Vectra AI Platform – 8.6 Release Notes

The Vectra® X-series appliances, B-series appliances, S-series sensors, VM and Cloud Brain, VM and Cloud Sensors, are scheduled to be updated to Vectra Network software release version 8.6. The version 8.6 release includes Scoring Enhancement, Traffic Validation Report, and two new M365 detections. The 8.6 release also includes a reminder for an end-of-life notice for the X80 and S2 hardware platforms.

8.6 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after July 30th, 2024
  - You can check if you have remote support enabled under Settings -> Services with Remote Support set to Enabled.
- **Customers Connected to Updater**: Customers who do not have remote support enabled but are connected to Updater will receive updates on or after August 6th, 2024
  - You can check if you are connected to Updater under Settings -> Services and see that Updater Destination shows as connected, while Remote Support shows disabled.
- **All Other Customers***: Will be able to download the update on or after August 6th, 2024
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Scoring Enhancement — Network

Starting in 8.6, Vectra has improved our AI Scoring and Prioritization engine to increase the signal of Host and Account based entities. This updates how the "Threat" score is calculated to provide a clearer signal of assets which require customer attention, while minimizing benign or inconclusive entities. This improvement simply impacts how the score is calculated, but does not impact the API, Syslog, or WebUI itself. The certainty score behavior has not changed, and no user action is required. Additionally, Syslog messages will now be sent only when the Threat score increases for a detection, if the syslog configuration does not include "score decreases".

Download Option for Traffic Validation Report — Network

Starting in 8.6, Vectra has added a Traffic Validation Report download option to the GUI. Enhanced Network Traffic Validation allows customers to see information related to the network traffic observed by Sensors paired to the Brain. This information is used to determine if the network traffic being observed meets quality standards required for detection and further processing. Please see Enhanced Network Traffic Validation (ENTV) for more details.

Detections

New Detection – M365 Phishing Simulation Configuration Change — M365/AAD

New coverage has been released to surface behaviors around defense evasion using Phishing Simulation accounts. The new M365 Phishing Simulation Configuration Change detection alerts when the configuration associated with a Phishing account is changed. Phishing providers are used to send simulated phishing e-mails that are not filtered by Microsoft. Attackers may configure a phishing provider to send malicious e-mails to users in the organization.

New Detection – M365 SecOps Mailbox Change M365/AAD

New coverage has been released to surface behaviors around persistence via SecOps accounts. The new M365 SecOps Mailbox Change detection alerts when the configuration associated with a SecOps account is changed. SecOps accounts are exempt from spam and malware filtering. An attacker can target these accounts and configure them to receive malicious e-mails without any obstruction from native Microsoft filters.

Reminder: X80 and S2 Platform End-of-Life Notice

The X80 and S2 hardware platforms will be EOL on January 7th, 2025.

After the 7th of January 2025, Vectra will no longer support:

- Software upgrades for X80 and S2 appliances.
- Software upgrades for brain appliances where an S2 sensor is paired.
- Hardware replacements for X80 or S2 appliances or their components.

Please contact your Vectra account team to discuss future options for replacing affected X80 or S2 hardware prior to the 7th of January 2025.

Bug Fixes

CS-8843: Conn Relay Triage Rule Issues

Resolved an issue in which some Hosts became active again after they were marked by the Triage Filter "False Positive - No Relay." This issue has now been addressed.

CS-9087: Syslog / Kafka Notifications Sent with Incorrect “Topic”

Resolved an issue where in some scenario's syslog / kafka notifications are being sent with a topic of “None” when it should be a unique topic name for each log type. This issue has now been addressed.

CS-9049: Display Issue When Tagging Detections

Resolved an issue on the Host and Account pages where upon tagging a detection, the modal to enter the tag displays on a different detection than one initially selected. This issue has now been addressed.

CS-9008: Opening Host Page from Shared Link

Resolved an intermittent issue for users when the Host page is opened from a Detection that includes a Shared Link, the Host page returned an error. This has now been addressed.

CS-9160: Unusual Keyboard Layout

Resolved an issue in which the Bulgarian Phonetic Traditional keyboard became unavailable, preventing multiple actions, including creating triage rules. This has now been addressed.

CS-9138: Advanced Search Issue

Resolved an issue in which content is pasted twice after said content was copied from the clipboard in the Advanced search. This issue has now been resolved.

Appendix:

Will this upgrade perform a reboot of the Brain or Sensors?

No, a reboot is not required as part of the 8.6 update.