In the Boxing Ring
NOVEMBER 2021

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

Welcome to the November 2021 edition of In the **Boxing Ring**

This month, we are talking about **Global Monitoring System Ticketing Rules**. The Network Box Global Monitoring System (GMS) monitors Network Box devices, cloud services, and Internet infrastructure; to provide a single global view of health status. A significant enhancement to GMS will be released this month, and on pages 2 to 3, we discuss this in greater detail.

Also this month, Network Box USA was at the 2021 HouSecCon, the primary Houston-area information security conference, held each year since 2010. During the event, Network Box USA's CTO, Pierluigi Stella, gave a talk titled, "Compliance and Security in the Supply Chain."

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
November 2021

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:

Global Monitoring System Ticketing Rules

This month, Network Box is releasing a significant enhancement to GMS, providing a facility for implementing extremely fine-grained control over raising tickets from GMS incidents.

What is GMS?

The Network Box Global Monitoring System (GMS) monitors Network Box devices, cloud services, and Internet infrastructure; to provide a single global view of health status. As well as monitoring individual sensors, GMS can raise incidents to alert SOC engineers and customers of problems that need to be addressed. These incidents can be raised on a GMS sensor changing state (for example, disk space running low on a device) and other incident types (such as dark web breaches, IP or domain reputation issues, SIEM detected issues, etc.).

The new GMS enhancements will allow our regional SOCs to implement customized ticketing depending on individual customer requirements and improve the content of raised tickets.

What are the new ticketing rules?

Whenever an incident is raised or updated, the new GMS ticketing rules will run, and these rules determine the resulting action to be performed. The standard Network Box 5 unified rules system is used for this, but now running in the cloud and maintained by our NBSIEM+ user interface. These rules are directly applied across all GMS incident types and are no longer limited to only health sensor alerts.

Extremely fine-grained rules can be defined on a per-SOC, per-owner, per-device, down to per-sensor level. Those rules can control whether to immediately raise/update a notification ticket or delay it to only alert on issues that persist for a given time period.

The raised tickets now support multiple languages so that we can raise the ticket in the device owner's native language. We can also support automatically categorizing, prioritizing, and assigning tickets appropriately.

Release Schedule

This new system lays the foundation for our future work in cloud services. GMS Incidents seamlessly support virtual devices and multi-tenanted cloud services in the same way that physical device health sensors have always been supported. This provides the first production release of our rules engine in cloud services, with upcoming cloud proxy releases (such as cloud web client protection, cloud mail protection, cloud SDWAN, etc.) leveraging the same technology and cloud-based infrastructure systems.

Fully integrated to the Box Office/NBSIEM+ notification system, users have fine-grained control over how they want to be notified (by email, mobile App PUSH, SMS, etc.), as well as times of days, or device groups to alert on.

The rules are maintained by SOC engineers according to customer requirements. If you have something you need regarding ticket notification and alerting, please ask your local SOC, and they will do what they can to assist.

Network Box HIGHLIGHTS

Network Box USA
HouSecCon 2021

Network Box USA was at the 2021 HouSecCon, which took place on October 6th and 7th at Marriott Marquis Houston. HOU.SEC.CON is the primary Houston-area information security conference, held each year since 2010.

During the event, Network Box USA's CTO, Pierluigi Stella, gave a talk titled, "Compliance and Security in the Supply Chain." For many industries, compliances and regulations are nothing new. The talk breaks down what compliance is and what it means for a company and defines the necessary first steps to tackling this new challenge.

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

Global Security Headlines

SC Magazine
Apache leak spotlights dangers of misconfigured workflow management platforms
LINK: https://bit.ly/3BlkFEh

NBC News
Baby died because of ransomware attack on hospital, suit says
LINK: https://nbcnews.to/3bm0rzP

SC Magazine
Ransomware attack on Quest's Repro-Source impacts data of 350K patients
LINK: https://bit.ly/3Gyexwo

SCMP
US Treasury unleashes cryptocurrency sanctions to fight ransomware
LINK: https://bit.ly/3jO2hhn

Daily Hive
TTC hit by ransomware attack, multiple services and systems down
LINK: https://bit.ly/3w1IErb

Threat Post
Critical Cisco Bugs Allow Code Execution on Wireless, SD-WAN
LINK: https://bit.ly/3mrtqbC