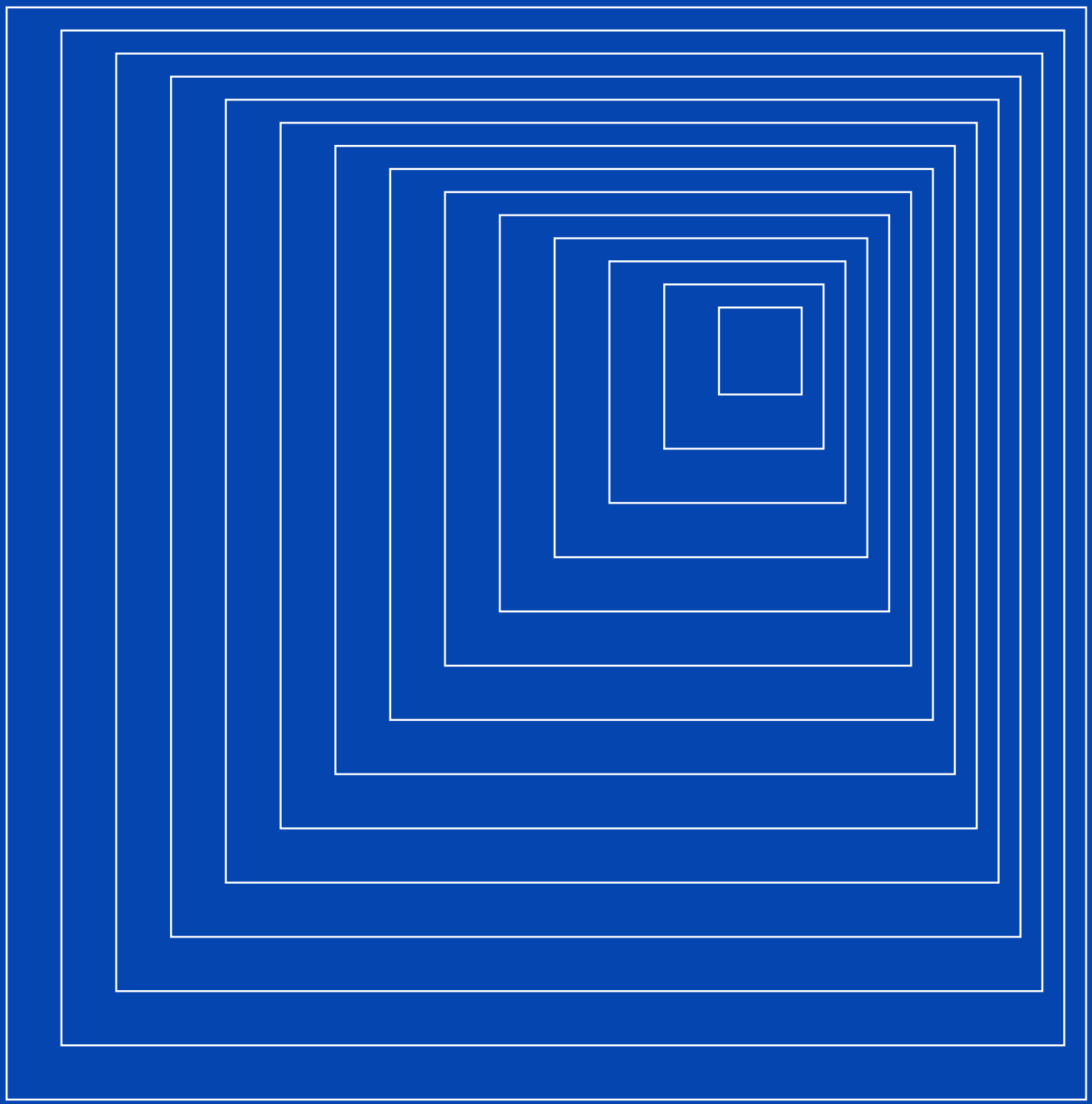
网络安全趋势

情报报告

2025



预期一个网络安全的未来世界

S2GRUPO

索引

引言

2025年的网络安全格局将标志网络威胁的演变、更完善的法律法规的出台以及一系列技术创新。随着恶意行为者完善其策略、系统漏洞日益增多，组织被迫采取更复杂的方法来保护其资产和敏感数据。

本报告基于S2GRUPO网络安全部门Lab52准备的分析报告。报告详细阐述了将定义网络安全格局的关键网络威胁：包括勒索软件的持续存在与演变，以及国家行为者（愿意组织或资助自身攻击的政府）威胁的日益增长，再到黑客行动主义的兴起。本文件对于理解2024年已记录的事件、幕后黑手以及2025年宏观层面的未来趋势极具参考价值。

此外，该文件还探讨了特别影响企业和组织的趋势与挑战，从法规收紧——即更严格、影响范围更广的法规——到适应云环境范式的转变需求。它还讨论了生成式智能网络安全带来的新兴影响，该技术有望彻底改变威胁的预防和管理方式。

重点也在于日益增长的对OT网络监控可见性和控制的需求，这是工业基础设施的关键领域。最后，建议通过采用一种将习惯和行为转化为抵御网络风险第一道防线的可行为安全模型，在提高安全意识方面取得更大进展。

通过这些要点，我们希望为首席信息安全官（CISO）和网络安全管理人员提供一份综合且扎实的分析，以明确今年的优先事项和行动方案。

网络安全概述：

2024年见证了网络犯罪即服务（CaaS）的兴起，这是一种商业模式，它将现成的网络攻击工具，如勒索软件（RaaS）和钓鱼即服务（PhaaS），提供给攻击者。这使得即使是非技术性人员也能发起复杂的攻击，并极大地扩展了威胁范围。此外，人工智能（AI）被整合到网络犯罪分子的运营中，进一步提高了他们的效率和破坏能力。

据美国联邦调查局和国际货币基金组织的估计，到2027年，全球网络犯罪成本可能飙升至230亿美元[1]，这表明了这一挑战日益严峻的规模。

另一方面，企业面临着严峻的内部挑战。全球范围内，每年几乎有2000亿美元投资于网络安全产品和服务，但如果没有合格专业人员的支持，这些开支仍显不足。据估计，到2030年，网络安全领域将出现8500万人的劳动力短缺，这可能导致巨大的经济损失。事实上，由于缺乏专业人才，每年可能产生850亿美元的财务影响[3]，这可能是由于意外攻击、运营中断，或由于安全措施不足导致创新放缓所致。

2024年，监管压力也显著增加。这一年是多项关键法规出台的年份，包括网络与信息指令2（NIS 2）、欧洲网络弹性法案（CRA）、美国国家网络安全战略（NCS）、运营技术网络安全总体规划，以及智利的网络安全和关键信息基础设施框架法案。这些法规对风险管理、供应链安全、运营弹性提出了严格要求，并对不合规行为处以严厉处罚。

网络安全已占欧盟IT投资的9%。

不仅如此：大多数组织预计，为应对日益复杂的威胁和监管压力，其预算将增加，无论是临时性的还是永久性的。在一个数字韧性已成为战略支柱的环境下，加强安全不仅是合规性问题，更是保障业务连续性、提升竞争力和建立数字信任的关键因素。

[1] 美国国务院（2023年）。与网络安全及新兴技术国家安全顾问安妮·纽伯格尔的数字新闻发布会。https://www.state.gov/digital-press-briefing-with-anne-neuberger-deputy-national-security-advisor-for-cyber-and-emerging-technologies/

[2] 美洲国家组织（OAS）。（2023）。网络安全人才报告。https://api.gcforum.org/api/public/cms/files/8eaba644-0889-49b4-8c7d-8de3840decac_one-Cybersecurity-Workforce-Report-(002).pdf.

[3] 世界经济论坛。（2024，四月）。新报告称网络安全行业面临人才短缺。https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/

[4] 欧洲网络安全局（ENISA）。（2023）。NIS 2 时代下的网络安全投资指南。https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

关键网络威胁：

2024年，网络安全环境日益严峻，威胁在复杂性和范围上都发生了演变。场上主要有三个主要向量：勒索软件、国家行为者（或：国家支持的攻击者）和网络行动主义，每个向量都有其独特的特征、动机和目标。

勒索软件，历史上与网络犯罪相关联，正将其目的从经济勒索扩展，被用作破坏关键运营并使攻击归因变得困难的工具。国家行为者则继续以战略精准性运作，投入大量资源进行网络间谍活动、破坏活动和虚假信息传播。最后，黑客行动主义在一个两极分化的世界中强化其影响，带来受政治和意识形态议程驱动的攻击，并以战略部门和行业为主要目标。

勒索软件

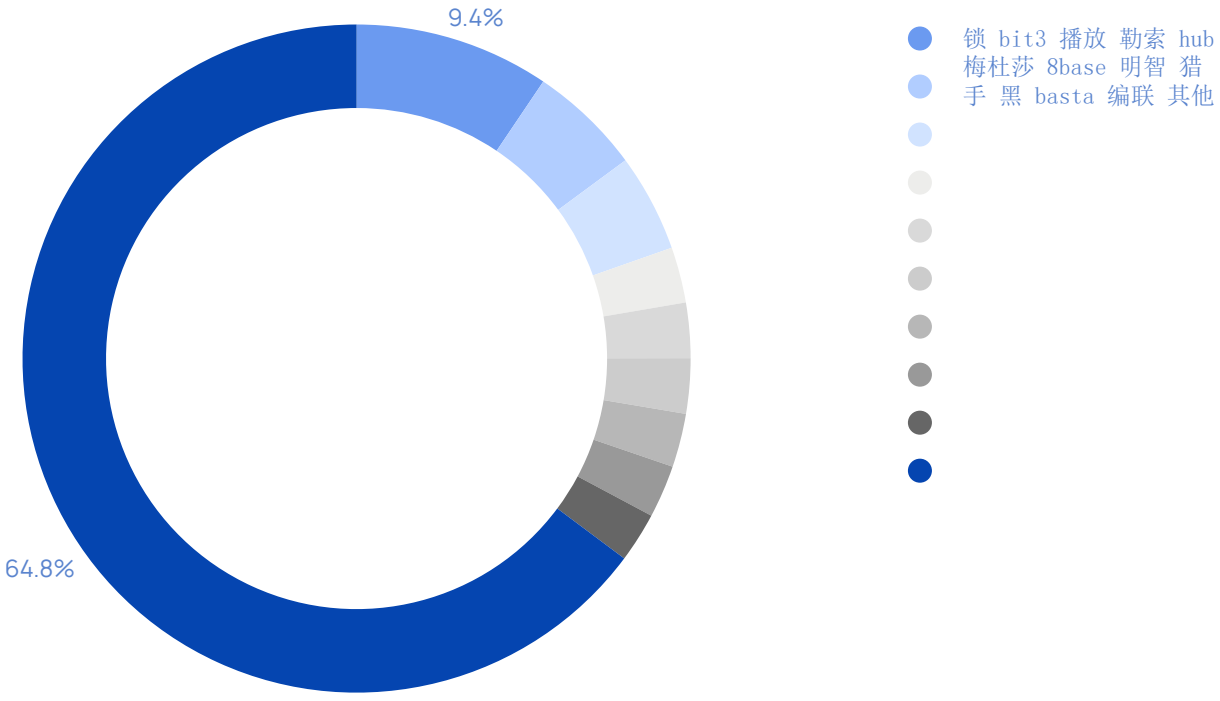
传统上，勒索软件一直与网络犯罪相关联，并被用作敲诈勒索以获取经济利益的手段。然而，在2024年，它也使网络犯罪分子能够破坏受害者的活动、抹去其活动踪迹或使攻击归因变得困难。

过去一年，平均每月记录了460起勒索软件事件。这一数字甚至可能更高，因为仅统计了组织决定公开的事件或攻击者团体在其网站上自行披露的事件。

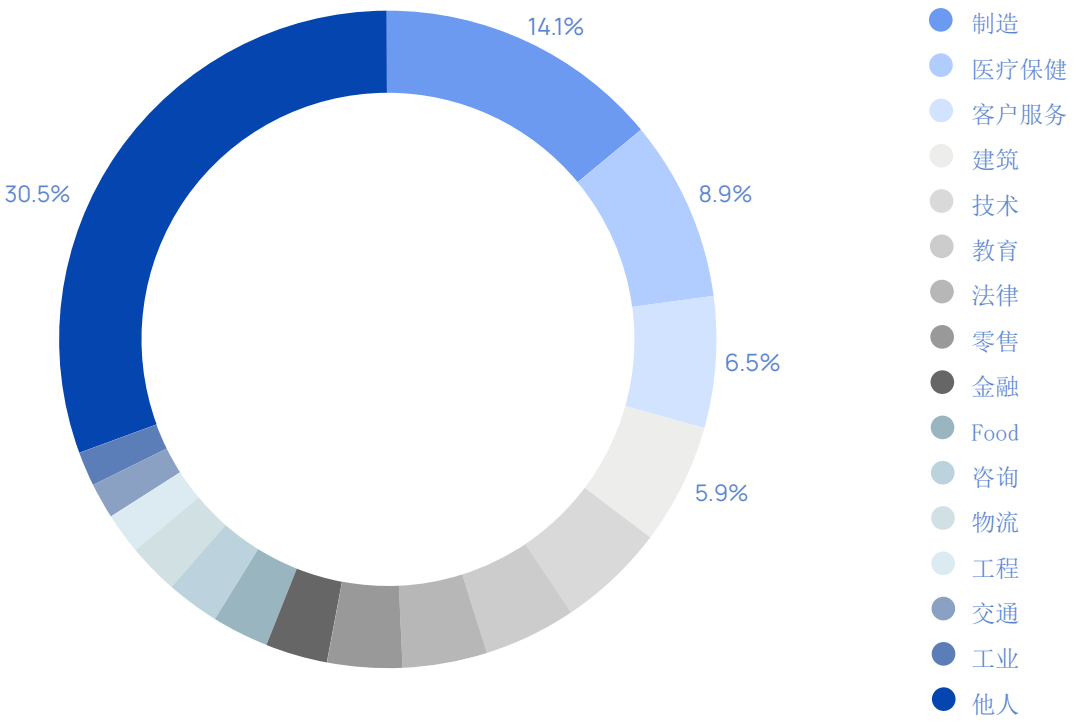
过去12个月，S2GRUPO的情报部门Lab52已识别出近一百个活跃的勒索软件团伙。Lockbit3（占攻击的9.4%）、Play（占5%）和Ransomhub（占5%）尤为突出。

受影响的行业呈现出同质化分布。受影响最严重的行业包括制造业（14%）和医疗保健业（9%）。在前者的情况下，高比例的攻击可能是因为该行业涵盖了广泛的组织。医疗保健业可能是一个反复被攻击的目标，这与其提供的服务的相关性有关：对组织的影响越大，攻击者的收益就越高。

2024年最活跃的勒索软件组织



2024年拉姆森软件受害者的行业分布



预测 2025

2024年，基于RaaS（勒索软件即服务）的商业模式被证明具有惊人的韧性和盈利能力，无视了国际当局试图摧毁这些网络的努力。因此，预计2025年与勒索软件相关的运营将继续扩张，利用新的攻击向量并提高网络犯罪分子的专业化程度。

与此同时，零日漏洞利用的增加——这些漏洞尚未被开发者知晓，因此尚未修复——加上全球供应链日益增长的复杂性，将使恶意行为者更容易在这些基础设施的关键节点进行渗透。鉴于组织之间的高度相互关联性，一次安全漏洞可能引发大规模且复杂的攻击，对战略性行业可能造成灾难性影响。

02. 国家行为体

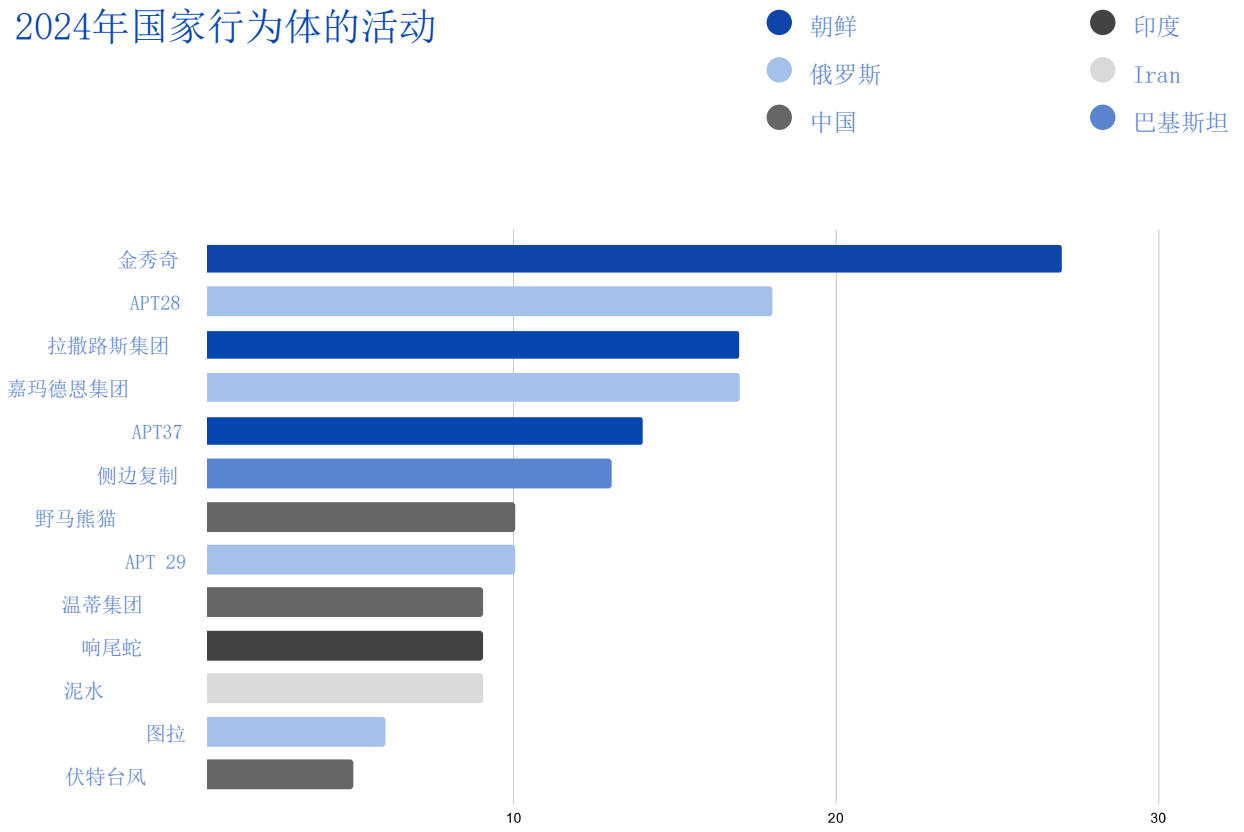
国家行为体是由专家组成的行动小组，他们为国家的战略利益而行动，并提供资金、技术和后勤资源。这些单位通常执行网络间谍、破坏和影响力行动，包括针对关键目标的虚假信息宣传活动。

2024年全年，Lab52识别出超过一百个参与网络行动的国家行为体的活动。其中，存在数量最多的国家包括中国（51个）、俄罗斯（18个）、朝鲜（14个）、伊朗（12个）、巴基斯坦（4个）和印度（3个），这些国家正在巩固其在网络空间中作为具备显著进攻能力的参与者的角色。

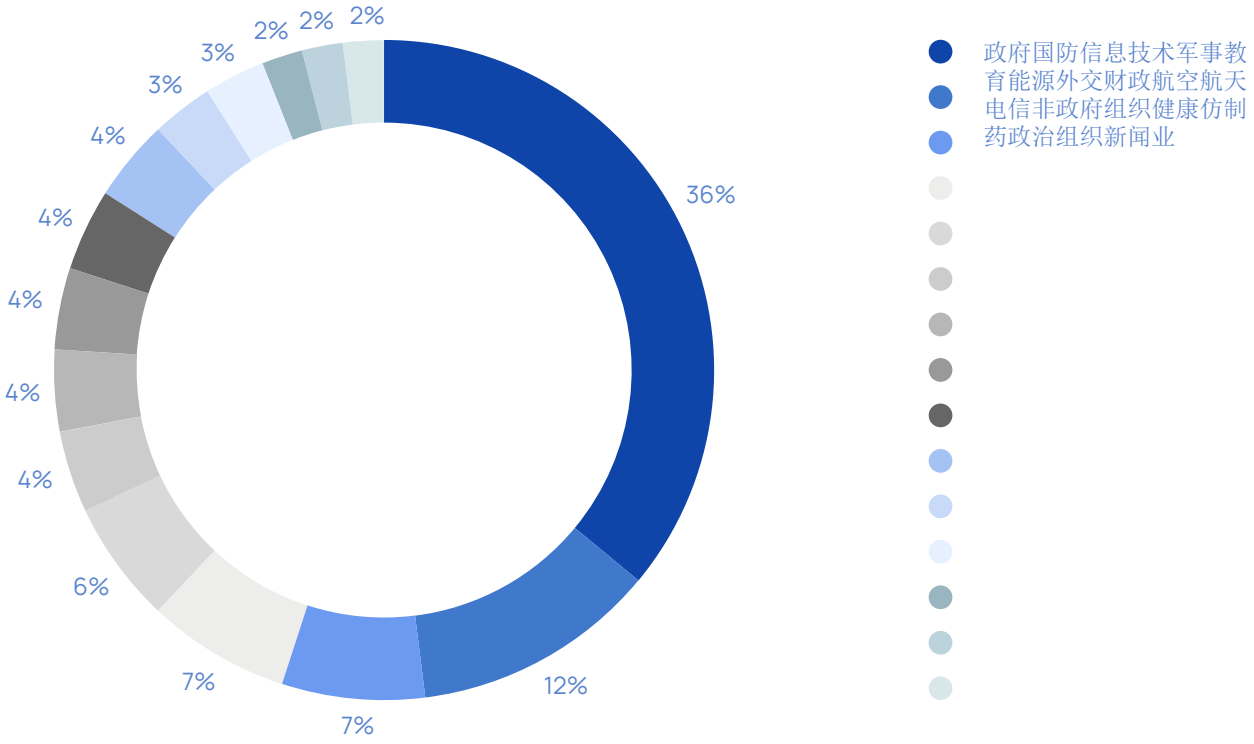
对国家行为者受害者的分布分析反映了其目标的战略性质，并明显集中于关键领域。超过三分之一的攻击针对政府实体（36%），考虑到政府管理着对其他国家具有高度战略价值的信息，这是合乎逻辑的。

国防（12%）和军事（7%）部门也是主要目标，因为它们管理着关键资源，从战略计划到先进技术。获取这些资产不仅威胁到相关国家的国家安全，还可能使敌对国家在情报、技术发展和作战能力方面获得显著优势。

2024年国家行为体的活动



2024年网络间谍活动行业分布情况



预测 2025

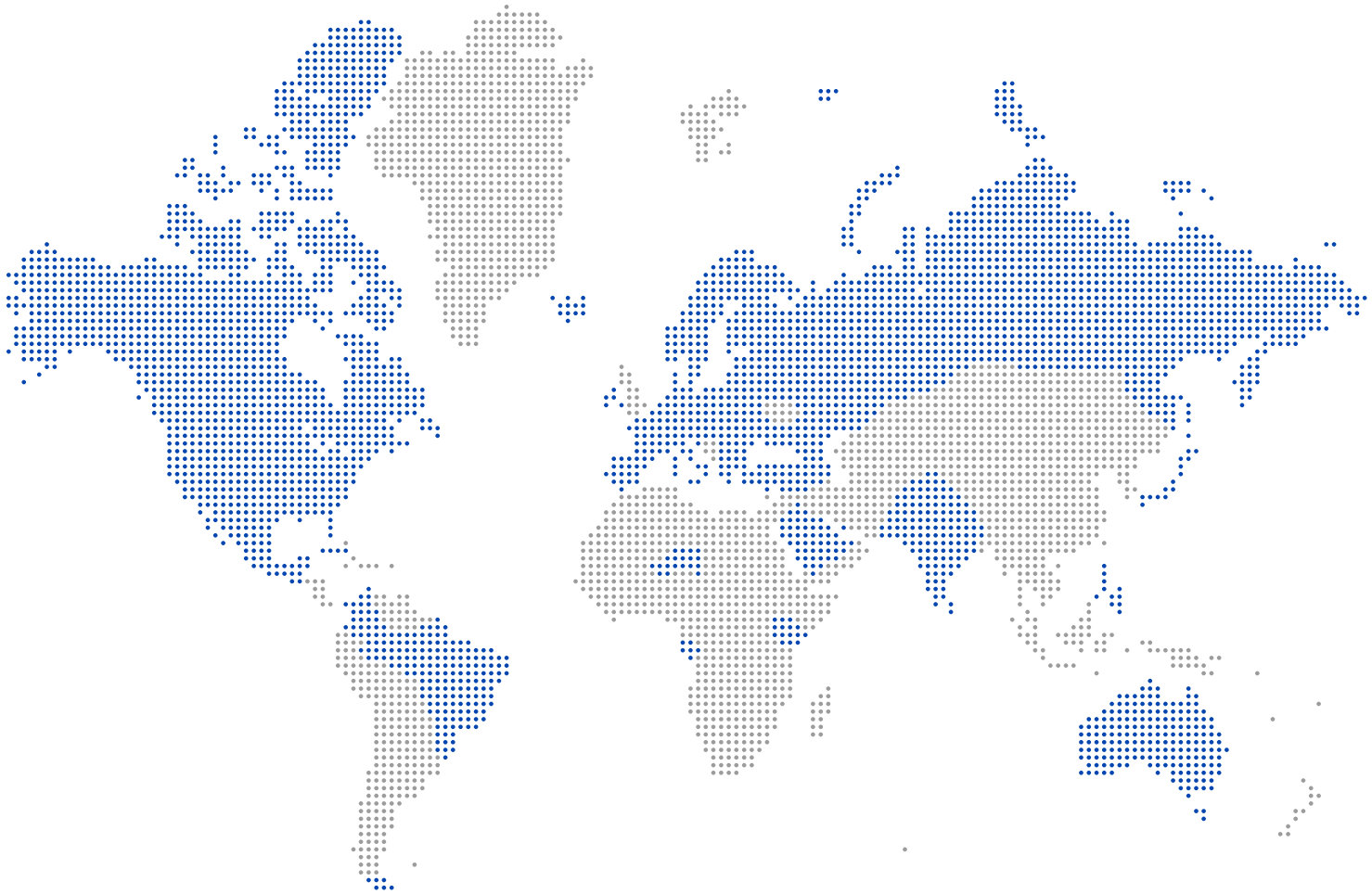
近年来，国际合作的恶化，在政治极化的加剧下，已使冲突不断升级。到2025年，随着全球政治格局的变化，这一趋势可能进一步加速。其结果，虚假信息行动将更加突出，国家和非国家行为体将利用人工智能生成极具说服力的内容、制造虚假身份，从而加大其对公众舆论和地缘政治稳定的影响。

03. 黑客行动主义

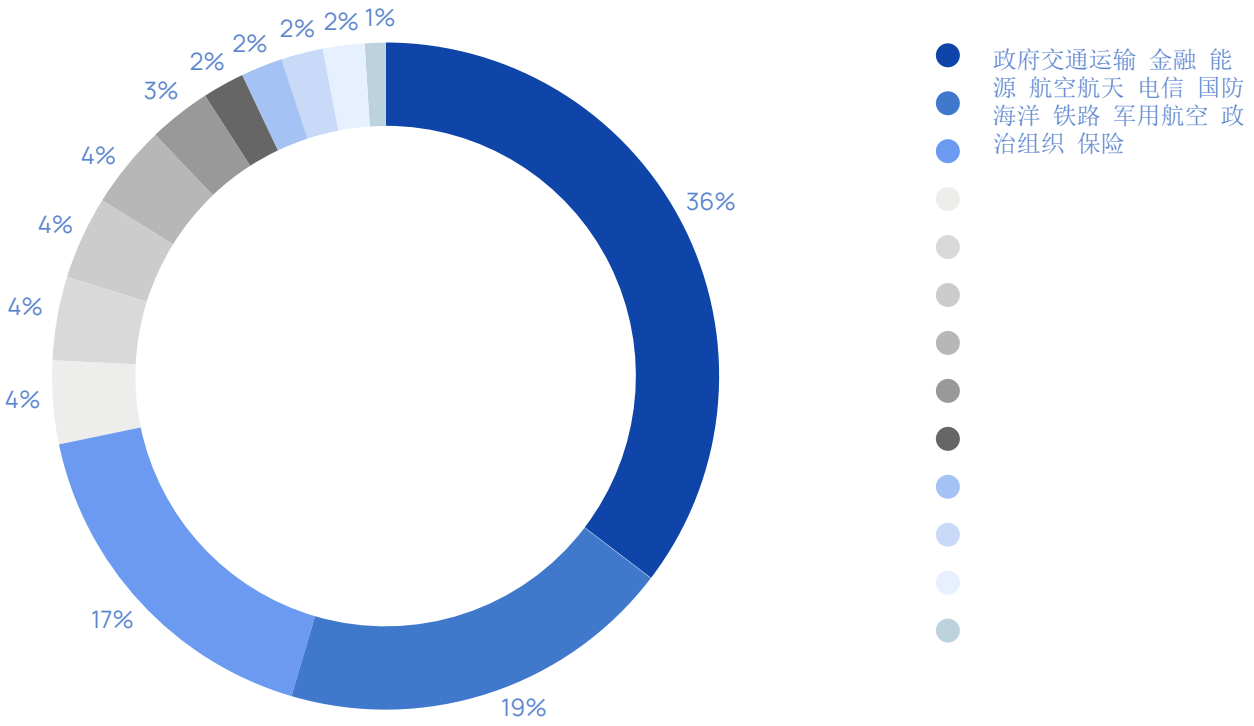
黑客活动分子在武装冲突中找到了他们行动的主要理由之一。2024年，有两个亲俄组织在活动量方面尤为突出：NoName05716，负责大约75%的黑客网络攻击，以及CyberArmyofRussia_Reborn，占比18%。

鉴于黑客行动主义具有政治和意识形态色彩，受影响最严重的领域往往包括政府（35%）以及对民众有直接影响的部分，例如交通（19%）、金融（17%）和能源（5%）。这些目标的战略性体现在，对其造成干扰可能引发高度混乱并吸引媒体关注。黑客行动主义者正是通过这种方式来推广他们的议程及其反对者。

2024年黑客行动主义受害国



2024年黑客行动主义受害领域



预测 2025

2025年，在现有冲突持续存在、新战事前线又不断涌现的背景下，黑客行动主义团体可能会加大活动力度，选择与一方或另一方结盟，并攻击其对手以及向其提供外交或物资支持的国家。

2025年网络安全趋势

立法的兴起：更严格、影响更广泛的法规

云环境中的范式转变

生成式智能网络安全时代

增强对OT网络监控的可见性和控制力

超越意识提升：迈向行为安全模型

立法的兴起：

更严格、影响更广泛的法规

去年，欧盟推动建立了一个监管框架，旨在统一提升其成员国以及公共和私营部门之间的网络安全水平。《DORA法规》是这一进程的先锋，因为它适用于金融行业——这一行业在安全事务上传统上监管更严格、更成熟，并且对其实施有明确的技术标准。

但欧洲并非唯一朝着这一方向发展的地区。智利通过于2024年4月颁布《网络安全和关键信息基础设施框架法》（第21.663号法律），将自己定位为拉美地区的网络安全领导者。该法规对关键服务和战略部门运营者提出了强制性要求，同时设立了国家网络安全局，负责协调事件应对并加强国家的数字韧性。

凭借这一进步，智利不仅加强了其对抗数字威胁的保护能力，也成为了区域内的标杆，吸引了公司、投资者和网络安全专家的注意。

这些关键新法规正为全球行业和网络安全标准定下基调，对政府和私营部门都具有重要意义。

3

2024年，新的欧洲法规已获批准或生效。

+100.000

欧洲公司受《NIS2指令》管辖，其范围是其上一版本的三倍。

5%

DORA法规不合规可能导致的罚款所影响的最高年营业额百分比是多少。 [5]

€1.200 M

这是因违反欧洲数据保护法规而提出的最大索赔金额。 [6]

[5] 欧洲议会和欧盟理事会，(2022)。关于金融业数字运营弹性的法规（EU）2022/2554。可在以下网址获取：https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81962

[6] 西班牙CNN（2023年5月22日）。欧盟因数据隐私泄露对Meta处以创纪录的13亿美元罚款。CNN西班牙语。https://cnnespanol.cnn.com/2023/05/22/union-europea-multa-meta-violar-privacidad-datos

趋势

2025年，网络安全将呈现出一种由更严格、更详细的规定所驱动的主动应对态势。NIS2、DORA以及网络弹性法案（CRA）等规定中，存在一些值得关注共同点。

首先，其影响范围显著扩大。它们不再仅影响提供基本服务的实体，也包括所有提供IT和OT领域服务的公司。在此新的监管框架下，不仅包括金融等传统受监管行业，也包括医疗保健、物流和能源等网络安全领域相对不成熟产业，这些产业现在将不得不适应更严格的标准。

后者的这些垂直领域正面临前所未有的监管束缚，这不仅带来了新的要求，也重新定义了组织运营的方式。网络安全已不再是可选项，或仅仅是技术团队的专属关注：它已成为一项战略和企业责任。适应这一环境将需要大量的投资、周密的规划，最重要的是，管理层思维方式的转变。

其次，供应链中的网络安全管理将是一项不可回避的挑战。无论规模大小，组织都必须确保其关键供应商的服务具有高度安全性。这代表了一种范式转变：仅仅保护内部边界已不够；风险现已扩展到整个合作伙伴与合作网络，需要持续的警惕和更严格的管控。

最后，高级管理层将不能再将网络安全视为纯粹的操作问题。数字风险如今已成为商业风险，CEO、CFO以及董事会将直接对其管理负责。例如，NIS2为高级管理层在安全事件中的疏忽行为引入了刑事处罚，建立了一个要求更高、问责更严的框架。问题已不再是你的公司是否会遭受网络攻击，而是何时会发生以及你将如何准备应对。

那些仍然将网络安全视为成本或创新阻碍的领导者注定会被淘汰。数字韧性不是一种选择：它是技术风险新时代中生存与消失的区别所在。

建议

为网络安全设立专项预算：尽管有欧洲资金和补助可用，但企业为网络安全分配稳定预算至关重要。此项投资应涵盖网络安全防御服务、法规合规以及增强抵御网络威胁的韧性。

将网络安全融入企业战略：它必须是战略规划的核心支柱，与业务目标保持一致。这涉及主动的风险管理、团队持续培训以及先进技术的采用。

保护供应链免受网络威胁：企业应与其供应商签订协议并设定严格管控，以最大程度降低共同风险。这包括要求安全标准、进行定期审计，并确保整个供应链网络遵守保护措施。

云环境中的范式转变

2024年，云基础设施的采用经历了显著增长，巩固为组织寻求利用灵活性并增强韧性而青睐的策略之一，并催生了混合云或多云环境。

根据欧盟的数字十年目标，预计到2030年，75%的公司和组织将已采用云技术。

然而，这一发展带来了新的挑战，并将导致网络攻击数量显著增加。CrowdStrike警告称，在2023年至2024年期间，这些攻击增加了75%。[11]。

近期重大事件凸显了配置不当的云环境的脆弱性。根据 Gartner 的预测，到 2027 年，云中 99% 的泄露记录将源于人为错误，例如配置错误或泄露的登录凭证，而非云服务提供商的故障。[12] 身份和访问管理（IAM）失败、数据窃取以及高级持续性威胁（APT）等问题正使采用更强大的网络安全策略的紧迫性倍增。传统方法已不再足够：清晰定义的安全边界概念已过时，取而代之的是对能够适应去中心化环境的更动态保护模型的需求。

75%

到2030年，许多公司和组织将采用云技术。[7]

75%

2023年至2024年间，云环境中的攻击记录是否有所增加？[8]

99%

到2027年，这些被泄露的记录将源于人为错误。[9]

3%

各公司均需在云安全所有关键领域维持最新的计划。[10]

[7] 欧盟委员会（n.d.）。云计算。欧盟委员会数字战略。https://digital-strategy.ec.europa.eu/es/policies/cloud-computing
[8] CrowdStrike。(2024)。全球威胁报告2024。[https://go.crowdstrike.com/global-threat-report-2024.html]
[9] 高德纳。（2023）。可用于评估云安全控制的成果导向型指标。https://www.gartner.com/en/documents/4789831
[10] CrowdStrike.（2024）.同上。
[11] 同上
[12] 高德纳。（2023）。同上。

趋势

尽管零信任模型近年来经历了显著增长，但随着向云环境的迁移，其采用预计将成为标准。

该范式基于怀疑论哲学，即网络内部或外部的任何实体均不被自动信任。在私有网络允许任何访问或数据传输之前，必须对所有用户和设备进行严格的身份验证和授权，无论它们是否位于该网络的边界之内。

致力于零信任方法的公司将需要深入理解生态系统，以克服四大挑战：

1. 管理共同责任模型：虽然云服务提供商负责底层基础设施的安全，但组织必须管理配置、存储数据以及资源访问的安全。忽视这种区别可能导致严重的安全漏洞。

2. 定义有效的策略和配置：网络安全团队必须实施基于角色的细粒度访问控制策略（RBAC），配置详细的权限，仅将访问权限限制在为每个用户或系统所需的资源范围内。此外，通过微边界对应用程序、服务和数据进行分段至关重要，利用下一代防火墙或软件定义网络（SDN）解决方案等技术隔离信息流并限制潜在的安全漏洞。最后，他们必须实施严格的控制措施，例如应用程序白名单、基于上下文（设备、位置、时间）的动态访问策略以及多因素认证（MFA），以减少攻击面并防止未经授权的访问，即使在初始入侵的情况下也是如此。

3. 复杂且去中心化环境中的可见性与控制：持续监控对于确保实时异常检测和响应至关重要。这需要使用先进工具，例如EDR（端点检测与响应）和SIEM，这些工具能够提供对云环境中访问模式、数据传输和可疑活动的全面可见性。

4. 人为错误：人为错误仍然是任何系统中最大的脆弱性之一。对于首席信息安全官（CISO）而言，这意味着要将他们的合作者转化为安全屏障，建立持续性的网络安全培训计划，强化多因素认证等实践，并定期评估团队对模拟攻击的响应能力。

建议

制定全面的云安全策略：确定云环境将如何进行监控，明确要使用哪些具体服务以确保全面且高效的覆盖。为此，必须确定监控工具，并建立流程以主动管理安全。

设计并维护高性能、抗毁和富有弹性的架构：确保所有组件——从虚拟机到应用程序——都经过验证并得到保护。确保进行适当的维护，执行更新并根据技术变化调整架构，以最大化运营效率。

强化云端高级监控与检测：实施检测与响应平台，确保对已部署的基础设施实现实时可见性和控制。

生成式智能网络安全时代

人工智能（AI）在商业领域的应用正蓬勃发展。各行各业、各种规模的公司都在探索如何利用这项技术来优化其生产力。斯坦福大学的一项研究表明，与2023年相比，企业AI投资增长了312%。[1][4]

然而，人工智能的进步也正在改变网络犯罪分子的战术，革新并重塑了威胁格局。网络犯罪分子利用生成式人工智能实施更复杂的攻击，这些攻击范围从鱼叉式网络钓鱼和语音钓鱼等技术，到勒索软件或恶意软件代码的创建，甚至由技术经验不足的用户执行。

鉴于这一情况，组织必须重新思考其网络安全防御策略，采取更具动态性和主动性的方法，以应对日益先进和适应性强的威胁。

79%

这些公司是否沉浸于某些人工智能工具的过程中？[13]

312%

是商业人工智能投资较去年的增长。[14]

70%

到2026年，应用程序设计和开发方面的大部分工作将受到生成式人工智能的影响。[15]

75%

到2030年，欧盟内公司将普遍采用人工智能。[16]

[13] 德勤。（2024）。企业人工智能现状2024。https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf
[14] 斯坦福大学。(2024)。AI指数报告2024。https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf
[15] Gartner。强化您的人工智能（AI）生态系统 https://www.gartner.com/en/information-technology/insights/artificial-intelligence
[16] 经济事务与数字化转型部（2023年）。人工智能和大数据在西班牙企业的应用。西班牙政府 https://www.ontsi.es/sites/ontsi/files/2023-02/Brújula_IA_Big_data_2023.pdf.
[17] 斯坦福大学。(2024)。同上。

趋势

为应对新威胁，各组织正将人工智能融入其防御战略，相关举措包括：

1. 网络钓鱼检测：人工智能可以分析大量电子邮件和消息，识别传统系统可能忽略的可疑模式。

2. 提升事件响应能力：生成式模型整合实时网络攻击数据，识别攻击路径并推荐具体应对措施，从而加速响应速度。

3. 弱点缓解：通过自动生成补丁和主动评估软件，人工智能极大地缩短了处理关键漏洞所需的时间。

4. 预测分析：人工智能通过识别异常行为和预见潜在攻击来提升威胁检测能力。

5. 强化访问策略：基于对用户行为的持续分析，人工智能建议优化配置，以提升身份验证效果并防止未经授权的访问。

2025年，网络安全将标志自动攻击与防御系统之间的博弈。在这个新环境中，速度、适应性和人工智能将成为决定性因素。威胁将随着人工智能而演变，同时改善数字防护的新机遇也将出现。

那些最能快速适应这一变化的组织，将在应对未来安全挑战方面占据有利地位。

建议

投资生成式人工智能（GAI）的培训与工具：仅仅实施人工智能是不够的，团队必须理解如何在网络防御中战略性地应用它。这需要生成式人工智能的专业培训，了解其对安全性的影响，以及使用先进模型进行威胁检测和响应。

制定清晰的技术治理政策：建立治理框架至关重要，该框架需界定企业使用人工智能的边界和标准。这包括关于安全、隐私、伦理和合规的内部规章，确保人工智能成为企业资产而非风险。

促进跨职能团队的协作：确保有效的AI集成需要网络安全、技术、法律与合规等领域的合作。只有采用多学科方法，才能确保实施在技术上稳健且符合国际法规。

增强对OT网络监控的可见性和控制力

技术进步和关键基础设施中数字系统的集成提高了效率和互联互通性，但也增加了网络威胁的风险。尽管面临这些挑战，在过去的这一年里，只有15%的关键基础设施报告了网络安全漏洞，与2021年报告的22%相比，这是一个显著的改进。

这主要是因为对控制网络中远程连接相关风险的认识不断提高，以及对NIS2指令影响的日益关注。该法规不仅对未能遵守其规定者处以严厉处罚，还要求将供应链的全面评估作为安全战略的基本组成部分。

2024年，15%的安全事件涉及第三方或供应商。这一风险不仅限于服务提供商或IT基础设施；与利益相关者的数字接触可能源自组织的任何领域。

特别值得关注的是供应链相关的风险，尤其是与安全远程访问机制实施相关的风险。在许多情况下，这些协议是由供应商自行实施的，这种情况可能导致组织建立的安全政策出现偏差。此外，将安全关键的基础设施边界点委托给第三方会增加潜在的安全漏洞。

与此同时，工业控制系统正越来越多地使用基于云的技术。

15%

这是报告了网络安全漏洞的关键基础设施组织的百分比。 [18]

15%

涉及第三方或供应商的安全事件 [19]

34%

关键基础设施组织发生的云数据泄露事件中，有相当一部分是由人为错误引起的。 [20]

30%

到2025年，关键基础设施将面临安全漏洞。 [21]

尽管它们提供了运营上的便利，但使用相关的风险以及为确保关键基础设施保护而需要更严格的管理，这些都是显而易见的。

如上所述，传统的周界概念正受到挑战，并在OT环境中标志着一个相关范式转变。通过适应性和动态解决方案来应对当今网络安全挑战，在IT/OT环境中加强可见性、监控和威胁检测能力至关重要。

[18] 泰雷兹 (2024)。2024 数据威胁报告 https://cpl.thalesgroup.com/sites/default/files/content/DTR_pages/2024/2024-thales-data-threat-report-critical-infrastructure-edition.pdf

[19] 威瑞森。(2024年)。2024年数据泄露调查报告 https://www.verizon.com/business/resources/Ta2d/reports/2024-dbir-data-breach-investigations-report.pdf

[20] 泰雷兹 (2024)。2024 数据威胁报告 https://cpl.thalesgroup.com/sites/default/files/content/DTR_pages/2024/2024-thales-data-threat-report-critical-infrastructure-edition.pdf

[21] 高德纳公司。(2021年，12月)。高德纳预测，到2025年，30%的关键基础设施组织将遭遇安全漏洞 https://www.gartner.com/en/newsroom/press-releases/2021-12-2-gartner-predicts-30--of-critical-infrastructure-organi

趋势

事实证明，部署了监控工具的公司可将响应时间缩短高达108天。因此，对提升被动网络监控解决方案可见性的日益增长的需求，正推动着创新技术的发展，以应对与资产清单、被动漏洞扫描和威胁检测相关联的挑战。

该领域的一个主要趋势是创建特定模块，旨在将轻量级采集器直接部署在网络电子设备中。

此外，正在开发一种“探索者”代理，它们能够分析所安装设备的连接以及附近的边界。这些代理的开发遵循一种优先考虑其与尽可能多的版本和技术兼容的策略，这有助于它们在网络多个节点部署而不产生干扰。

与此同时，这一技术演进也伴随着EDR解决方案的日益普及。尤其值得注意的是，人工智能被大量用于提升检测和响应能力。EDR代理程序也正被专门开发以适应工业环境，这是加强控制系统和关键操作网络安全的一个关键进展。

建议

为确保工业环境中的有效防御，应对NIST框架（识别、保护、检测、响应和恢复）所确立的五个行动领域至关重要，从而确保对OT网络安全的全面方法。

1. 制定识别和管理供应链相关网络风险的过程。

2. 基于NIST 800-207，采用零信任架构（ZTA）方法，优先保护资产而非网络区域。

3. 建立综合检测系统，整合IT与OT网络的可视化能力，强化两个层面的威胁识别能力。

4. 设计并维护更新版的事件响应计划，整合IT与OT团队，明确界定角色、职责和协调机制。

制定远程访问策略，以降低供应商解决方案带来的风险，并为这些工具建立具体的安全要求。

超越认知

迈向行为安全模型

网络威胁的演变凸显了传统网络安全意识方法的局限性。在人类互动仍然是主要脆弱性传播途径的情况下，仅仅依赖重复且笼统的培训是无效的。根据最近的研究，人为错误导致高达95%的公司安全漏洞：行为方面凸显为一个关键挑战。

此外，人工智能的兴起使网络犯罪得以完善其策略，并发起快速、个性化及自动化的攻击，利用行为漏洞。组织必须做好准备，应对由人工智能驱动威胁所加剧的网络犯罪日益增长的复杂性，例如超个性化网络钓鱼、高级恶意软件和基于深度伪造的攻击。

尽管问题已被识别，但员工的安全意识疲劳和情感疏离是实施真正有效策略的关键障碍。

这种动态且充满挑战的环境要求网络安全领域进行范式转变，即组织不仅要遵守法规，还要将安全作为企业文化的战略支柱来整合。安全意识必须超越培训课程，成为组织行为的基本要素，使员工在面对数字威胁时具备前瞻性的视野。

95%

安全漏洞多是由人为错误造成的。 [22]

38%

有五分之一的员工会将机密的工作相关信息分享给人工智能工具。 [23]

25%

过去两年发生的网络事件中，有相当一部分是由于使用了弱密码。 [24]

75%

西班牙首席信息安全官（CISO）中，许多人认为人为错误是网络攻击的最大脆弱性。 [25]

[22] 世界经济论坛（2022年）。“2022年全球风险报告。” https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf。
[23] 马托雷尔，S. D（2024年9月）。“三分之一员工向AI工具共享机密工作信息”。Bit Life Media https://bitlifemedia.com/2024/09/employees-share-confidential-work-information-with-ai-tools/
[24] 卡巴斯基。（2023）。网络安全中的人为因素：360°报告。https://media.kasperskydaily.com/wp-content/uploads/sites/92/2023/11/22070742/ KasperskyHumanFactor360Report2023.pdf
[25] Proofpoint。（2024）。首席信息安全官的声音2024。https://www.proofpoint.com/es/resources/white-papers/voice-of-the-ciso-report

趋势

在预防和文化建设方面最先进的组织已开始推动方法上的转变：从单纯意识提升到行为安全。这一趋势源于应对日益复杂的威胁、强化组织安全态势的需求。

仅仅开展年度、半年度或月度培训已经不够了，这些培训在很多情况下只是为了满足某些监管要求。尽管这些措施很重要，但它们不足以建立真正的网络安全文化，也无法让员工成为公司在面对周边风险时的积极盟友。

与其只关注提高意识，行为安全则侧重于识别和强化那些能降低实际风险的行为。这一目标意味着要摒弃笼统的建议和标准化的培训，转向个性化的策略。

为使这一新愿景得以实现，在组织层面以及各团队或部门更小的范围内，推动对具体威胁的分析和建模至关重要。随后，将识别出需要解决的关键行为，并制定量身定制的计划，以直接影响人们的日常行为。

这种方法通过创建行为保障措施得到加强，这些措施整合了技术、程序和文化措施，以有效管理风险。通过这种方式，采取的行动将产生风险指标，使策略能够与每个群体的具体需求和脆弱性相一致，从而最大限度地提高影响力和效率。这种整体方法将为重视安全文化的组织构成差异化和竞争优势。

建议

识别并绘制行为脆弱性：根据角色和活动准备诊断，以了解风险区域。

实施定制化项目：用针对独特挑战、促进安全行为的目标干预措施，取代通用培训。

实时监控与调整：利用基于人工智能的系统追踪风险指标并实施主动纠正。

倡导共同责任：让组织各级别——从高层管理到运营团队——都参与到采纳和保持安全习惯中来。

评估行动的影响：以风险降低和组织韧性提升来衡量策略的成功。

我们是网络安全、情报和国防领域的领先西班牙公司。

我们不仅保护基础设施，更将网络安全转化为贵组织在相互联系且充满不确定性的世界中发展、创新和繁荣的战略资产。

独立纯玩家

我们提供独立服务，并提供符合客户需求的定制解决方案。

全生命周期内的运营卓越

从早期威胁检测到先进的响应能力，我们确保在整个安全周期内都能取得卓越成果，即使在最复杂、风险最高的环境中也是如此。

行业经验

我们专注于公共管理、国防、工业、能源和医疗保健等高影响力领域，为每个领域提供量身定制的解决方案。

技术独立与主权

我们提供可靠解决方案，该技术为欧盟100%自主研发，具备自主性与欧洲标准一致性，保障客户的技术主权。

整体解决方案

我们拥有跨界能力，并作为真正的端到端合作伙伴，在信息技术（IT）和运营技术（OT）领域拥有丰富的经验。我们引领信息技术（IT）与运营技术（OT）的融合，为关键基础设施的保护提供集成解决方案。

想知道更多？

安排与我们的专家进行一对一会议，讨论报告，明确您的安全需求与优先级。

联系我们

情报报告

勒索软件展望2024

安排与我们的专家进行一对一会议，讨论报告，明确您的安全需求与优先级。

下载 >

网络弹性法案

我们介绍您应了解的这项新法规的关键要点、其对公司的影响以及您应采取何种措施以应对其实施。

下载 >

虚假信息宣传活动

2024年是全球事件和关键选举之年，虚假信息活动达到了前所未有的复杂程度。这份由S2GRUPO发布的网络情报报告揭示了主要行动的策略和目标，并展示了这些举措如何试图影响和操纵公众舆论。

下载 >


S2GRUPO
Anticipating a cyber secure world