是由 HR 还是 IT 部门负责，都必须确保其涵盖针对 OT 的网络安全威胁及最佳实践。我们还建议进行渗透测试，以帮助找出需要加强员工培训的领域。

建议

威胁主体不断在寻找漏洞。没有任何一个组织，尤其是关键基础设施行业的组织，能够始终保持"一切如常"的状态。随着网络攻击造成的停机风险不断增加，鉴于潜在损失和损害极大，不作为和最终解决 OT 修补复杂性之间的风险收益平衡从本质上应倾向于预防。

行之有效且高效的 OT 补丁管理始于丰富的工业经验和 OT 网络安全专业知识。这些专业知识可帮助您避开常见误区以及利用众多成功实施的最佳实践经验。如果合作伙伴也了解生产环境动态以及网络事故停机会导致的严重影响，您就能更轻松地完成这一复杂但又必要的流程，并且以最短的中断时间执行 OT 修补。

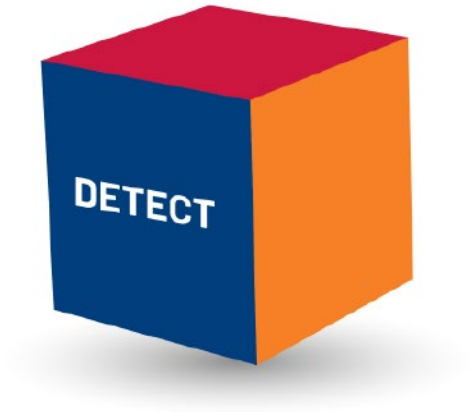
[4] Verizon，"2021 数据泄露调查报告"，2021 年 5 月

第 3 部分

检测威胁并识别网络安全事件

零信任安全策略的核心原则是：假设已经发生了攻击；对于每一个连接或访问请求，在未进行动态验证和身份认证之前都不应给予信任。这一原则强调实时持续监测恶意活动，从而检测和缓解威胁。

遗憾的是，调查结果显示，威胁检测仍是关键基础设施组织的盲点所在。这意味着对 OT 系统的攻击可能会被忽视，组织没有解决频繁的攻击风险，例如可能会削弱运营能力的勒索软件；从事长期间谍活动的民族国家主体；以及活动于企业系统和供应链内部、准备实时大规模攻击的攻击者。



通过 OT SOC 检测威胁和异常

OT 安全运营中心 (SOC) 汇集了技术、工具、人才和其他资源，旨在全天候监控和应对威胁。OT SOC 对于快速检测威胁和异常以及最大限度降低对业务关键系统的影响是不可或缺的。我们的调查发现，43% 的组织目前尚未通过 OT SOC 部署实时威胁和异常检测能力（图 4），这表明他们在网络安全就绪度方面普遍存在短板。

亚太地区、澳大利亚和新西兰地区在 OT SOC 实施方面步伐落后，高居榜首的答案是“尚未规划”。在该地区的受访组织中，31% 没有规划 OT SOC，而就全球而言，该比例为 16%。对数据进行深度挖掘后，我们发现，在该地区的能源、电力和核工业行业中没有任何组织部署 SOC，甚至连规划都没有。相比之下，在中东和非洲，74% 的组织已经实施或正在实施自动化 SOC，而两个垂直领域 —— 金融和银行业以及能源、电力和核工业也在开拓前路。

此外，47% 的受访组织尚未实施安全信息与事件管理 (SIEM) 平台（用于分析来自应用程序和网络硬件的安全警报）。虽然大多数 SIEM 系统不会真正“实时”生成警报，但有些已经非常接近，这使得它们成为 SOC 工具组合中的支柱，也是关键基础设施有效防御的关键组成部分。

通过 OT SOC（自有或托管服务）实施实时威胁和异常检测（针对恶意软件、勒索软件和安全漏洞）方面进展如何？

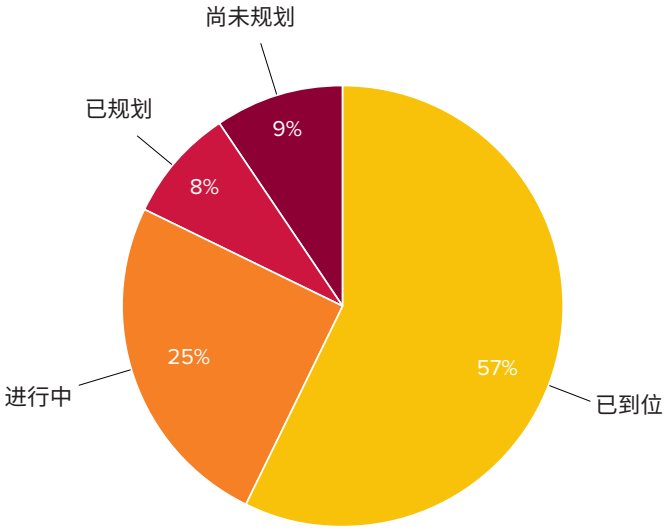


图 4

建议

内部人才短缺等资源限制可能会给许多组织监控和检测威胁带来难以逾越的障碍，而这也是在当今不断演变的 OT 威胁环境中的必备能力。应充分利用第三方 OT SOC 解决方案，包括持续威胁监控和事件响应等服务。

如果与可靠的 OT SOC 合作伙伴合作，您将会获得训练有素的安全团队所提供的本土专业知识，同时还将获得所有 SOC 服务用户带来的实时见解。托管型 OT SOC 还可避免高昂的资本支出 (CapEx) 成本，并确保以您的名义部署最新的工具、技术和威胁情报洞察力，鉴于全球高素质安全专业人员的巨大缺口 —— 估计为 272 万人（数据来自 ISC² 发布的《2021 年网络安全从业研究报告》），这一托管服务意义重大。

保障端点安全

从工业物联网传感器和员工个人设备到控制器，端点数量的激增使得 OT 攻击面显著扩大。在这种环境中保护运营越来越难。在受访的安全负责人中，有 46% 目前不具备全天候实时监控端点 的能力（图 5）。这意味着连接到 OT 系统的大部分设备没有正确配置或包含安全漏洞。组织可能会觉得幸运，但在大多数情况下，威胁主体迟早会在网络攻击中利用这些未采取保护且不受监控的端点。

全天候实时控制和监控所有端点访问方面进展如何？

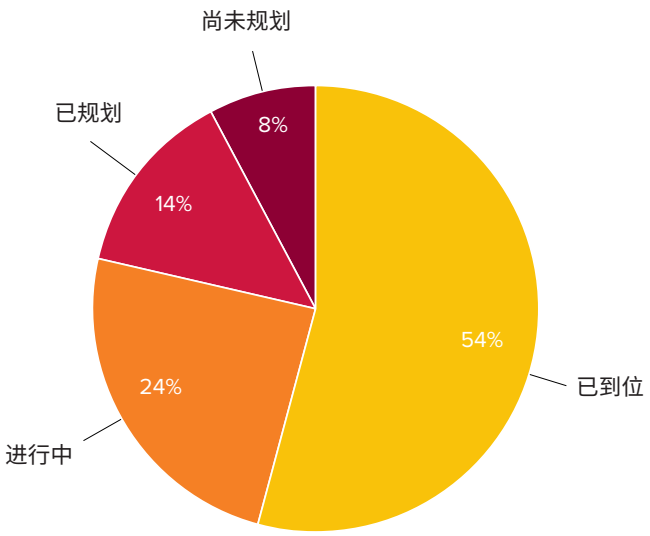


图 5

建议

端点是一个需要快速改善的领域。首先执行上文所述的网络资产清单评估，以确定所有联网端点。识别并评估端点面临的安全风险后，您就可以根据已确定的业务关键系统和安全优先级制定巩固入口点边界安全所需的工具、人员和服务规划了。

第 4 部分

对网络事件做出响应

事件响应计划和准备工作至关重要。适当的准备将最大限度减少网络安全事件带来的停机时间、经济损失、客户业务中断以及其他负面影响。对于关键基础设施供应商而言，鉴于可能造成的损害程度，响应速度格外重要，这些损害包括公共服务和安全问题，在某些情况下，可能会影响到数百万人。

关键基础设施组织不断取得进展，57% 的组织报告其具备分析、遏制和缓解网络威胁的能力（图 6）。然而，我们也发现这是一个令人担忧的领域，可能是由于威胁形势在持续快速变化。一位受访者提出："有人想出解决办法了吗？"另一位受访者问道："在研究如何制定基本事件响应策略的同时，关键基础设施组织又该如何规划解决业务连续性和弹性问题？"

网络威胁分析、威胁遏制和威胁缓解能力方面进展如何？

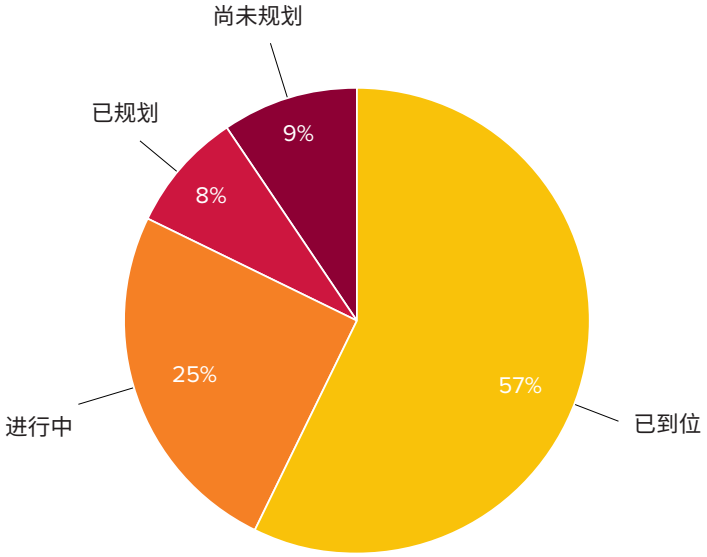


图 6

建议

如果制定事件响应策略时缺乏资源和专业知识，鉴于全球相关从业人员短缺，可以考虑通过托管服务供应商（如 OT SOC 合作伙伴）来推动进展，避免在直接雇佣资深网络安全人才时碰壁。找到一家拥有深厚工业领域经验积累的 OT SOC 合作伙伴（比如罗克韦尔自动化），不仅可以确保您获得高效的事件响应计划，还可以代表您采取行动，在需要时帮助阻止和缓解攻击。专家团队还会开展长期培训和场景测试，以验证快速响应能力。此外，一流的 OT SOC 合作伙伴还将带您深入了解 OT 合规要求和报告。

第 5 部分

事件后恢复

46% 的受访组织表示，他们现在已准备好恢复流程，系统、数据和操作方面的程序均已部署到位，有能力在网络攻击后快速恢复运营。

就从网络攻击中恢复而言，怎样才算“快”?在某些情况下，一周算比较合适的时间。而在另一些情况下，我们必须分秒必争。

例如，在 2021 年得克萨斯州的暴风雪天气中，电力公司遭遇大规模停电，停摆一周会导致数百人丧命。在 Colonial Pipeline 遭遇的勒索软件攻击事件中，即使只是耽搁 24 小时时间，也会因为美国东海岸天然气断供带来数百万美元损失和难以估量的经济影响。

恢复正常运营是事件恢复阶段的重点事项，同样也蕴藏着找出待改进领域的机会。根据事件的经验教训实施有意义的变革，营造持续改进网络安全的文化，从而打造更具弹性、保护力度更强的系统。

充分利用联邦资助

2021 年 11月，美国国会颁布了一项基础设施法案（H.R. 3684，《基础设施投资和就业法案》），规定将拨款约 20 亿美元用于升级和增强关键基础设施的网络安全。其中 10 亿美元将用于资助州、地方、部落和某些非营利组织。拨款申请指南待定，但罗克韦尔自动化预计，鉴于联邦网络安全和基础设施安全局 (CISA) 使用 NIST 网络安全框架，是否符合该框架规定的功能要求将成为获得拨款的依据。

约三分之一 (29%) 的受访组织已拥有符合拨款申请资格的网络安全计划。另有 25% 的受访组织正在制定计划。还有约 40% 的受访组织尚未着手此类准备工作。

网络安全计划不仅可以促使目标组织中的人员快速采取行动申请拨款，还有助于打造合适类型的系统性网络安全方案，以便揭示防范缺口、降低风险，并帮助确定能让组织及其客户免遭有害影响的工作优先顺序。

罗克韦尔自动化鼓励所有关键基础设施行业领导者熟悉本法规，准备好基线计划，只要拨款法案适合自身组织，就积极争取拨款。不要等到拨款要求发布后才行动，而应现在就开始准备和制定计划。罗克韦尔自动化基于 NIST 框架制定了网络安全计划模板和检查表：下载计划模板

建议

恢复和还原计划应成为与资产维护一样的常态化实践行动，作为保证正常运行时间的核心环节。停机导致的财务和人力成本持续上升，您不能指望将风险负担转嫁给保险公司。随着责任的增加以及可保险性限制日趋严格，风险负担将回到被保险人一方，由其承担大部分损失和恢复成本。

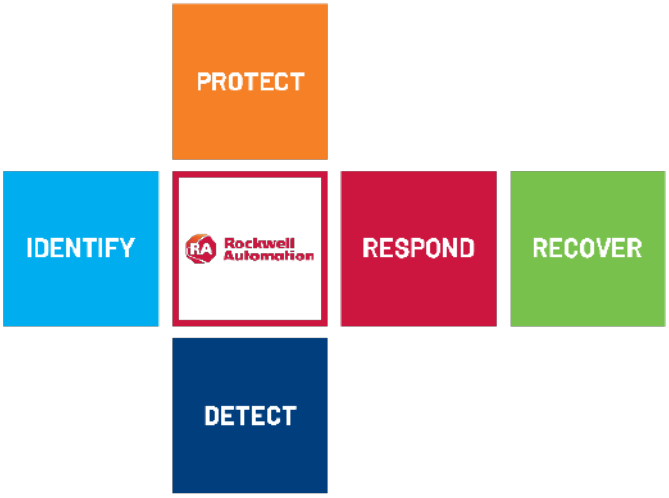
下一步行动

为未来做好准备

每家关键基础设施供应商都必须立即采取行动，以避免“大停摆”发生。因为他们关乎人们的生活、福祉、安全和生计。

保障 OT 网络安全绝非易事。从另一方面来说，大多数攻击行为都有已知的抵御措施。通过数字化转型和自动化举措，关键基础设施组织在效率和可靠性方面取得了巨大进步；现在，他们必须以同样的毅力解决网络安全问题。调查结果表明，该行业已经意识到对现代化、有侧重点的网络安全的需求，尽管进展缓慢，且仍存在防范缺口众多、优先事项不明确以及对风险和最佳实践缺乏明确性的问题。

然而，关键基础设施行业领导者已经开始给予关注。许多受访组织报告说已规划或正在部署重要保护措施。这一领域正在发生积极转变，从最初的意识薄弱，到现在看到重大攻击新闻以及政府回应之后做出反应，甚至开始主动询问如何加快其组织的网络安全进程。



罗克韦尔自动化：保障世界根基安全。

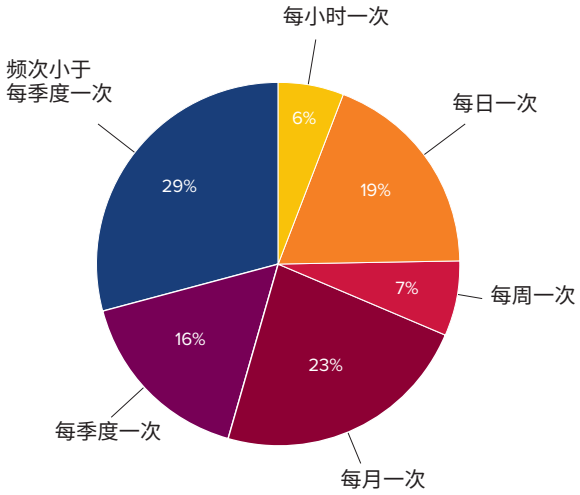
罗克韦尔自动化提供一系列工业安全解决方案和服务，帮助您管控威胁，并提高 OT 和 IT 生态系统的弹性。我们的专家可以帮助您构建稳健且安全的网络基础设施，同时帮助抵御威胁并快速响应事件。除了深厚的专业知识和最新的最佳实践知识，我们还为您提供 100 多年来在工业自动化领域积累的生产运营智慧。我们的业务据点遍布全球，能够帮助客户实现全球多站点网络安全保护，同时提供定制后勤服务，满足您对工业自动化行业巨头的所有期望。

建议

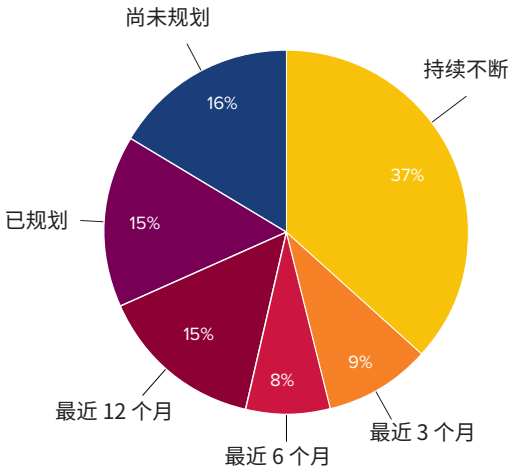
- 参加罗克韦尔自动化网络安全就绪度评估，接收以原始调查对象为基准的定制报告。查看贵组织在行业、公司规模和所在地区方面的对比结果。
- 下载我们的 OT 网络安全计划模板，深入了解有效保护运营所需的工具、服务和人员配置。美国关键基础设施组织：使用计划模板帮助做好拨款申请准备，积极支持弥合网络安全缺口。
- 与罗克韦尔自动化专业人员对话，了解我们如何帮助您制定合适的 OT 网络安全计划，以最大程度保护您的工业运营。

附录

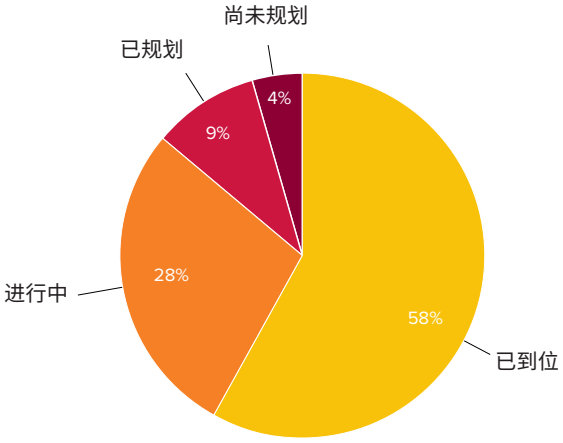
多久进行一次既有资产清单评估?



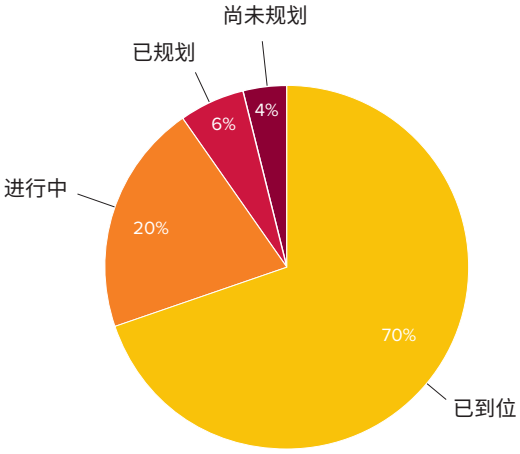
多久进行一次供应链风险评估?



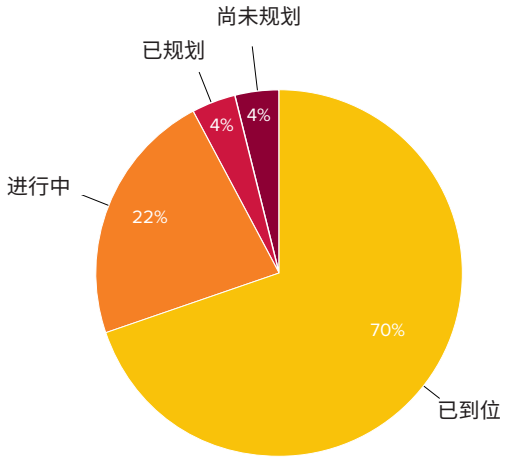
是否识别了业务关键系统及其优先级?



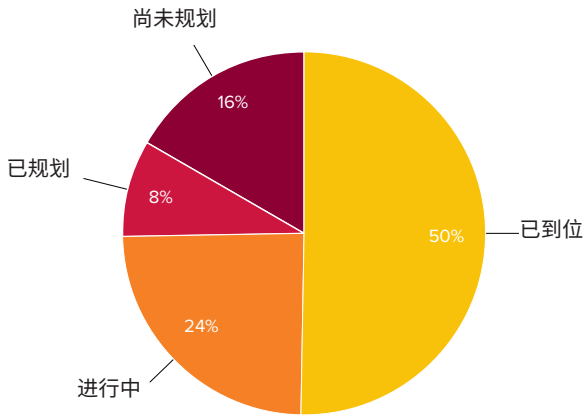
远程访问控制(用于实现安全异地登录)方面进展如何?



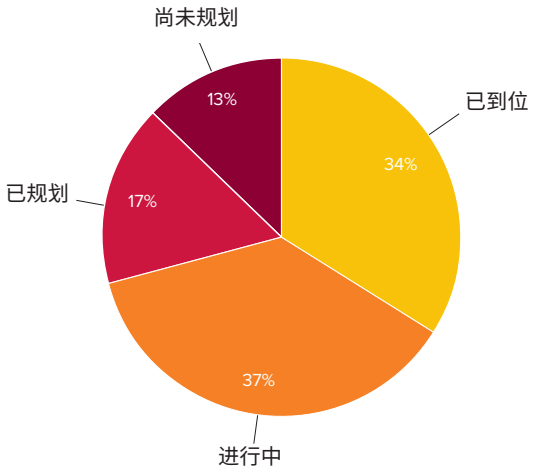
物理访问控制（用于识别和防止非法系统访问）方面进展如何？



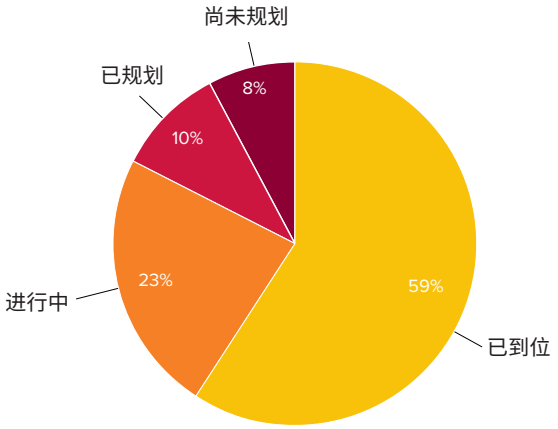
在 OT 安全架构中实施工业非军事隔离区 (IDMZ) 方面进展如何？



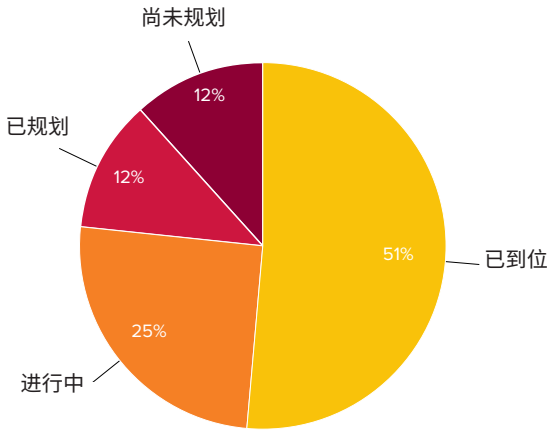
实现有效的 OT 补丁管理方面进展如何？



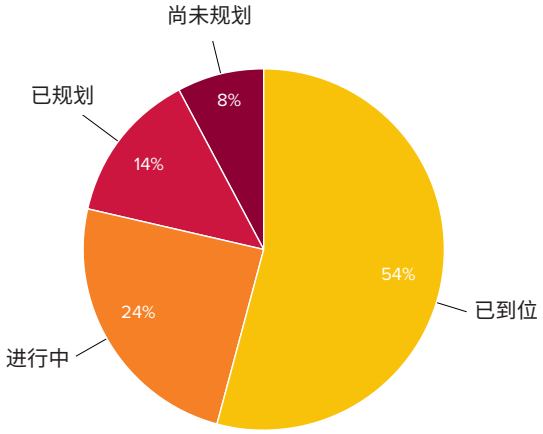
是否定期执行操作系统数据备份流程？



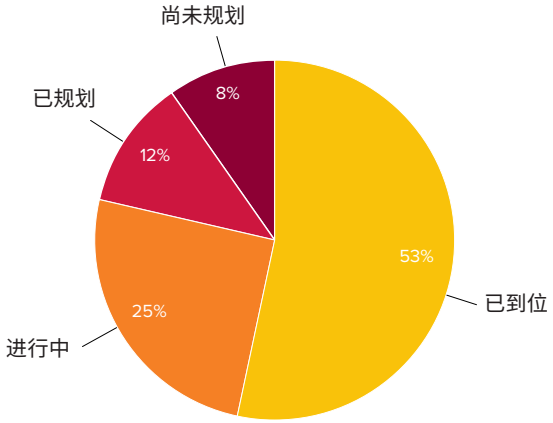
保护技术：实施有效的可移动介质安保程序方面进展如何？



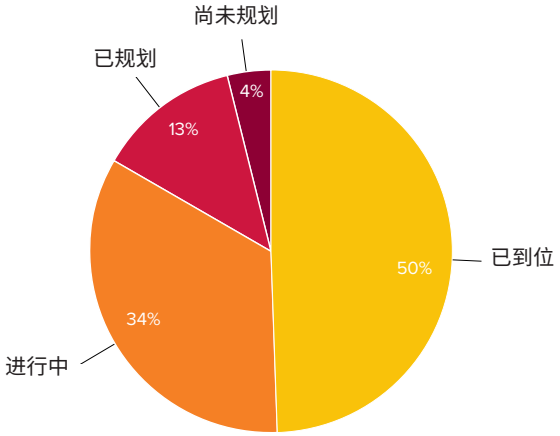
全天候实时控制和监控所有端点访问方面进展如何？



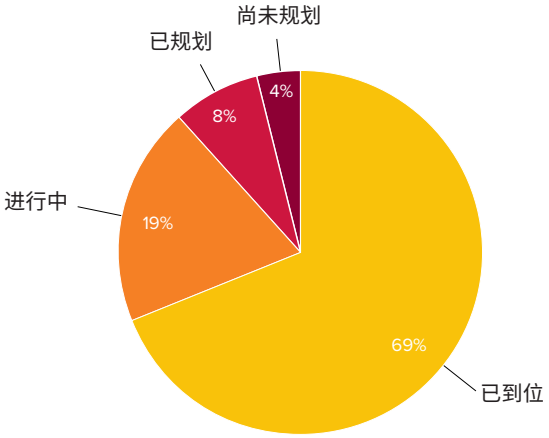
安全事件信息管理 (SIEM) 系统（实时分析由应用程序和网络硬件生成的安全警报）方面进展如何？



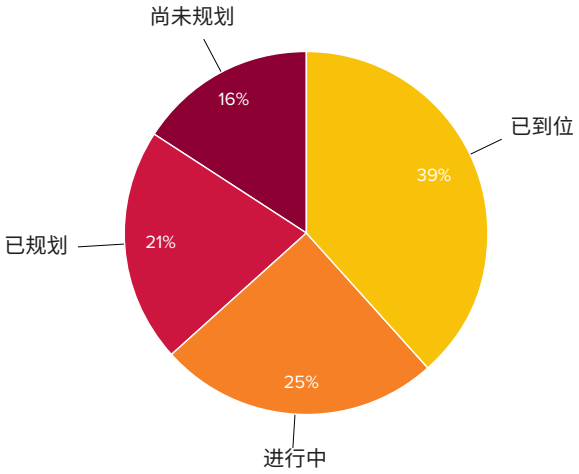
网络分段/微分段架构实施（用于在关键业务系统周围设置安防边界）方面进展如何？



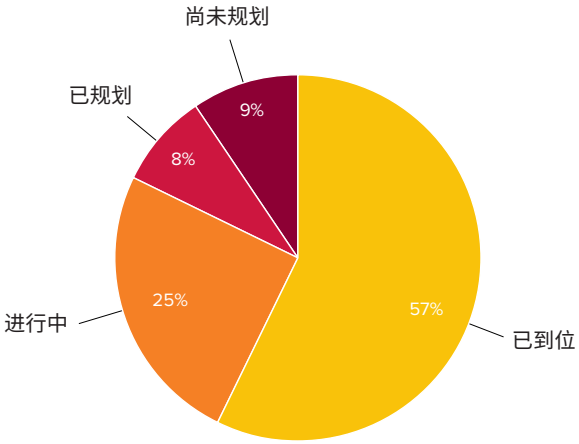
是否提供员工安全意识培训和测试?



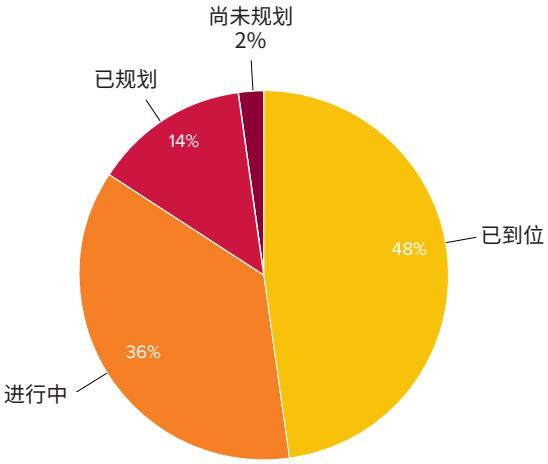
通过 OT SOC(自有或托管服务)实施实时威胁和异常检测(针对恶意软件、勒索软件和安全漏洞)方面进展如何?



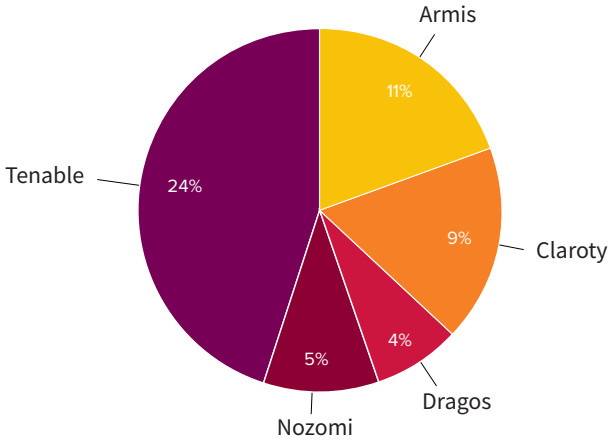
网络威胁分析、威胁遏制和威胁缓解能力方面进展如何?



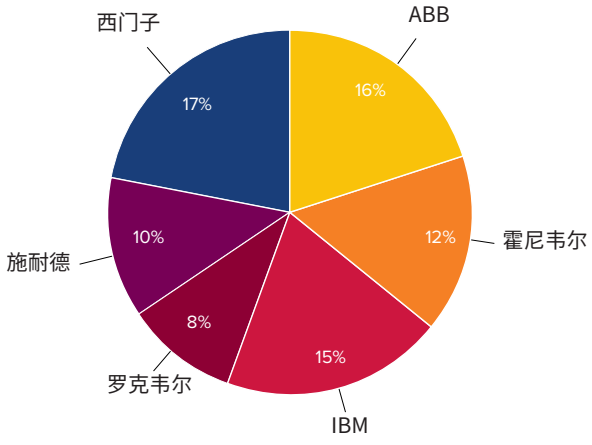
系统、数据和运营程序在发生网络攻击后快速恢复方面进展如何?



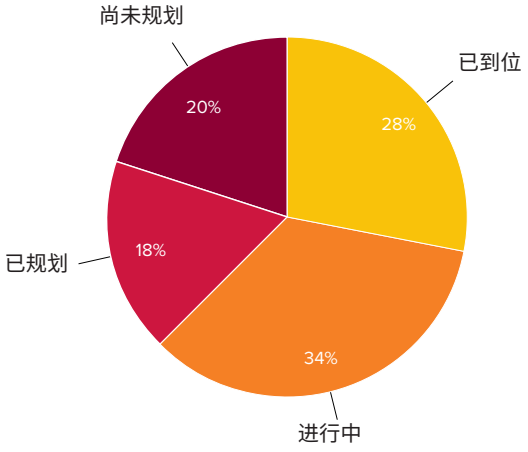
正在使用哪些 OT 威胁检测平台或服务?



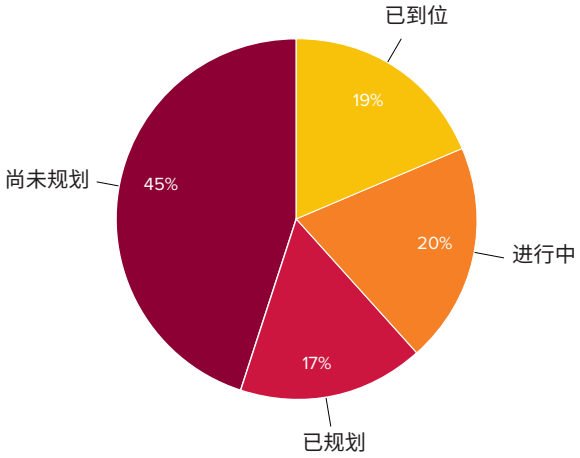
正在使用哪些工业自动化服务供应商?



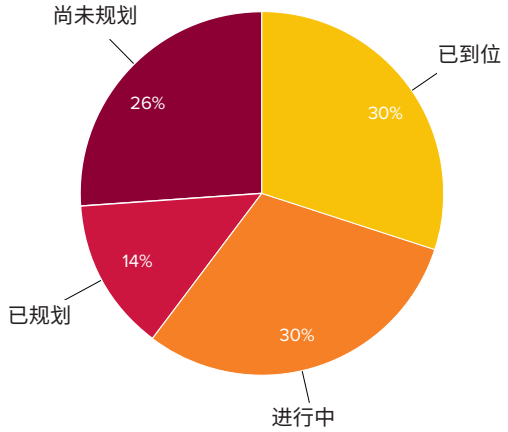
IT/OT 融合网络安全路线图实施方面进展如何?



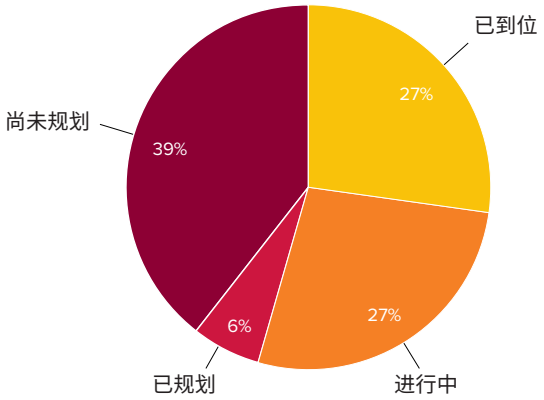
使用通用工业协议 (CIP) 认证产品保护和加密以太网通信方面进展如何?



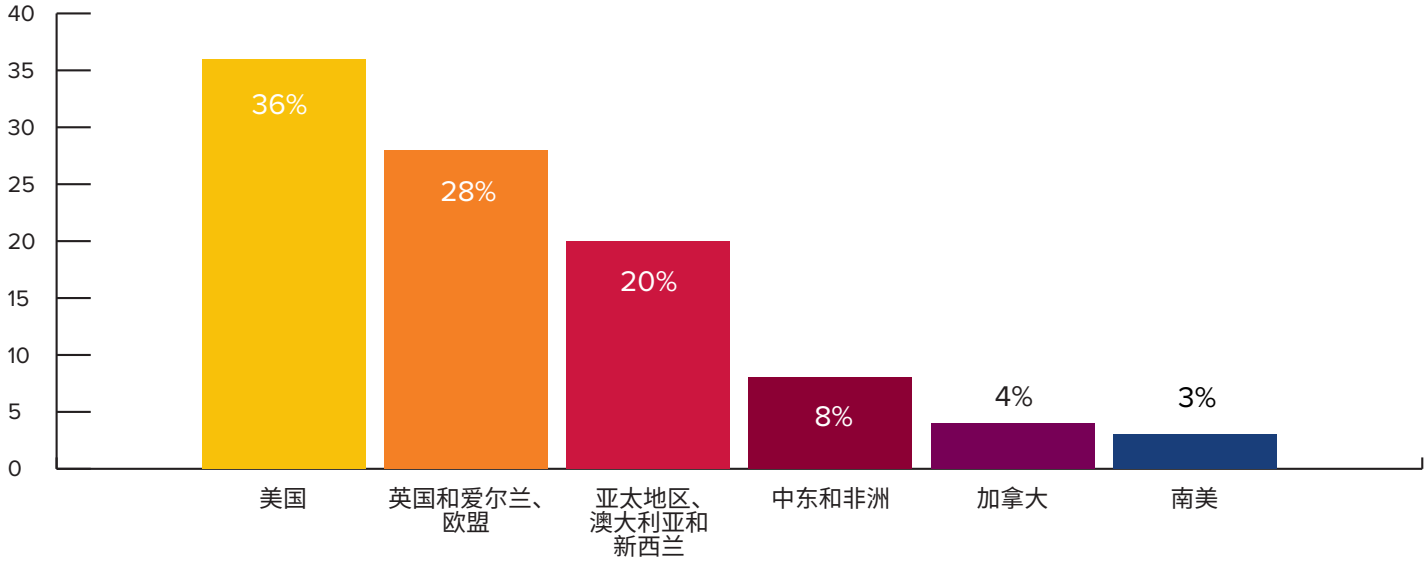
贵组织是否与一家或多家知名网络安全合作伙伴合作，以获取可动态更新、可扩展的 OT SOC 服务？



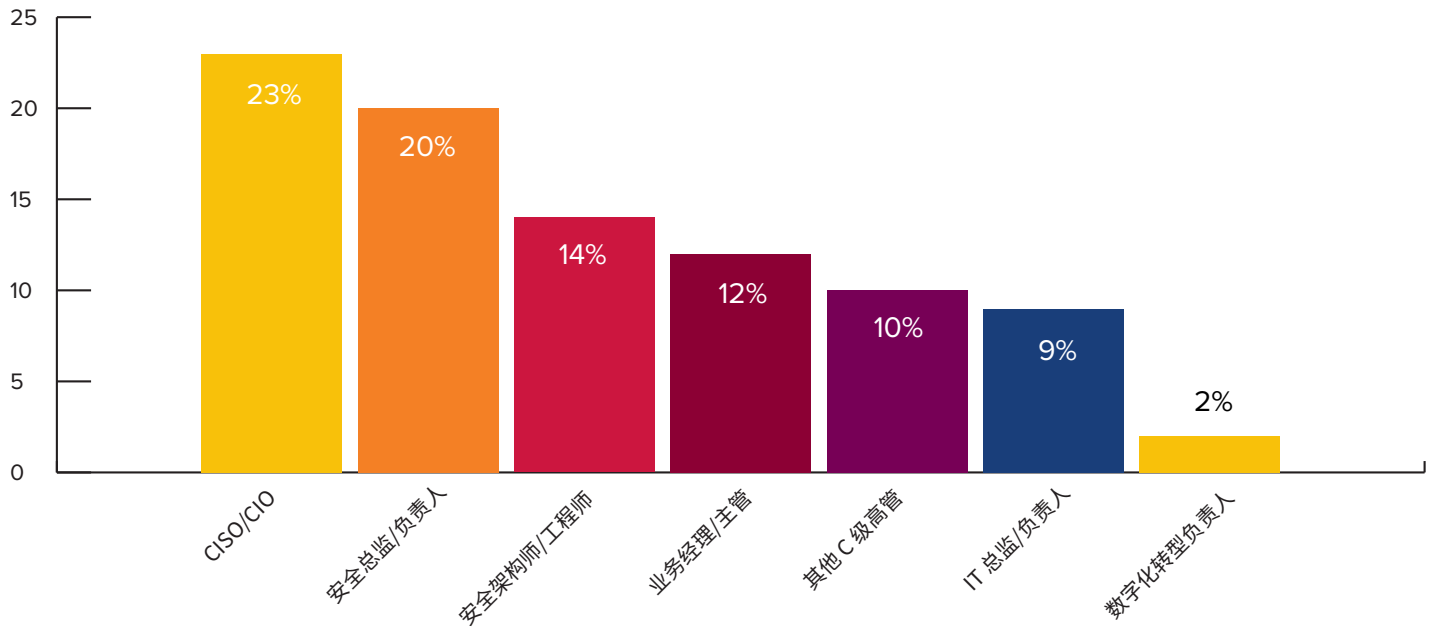
贵组织是否拥有适合申请美国基础设施法案拨款的网络安全计划？



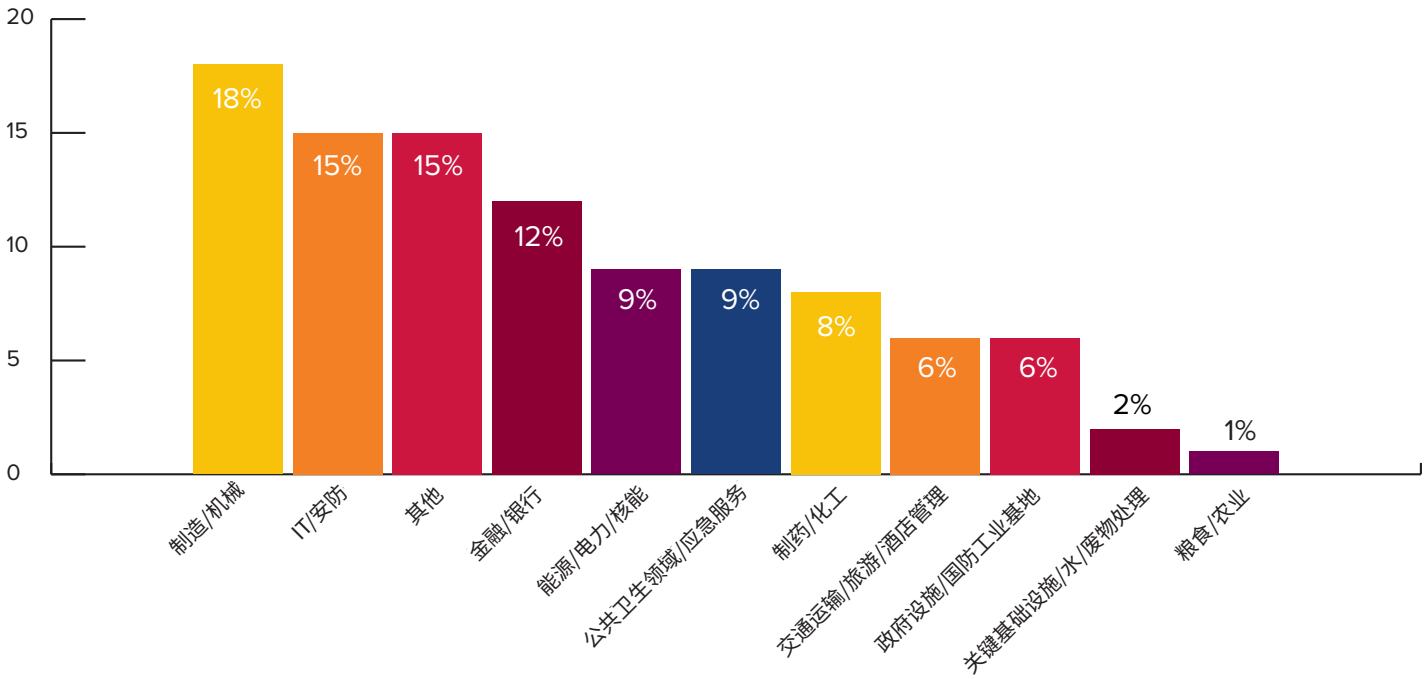
受访者（按地区划分）



受访者(按角色划分)



受访者(按行业领域划分)



关注我们。

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

出版物 GMSN-SP016A-ZH-P – 2022 年 6 月