+

Vectra AI Platform – 8.8 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 8.8. The version 8.8 release includes troubleshooting enhancements, improved group management, and additional Azure AD / M365 detections. The 8.8 release also includes a reminder for an end-of-life notice for the X80 and S2 hardware platforms.

8.8 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after September 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 October 8th, 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 October 8th, 2024
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Troubleshooting Enhancements Network

Starting in 8.8, Vectra is improving the Troubleshooting facilities available in the platform. The following enhancements are introduced:

- Generate status-report for sensors from Brain (status-report generate -s <Sensor/stream serial>)
    - For more information see: https://support.vectra.ai/s/article/KB-VS-1030
- Show system-health for sensors from the Brain (show system-health -s <Sensor/stream serial>)
    - For more information see: https://support.vectra.ai/s/article/KB-VS-1068

These commands exist today, but only work on the Sensor or Brain the user is logged in on. Starting in 8.8, you can run commands for Sensors/Stream from the Brain, reducing the hassle and complexity of logging in to individual systems.

Faster Group Management Network

With 8.8, Vectra is speeding up how groups are managed in QUX. The primary improvement is with the page load performance of the groups management page, and the workflow has been streamlined to allow for simpler management actions and for future dynamic group specification. Group management actions such as editing details, importance and adding/removing members has been moved from a modal on the Manage -> Groups page to a new single group page.

Detections

Azure AD Cross Tenant Access Change M365/AAD

New coverage has been released to surface persistence behaviors leveraging cross tenant access settings. The new Azure AD Cross Tenant Access Change detection alerts when a partner's cross tenant access settings are added or updated. This access setting manages how your organization collaborates with external organizations (partners) and the level of access users in external organizations have to your organization's resources. Attackers may configure cross tenant access settings to set up backdoor access from a malicious organization they control.

Azure AD Domain Settings Modified M365/AAD

New coverage has been released to surface behaviors surrounding persistence using domain settings. The new Azure AD Domain Settings Modified detection alerts when a new unverified or verified domain is suspiciously added to the environment. Attacks may use domains to set up malicious federation and create backdoors to access target environments.

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-9206: Hunt page not Correctly Reflecting Searches, Groups Disappear after Use

Resolved an issue where the hunt page did not accurate complete searches for group filters, as well as the same group type disappearing in another tab opened to the same page. This issue has been resolved.

CS-9277: VTIM Detection Showing Out-to-In-Traffic

Resolved an issue that Threat Intel Match detection generates from Out-to-in-traffic. This has been solved by adding consideration of whether any packets have been sent from an internal IP to an external IP.

CS-9287: Offline Upgrades Issues

Resolved an issue where offline updates were not working. This issue has been resolved.

CS-9297: Recall Shows Destination IP as Source

Resolved an issue in Recall if the IP was mentioned in destination, but it was identified as the malicious source initiating connections towards our servers. This issue has been resolved.

CS-9341: Accounts with no Detections are Getting Alerted

Resolved an issue where an account alerted a detection, but the detection information was incomplete, and the number of occurrences was zero. This issue has now been resolved.

GEM-508: Duplicate Validation Showing for Multiple Members of IP/Domain Groups

Resolved an issue when adding members to a IP or Domain group, if the user tries to add multiple members, there is a validation error for ‘duplicate’ members even if there are no duplicates. This issue has been resolved.

GS-8723: Account Association Setting cannot be Turned off if Assoc. Type is Automatic

Resolved an issue with the account association setting can now be turned off whether the association is manual or automatic. Account association could only be turned off if the association type was manual. This issue has been resolved.

GS-9196: Account Association Setting unclear when AD Disabled & Acct Assoc. Automatic

Resolved a clarity issue with account association settings. The overview section seems disabled, but the edit panel shows the account association is on. It was also unclear whether the account association was automatic or manual. This issue has been resolved.

LUNA-687: Advanced Search Shows Loading Page if Request Fails

Resolved an issue with Advanced Search inaccurately handling invalid input. When a user inputs an invalid character to the Advanced Search page, the page persists instead of showing an empty table. This issue has been resolved.

VULNS-1616: ACVE-2024-6387 OpenSSH vulnerability (iDRAC)

Resolved an issue that left many different hosts vulnerable to the CVE-2024-6387 OpenSSH vulnerability, many of which were iDRAC hosts which had the default SSH connection open and returned a vulnerable SSH version. This issue has been resolved.

Appendix:

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

No, a reboot is not required as part of the 8.8 update.

Note: The 8.8 release will upgrade the firmware on your system. Do not stop the 8.8 upgrade while in progress—doing so may render your system unstable.