Vectra Detect Platform Software Update

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 8.4. The version 8.4 release includes Match Support in Stream, MITRE Mapping in Syslog Detection events, and Mutli-Server AD Enhancements. Additionally, improvements to current detection algorithms and various bug fixes. The 8.4 release also includes an end-of-life notice for the X80 and S2 hardware platforms.

Platform

Match Support in Stream Network

Starting in 8.4, Vectra has introduced Match support in Vectra Stream. This enables you to send Match metadata over all of the Stream supported transmission types. To enable this, simply go to the Settings -> Stream -> Metadata Types, and enable Match.

Multi-Server AD Enhancements Network

Vectra has enhanced various components related to multi-server AD such as additional tool tips for user clarification, verbiage when closing multi-server AD modal, and disable the ability to add two ADs with the same profile name from the UI. Lastly, updated the overview page to be clear and concise when AD profiles are enabled but do not have any profiles.

MITRE Mapping in Syslog/Kafka Network

Vectra has enhanced Syslog to include the MITRE Technique T-Numbers within the Detection Syslog/Kafka messages. There is no user action required for Kafka. For Syslog, this will only be included if the “Include Enhanced Detail” is enabled. This will include all of the MITRE T-Numbers which are displayed in the Detection UI and One pagers, but now will be included in the Syslog/Kafka notifications. See the Syslog for additional details.

Detections

Kerberoasting: Triage Support on Target Domain Controller Network

Vectra has introduced the ability to triage the target domain controller for Kerberoasting detections. Previously to this change, Kerberoasting detections only allowed Target Domain Controller Host / Host Groups to be triaged.

ICMP Tunnel: Various Enhancements Network

Vectra has introduced improvements to the ICMP C2, Exfil, ICMP Tunnel Client, and ICMP Tunnel Server detections to eliminate benign true positives in some environments. No action is required.

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-8798: License Expiry Format in GUI

Resolves an intermittent issue where the license expiry format in GUI displays incorrectly. This has now been addressed.

CS-8485: No Connection Check Result for vCenter Integration

Resolves an intermittent issue where users see ‘no connection’ for vCenter integration when the integration functions normally. This has now been addressed.

CS-8405: Backup Transfer to SFTP Server

Resolves an issue where some users in certain situations cannot backup the Brain due no ability to adjust the timeout value on the SFTP server side. This has now been addressed.

DATA-8678: Traffic Stats Displaying Inaccurate Values

Resolves an intermittent issue where in certain scenarios some users will see negative traffic stats. This has now been addressed.

PROD-747: Advanced Search Error on Accounts Page

Resolves an issue when users add search options too quickly on the Accounts Page which results in an error. This has now been addressed.

CS-8903: Advance Search Disables Issue

Resolves an issue when a users selects the ‘Accounts Assigned To’ dropdown, Advanced Search disables when it should not. This has now been addressed.

Appendix:

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

No, a reboot is not required as part of the 8.4 update.