

In the Boxing Ring

APR 2025

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2025年4月的 In the Boxing Ring

本月，我们发布了首个完全基于生成式人工智能技术的系统：NBSIEM+ 事件工单的自动建议功能。迄今为止，当 NBSIEM+ 决定将某个上报事件升级为事件工单时，通常只使用一些模板化的文本来生成工单。而此次的新功能则是在此基础上，利用我们训练的生成式人工智能模型（以生成的事件工单文本和事件本身作为上下文附件）来自动生成建议，作为工单文本的一部分提供。这些建议包括背景信息的说明、事件的解释以及应对建议。我们将在第2至第3页中对此进行详细讨论。

此外，NBSIEM+ 应用程序也将迎来令人振奋的升级！新版将于本月晚些时候推出，带来了多项强大更新，使安全管理变得比以往更加顺畅、高效且直观。

另外，我们很高兴地宣布，Network Box 荣获 2025 年 APAC Insider 新加坡商业大奖的“最受信赖的网络防护公司”奖项。这是 Network Box 连续第四年获得该奖项——热烈祝贺我们的新加坡办公室，感谢他们的辛勤付出和杰出表现！



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

本月摘要：

第 2 - 3 页 NBSIEM+ 事件工单的自动 化建议

Network Box 在其产品中使用人工智能技术已有 20 多年。我们已成功将这些技术应用于恶意软件、垃圾邮件、前线防御等入侵引擎中，以及 URL 分类、恶意软件分析等后端系统中。如今，我们推出了首个完全基于生成式人工智能技术的系统：NBSIEM+ 事件工单的自动建议功能。该系统旨在通过提供自动化建议和支持，提升事件管理与分析的效率。

在本期专题文章中，我们将更深入地探讨这一新系统，并展望未来的生成式人工智能技术发展。

第4页 Network Box 亮点：

- Network Box 荣获 2025 年新加坡商业大奖
- Network Box NBSIEM+ App 更新

自动化 建议 NBSIEM+ 事件工单

近几个月来，生成式人工智能的普及与应用呈爆炸式增长，这一点我们都有目共睹。虽然这项技术在过去早已悄然酝酿，但随着 ChatGPT 的发布，它才真正走到聚光灯下，成为公众关注的焦点。

Network Box 在其产品中使用人工智能技术已有 20 多年。无论是统计方法（如贝叶斯和其他学习系统）、启发式方法，还是基于神经网络的模型，我们都成功地将这些技术应用于恶意软件检测、垃圾邮件过滤、前线防御及其他入侵引擎中，同时也广泛用于 URL 分类、恶意软件分析等后端系统。早在十多年前，我们就已经清楚，仅依赖传统的特征码检测方式，无法应对层出不穷的恶意软件攻击。正是因为我们积极采用非特征码检测方法，才得以持续领先于网络攻击者。

然而，在我们对“人工智能”技术充满热情的同时，也必须清醒地认识到其局限性。尽管人工智能（尤其是生成式 AI）能够带来令人惊艳的成果，但它同样可能生成令人震惊的荒谬输出。正如那句老话所说：“犯错是人类的本能，但搞砸事情需要一台计算机。”我还想补充一句：“……而要真正彻底崩盘，那就得靠 AI 了。”

在目前这个阶段，AI 还无法在没有人类监督的情况下独立做出可靠决策。我们还不能完全信任它来驾驶汽车、操控机器人，或决定是否允许或拒绝网络流量。即使它能在 99% 的情况下做对，剩下的 1% 却往往是最严重、最不可接受的错误。



今天，我们自豪地宣布推出首个完全基于生成式人工智能技术的系统：

NBSIEM+ 事件工单的自动化建议

直到目前为止，当 NBSIEM+ 决定将某个上报事件升级为事件工单时（无论这种升级决策是由 AI、启发式方法，还是特征规则做出的），系统生成的工单内容仅仅是一些模板化的文本。

今天这一功能得到了增强——我们引入了经过训练的生成式 AI 模型（以生成的事件工单文本和事件本身作为上下文附件），用于自动生成建议，并作为工单文本的一部分提供。这些自动化建议将包括背景信息说明、事件的解释以及处理建议。

一如既往，客户仍可通过该工单继续与我们的安全运营中心（SOC）工程师交流，获得专业的人工建议与支持。

这些自动化建议不可能做到百分之百准确，也永远无法完全取代人类分析师所提供的专业判断。但它们有时能发现人类分析师可能忽略的信息，并可作为决策时的基础参考资料。我们会明确将这些建议标注为“自动化分析”，并始终为客户保留与真实的安全分析师进一步沟通的选项。

您可能已经注意到，从 2025 年 3 月 25 日起，一些由 NBSIEM+ 生成的事件工单上已开始出现自动化分析内容。而从今天起，这项功能将正式向全球所有用户全面开放。我们也很高兴地宣布，此项服务将不会产生任何额外费用。

类似地，我们将在即将进行的 NBSIEM+ 重大更新中推出第二个生成式 AI 系统（计划于今年第二季度发布）：事件自动建议功能。用户可以点击一个事件，获取该事件的摘要、分析以及如何最佳处理该事件的建议。这项服务同样不会收取任何额外费用，并且大多数事件的自动化分析将能够在 10 至 15 秒内完全生成。

正如所提到的，激动人心的时刻即将到来，我们希望这些首批集成生成式 AI 技术的 Network Box 产品能够帮助我们的客户更好地理解和这些事件和事故。

举个例子，下面是最近一张 NBSIEM+ 事件工单的自动化分析：

Incidents Tickets

🔍

joe.user
▼

☰

Ticket # 789321456
🔒

Ticket Description

Message: ET EXPLOIT Korenix JetWave formSysCmd Command Injection Attempt (CVE-2016-20017) [Classification: Attempted Administrator Privilege Gain]
Result: deny
Protocol: tcp

Remote IP: (redacted)
Remote Port: (redacted)

Local IP: (redacted)
Local Port: (redacted)

The activity should be investigated and workstation/-server checked for possible compromise.

Raised by: SIEM rule [nbsiem] Network Box Possible Exploit Activity Detected
Rule ID: (redacted)
Event ID: (redacted)

Automated analysis result:

Summary of the Event:

- Threats: 1:2049120:2
- Message: ET EXPLOIT Korenix JetWave formSysCmd Command Injection Attempt (CVE-2016-20017) [Classification: Attempted Administrator Privilege Gain]
- Result: deny
- Protocol: tcp
- Remote IP: (redacted)
- Remote Port: (redacted)
- Local IP: (redacted)
- Local Port: (redacted)
- Timestamp: 2025-03-20T(redacted)Z
- Local Country: Hong Kong (hk)
- Remote Country: Singapore (sg)
- Application: ips
- Priority: 3 (on a scale where higher values indicate higher priority)
- Asset Name: (redacted)
- Asset Type: networkbox

Severity Assessment:

The event involves a detected and blocked attempt to exploit a known vulnerability (CVE-2016-20017) in the Korenix JetWave formSysCmd. The classification indicates an attempted administrator privilege gain, which is a high-severity threat. The severity of this event is elevated due to:

- 1.The nature of the exploit (attempted privilege escalation).
- 2.The fact that the attempt was detected and denied, indicating that the IPS is functioning correctly but still highlights an attempted breach.

Recommendations:

1.Immediate Action:

- *Verify the Status of the Local Device:* Check the workstation/server (local IP: (redacted)) for any signs of compromise or unusual activity.
- *Review Logs:* Examine logs from the local device and the Network Box IDS/IPS for any other related suspicious activity or repeated attempts.
- *Update Signatures:* Ensure that all intrusion detection and prevention systems have the latest signatures and rules to effectively block known exploits.

2.Network Security:

- *Network Segmentation:* Ensure that critical systems are properly segmented from less secure parts of the network to limit the potential impact of successful exploits.
- *Access Controls:* Verify that appropriate access controls are in place to limit exposure to potentially vulnerable services.

3.Patch Management:

- *Apply Patches:* Confirm that all systems, especially those running vulnerable services, are up to date with the latest security patches to mitigate known vulnerabilities.

4.Monitoring and Detection:

- *Enhanced Monitoring:* Increase monitoring on the involved systems and network segments to detect any further attempts or related activities.
- *Threat Intelligence:* Integrate threat intelligence feeds to stay informed about new vulnerabilities and emerging threats.

5. Incident Response Planning:

- *Review and Update IR Plan:* Assess and update the incident response plan to ensure it addresses detection and response to similar exploit attempts.
- *Conduct Drills:* Perform regular drills and simulations to ensure readiness in responding to such incidents.

By following these recommendations, the organization can enhance its security posture and better protect against similar threats in the future.

Disclaimer

This analysis was crafted with the assistance of AI, using the information available at the time. Generative AI is an exciting and experimental technology, but it's not perfect - so there might be errors or misinterpretations in the content. If you'd like a second look or need help from a human expert, feel free to reach out to your local Network Box Security Operations Centre. We're here to support you!

🔒
User: joe.user
IP: 852.123.1.23
2025-03-20 00:30:00 HKT

Copyright © 2001-2025 Network Box Corporation

Network Box HIGHLIGHTS



Network Box 荣获 2025 年新加坡商业大奖

Network Box 很高兴地宣布，公司荣获 2025 年 APAC Insider 新加坡商业大奖“最受信赖的网络防护公司”奖项。这是 Network Box 连续第四年获得该奖项，充分体现了我们在提供有效网络安全保护方面的不懈努力。热烈祝贺我们的新加坡办公室，感谢他们的辛勤工作并荣获此奖。



Network Box NBSIEM+ App 更新

NBSIEM+ 应用即将迎来激动人心的升级！我们将为您带来全新的 Network Box 使用体验！NBSIEM+ App v6.5 即将上线，搭载多项强大更新，让安全管理变得前所未有的顺畅、高效与直观。

主要功能

- **增强对 Android 14 与 15 的支持**
大屏设备用户，我们听到了你们的呼声！全新优化的体验即将上线，助您在各类设备间顺畅操作，无缝切换。
- **性能与兼容性全面提升**
无论您使用的是 iOS 还是 Android，都能享受到更快的速度、更高的稳定性和更强的运行效率。
- **面向未来的集成支持**
我们即将推出对 NBSIEM+ 2025 年第二季度重大版本更新的支持，助您始终走在技术前沿。

此次更新已进入最后阶段，正在等待 App Store 审核通过。一旦批准，本月内即可登陆您的设备。敬请期待——精彩不容错过！



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 CNNOG
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