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 8.1. The Version 8.1 release introduces UI support for Vectra Match, Stream support for Splunk HEC publishing, the option to disable communications to Vectra, an enhancement to the Hidden HTTPS Tunnel Abnormal Beacon Signal detection, improved coverage for Token Theft kits, and new detection coverage for attackers adding Azure AD persistence.

Release Schedule

8.1 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after Jan 2, 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 Jan 16, 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 Jan 16, 2024
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Vectra Match WebUI Support — Detect for Network

Vectra Match now supports configuration via the Vectra Match WebUI in the Quadrant UX in addition to the existing API support for management. The ability to configure Vectra Match via the WebUI includes support for Enabling/Disabling Sensors, Uploading Rulesets, applying Rulesets to sensors, and collecting status information. You can get more information about managing Vectra Match via the WebUI via the Deployment Guide: https://support.vectra.ai/s/article/KB-VS-1636

Stream support for Splunk HEC publishing — Stream

Added a new output type for Stream to support export to Splunk using HEC. This supports sending Stream via HEC to either Splunk Cloud, or to Splunk Enterprise.

Option to disable communications to Vectra — Detect for Network

Vectra supports customers deploying in air-gapped modes, but previously Vectra would still attempt to “dial home” for updates and health monitoring. While customers could easily block this, it created unnecessary and unwanted network traffic. Now, customers have the option to disable these communications from within the Vectra platform.

Detections

Hidden HTTPS Tunnel Abnormal Beacon Signal Improvement — Detect for Network

Starting in 8.1, Vectra has improved the Hidden HTTPS Tunnel (Tunnel Type: Abnormal Beacon) Detection to reduce benign true positive scenarios where the Abnormal Beacon tunnel type is triggered due to anomalous connection properties with certain sites. There is no action required from users, and no change to the UI itself. This improvement only affects the Hidden HTTPS Tunnel Type Abnormal Beacon

Improved Coverage for Token Theft Kits — IDR for Azure AD

An enhancement to Vectra's Azure AD Suspicious Sign-on and Azure Compromised Access detections enable better coverage for recent AiTM kits like EvilProxy. Vectra alerts on more scenarios where the initial access is suspicious and appears to be associated with a phishing kit by tracking additional error code events associated with token theft attacks.

New Coverage for Attackers Adding Azure AD Persistence — IDR for Azure AD

Two new detections Azure AD Suspicious Device Registration and Azure AD Suspicious Factor registration enables coverage for attacker's registering a device or authentication method to add persistence following an identity compromise. The new detections use machine learning to learn where users normally register devices from and alerts on devices registered from abnormal locations. This in conjunction with a Suspicious Sign-on event will be rapidly prioritized for review in the Vectra platform.

Bug Fixes

PROD-58: Limit Auto-Retry of Host and Account Unlocking

Resolves an issue where excessive email notifications may be sent when automatic host or account unlocking failures occur.

CS-8313: Error calling memory health API

An error, returned from memory health API calls, has been resolved.

CS-8294: Sensor "Not Forwarding" after re-pairing

After IPs change, when re-pairing a sensor manually or through auto-pairing, occasionally the sensor to brain communication would get an invalid configuration. This has been addressed to ensure the correct configuration is used.

CS-8240: Network Stats -> Ingested Traffic not showing data

In a very limited number of cases, it was found that the Ingested Traffic graph showed no data even though traffic was being ingested. This has been resolved.

CS-8229: UI becomes unavailable when setting timezone to specific values

Specific values for the timezone setting were found to cause the UI to become non-responsive. This issue has now been resolved.

CS-8226: Non-English characters in Host Names not rendering correctly

In the Host Severity report, it was found that certain non-English characters in Host Names, would fail to render correctly. This has been resolved.

CS-8216: Detection misattribution

An issue was found whereby detections were in certain rare cases attributed to the incorrect host. This has been resolved.

CS-8127: Unable to delete IPs from the Dropped Ips list

An issue was found with deleting previously created IPs in the Dropped IPs list. This issue has been revolved, and these list items can now be deleted.

CS-8124: Windows Event Log Ingestion fails occasionally

An issue was found with charset handling for Windows Event Log Ingestion which would occasionally cause the ingestion to fail. This has been resolved.

CS-8011: Stream “Aggregated Metadata Volume” graph slow to load for larger customers

An issue was found with performance of the Stream “Aggregated Metadata Volume” graph for larger customers. This has been improved.

CS-7885: Recall traffic dashboard missing monthly P95 in some cases

An issue was found with missing P95 lines on the Recall traffic dashboard. This has been resolved.

CS-8113: Inconsistent STIX file upload sizes for different API versions

An issue was found with different file upload limits for STIX files on different versions of the API. This 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 8.1 update.