In the Boxing Ring
AUG 2025

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2025年8的 In the **Boxing Ring**

本月，Network Box 常务董事 Michael Gazeley 探讨了**为什么一个真正 全年无休、全天候（24×7×365）运行的安全运营中心（SOC） 对现代组织的网络安全至关重要**。在当今的威胁环境中，网络攻击可能发生在凌晨 3 点、周末，甚至节假日期间。一个小小的盲点就可能让攻击者在数秒内渗透并破坏您的网络。只有一个为此专门建立、配备人工值守、真正 24×7×365 运行，并由共享威胁情报与严格的国际认证支持的安全运营中心，才能提供实时、全面的网络防护。
在第 2 至第 4 页，我们将探讨这样的 SOC 如何将网络安全从被动的“救火”转变为主动的防御。

在第 5 页，我们重点介绍了本月 补丁星期二 中即将发布的针对 Network Box 5 与 8 以及我们云服务的一系列改进和修复。

在其他新闻方面，Network Box 香港参与了由 WTIA 合作举办的 Tech Connect 活动。与此同时，我们欣然宣布本月正式推出 S-88i 硬件设备。此外，针对近期发生在 国泰航空、路易威登以及香港邮政 的数据泄露事件，Network Box 常务董事 Michael Gazeley 在《南华早报》（SCMP）上分享了他的专业见解。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2025

本月摘要:

为什么一个真正24×7×365的安全运营中心（SOC）对现代组织的网络安全至关重要

网络对手从不休息。无论是凌晨三点、周末，还是公共假期，他们都会不断探测漏洞。黑客、恶意软件以及不良内容始终试图进入您的网络，网络犯罪分子也在不停地尝试窃取您的机密数据。
如果缺乏 不间断的监控，从出现入侵迹象到攻入网络之间，就会存在一个时间窗口——有时仅以秒计算。

by Michael Gazeley
Managing Director
Network Box Corporation Limited

一个真正 24×7×365 运行的安全运营中心（SOC），依托专门建设的设施，由分析员分三班倒、全天候值守，确保监控无死角。相比之下，那些所谓的“云 SOC”或内部“虚拟 SOC”，往往只由一个有限团队运营，缺乏全职人员值守，更多依赖 工作时间内的自动告警 以及 非工作时间的工人待命处理。
这种差别绝不仅仅是文字上的区别，而是 持续警戒 与 被动救火 之间的鸿沟。

尝试用内部云驱动的方案来替代专业 SOC，表面 上似乎很有吸引力：租用 虚拟基础设施，部署 安全信息与事件管理平台（SIEM），订阅威胁情报，安排少数安全工程师在上班时段监控。
然而，一旦办公室关闭，这个有限团队只能依靠 待命轮值、VPN 访问和个人设备 来应对。结果是响应时间延长、人员疲劳增加，小型事件可能迅速升级为严重的安全漏洞。

相反，一个 有人值守、真正 24×7×365 运行的物理 SOC 能保证随时有分析师在第一时间发现、调查并处置威胁，而无需依赖下班后的临时支援。

财务优势

选择托管 SOC 的财务理由同样十分充分。内部运营成本高昂：夜班和非正常工时的分析师需要额外津贴；SIEM、终端检测与响应工具、威胁情报订阅、安全日志存储的许可证费用持续累积；工程师还需要不断更新认证（如 CISSP、GIAC GCIH、CREST、OSCP 及各类厂商认证），哪怕他们处理事件的频率并不高。
托管 SOC 优势明显：这些费用由广泛的客户群体分摊，实现规模经济，同时提供可预测的定价。相比之下，内部虚拟方案往往陷入不可控的加班成本、许可证续费，以及“名义上的 24×7×365 覆盖”所带来的虚假经济性。

超越防火墙的专业能力

真正的 SOC 拥有多层次的专家队伍：一级与二级分析员、威胁情报专家、事件响应人员和取证工程师。他们能够剖析各种攻击手法，从零日漏洞利用到供应链入侵，借助跨行业的经验积累，形成丰富的威胁应对能力。
反观内部团队，他们通常只能看到自己网络的告警，错过了跨行业攻击模式、大规模红队演练，以及成熟的事件响应流程。这种局限意味着他们难以提前预判 防火墙之外的威胁。

认证体现卓越

保持顶级国际认证进一步凸显差距。一个合格的 SOC 通常持有：

- ISO 9001（质量管理）
- ISO 20000（IT 服务管理）
- ISO 27001（信息安全管理）
- ISO 31000（风险管理）
- PCI DSS（支付卡行业数据安全标准）
- 以及 SG CyberSafe、GB Cybersecurity 等认证。

这些认证均需要巨额投入与专业机构（如瑞士 SGS、德国 TÜV）的深度合作与审核。

实时共享情报

共享情报 是只有外部 SOC 才能提供的强大倍增器。
当某个客户的系统在凌晨 3 点发现一种新的勒索软件变种时，托管 SOC 能够实时在全球范围内更新检测规则。
而一个封闭的“云 SOC”必须等到内部事件复盘后才会更新规则集，使您的防御在此期间处于暴露状态。
托管服务商会聚合跨地域、跨行业的威胁数据，快速增强防御能力——通常还结合人工智能，对新兴攻击行动形成整体应对。这种全局视角是任何单一企业在虚拟边界内都无法复制的

全面能力

一个真正的 SOC 集结了完整的专业技能组合：

- 告警分级与处置
- 深度调查
- 威胁狩猎
- 漏洞评估
- 事件隔离
- 合规映射
- 暗网监测

内部团队往往缺乏其中一项或多项功能，只能外包或推迟复杂任务。结果就是一种 “补丁式、祈祷式”安全，而非全面战略。
外部 SOC 则能整合 治理、风险与合规（GRC）专家，将技术遥测数据转化为董事会层面的报告，确保既满足监管要求，又提供可执行的安全建议。

有价值的指标

指标很重要。托管 SOC 提供透明的 关键绩效指标（KPIs）：平均检测时间（MTTD）、平均响应时间（MTTR）、误报率、以及映射至公认框架的威胁覆盖率。这些 KPI 为业务决策提供依据，并能客观展示安全计划的有效性。相比之下，内部云 SOC 往往缺乏严格的服务等级协议（SLA）与报告纪律，使管理层只能依赖零散的口头更新，而非量化证据。

提升战略聚焦

将 24×7×365 安全运营外包，能让内部团队专注于战略性项目，例如：

- 将安全嵌入开发生命周期（DevSecOps）
- 构建零信任架构
- 自动化合规检查

摆脱了夜间告警处理的压力，核心人员就能推动 数字化转型与风险缓解项目，从而加速企业业务增长。

持续合规验证

可信赖的 SOC 服务商会接受严格的审计，如 SOC 2 Type II、ISO 27001、PCI DSS，并定期进行红队/蓝队演练。
这种持续的验证与改进循环可以避免组织陷入自满。
相比之下，云端或虚拟的内部 SOC 也许在初期能达成某些合规里程碑，但随着人员流动和预算调整，往往难以长期维持。

实体 **SOC** 与内部云 **SOC** 之间的差距极为明显。一个真正 **24×7×365** 全天候运作、三班倒值守 的实体 **SOC**，依托共享情报与完整的专家团队，能够提供始终如一的实时防御；
而一个由小型内部团队管理的云端或虚拟 **SOC**，则受限于人力、专业能力和被动的工作流程，必然会留下被有心攻击者利用的安全缺口。

投资于真正的 **SOC** 并非可有可无的成本，而是必不可少的战略资产。
它能将网络安全从“成本中心”转变为 韧性之盾，确保您的组织 始终安全、随时响应、全面准备——每一天、每一小时、全年无休。

Network Box 5
NEXT GENERATION MANAGED SECURITY

NETWORK BOX 8

Network Box 5 和 8 新特性
2025年8月

2025年8月5日星期二，Network Box 将发布本月的 Patch Tuesday 更新包。区域安全运营中心（SOC）将在接下来的14天内分阶段推进新功能的部署。

本月, 针对Network Box 5 和 8 的更新如下:

NBRS-5

- 改进 Office 365 实体同步（特别针对网络连接不佳时的情况）
- 增强对 DNS 服务器和根递归解析器配置选项 的支持
- 优化搜索功能，以支持即将上线的 Box Mail 移动应用 改进
- 在 管理门户中新增对 S-80i 设备型号 的支持
- 改进防火墙规则中 备注信息的处理
- 修复 VPN-5QB 设备型号识别 的问题
- 引入 网络代理中流量“tickling”机制的可配置选项
- 针对 区域 SOC IP 地址 进行常规维护与整理

NBRS-8

- 实现系统级的 审计功能，支持细粒度的可配置控制，以提升 主机入侵检测系统（IDS）
- 改进 软件包更新系统
- 优化 “show network utilisation summary” 命令输出
- 改进 “show disk utilisation detail” 命令输出
- 优化 “show disk status” 命令输出，特别是对 NVMe 硬盘 的支持
- 新增对 M-298i 和 M-398i 设备型号的可选网络接口模块 支持
- 增强基于时间的防火墙规则支持，并支持本地时区
- 防火墙与系统日志 进行全面优化
- 增强对 DNS 服务器和根递归解析器配置选项 的支持
- 改进 设备配置（provisioning）速度与可靠性
- 新增 磁盘分区维护支持
- 改进对 Wireguard VPN 日志的支持
- 在未配置的网络接口上禁用 DHCP
- 改进 Office 365 实体同步（特别针对网络连接不佳时的情况）
- 引入设备类型指纹识别，特别针对虚拟设备

在大多数情况下，以上变更不会影响正在运行的服务，也不需要重启设备。然而，在某些情况下（根据配置不同），可能需要重启设备。如果需要，您的本地SOC将与您联系并安排相关操作。

如果您需要以上内容的进一步信息，请联系您的本地 **SOC**。
他们将负责安排部署和协调工作。

Network Box HIGHLIGHTS

NETWORK BOX

S-88i 硬件平台
面向小型办公室

Network Box 欣然推出全新 S-88i，专为小型办公室、分支机构、家庭办公室或任何寻求强大 UTM+ 与 VPN 防护 的紧凑型场所设计。
S-88i 拥有卓越的硬件规格，并基于 NBRS-8 平台运行，将逐步取代 S-80i（S-80i 的官方支持将于 2028 年 6 月 结束）。

Processor	64bit, 4.4GHz x 2 Performance Cores 64bit, 3.3GHz x 8 Efficiency Cores
RAM	16GB, 3200MHz DDR4
Storage	320GB M.2 NVME SSD
Networking	6 x 2.5Gb RJ45
I/O Interface	1 x SIM card slot 1 x reset button 1 x RJ45 management console 2 x USB 3.1

Network Box 香港
参加 Tech to Connect 网络安全研讨会

Network Box 香港参与了由 香港无线科技产业协会（WTIA）合作举办的 Tech to Connect 网络安全研讨会。
Network Box 常务董事 Michael Gazeley 担任活动主讲嘉宾，并发表了题为 “AI Shield：人工智能如何改变网络安全” 的演讲。
此次活动吸引了高级管理人员、IT 专业人士、SEO 工程师、数据分析师、企业领导及科技爱好者，地点为 KOHO 中心。

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581
www.network-box.cn

Network Box 媒体报道

SCMP
解析 | 香港三起数据泄露事件后，如何保护您的个人信息

LINK:
https://tinyurl.com/ykhycv7v

South China Morning Post

翻译：Jason