In the Boxing Ring
AUG 2025

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the August 2025 edition of In the **Boxing Ring**

This month, Network Box Managing Director Michael Gazeley discusses **why a true 24×7×365 Security Operations Centre is indispensable for modern organisations' cybersecurity**. In today's threat landscape, a cyber attack can happen at 3 am, over weekends and during holidays. A single blind spot can let attackers infiltrate and compromise your network in seconds. Only a purpose-built, human-staffed Security Operations Centre (SOC) running true 24×7×365, backed by shared threat intelligence and rigorous international certifications, can provide real-time, comprehensive cyber protection. On pages 2 to 4, we discuss how such an SOC can transform cybersecurity from reactive firefighting into proactive defence.

On page 5, we highlight the set of enhancements and fixes to be released in this month's Patch Tuesday for Network Box 5 & 8, and our cloud services.

In other news, Network Box Hong Kong participated in **Tech Connect**, organised in association with WTIA. Also, this month, we are pleased to announce the release of the **S-88i** hardware unit. In addition, following the recent data breaches at *Cathay Pacific*, *Louis Vuitton*, and *HK Post*, Network Box Managing Director Michael Gazeley shared his insights with the **SCMP**.

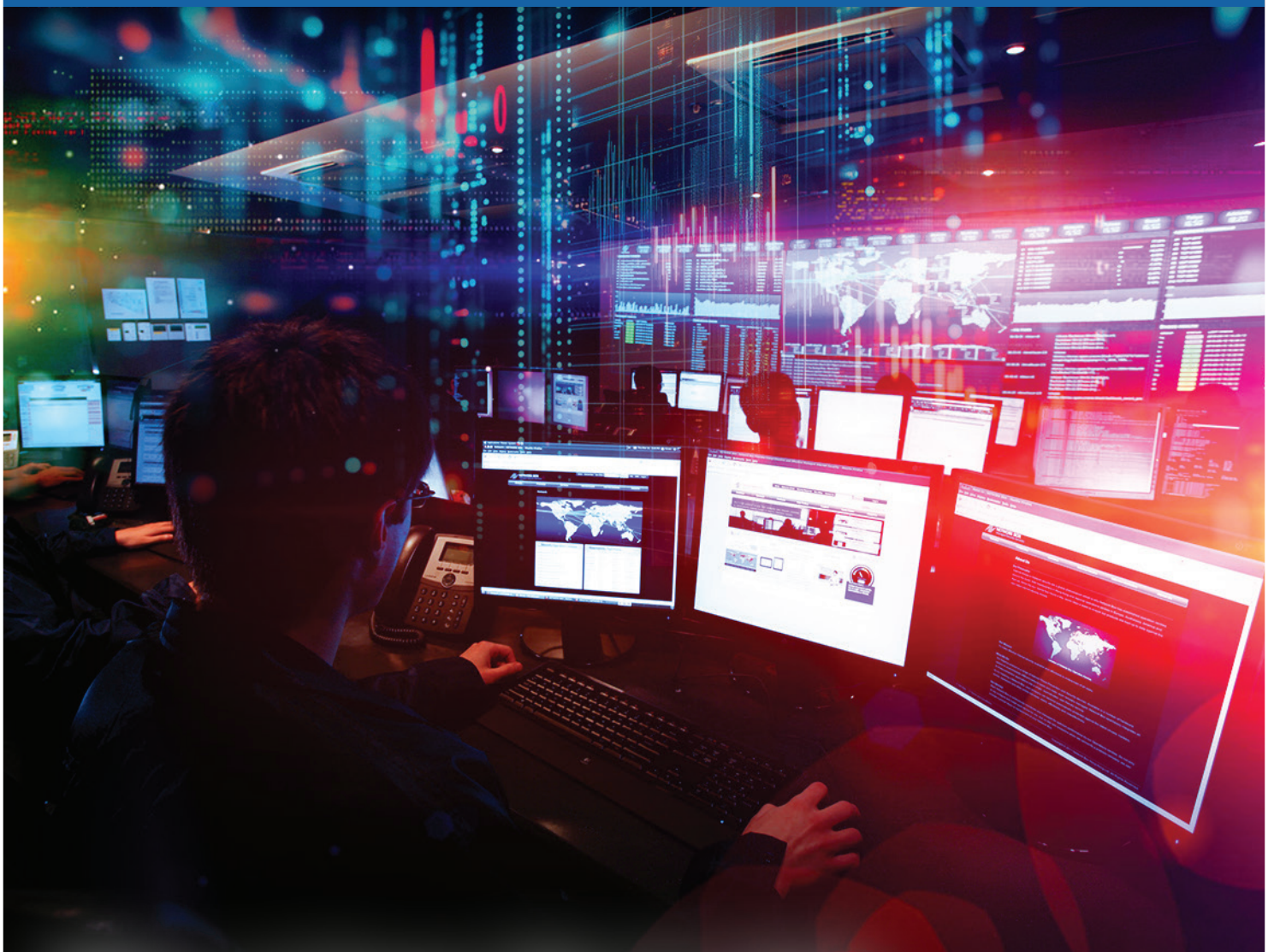
Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2025

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with several social networks:

https://x.com/networkbox
https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse
https://www.linkedin.com/company/network-box-corporation-limited/
https://www.youtube.com/user/NetworkBox

In this month's issue:



Why a true 24×7×365 Security Operations Centre is indispensable for modern organisations' cybersecurity

by Michael Gazeley
Managing Director
Network Box Corporation Limited

Cyber adversaries never rest. They probe for vulnerabilities at three in the morning, at weekends and on bank holidays. Hackers, malware, and undesirable content are always trying to get into your networks. Cybercriminals are always trying to steal your confidential data. Without uninterrupted monitoring, there is a window—sometimes measured in seconds—between the first sign of compromise and the moment attackers entrench themselves.

A genuine 24×7×365 Security Operations Centre (SOC), operating from a purpose-built facility with analysts working eight-hour shifts around the clock, ensures there are no blind spots. In contrast, a so-called cloud or virtual SOC run in-house by a limited team typically lacks full-time human presence, relying instead on automated alerts during business hours and manual intervention when personnel are on call. The difference is not merely semantic: it is the divide between constant vigilance and reactive firefighting.

Attempting to replicate this with an internal cloud-driven solution can appear superficially attractive. You lease virtual infrastructure, deploy a Security Information and Event Management (SIEM) platform, subscribe to threat feeds and designate a handful of security engineers to monitor dashboards during the working day. However, when the office closes, that limited team relies on on-call rotas, VPN access, and personal devices to respond. Response times lengthen, fatigue soars, and minor incidents can escalate into major breaches. By contrast, a physical SOC staffed 24×7×365 guarantees analysts see, investigate, and contain threats at any hour without dependence on after-hours call-outs.

The financial advantage

The financial case for a managed SOC is compelling. Staffing costs for analysts working unsociable hours demand premium pay. Infrastructure licences and recurring fees for SIEM, endpoint detection and response tools, threat intelligence subscriptions, and secure log storage quickly mount up. Training budgets balloon as each engineer continually updates certifications—CISSP, GIAC GCIH, CREST, OSCP and vendor-specific accreditations—even if they engage only sporadically with incidents. In a managed SOC, these expenses are shared across a broad client base, delivering economies of scale and predictable pricing. In-house virtual setups, by contrast, struggle with unpredictable overtime, licence renewals, and the false economy of nominal 24×7×365 coverage.

Expertise beyond your firewall

Expertise is another gulf. A true 24×7×365 centre fields Tier 1 and Tier 2 analysts, threat intelligence specialists, incident responders and forensic engineers. They dissect diverse attack vectors, from zero-day exploits to supply-chain intrusions, drawing on collective experience across multiple sectors. An in-house team tethered to internal systems sees only your network's alerts, missing attack patterns shaped by other industries, large-scale red team exercises, and sophisticated incident-response playbooks. They lack the breadth to anticipate what lies beyond your firewall.

Certified excellence

Maintaining top-tier international certifications further emphasises the disparity. A properly certified SOC holds ISO 9001 (Quality Management), ISO 20000 (IT Service Management), ISO 27001 (Information Security Management), ISO 31000 (Risk Management), PCI DSS (Payment Card Industry Data Security Standard) and other accreditations such as SG CyberSafe and GB Cybersecurity. Each requires significant investment and engagement with expert consultants such as SGS of Switzerland or TÜV of Germany.

Real-time shared intelligence

Shared intelligence is a potent force multiplier available only to external SOCs. When one client's systems report a novel ransomware variant at 3:00 am, the managed SOC adapts its detection rules globally in real time. A siloed cloud SOC must wait for internal incident reviews before updating its ruleset, leaving your defences exposed. Managed providers aggregate threat data across geographies and industries, rapidly bolstering defences—often augmented with AI—against emergent campaigns and harnessing a collective view that no single enterprise can replicate behind a virtual perimeter.

Holistic capabilities

A genuine SOC also assembles a comprehensive skill set: alert triage, deep-dive investigation, threat hunting, vulnerability assessment, incident containment, compliance mapping, and dark web monitoring. In-house teams often lack one or more of these functions, outsourcing or deferring complex tasks. The outcome is patch-and-pray security rather than a holistic strategy. External SOCs integrate governance, risk, and compliance experts who translate technical telemetry into board-level reports—ensuring regulatory alignment and actionable recommendations.

Metrics that matter

Metrics matter. Managed SOCs deliver transparent Key Performance Indicators (KPIs): mean time to detect, mean time to respond, false-positive rates, and threat-coverage percentages mapped to recognised frameworks. These KPIs frame business decisions and demonstrate the effectiveness of your security programme. In-house cloud SOCs typically lack the disciplined service-level agreements and reporting rigour, leaving stakeholders dependent on anecdotal updates rather than quantifiable evidence.

Elevating strategic focus

Outsourcing 24×7×365 operations liberates internal teams to focus on strategic projects such as embedding security into development lifecycles, architecting zero trust frameworks and automating compliance checks. Freed from the grind of night-time alert queues, core staff can drive digital transformation and risk-mitigation initiatives—accelerating business growth.

Continuous compliance validation

Finally, reputable SOC providers submit to rigorous audits—SOC 2 Type II, ISO 27001 and PCI DSS—and engage in periodic red team/blue team exercises. This continuous cycle of validation and refinement prevents complacency. In contrast, a cloud or virtual in-house set-up may achieve an initial compliance milestone but struggles to sustain it over time as staff churn and budget realignments erode capabilities.

The gulf between a brick-and-mortar SOC staffed 24×7×365 with eight-hour shift rotations and a cloud or virtual SOC managed by a small in-house team is stark. One guarantees unwavering real-time defence underpinned by shared intelligence and a full complement of specialists. The other, limited by capacity, expertise, and reactive workflows, leaves gaps that determined adversaries will exploit. Investing in a true SOC is not a discretionary cost but an essential strategic asset. It transforms cybersecurity from a cost centre into a shield of resilience—ensuring your organisation remains secure, responsive and ready; every hour, of every day, of every year.

Network Box 5
NEXT GENERATION MANAGED SECURITY

NETWORK BOX 8

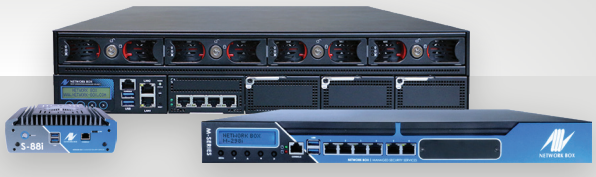
Network Box 5 and 8 Features
August 2025

On Tuesday, 5th August 2025, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

This month, for Network Box 5 and 8, these include:

NBRS-5

- Improvements to Office 365 entity synchronization (particularly in the event of poor network connectivity)
- Enhanced support for options in DNS server and root recursive resolver configurations
- Search enhancements to support upcoming improvements to Box Mail mobile App
- Support for S-80i box model in Admin Portal
- Improvements to handling of comments in firewall rules
- Fix to box model identification for VPN-5QB model
- Introduce configurable options concerning ‘tickling’ of traffic in network proxy
- General maintenance housekeeping regarding regional SOC IP addresses



NBRS-8

- Implement system wide audit facility with fine-grained configurable control for improvements to host IDS
- Improvements to package update system
- Improvements to 'show network utilisation summary' command output
- Improvements to 'show disk utilisation detail' command output
- Improvements to ’show disk status’ command output, related to NVME drives
- Enhanced support for time based firewall rules, with local time zone support
- Add support for optional network interface module on M-298i and M-398i box models
- General improvements to firewall and system logging.
- Enhanced support for options in DNS server and root recursive resolver configurations
- Improvements to speed and reliability of device provisioning
- Add support for disk partition maintenance
- Improved support for Wireguard VPN logging
- Disable use of DHCP on un-configured network interfaces
- Improvements to Office 365 entity synchronization (particularly in the event of poor network connectivity)
- Introduction of device type fingerprinting, particularly for virtual devices

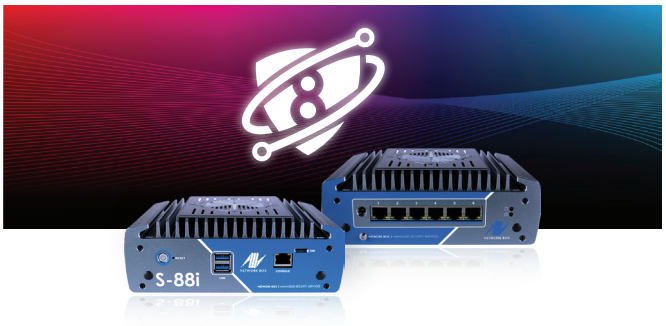
In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box HIGHLIGHTS

S-88i Hardware Platform for small offices

Network Box is delighted to unveil the all-new **S-88i**, tailored for small, branch and home offices, or any compact site seeking robust UTM+ and VPN protection. Boasting superior hardware specifications and powered by the NBRS-8 platform, the S-88i steps in to replace the S-80i *(official support for the S-80i will conclude in June 2028)*.



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 Hong Kong Tech to Connect Cybersecurity Workshop

Network Box Hong Kong took part in the **Tech to Connect** cybersecurity workshop, organised in association with the HK Wireless Technology Industry Association (WTIA). Network Box Managing Director Michael Gazeley was a keynote speaker at the event, and gave a talk titled *"AI Shield: How AI is transforming Cybersecurity."* The event, attended by senior executives, IT professionals, SEO engineers, data analysts, business leaders, and technology enthusiasts, took place at the KOHO centre.

Network Box Media Coverage

SCMP

Explainer | After 3 Hong Kong data breaches, here's how to protect your private info

LINK:
https://tinyurl.com/ykhycv7v

South China Morning Post

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong.

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com