In the Boxing Ring 2024年1月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2024年1月份的 In the **Boxing Ring**

新年快乐！本月，我们将讨论NBSIEM+在2024年1月即将推出的优化，以及我们在2024年及以后对这个统一平台的计划。正如您可能知道的那样，我们的目标是将所有Network Box报告和用户/管理界面统一到一个名为NBSIEM+的系统中。这使得无论Network Box服务是通过物理设备、虚拟设备还是多租户云交付的，都可以实现无缝的查看、管理和操作。在第2至第3页，我们会更详细地讨论这些优化功能。

在本月的全球安全头条中，谷歌、23andMe和苹果iPhone都出现了安全问题，当局还从3500名网络欺诈者中追回了3亿美元。此外，Network Box德国的Dariush Ansari在Connect-Professional上发表了一篇关于人工智能在网络犯罪中的文章，最新的HPCC Hackpod Club剧集也已经上线。最后，Network Box在2023年的《Network Box技术评论》中汇编了关键的"In the Boxing Ring"文章。

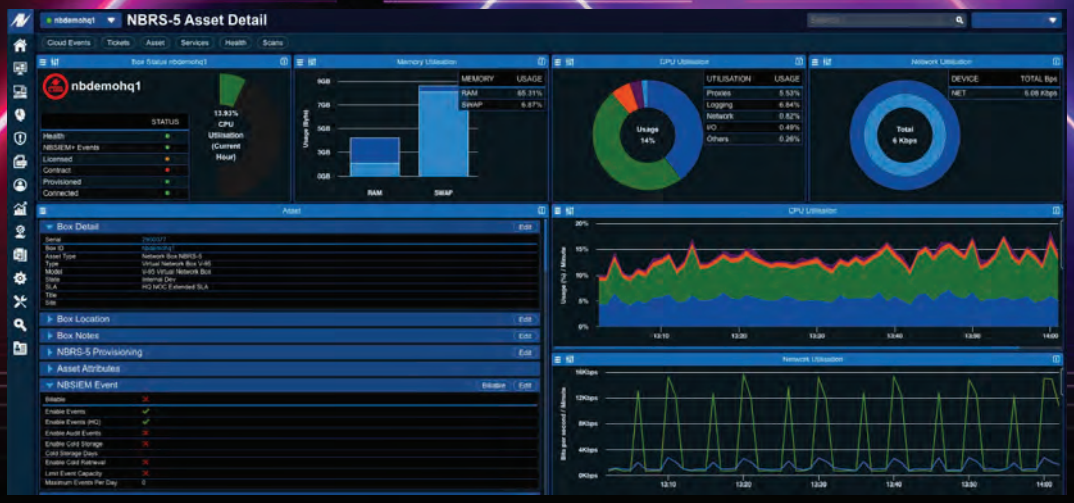
Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
January 2024

本月摘要:

NBSIEM+

2024年1月优化

正如您可能已经了解的那样，我们的目标是将所有Network Box报告和用户/管理界面统一到一个名为NBSIEM+的单一系统中。这使得可以在不论服务是通过物理设备、虚拟设备还是多租户云交付的情况下，实现对Network Box服务的无缝查看、管理和操作。因此，它最终将整合用户门户、管理门户、Box Office等所有功能。



本月，我们向公众发布了NBSIEM+的测试版（https://beta.siem.network-box.com/），以进一步朝着我们的目标迈进。这些更新包括：

1. 对后端系统进行了增强，提高了可靠性、性能，并具备足够的扩展性，以支持所有用户。

2. 引入多级报告系统，结合基于标签的灵活方法来定义自定义层级--使我们能够为管理多个设备/地点的客户生成综合报告。

3. 将报告生成、数据导出和其他类似的大宗任务转移到专用的后端服务器上--提高我们以企业级规模提供数据和报告的能力。

4. 引入了仪表板功能，使任何NBSIEM+小部件都可以添加到自定义仪表板，以创建个性化的界面和用户体验。此功能先前在用户和管理员Web门户中可用，NBSIEM+的实施类似（支持4x3网格或移动端的1x12，以及多个仪表板页面）。

5. 新增一份报告，显示我们定期进行的外部扫描的结果。在管理特定资产时，可以在“SCANS”链接下找到此报告。

6. 新增一份显示GMS健康状况的报告。类似于扫描报告，可以在管理特定资产时在“HEALTH”链接下找到。

7. 我们还在NBSIEM+的SOC系统中引入了一些增强功能，以帮助我们的工程师更好地协助客户管理Network Box设备。其中一个例子是NBNIDAN - 类似于Shodan系统，允许我们的工程师快速搜索外部扫描数据库，查找所有受管设备，识别易受攻击的服务（因此易受攻击的客户），加快我们的响应时间。这些增强功能中的大部分将在未来几个月内开放给最终用户使用。对于管理多个设备/位置的客户，此增强功能将特别有用。

资产详情页面就是 NBSIEM+ 与所管理设备之间紧密集成的一个例子。选择一个您管理的 Network Box 资产，您会发现资产名称旁边有一个绿色或红色的小圆点。这表示 NBSIEM+ 目前是否可以联系到该资产（绿色）或无法联系到（红色）。如果可以联系到，NBSIEM+ 将显示利用率、健康状况等图表。所有这些信息都是直接从所管理的资产中实时获取的，就像登录本地网络管理界面一样。在未来几个月内，我们将在NBSIEM+内直接发布完整的管理门户功能（网页端和移动应用程序）。

现在在NBSIEM+中几乎可以完成在Box Office中可以完成的所有操作，而且这两个系统可以协同工作（共享相同的数据）。我们预计将在2024年初春的某个时候将这个测试版的NBSIEM+发布为正式版本。

NBSIEM+ 今天

您可以访问正式版的NBSIEM+:
https://siem.network-box.com/

或者参与BETA版本的发布:
https://beta.siem.network-box.com/

移动应用的版本可在Google Play和Apple App Store中找到:

GET IT ON Google Play
https://play.google.com/store/apps/details?id=com.networkbox.siem

Download on the App Store
https://apps.apple.com/hk/app/network-box-siem/id1532859749

Network Box HIGHLIGHTS

Network Box 技术评论2023

作为一项特别的年底回顾，Network Box已经整理了来自2023年的关键《In the Boxing Ring》技术新闻、特性和文章。

链接:
https://mcdn.network-box.com/ItBR/2023/Technology_Review_2023.pdf

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

翻译：James

媒体报道 和安全头条

CONNECT-PROFESSIONAL
人工智能在网络犯罪中的应用: Deepfakes and WormGPT
链接: https://bit.ly/47oEzhI

HPCC Hackpod Club
第 21 集
回顾与展望
链接: https://anchor.fm/hackpodclub

Bleeping Computer
恶意软件滥用Google OAuth端点来“恢复”Cookie，劫持账户
链接: https://bit.ly/3RLHzPC

The Register
菲律宾、韩国和国际刑警逮捕了3,500名涉嫌网络欺诈的嫌疑人，追回了3亿美元。
链接: https://bit.ly/3S2iscs

SC Media
23andMe确认近700万名客户受到数据泄漏的影响。
链接: https://bit.ly/3vi0Twe

Ars Technica
一场为期四年的攻击活动通过可能是有史以来最先进的漏洞利用手段，对iPhone进行后门攻击。
链接: https://bit.ly/3TDBRlo