MAR 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the March 2018 edition of In the Boxing Ring

This month, we will be talking about **Moving from Log Event to Security Incident based Response**. Earlier this year, we talked about Security Incident Event Management, and outlined our plan of integrating all security and incident logs of both client and server based security into one centralized system. By adopting this approach, Network Box will be able to provide an overview of a customer's entire network, and be able to apply Integrated Security Intelligence, Digital Forensics, and Security Incident Management. On pages 2 to 3 we explain in greater detail how this will be achieved.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, we are pleased to announce, the launch of our new Managed Security platform: **Network Box 5.5**, later this month. New features include: dashboard enhancements, SIEM client support and other enhancements. In addition, Network Box Germany was at the **comTeam Partner Conference 2018**, held in Leipzig; and Network Box customer, **F1 Experiences** was interviewed by it.daily.net, about the advantages of using Network Box and how our Managed Services have helped them strengthen their IT security.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2018

You can contact us here at 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:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

Moving from Log Event to Security Incident based Response

Back in the January 2018 edition of *In the Boxing Ring*, we talked about Security Incident and Event Management. We introduced our plan for this year for how Network Box appliances will operate both as a source of incident logs to industry standard SIEM products, as well as collectors for customer equipment (routers, switches, servers, workstations, etc). We outlined how we are integrating both with client based (such as workstation based Host IDS and blacklist/whitelist systems) as well as server based SIEMs. The goal here is to integrate all the security logs and incidents into one centralized system, to provide an overview of the entire network, and to be able to apply Integrated Security Intelligence, Digital Forensics, and Security Incident Management; all delivered as cloud based and/or on-premises solutions.

This month, we'd like to explain in more detail how this will be achieved.

Data Sources

Event data enters the system from both Network Box appliances, as well as other security, server, and workstations devices, using a variety of formats (mostly syslog based). This data takes the form of:

- Blocking logs; records of activity that was blocked
- Alert logs; records of activity that was of concern but not blocked
- Activity logs; records of activity that was not blocked
- Event logs; significant events (such as user logins, logouts, devices rebooting, services restarting, etc)
- Statistics; bandwidth, network flows, utilization, etc

The appliances and data sources can be either centrally located, or globally distributed.

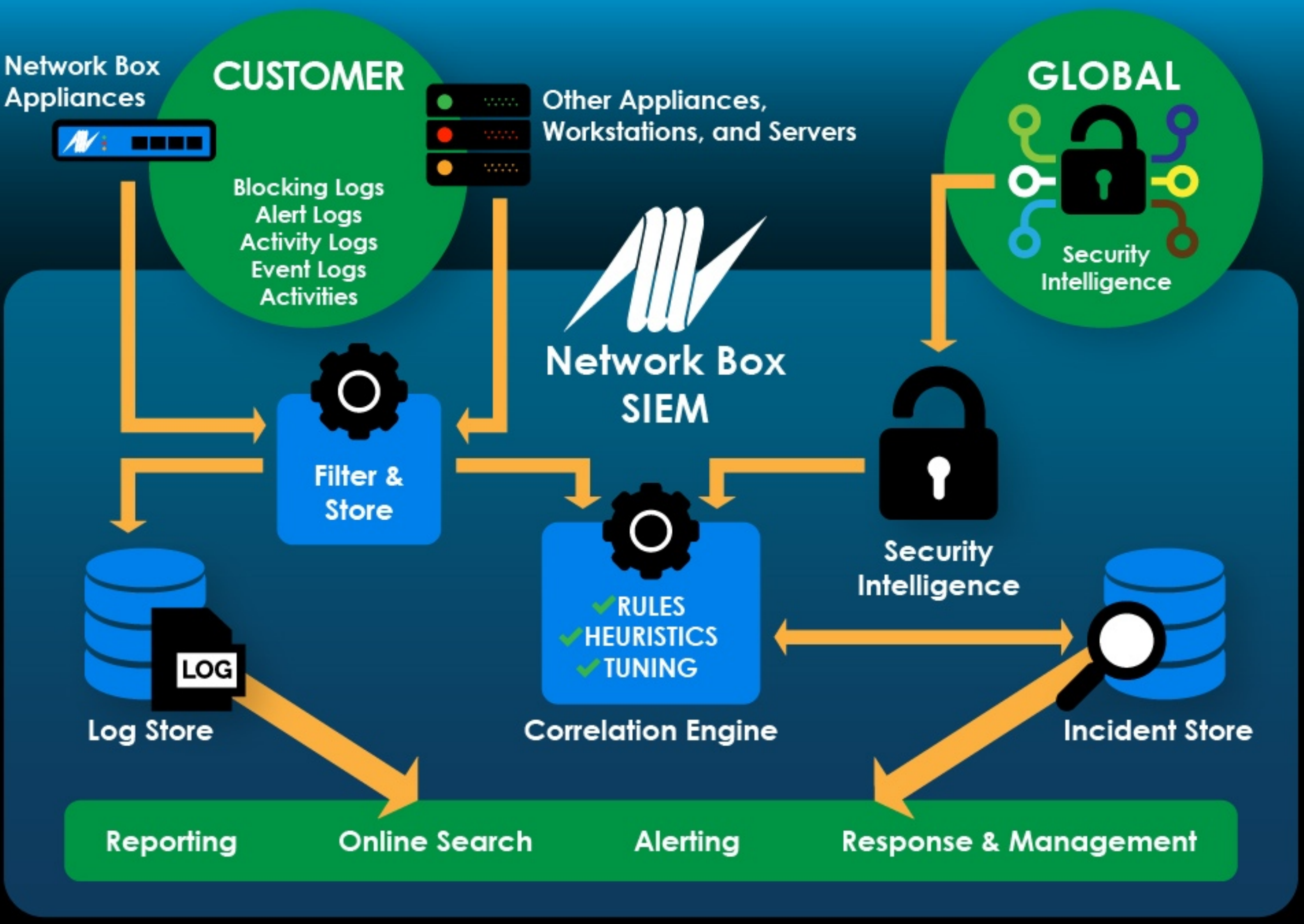
Event Store

All this data streams into the Network Box Security Incident and Event Management (SIEM) system. It can also be sent to other SIEMs.

Filters operate on the incoming data streams, identifying particular sources of information, classifying, categorizing, and storing the raw event data in the Log Store (a highly optimized, reliable, and scalable storage database for security event logs) in a universal standard format (irrespective of the actual source of the data). Network Box Security Response engineers maintain these filters, and adjust them to support the security equipment the customer uses and their log record formats.

Security Intelligence

Security Intelligence feeds (from Network Box RepDB, as well as other sources) are brought into the system to provide threat indicators. These are indicators of potentially malicious activity seen globally, and can be used as such by the correlation engine.



Correlation Engine

While individual appliances raise individual events recording their view of the network activity as it happens, and security intelligence feeds provide threat indicators, it is the role of the Correlation Engine to take a high level overview of those individual data items, and correlate them into actionable security incidents. Built on 18 years of experience managing security events, we use rules, heuristics, and custom tuning, to first identify and then classify incidents encompassing security events. Active, and past, security incidents are maintained in a separate highly optimized, reliable, and scalable storage database.

Reporting, Analysis, Alerting, and Response

According to incident severity and magnitude, the Network Box Notification system is used to alert on new and updated security incidents. Powerful on-line search facilities will be provided to search across, and drill-down into, both security incident data, as well as the raw log records.

Periodic and on-demand reporting, as well as real-time dashboards are provided.

Response management tools are provided to be able to assign incidents, update, and response appropriately.

Conclusion

The Network Box SIEM will be released later this year, and will be delivered both as cloud based and on-premises solutions. This new product will correlate individual security log event records, to record and track security incidents in a standards conforming manner. This new approach will comply with best practice requirements such as the Payment Card Industry (PCI) standards.

In addition, Network Box 5 appliances will be able to feed security event logs to external SIEMs using industry standard protocols.

Network Box 5

NEXT GENERATION MANAGED SECURITY

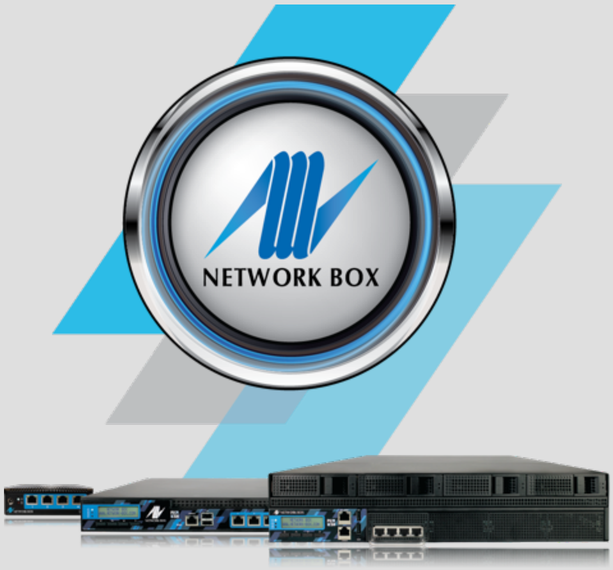
On Tuesday, 6th March 2018, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features

March 2018

This month, for Network Box 5, these include:

- Support for stopping, starting, and restarting, IPSEC tunnels in admin web portal
- Improved form layout when resizing window in admin and user web portals
- Option to selectively generate user portal report only when user has quarantine records
- Support for 3G/4G modems (via PCI interface in supported box models)
- New option to filter firewall logs by entity name
- Optional provision of SSL session ID to HTTP server (X-Sslsession header)
- Support for SSL session resumption
- New feature for dynamic SSL pinning heuristics
- Optional BitDefender anti-malware and anti-spam security modules



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 ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 5.5
NEXT GENERATION MANAGED SECURITY

Launch Announcement

We are excited to announce that later this month, we will be launching new enhancements to the Network Box Managed Security platform: **Network Box 5.5**.

In addition to providing new enhancements to the Network Box HTML-5 dashboard, it will also include following features:

- Performance improvements throughout admin web portal
- Security news feed, with indicators of compromise
- SIEM client support (Network Box client to external SIEMs)
- SIEM client support for OSSIM/USM
- SIEM client support for Splunk
- Policy control of DKIM signature verification
- DKIM signing for outbound SMTP email
- FTP server support (in addition to the existing FTP client support)

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 © 2018 Network Box Corporation Ltd.

Network Box Germany

comTeam-Partnerkonferenz 2018

Network Box Germany was at **comTeam** conference which took place at the Salles de Pologne, in Leipzig. During the event, attendees were introduced to the Network Box UTM+ appliances, and Managed Services.

comTeam Leipzig PARTNERKONFERENZ 2018

Formula 1 Experiences

it-daily.net Interview

Network Box customer: *Formula 1 Experiences*, was interviewed by *it-daily.net*, about the benefits of using Network Box Managed Services, and how Network Box has helped them secure their IT network.

LINK: https://www.it-daily.net/it-sicherheit/enterprise-security/17954-it-sicherheit-auf-der-rennstrecke