网络空间安全丛书

零基础快速入行 SOC 分析师

(第 2 版)

[美] 泰勒·沃尔(Tyler Wall)
贾勒特·罗德里克(Jarrett Rodrick) 著
贾玉彬　张　超 译

清華大學出版社
北　京

北京市版权局著作权合同登记号　图字：01-2024-5505

图书在版编目(CIP)数据

零基础快速入行 SOC 分析师 ：第 2 版 / (美) 泰勒 • 沃尔 (Tyler Wall), (美) 贾勒特 • 罗德里克 (Jarrett Rodrick) 著 ；贾玉彬, 张超译. -- 北京 ：清华大学出版社, 2025. 5. -- (网络空间安全丛书).--ISBN 978-7-302-69137-2

Ⅰ. TP393.08

中国国家版本馆 CIP 数据核字第 20251YZ429 号

责任编辑：王　军
封面设计：高娟妮
版式设计：思创景点
责任校对：成凤进
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-83470000　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京同文印刷有限责任公司
经　　销：全国新华书店
开　　本：148mm×210mm　　**印　　张**：7.375　　**字　　数**：198 千字
版　　次：2025 年 6 月第 1 版　　**印　　次**：2025 年 6 月第 1 次印刷
定　　价：59.80 元

产品编号：109499-01

关于作者

泰勒·沃尔(Tyler Wall)是 Cyber NOW Education 的首席执行官，该公司专门提供便捷且价格合理的全球网络安全培训和认证服务。泰勒是一位经验丰富的安全专家，曾在全球多家大型企业任职，具有长达十年的安全运营经验。

泰勒拥有普渡大学网络安全管理理学硕士学位，还获得了 CISSP、CEH、CSSK、Terraform Associate、CFSR、LRPA、Security+、Network+和 A+认证。

他喜欢和儿子一起共度闲暇时光，并且喜欢发挥创造力。

关于合著者

贾勒特·罗德里克(Jarrett Rodrick)是 Omnissa 公司的安全运营高级经理，曾任 VMware 安全运营中心的高级经理。他曾是美国陆军的网络防御专家和网络战专家，现已退役。在美国陆军网络司令部和财富 100 强公司主导的世界级安全项目中，他积累了超过 11 年的防御性网络运营经验。贾勒特的教育背景包括获得 SANS 技术学院的应用网络安全理学学士学位和 17 项 GIAC 网络安全认证。他定居在得克萨斯州的梅利萨市，喜欢和儿子一起打高尔夫球，和家人一起玩棋盘游戏。

关于特约撰稿人

马修·彼得森(Matthew Peterson) 是一位有抱负的 SOC 分析师，拥有超过十年的金融服务行业经验，并在软件开发、人工智能和图形设计方面拥有深厚的背景。他获得了雷鸟全球管理学院的全球管理硕士学位和太平洋海岸银行学院的研究生证书。在这本书中，马修将他的专业知识运用到创建图形主题和撰写第 6 章“云端 SOC”中。他擅长将复杂的技术概念转化为清晰、引人入胜的视觉效果和故事叙述。

马修现居亚利桑那州的斯科茨代尔市，他喜欢陪儿子们打棒球，以此平衡职业成就和家庭生活。

杰森·图尼斯(Jason Tunis)是全球最大信贷联盟的安全自动化经理。他主要负责安全和欺诈事件响应、威胁情报以及安全自动化和编排。杰森是一位经验丰富的网络安全专家，拥有超过 15 年的工作经验，他获取的认证包括 CISSP 和 GSLC。他与妻子和三个孩子一起生活在中西部。

关于技术审校者

扎克·加西亚(Zach Garcia)开始从事网络安全事业之前，审校技术图书只是他的业余爱好。他一直对事物的运作方式充满好奇，喜欢创造性地思考用于提高安全性的有趣方法(有时甚至是通过破坏安全性来进行)。

他的职业生涯涉及多个领域，从数字取证、事件响应(Incident Response，IR)角色，到逆向工程恶意软件，再到为多个行业编写恶意软件和进行渗透测试等多个方面。

无法抑制的好奇心，加上对谜题和与人交流的热爱，激发了他对网络安全行业的热情。在闲暇时，扎克喜欢园艺、与家人共度美好时光，以及破解他能接触到的每一台智能设备。

致谢

首先，我要感谢我的妻子海蒂·沃尔(Heidi Wall)无条件地爱着我。我还要感谢我的母亲凯伦·霍奇斯(Karen Hodges)，从小她就让我读书，与我已故的祖母弗吉尼亚·格罗斯·斯特宾斯(Viriginia Gross Stebbins)一起成为我生命中接受教育的明灯，照亮了我的求知之路。我要感谢马修·彼得森(Matthew Peterson)，他是一位有抱负的 SOC 分析师(来自亚利桑那州凤凰城)，为本书的图形展示做出了卓越的贡献，本书中的所有配图都是他设计的。我要感谢我的前任经理扎克·加西亚(Zach Garcia)，自从我遇到他并加入这个项目以来，他一直支持我，并发现了很多我在审校过程中遗漏的内容。我要感谢所有 SOC 故事的作者，希望他们的职业生涯能够充实，并成为世界各地其他人的灵感来源。我要感谢视频制作人迈克尔·阿楚列塔(Michael Archuleta)，感谢他在 Cyber NOW Education 的辛勤工作，感谢他帮助 Cyber NOW Education 走进大众视野。

——泰勒·沃尔

首先，也是最重要的，我要感谢我美丽且可爱的妻子斯泰西(Stacey)。她不断给予我的爱和耐心为我提供了成为网络专业人士所需的支持。我还要感谢无数士兵和军队领导人，在我 16 年的职业生涯中，我有幸向他们学习。从诺克斯堡的军训教官到网络防护旅的

高级军官，他们都在我成长的过程中发挥了重要作用。最后，我要感谢 VMware 为一位即将退役的士兵提供了机会，让我开启了军队以外的职业生涯。能够加入这样一家出色的公司，我倍感荣幸。谢谢！

——贾勒特·罗德里克

序

斯蒂芬·诺思卡特(Stephen Northcutt)
SANS 技术学院和 GIAC 认证创始人

安全运营中心(Security Operation Center，SOC)每天 24 小时不间断地检测、分析和响应网络安全不良事件。这是一项艰巨的挑战，需要资源、管理和可靠的流程。在开始应对这项挑战之前，了解使命和愿景至关重要，这也是本书具有的重要性和相关性的基础。在本书中，我们将了解 SOC 是什么、如何运作、它的重要性，以及如何进入这个领域。在当今的数字环境中，威胁无处不在，SOC 作为防御的堡垒，负责监控、调查、分类和消除不良安全事件。

泰勒和贾勒特具备深入了解组织安全构成部分的知识、经验和热情，明白安全在组织中所发挥的关键作用。无论是内部运营还是外包给托管安全服务提供商(Managed Security Service Provider，MSSP)，SOC 都肩负着保护数字资产免受不断演变的网络威胁的关键任务。

在本书中，作者揭示了 SOC 运作的复杂性，探讨了其责任范围如何因人员配置模型而有所不同。即使你对网络安全完全陌生，作者也提供了所有基础知识。如果你发现自己在说：“我见过这个知识”，请务必在章节末尾做测验，以区分“你见过它”和“是的，你知道它”之间的区别。从内部 SOC 凭借其高级权限，在事件发生时能够快速采取补救措施，到 MSSP 对多个企业网络进行的不间断监管，每种 SOC 方法都有其独特的优势和挑战。

他们全面讨论了基于云的 SOC，以及它在应对云计算固有安全

风险方面所扮演的重要角色。识别这些风险对于制定有效的缓解策略以保护云中的数据至关重要。尽管云计算有明显的优点，如可扩展性和灵活性，但在没有充分了解相关安全风险的情况下，盲目采用云服务是不明智的。

基于云的 SOC 利用先进的技术和监控能力，实时检测和响应安全威胁，从而确保对敏感数据和关键资产的保护。通过将安全运营集中在云端，组织可以增强可见性、简化事件响应流程，并保持对法规要求的遵从性。此外，基于云的 SOC 还支持主动威胁狩猎和持续监控，使组织能够在不断演变的网络威胁面前保持领先，以有效降低风险。

在阅读有关技术的文章时，你不可能没听过 AI，但基于云的解决方案是数字助理最先和最快发展的领域。如果你尚未采用云解决方案，那么本书的作者显然在利用通用的 LLM 工具来提升本地 SOC 能力方面拥有丰富的经验，并且他们还提供了一些技巧和实例。

本书最有价值的内容之一是关于分析的章节：你该如何教会人们解决他们从未见过的问题？你必须制定一个流程或一种方法，并引导他们逐步掌握，这一过程将会在本书中逐步展开。这一模型是作者在无数小时的压力下进行分析的结果。

读完这本书后，我清楚地感受到，作者希望你获得成功。本书内容详尽且条理清晰。我希望你能享受这段旅程。

祝你好运。

前　言

欢迎来到《零基础快速入行 SOC 分析师》的精彩世界！你之所以选择阅读本书，是因为你想参与其中！想要迎接挑战，获取财富！我们会告诉你这个职业的美好前景与无限价值，但首先，我们会谈谈信息安全。如果你进入网络安全行业却没融入这个圈子，那你会错过很多机会。有各种各样的信息安全微社区和针对特定人群的社区，但相对而言，大部分社区希望接纳所有人。有一些社区极为深奥，充满了秘密；有些社区面向首席信息安全官(Chief Information Security Officer，CISO)或工程师；还有军事社区、政府部门的社区，以及破坏者和创造者共存的社区……新进入安全领域的人都有一个共同的渴望，那就是归属感——而信息安全领域恰恰具备这一点！有时，与普通世界的人相处真的很困难，尤其是在你刚起步，独自敲打键盘时(译者注：作者在此想表达的是，在刚入行并独自工作时，可能会感到孤独和难以与外界交流，而信息安全社区可以提供支持和归属感，帮助人们克服这种孤立感)。我们向你保证，还有很多人愿意和你并肩作战。这种情况在会议上经常发生！社区里有很多了不起的人，一开始他们并不总是能够融洽相处，但过了 3～6 个月，一切就像从未发生过一样。本书的目标是让你坐上你梦想的 SOC 分析师宝座，让你意识到，无论你是谁，网络安全都适合你。

本书将涵盖作为 SOC 分析师所需了解的重要内容。网络安全领域有很多空缺岗位，但同样也有很多候选人想要得到这些职位。挑战在于，适合填补这些职位的候选人并不多。我们会向你解释什么是合适的候选人，并提供相关知识来帮助你准备面试。我们不能保证通过阅读本书的内容可以让你从技术领域的初学者变成顶尖高

手。作为作者，我希望你能信任我，我会告诉你如何利用这本书获得成功，但你需要具备一定的技术基础。理想情况下，当你拿起这本书时，你应该已经学习了一段时间的 IT 技能。本书作者泰勒·沃尔和贾勒特·罗德里克，以及撰稿人马修·彼得森和杰森·图尼斯共同努力，旨在使读者能够在所关注的领域中获得显著的专业优势。在本书的结尾，讲述了六个曾经从事过 SOC 分析师职业的人的故事。

通往网络安全成功的道路漫长且时常不易。这条路对于某些人来说也不是一帆风顺，而是蜿蜒曲折、时宽时窄，四处延伸。对很多人来说，成功的定义各不相同。对某些人来说，这可能意味着掌握 CISO 的权力并承担相应的责任，但如果你认真思考这条道路，可能会发现它并不适合你。有些技术专业人员的收入超过 CISO，而且工作更加稳定，每当出现问题时，他们并不会面临被责怪的风险。这并不是说担任 CISO 和领导安全团队没有回报；我只是用这个例子来说明，不同的技术人员根据个人追求的不同，其职业路径和最终目标也是不同的。但迈向有意义职业的第一步始终相同：进入这个行业。在从事网络安全职业的所有步骤中，这是最重要的一步。担任 SOC 分析师的第一年可以为你的网络安全职业生涯奠定基础，这一年可能会令人难以承受，就像从消防水带中喝水一样，虽然能满足需求，但过程极为不适。书中的内容将帮助你开启 SOC 分析师的职业生涯，并使你能够在入职的第一天就能顺利上手。

另外，本书提供了一项免费认证，只需通过书中所涵盖主题的考试即可获得。有关该认证的信息和获取途径可通过扫描本书封底的二维码获得。

请准备好迎接有意义的网络安全职业生涯挑战吧……在第一天上班时，记得挑一把好椅子。

目　　录

第 1 章

对网络安全和SOC分析师的需求

在本章中，我们将分三个不同层次来讨论对网络安全专业人员的需求。首先讨论对网络安全工作人员的需求，然后分析对网络安全分析师的需求，最后探讨对安全运营中心(Security Operation Center，SOC)分析师的需求。

1.1 危机期间的网络安全

2020 年初，全球开始遭受新冠疫情的侵袭。全球各地纷纷封锁，人们被要求居家隔离。许多工作岗位被裁撤或员工被暂时休假，直到隔离措施解除，但许多雇主能够成功过渡到“远程办公”模式。因此，互联网服务提供商的流量出现了持续上升的趋势，视频会议的需求也达到了新的高峰。美国国土安全部将网络安全人员指定为维持基础设施持续运转的必要劳动力，对网络安全人员的需求量比以往任何时候都更为迫切。在此期间，仅在美国就已缺少近 50 万个网络安全岗位，而该行业需要增长 62%的职位才能满足需求。[1]

1 http://www.isc2.org/Research/Workforce-Study.

目前网络安全人员短缺，再加上新冠疫情、网络战争或其他紧急情况等危机，对网络安全人员的需求便进一步增加。网络工作人员短缺的情况愈发严重，网络安全人员的资源也更加匮乏。除了工作时间更长、工作更努力，没有其他解决办法。随着工作压力和工作时间的增加，网络安全工作人员的身心健康都受到了影响。目前没有快速的解决方案或培训新网络安全工作人员的方法，因此产生的结果是劳动力负担过重。

在新冠疫情期间，全世界都在努力保持居家办公的高效性。尽管美国政府一度关闭了除“必要”企业以外的所有企业，但网络安全是其中一种被认为必不可少的职业，并且对技术人员的需求一夜之间激增。[1]

行业从疫情中学到了什么？新冠疫情证明了大量的劳动力在远程工作时可以保持高效。多年来，美国公司一直在努力变得更加环保。无论是为仓库提供可持续能源、实施回收项目，还是为送货车辆使用替代燃料，数千家公司都在全球范围内接受使用可持续资源。现在，居家办公成为可行的选择，公司便利用这一机会减少温室气体排放、提升员工幸福感……当然，还能降低运营成本。从那时起，远程工作便成为一些 SOC 分析师生活的一部分。

这并不意味着所有公司都接受了远程工作带来的好处。根据 JLL 在 2023 年底进行的一项研究[2]，财富 100 强公司的员工平均每周在办公室工作 2.96 天。这是一种混合工作模式，许多公司在新冠疫情后将其作为新的常态。

1.2 对网络安全分析师的需求

如今，我们正身处一场全球网络战争之中。每个国家的每个行

1 https://workingnation.com/covid-19-cybersecurity-and-it-workers-are-essential-in-demand-employees/.

2 http://www.us.jll.com/en/trends-and-insights/research/office-market-statistics-tren.

业都成为网络犯罪分子、政府支持的黑客和从事商业间谍活动的公司的攻击目标。这听起来像是一部由你最喜欢的 20 世纪 90 年代动作明星主演的低成本电影的情节，但事实是每个人都是攻击目标。更令人不安的是，这一切并非始于新冠疫情，这种情况已经持续了几十年。直到最近十年，组织机构才意识到需要加大对网络安全的投资。

备受瞩目的入侵事件给全球各行各业都带来了惨痛教训。2014 年 11 月，索尼影视娱乐公司宣布他们遭遇数据泄露。路透社分析师估计，此次入侵将使索尼公司损失超过 7500 万美元的恢复成本和收入。2019 年 8 月，Capital One 入侵事件导致 1 亿份消费者信贷申请被盗。这两起攻击事件让人们意识到，组建专门的网络安全队伍势在必行。

事实上，根据美国劳工统计局的数据，预计从 2022 年到 2023 年，美国的信息安全分析师职位将增长 32%，而其他计算机相关职位的增长率为 12%，所有职位的总增长率为 0.3%。[1] 对于那些考虑进入网络安全领域的人来说，一个显著的好处是进入该职业领域的门槛相对较低。

几十年来，人们一直秉持着“考上大学，获得四年制学位，找到一份工作”的观念。本书将用一章(第 10 章)来介绍进入网络安全分析师领域的不同途径。但就目前而言，上大学并不是通往美好职业领域的唯一途径，一些高级学位课程对于入门级职位来说完全是在浪费时间和金钱。

当组织机构意识到网络安全的必要性时，通常从构建安全运营中心(Security Operations Center，SOC)开始入手。SOC 负责对网络安全事件进行分类、调查和响应。这个概念并不新鲜。几十年来，军事和执法机构一直在使用战术行动中心(Tactical Operation Center，TOC)来协调冲突期间的行动。与战术行动中心一样，SOC 也是网络安全事件第一响应者的指挥和控制中心。

1 http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

定义 根据 SANS 研究院的定义，网络安全事件是指信息系统或网络中发生的不良网络事件，或此类事件产生的威胁。[1]

SOC 并不是唯一专门应对网络安全事件的团队。许多公司都有专门的数字取证和事件响应团队来支持 SOC 进行调查和响应。

通常，数字取证和事件响应团队负责从 SOC 接手长期调查工作，这样 SOC 可以专注于日常运营和新事件。实际上，大多数数字取证和事件响应分析师都是从 SOC 分析师开始他们的职业生涯的。

1.3 对 SOC 分析师的需求

现在我们已经了解了对网络安全分析师的一般需求，下面我们将讨论你选择阅读本书的原因。也许你正从军队转型到民用部门，或者是一位希望踏入职场的应届大学毕业生。也可能你已经在信息技术领域工作，或者只是自学成才。无论如何，这本书的目的是帮助你成为一名 SOC 分析师。无论你是希望加入网络安全领域的众多专业之一，还是希望逐步晋升到管理层，SOC 分析师职业都是进入网络安全领域门槛最低的职业。成为一名 SOC 分析师是进入这个行业的绝佳战略职位。

在为 SOC 配备人员时，招聘经理会不断面临一些挑战。其中最普遍的挑战是 SOC 的人才流动性。在 SOC 经理为空缺职位招聘到新人员后，他们需要花费几个月的时间来培训新分析师。培训完成后，留住新分析师就成了一个问题，因为新分析师经常被猎头争相招揽，用更高的薪水诱惑他们。安全分析师在一家公司的平均任期仅为 1～3 年。[2] 如今，公司提供的薪酬方案非常丰厚，通常与在公司工作的时间挂钩。一种常见的做法是在 3～4 年内分批提供股票期

1 http://www.sans.org/security-resources/glossary-of-terms.

2 http://www.indeed.com/salaries/security-analyst-Salaries.

权来确保员工留在公司(见图 1-1)。

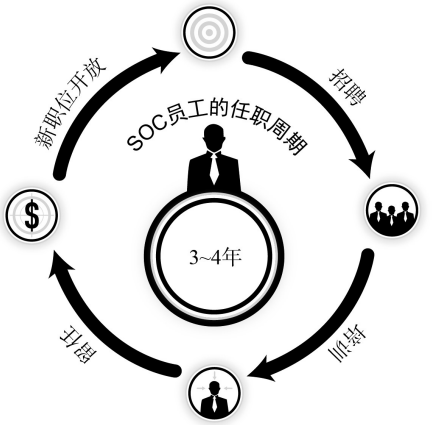

图 1-1　SOC 分析师的常规留任计划

一旦 SOC 分析师熟练掌握工作流程并感到不再有挑战性，他们可能就该寻求更高职位了。向上发展的最常见路径之一是成为高级 SOC 分析师。“高级”这一头衔伴随着更高的薪水和更多的责任，例如，指导加入 SOC 的初级分析师。高级 SOC 分析师还处理更复杂的工作，因为初级分析师会将具有挑战性的任务上报给他们解决。担任这个职位使分析师能够变得更加专业，并有机会学习如何培训和指导他人。这个角色是成为 SOC 经理的绝佳途径，为他们在 SOC 中的下一个领导角色做准备。在美国几乎所有地方，高级 SOC 分析师的年薪都超过六位数。

作为一名新的 SOC 分析师，要为自己设定更高的目标以达到这一里程碑。然而，这也意味着招聘经理可能需要再次为你造成的这个职位空缺寻找合适的人选！

SOC 经理还面临的另一个问题是员工倦怠或告警疲劳。例如，分析师可能在处理大量告警时，忽视了某些重要信息，导致其在“噪音”中迷失。SOC 分析师通常轮班工作，工作时间为 8 小时、10 小时或 12 小时，有时还包括晚上和夜间班次。随着时间的推移，任务

可能会显得单调乏味。当工作变得习以为常时，很容易变得自满，工作也可能变得枯燥。SOC 中的大多数人都很聪明，需要不断接受挑战。

SOC 经理面临的第三个挑战是全天候的运营，这意味着他们需要在正常工作时间之外以及节假日进行工作。许多国际化公司采用“全天候”(follow the sun)的 SOC 模式，即在不同地理位置建立三个 SOC，以实现 24 小时覆盖。通常，公司会在美国设立一个 SOC，在新加坡或澳大利亚设立第二个，在印度或欧洲设立第三个。然而，在某些情况下，公司需要用到具有特定国籍的分析师来处理他们的数据。为托管安全服务提供商(Managed Security Service Provider，MSSP)配备人员时尤其如此。

招聘早班和夜班员工并不容易，而且这些岗位上的员工通常不会待太久，就希望回归正常的工作时间。泰勒的第一份安全工作是在一家托管安全服务提供商(Managed Security Service Provider，MSSP)的 SOC 担任第二班(夜班)分析师。这份工作在当时对他来说非常合适。他有一份基本工资，并因为是第二班而获得少量的班次补贴。他刚刚大学毕业，真的需要在中午之前就起床吗？他将自己的职业发展归功于当时做出的这一牺牲，因为这给他提供了宝贵的经验，至今仍然对他有帮助。经过一年时间的工作，他决定利用自己的经验寻找新的机会。这是一个艰难的决定，因为那是一家很棒的公司，但他等不及一个白班的职位空缺出来。夜班的工作开始对他的身体产生影响。这并不是任何人的错，但这是 SOC 人才流动频繁问题面临的另一个挑战。

SOC 不会很快消失。随着每一项新的隐私法的发布和企业必须遵守的合规与监管要求的增加，对 SOC 的需求也在增长。SOC 在企业中是一个昂贵的成本中心。除非 SOC 是你产品的一部分并带来收入，否则它会给公司增加成本。所需招聘的 SOC 分析师越多，企业就越会寻找创造性的方法来减少在 SOC 上的支出。这一需求催生了一系列工具，这些工具有望自动化 SOC 分析师的部分日常工作。

提示　安全编排自动化和响应(Security Orchestration Automation and Response，SOAR)工具有望减少 SOC 分析师完成任务所花费的时间。第 7 章将对此进行详细说明。

1.4　本书内容

截至 2023 年 10 月，全球大约有 550 万名网络安全专业人员，但这一数字必须增长近一倍才能满足日益增长的需求。[1]这对你意味着什么？这意味着拥有适当技能和资格的个人应该会相对容易找到工作。如果我们研究一下公司当今面临的招聘挑战，就会发现技术精湛的网络安全专业人员仍然供不应求，更不用说找到具有商业头脑的候选人。网络安全专业人员的需求源于互联网已成为一个全球战场。互联网上的每个人都在不断受到攻击，每几秒钟就可能遭遇一次。网络安全专业人员保护企业免受成功入侵，并在攻击者突破防线时做出有效应对。这个领域为专业人士提供了巨大的机会。由于需求如此之高，具备本书所述技能的合格人员更有可能被聘用。

候选人不仅需要具备专业技能，还需要知道如何与业务的其他团队互动，以展示他们对业务目标、目的和文化的理解。认识到网络安全招聘经理面临的这些挑战，可以帮助你为面试做好准备或与上司讨论晋升事宜。这本书将为你提供所需的工具，以制定良好的策略，从而顺利过渡到网络安全的前线。

当你阅读本书时，我们将通过解释典型的安全组织如何自上而下构建，为你提供应对商业洞察力挑战所需用到的知识。理解网络安全的“全局视角”至关重要，因为如上所述，了解公司内部的工作方式对于你能否成为合格的 SOC 分析师至关重要。

1 www.statista.com/statistics/1172449/worldwide-cybersecurity-workforce/#:~: text=Number%20of%20cybersecurity%20professionals%20worldwide%202023%2C%20b y%20country&text=The%20number%20of%20professionals%20working,from%204.6%20million%20in%202022.

在基本层面上，同样受到资金支持的网络安全项目通常具有相似的结构，唯一的例外是当安全是业务的产品时。托管安全服务提供商(Managed Security Service Provider，MSSP)向客户出售安全解决方案，其中许多 SOC 角色是面向客户的。MSSP 往往有更强大的层级结构，有时会包括诸如 SOC 总监这样的职位。根据我们的经验，MSSP 的文化也有所不同，因为安全是 MSSP 营利的方式，所以 CEO 始终是“安全人员”。

另一方面，内部 SOC 往往对企业的安全架构和工程拥有更多控制权。SOC 分析师可以深入基础设施，了解网络的细节。与 MSSP 的客户是外部第三方公司和组织不同，内部 SOC 的客户是公司本身。这些 SOC 分析师在安全事件发生时被赋予更多干预权，以便解决问题。虽然这听起来是件好事，但一次错误的决策可能会对整个网络产生负面影响，并成为一个“简历生成事件”(resume-generating event)。(译者注：“简历生成事件”指的是一种严重的失误或事故，这种情况可能会对个人的职业生涯产生重大影响，甚至可能导致他们在未来找工作时不得不在简历上提及这一事件。通常，这种事件会被视为一个显著的失误，可能影响个人的声誉和职业发展。这里指的是分析师在日常工作中犯的一个错误导致他们被解雇。)

一旦你被聘用，你在安全运营中心的第一天可能是你经历过的最具挑战性的一天。你可能会因为各种术语、新的安全工具以及一些在正规教育中未曾涉及的技术而感到无所适从。而且，外行人会认为你是网络安全专家，他们会向你寻求建议。你可能需要长达一年的时间来适应这一切，直到你感到舒适并能够松一口气。记得对自己宽容一点，保持耐心。我们的目标是帮助你缩短不适应的时间。我们将通过让你熟悉日常可能使用的标准工具，帮助你解决招聘经理面临的技术能力挑战。

我们还将帮助你克服技术熟练度挑战，引导你像 SOC 分析师一样思考。学习分析性思维的方法有很多，对于某些人来说，这种分析性思维可能更自然。重要的是要知道，对于任何人而言，这种分析性

思维并非遥不可及，我们指的是任何人。传授高难度的技术技能最好留给 SANS 的专业人士，但本书将填补你快速入行 SOC 分析师职业所需的空白。

对网络安全人员的需求非常巨大，但职位空缺是因为缺乏合适的求职者，而不是求职者的数量不足。很多人都想获得与业内从业者一样的薪水和生活方式。然而，招聘经理现在迫切需要帮助，他们会选择那些需要经过最少培训的候选人。他们需要聘用那些能够立即上手工作的人员！

通过阅读本书，我们将帮助你识别与你每日互动的 SOC 外部人员和业务部门的优先事项和目标，以便你能够有针对性地与他们进行沟通。我们还会向你展示如何在你的结论中使用能够保护你和公司利益的语言，尤其是在你刚担任这一角色时。

1.5　小结

对网络安全专业人才的需求正在迅速增长，远远超过行业培训候选人和填补职位的速度。招聘经理面临的挑战至少有两个方面：他们无法找到技术熟练的候选人，也找不到了解业务的候选人。这种技术与业务技能的结合至关重要，尤其是在你的网络安全职业生涯发展过程中，这种能力变得愈加重要。

仅在美国，网络安全分析师职位预计从 2022 年到 2023 年将增长 32%，而 IT 相关职位的增长率为 12%，所有职位的总增长率仅为 0.3%。当世界面临危机时，网络安全工作者至关重要。随着我们所做工作的需求急剧增加，这往往意味着现有员工必须加班加点，而招聘新员工可能需要花费数月时间。

SOC 分析师是进入网络安全领域的最低门槛，而本书将帮助你为获得第一份工作做好准备。SOC 的人员流动频繁，这意味着总有新的职位可以申请。在下一章中，我们将讨论应关注的职位名称、典型的招聘网站以及将求职申请转变为面试的策略。

第 1 章　测验

① 预计仅在美国，2022 年至 2023 年期间信息安全分析师职位的数量就会增长_____。

Ⓐ 5%　　Ⓑ 32%

Ⓒ 12%　　Ⓓ 15%

② SOC 代表_____。

Ⓐ 标准运营委员会　　Ⓑ 安全运营中心

Ⓒ 安全运营委员会　　Ⓓ 安全绿洲中心

③ SOC 负责网络安全事件的分类、调查和_____。

Ⓐ 响应　　Ⓑ 报告

Ⓒ 经验教训　　Ⓓ 取证

④ 信息系统或网络中发生的不良网络事件称为网络安全_____。

Ⓐ 事件　　Ⓑ 事项

Ⓒ 错误　　Ⓓ 伤亡

⑤ 以下都是 SOC 招聘经理面临的独特挑战，但_____除外。

Ⓐ 合格的 SOC 申请人数多于空缺职位

Ⓑ 培训新的 SOC 分析师，然后他们流失到其他公司

Ⓒ 处理分析师倦怠问题

Ⓓ 配备全天候运营人员

⑥ 为了在内部为 SOC 配备合适的人员，组织通常会使用_____方法。

Ⓐ 追逐月亮(Chase the moon)

Ⓑ 全天候(follow the sun)

Ⓒ 忽略时钟(ignore the clock)

Ⓓ 避开紫外线(avoid uV rays)

⑦ MSSP 代表_____。

Ⓐ 管理超级安全提供商

Ⓑ 托管的安全盾牌生产商
Ⓒ 管理保障盾牌提供商
Ⓓ 托管的安全服务提供商

⑧ 以下关于 MSSP 的论述均正确，除了_____。
Ⓐ 他们销售安全解决方案
Ⓑ 他们深入研究基础设施，了解网络的来龙去脉
Ⓒ 他们拥有更强大的人员层次结构
Ⓓ 他们解决了许多公司不愿面对的网络安全人员配备难题

⑨ 作者表示，可能需要_____才能适应新的 SOC 分析师角色。
Ⓐ 60 天　　Ⓑ 三个月
Ⓒ 六个月　　Ⓓ 一年

⑩ _____思维在 SOC 分析师职业中最为重要，而且它是可以传授的。
Ⓐ 感性　　Ⓑ 创造性
Ⓒ 分析性　　Ⓓ 抽象性

⑪ 在网络安全领域的所有工作中，SOC 分析师面临的进入门槛是_____。
Ⓐ 最高的　　Ⓑ 最低的
Ⓒ 最长的　　Ⓓ 最大的

第 1 章　测验答案

① 预计仅在美国，2022 年至 2023 年期间信息安全分析师职位的数量就会增长_____。

Ⓑ 32%

根据美国劳工统计局的数据，预计 2022 年至 2023 年，美国信息安全分析师职位将增长 32%，而其他计算机相关职位的增长率为 12%，所有职位的总增长率为 0.3%。

② SOC 代表_____。

Ⓑ 安全运营中心

SOC 代表安全运营中心。

③ SOC 负责网络安全事件的分类、调查和_____。

Ⓐ 响应

首先进行检测，然后对告警进行分类、调查和响应。SOC 以检测和响应而闻名。

④ 信息系统或网络中发生的不良网络事件称为网络安全_____。

Ⓐ 事件

信息系统或网络中发生的不良网络事件称为网络安全事件。

⑤ 以下都是 SOC 招聘经理面临的独特挑战，但_____除外。

Ⓐ 合格的 SOC 申请人数多于空缺职位。

对于大多数 SOC 来说，拥有比空缺职位更多的合格 SOC 申请人通常不是什么挑战。

⑥ 为了在内部为 SOC 配备合适的人员，组织通常会使用_____方法。

Ⓑ 全天候(follow the sun)。

大多数 SOC 采用“全天候”人员配置方式，提供 24/7/365 全天候服务。

⑦ MSSP 代表_____。

Ⓓ 托管的安全服务提供商

首字母缩略词 MSSP 是托管安全服务提供商。

⑧ 以下关于 MSSP 的论述均正确，除了_____。

Ⓑ 他们深入基础设施，了解网络的来龙去脉。

通常，MSSP 对其客户网络的熟悉程度不如在公司工作多年的内部员工。

⑨ 作者表示，可能需要_____才能适应新的 SOC 分析师角色。

Ⓓ 一年

如果你是网络安全新手，这可能是一次难以承受的经历，并且可能需要整整一年的时间才能适应工作惯例。

⑩ _____思维在 SOC 分析师职业中最为重要，而且它是可以传授的。

Ⓒ 分析性

虽然其他思维有助于你取得成功，但分析性思维至关重要。

⑪ 在网络安全领域的所有工作中，SOC 分析师面临的进入门槛是_____。

Ⓑ 最低的

由于招聘经理面临许多挑战，因此 SOC 职位通常是最容易获得的。