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 Detect for Network software release version 7.9. The Version 7.9 release introduces Vectra Match Recall support, Recall Custom Model support, a new Recall dashboard, and support for Microsoft OAuth 2.0 for SMTP notifications. Furthermore, enhancements have been made to Priority Triage, additional restore options upon generating a backup file, and disk space improvements.

Release Schedule

7.9 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after August 24, 2023
    - 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 Sept 5, 2023
    - 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 Sept 5, 2023
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Vectra Match Recall Support — Vectra Match / Recall

Vectra Match now supports sending Vectra Match alerts directly to Recall to power threat hunting and investigations. If you have Vectra Match enabled and Recall, the Vectra Match alerts will automatically be sent to Recall, no user action is required. Vectra Match alerts will appear in the new metadata index metadata_match. Recall Vectra Match support includes the traditional Discovery, Dashboards, Alerts, Saved Searches, Visualizations just like other metadata streams. For information about the new metadata fields please see: https://support.vectra.ai/s/article/KB-VS-1245. For additional information, please see the Vectra Match FAQ: https://support.vectra.ai/s/article/KB-VS-1635

Vectra Match Recall Custom Model Support — Vectra Match / Recall

Vectra Match in Recall supports the ability to leverage Custom Models to create scored detections in Detect for Network. For instance, if you have a particular IDS alert or class of alerts that you want to contribute to a Host Score in Detect, you can leverage a custom model to match any alerts for a given signature ID or signature name/substring which will result in associated detections appearing and being scored by Detect for Network. Vectra Match Custom Models in Recall work the exact same way as Custom Models generated by traditional metadata. For additional details, please see: https://support.vectra.ai/s/article/KB-VS-1179

Vectra Match Recall Dashboard — Vectra Match / Recall

The Match Dashboard offers holistic insights into IDS alerts across your environment. The dashboard offers interactive widgets to interact with the data and quickly pivot into information of investigative

interest. Patterns from the dashboard can be analyzed and combined with other detections to investigate a suspicious activity.

Priority Triage Enhancements — Vectra Platform

Vectra has introduced the following Triage enhancements to provide more granularity triaging detections.

- Port Scan: You can now configure triage filters for the Port Scan detection based upon the Destination Ports observed in the scan.
- Port Sweep: You can now configure triage filters for the Port Sweep detection based upon the Destination IPs observed in the scan.
- SMB Account Scan: You can now configure triage filters for the SMB Account Scan detection based upon the Account Name
- Kerberos Account Scan: You can now configure triage filters for the Kerberos Account Scan detection based upon the Account Name
- Smash and Grab: You can now configure triage filters for the Smash and Grab detection based upon the Destination Ports and Protocols
- File Share Enumeration: You can now configure triage filters for the File Share Enumeration detection based upon the Account Name and the File Share. For the File Share you can also use simple Wildcarding (*) to match any characters preceding or following the wildcard. E.g. *Corporate would match any File Shares that started with any string and ended in “Corporate.”
- M365 Suspicious Mail Forwarding: You can now configure triage filters for the M365 Suspicious Mail Forwarding detection based on the Destination mailbox and Forwarded Mailboxes using Wildcarding (*) to match any characters preceding or following the wildcard
- Azure AD Suspicious Scripting Engine: You can now configure triage filters for the Azure AD Suspicious Scripting Engine detection based on the User Agent field using Wildcarding (*) to match any characters preceding or following the wildcard

*Note that all of these enhancements will match when there is either an exact match, or the triage criteria is a super set of the Detection objects. A subset will not be considered a match. For instance, if you have a detection with Object A and Object B, we’d expect the following behavior:

1. Triage rule with Object A and B: Match
2. Triage rule with Object A, B, and C: Match
3. Triage rule with Object A: No Match

Microsoft OAuth 2.0 for SMTP Email Notifications — Vectra Platform

Microsoft recently deprecated support for basic auth in Exchange Online which resulted in some SMTP email notifications not be delivered. Vectra now leverages Microsoft OAuth 2.0 for SMTP email notifications. For more information on how to setup SMTP on a Vectra Brain, please see: https://support.vectra.ai/s/article/KB-VS-1051

Disk Maintenance Improvements — Vectra Platform

Release 7.9 introduces enhanced monitoring checks and improvements to increase the amount of available disk space.

Preserve SAML Config and UI Certs on Restore from Backup — Vectra Platform

Version 7.9 has added three new options to the "restore run" command. They include:

`--preserve-saml`

- Keeps the SAML configuration that was present on the target brain prior to the restore
- For example, this can be helpful when SAML configuration is tied to an IP address that will be different on the target Brain.

`--preserve-ui-certs`

- Keeps the UI certificates that were present on the target brain prior to the restore
- This can be useful when the restore target will have a different IP/hostname that would invalidate the UI certificate configuration.

`--replace`

- This option is meant to be used when a brain is being fully replaced by another brain and ensures that internal processes at Vectra properly link this new brain with our back end as a replacement. For customers running the Respond UX with network data sources, this option will ensure your replacement brain can automatically connect to your GUI that is being served from the Vectra AI platform.

For more information on Backup Restore, please see: https://support.vectra.ai/s/article/KB-VS-1118

Detections

M365 Suspicious Mail Forwarding — Vectra Detect for M365

Attackers will look to exfiltrate mailbox information by creating mailbox rules that forward entire mailboxes to external destinations. In this release, we have extended detection coverage for additional methods of rule creation. To support any increase in detections that may come from this enhancement additional triage rule functionality has been added to support wildcard filtering by Destination mailboxes.

Bug Fixes

PROD-55: Deleted User with Associated Detections

Addresses an issue where a user is deleted, *all* detections that the user marked as fixed are deleted with the user.

PROD-14: IP Validation to extend to Host Group Configurations

Addresses an issue where the validation only matches the formatting.

PLAT-10400: Logrotate Permission Issue

Addresses an issue where logrotate can sometimes fail to rotate the colossus vsupport CLI logs due to permissions issues.

CS-6846: Sensor Filter on Host Page Issue

Addresses an issue where the Sensor filter on the Host page does not accurately represent the entities associated with that sensor.

CS-7837: Incorrect Time Window for Host Severity Report

Addresses an issue where upon generating the Host Severity Report

CS-7867: Triage Advisor showing [object Object] for conditions

Addresses an issue where the triage conditions field incorrectly shows [object Object] on the Triage Advisor page.

CS-7882: Detection Page Tag Search Box Does Not Display

Addresses an issue on the Detection page upon clicking the ‘Tag’ button, the screen may blur and search box may disappear. This has now been addressed.

Appendix:

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

Yes, a reboot is required as part of the 7.9 update.