



In the Boxing Ring AUG 2022



Network Box Technical News

from **Mark Webb-Johnson**

Chief Technology Officer, Network Box

Welcome to the August 2022 edition of In the **Boxing Ring**

This month, we are talking about the upcoming Summer 2022 Release of **NBSIEM+**. It is planned to be released to open BETA testing within the next 7 to 14 days. It will remain in beta for a month before replacing the existing NBSIEM+ in September 2022.

Over the past year, we've received your feedback and incorporated that into over 100 enhancements to be released in the coming weeks. While several of these changes are structural, many are visible to users. On pages 2 to 3, we highlight some of the notable changes.

In other news, Network Box Indonesia participated in the cybersecurity event at the Hilton Bandung in West Java. During the event, Network Box Indonesia's Director Lindra Hismanto gave a high-level talk on Next Generation Firewall and Managed-Security Services. Additionally, Network Box was featured in The Seattle Times. And in this month's security headlines, security issues were encountered by Marriott, Google PlayStore, Cisco, WhatsApp, JPMorgan Securities, UBS Financial Services, and TradeStation Securities.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2022

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 us by several social networks:



<https://twitter.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:

Page 2 to 3

NBSIEM+ Enhancements

In our featured article, we highlight key enhancements for the upcoming release. Features include: Navigation Improvements, Live Connection to NBR5-5 Network Boxes, NBSIEM+ Events, Reporting, and Cloud Services.

Page 4

Network Box Highlights:

- **Network Box Indonesia Cybersecurity Event:**
Managing a secure infrastructure in a hybrid working environment
- **Media Coverage:**
 - The Seattle Times
- **Global Security Headlines:**
 - Marriott
 - Android Malware
 - Cisco
 - WhatsApp
 - JPMorgan, UBS, TradeStation



NBSIEM+ Enhancements

Summer 2022 Release

Our big news this month is the upcoming Summer 2022 enhancement to NBSIEM+. Over the past year, we've received your feedback and incorporated that into over 100 enhancements to be released in the coming weeks. While several of these changes are structural, many are visible to users, and we'll introduce some of the more notable changes here.

Navigation Improvements

We've enhanced the right-click popup menu options for all links. This will allow you to open links in place, in a new tab, or in a new window. On desktop browsers, ctrl-click will open the link quickly in a new tab. We've also improved the browser back button to restore the previous form and filter state. A shortcut bar has been introduced to allow for quick switching between screens related to the same item (asset, event, etc.), and a selection field at the top of the screen shows at a glance the currently selected item (as well as allowing for changing that selection). We've also worked on optimizing NBSIEM+ displays across each of the mobile, tablet, and desktop browser environments we support (in particular, adding support for accessibility font sizes and scaling).

Live Connection to NBR5-5 Network Boxes

We earlier wrote about the direction we are taking to provide access to, and ultimately merge in the admin portal from NBSIEM+. With this release, we are providing access to the first screens with this capability. Now, calling up an NBR5-5 asset within NBSIEM+ will show widgets such as the memory, CPU, and network utilization live from the box itself without having to log in and access the admin portal. To support this functionality, a number of new widgets and appearance types have already been introduced. Over the coming months, more of these widgets and screens will be released in NBSIEM+.

Asset	2022-07-26 - 2022-08-01	2022-07-18 - 2022-07-25
Network Box	REPORTED	REPORTED
Incident: Network Box Web Client Malware Detection	27	24
Incident: Network Box User Portal Brute Force	13	25
Incident: Network Box Admin Portal Brute Force	31	23
Windows Server	REPORTED	REPORTED
Incident: Windows Account Modified	106	119
Incident: Windows Account Locked Out	44	84
Incident: Windows Account Created	2	4
RDP: Successful Login Notifications	84	134
RDP: Failure Login Notifications	0	2
Incident: Windows User Group Modified	2	0
Windows Firewall Login Notifications	121	560
Incident: Windows Administrator Account Brute Force	8	9
Incident: Windows Administrator Account Locked Out	2	0
Incident: Windows Account Brute Force	109	645

NBSIEM+ Events

We continue to see great progress with our customers' wider adoption of NBSIEM+, and we are already collecting and analyzing more than 200 million events daily. We now introduce optional data capacity limits, allowing you to set a limit on how many events per day come in from each asset and to suspend submission from assets that exceed those limits. We've also introduced a new unified field type to uniquely identify classes of events irrespective of the platform generating the event.

The biggest change with this release is the introduction of 'reportable events.' We now tag events of interest (such as password failures, account lockouts, etc.), grouped by platform and category, and report these to you in a summary and detailed breakdowns. Should the event be serious enough, as before, we will raise an incident ticket for a more in-depth investigation and response.

Reporting

We've brought across the dashboard reporting system from user and admin portals to NBSIEM+. Now, any dashboard widget can be added to a custom report and delivered by email as a PDF according to user-defined schedules. If missed, previous reports can also be downloaded, and templates are built to be shared between team members.

Many more reports and dashboard widgets have been introduced in this release, including several related to NBSIEM+ Event Reporting and Incident management (Events by Asset Type, Reported Events List, Reported Events Summary, Reported Incident Detail, and NBSIEM+ Asset Inventory).

Cloud Services

We continue to migrate all Network Box cloud services to the unified NBSIEM+ platform and now release Cloud SSL Certificate, Cloud SSL Service, Cloud IP Reputation, and Cloud Domain Reputation. The remaining services will follow in the coming months. For multi-tenanted cloud services, a number of service-specific reports have also been released, such as Cloud Web Client Events, Cloud Mail Events, etc.

Release Schedule

The summer 2022 NBSIEM+ is planned to be released to open BETA testing (<https://beta.siem.network-box.com/>) within the next 7 to 14 days. We currently estimate it will remain in beta for a month or so before replacing the existing NBSIEM+ (<https://siem.network-box.com/>) in September 2022. The companion iOS and Android mobile Apps also have corresponding updates and will be released in a corresponding timeframe.

Network Box HIGHLIGHTS



Network Box Indonesia Cybersecurity Event

Network Box Indonesia participated in the cybersecurity event titled "Managing a secure infrastructure in a hybrid working environment" at the Hilton Bandung in West Java.

During the event, Network Box Indonesia's Director Lindra Hismanto gave a high-level talk on Next Generation Firewall and Managed-Security Services. Highlighting their relevance and how companies can protect their network environments from cyber threats more effectively.



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

Copyright © 2022 Network Box Corporation Ltd.



Media Coverage and Security Headlines



The Seattle Times

Alleged Chinese police database hack
leaks data of 1 billion

LINK: <https://bit.ly/3BpOBTv>



The Cyber Throne

Marriott Breached Again
for Third Time

LINK: <https://bit.ly/3oFiZlm>



Bleeping Computer

New Android malware on Google
Play installed 3 million times

LINK: <https://bit.ly/3oFiZlm>



The Hacker News

Cisco Releases Patches for Critical
Flaws Impacting Nexus Dashboard
for Data Centers

LINK: <https://bit.ly/3zEceGI>



Cyware Social

WhatsApp Warns Users of
Fake App Versions

LINK: <https://bit.ly/3zH0qDy>



The Register

JPMorgan, UBS among trio accused
of shoddy ID theft protection

LINK: <https://bit.ly/3JbM14d>