简译版

“SOC 即服务”：在资源不足的情况下防御网络威胁

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	SOC-as-a-Service promises threat protection in a world of scarce resources		
原文作者	A.N.Ananth	**原文发布日期**	2019 年 8 月 13 日
作者简介	A.N.Ananth 是 Netsurion 公司首席战略官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2019/08/13/soc-as-a-service/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

“SOC 即服务”：在资源不足的情况下防御网络威胁

A.N.Ananth

2019 年 8 月 13 日

尽管近几十年来技术不断进步，且各方投入了数百万美元进行研究，但是网络威胁仍然喧嚣尘上。网络威胁不断肆虐，对全球几乎每个行业都造成了巨大的经济损失。据 Ponemon 研究所的研究报告指出，在过去的 5 年中，数据泄露的平均成本增长了 12%，达到 392 万美元。对大多数公司来说，这笔钱本可以用在更好的地方。

目前，市场上有近千种网络安全技术。这本是个好消息，但是还存在两个重要问题。第一，创建安全运营中心（SOC）所需的硬件和软件成本高昂；第二，企业缺乏熟练的安全分析师，难以将这些技术应用到企业的实际环境中，保护企业的网络安全。

事实上，大约 80%的企业表示，他们没有足够的分析师来运营 SOC；48%的企业表示他们甚至没有 SOC。那些有 SOC 的公司，通常是能够提供必要资源的全球 500 强企业。这些资源包括完整的、适合其企业特定环境的安全信息和事件管理（SIEM）系统，该 SIEM 系统能够为 SOC 平台提供可视性。总而言之， SOC 平台是资源高度密集型的。

在这种情况下，一种实用又经济的方法——“SOC 即服务”（SOC-as-a-Service），开始受到关注。该方法通过外包的 SOC 团队，来帮助企业内部员工监控和发现威胁、实现企业业绩目标并增强企业风险承受能力。该 SOC 即服务团队能够将大多数（如果不是全部）基本安全监控技术（包括 SIEM）集中在一个平台上。

这不是千篇一律的而是预配置了安全控制措施的 SIEM。这是一个 SOC，允许企业将精力放在其他地方，同时还能让企业安全运行——一旦出现威胁，该 SOC 就会向企业发送告警和说明。此外，鉴于企业了解自己网络和业务，企业清楚哪些才是正常的网络行为。

通过与外包团队分享这些信息，企业可以帮助他们快速了解其业务和运行环境。这样一来，企业可以获得两全其美的优势：既获得了高级威胁防护，同时付出较低成本，将企业风险控制在可承受范围内。在一些 SOC 外包服务中，企业可以与他们协商，指定关注特定的重要威胁，并约定如何升级和优先处理这类威胁。同时，将这些问题交给外包安全专家团队，能够显著降低企业人员、流程和平台问题的成本和复杂性。

但是，当企业的网络连接断开时会如何呢？当然，任何收集网络事件数据并将其关联到其他地方（例如，关联到云托管环境或数据中心，以便远程 SOC 团队使用）的 SOC 即服务，依赖于企业与服务提供商之间的网络连接。因此，企业应向潜在 SOC 即服务提供商询问这一问题，这一点很重要。理想情况下，SOC 团队会将网络中断视为一种告警，他们会识别企业网络中断，帮助企业确定网络中断的范围以及可能出现的任何漏洞。

在网络中断期间，只要每个端点上的基于软件的安全探针仍在运行，用户和企业的数据收集就不会中断，这一点很重要。这类数据仍然要被收集，防止网络连接恢复后出现审计跟踪差距。此外，企业应审查与服务提供商签订的合同，并认识到服务提供商的服务水平与价格成正比。

在合同方面，每个 SOC 即服务提供商都会提供独特的服务和支付条款。但这些通常是基于订阅的服务，包含年度和/或月度支付条款，以及向上或向下扩展功能以满足企业特定需求的可选条款。关于提供商的服务，企业应询问以下问题：

- 除了纵向（出入企业）网络流量，该服务是否保护横向（企业内部）网络流量，以便检测横向移动攻击。
- 该服务是否允许客户访问 SIEM 系统和报告
- 该服务在进行威胁检测时是否满足法规合规性

许多网络安全公司提供了各种形式的 SOC 即服务，这些服务之间存在很多差异。其中一些公司是托管安全服务提供商，他们拥有员工，但是通过特定的 SIEM 平台将技术标准化。也有一些公司是托管检测和响应提供商，他们依赖并帮助客户选择 SIEM。

此外，还有一些公司使用各种网络流量分析工具，而不采用 SIEM 平台，并提供“守门人”服务，通常不会为客户提供任何可见性，也不让客户参与安全策略。最后，还有一些公司是 SIEM 平台供应商，他们有自己的 SOC 团队，提供共同托管 SOC 服务，为客户完成繁重的工作，同时让客户的 IT 员工参与安全策略，解决客户环境的独特问题。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十五亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com