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 7.8. The Version 7.8 release introduces support for DirSync for Active Directory, Real-time Cloud and Cloud Identity Detections, detection coverage enhancements, two new Recall dashboards, and several bug fixes.

Release Schedule

7.8 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after July 25, 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 Aug 1, 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 Aug 1, 2023
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

DirSync for Active Directory — Vectra Detect for Network

Detect for Network administrators can now use native Microsoft DirSync capability to synchronize Active Directory host and account data used for additional context and Lockdown. DirSync is ideal for very large AD deployments where it may be preferable to retrieve only updates to the data with the goal of reducing overall system load on your AD.

More information on enabling DirSync for Active Directory can be found here.

Detections

Vectra constantly evaluates detection algorithm coverage and efficacy using opt-in metadata and direct user feedback, which drives targeted enhancements in our algorithms. We encourage your feedback via the Vectra user community.

Real-time Cloud and Cloud Identity Detections — Vectra Detect for M365, AWS and AAD

All of Vectra's detection focused on finding cloud threats have been enhanced to report in real-time. This means that 100% of the Vectra Platform from AWS, Azure AD, M365 to the network report on threats as they occur, ensuring defenders can stop attackers wherever they are before they can do damage.

Enhanced Coverage for Risky OAuth Apps — Vectra Detect for AAD and M365

Attackers, after compromising an Azure AD credential, will use it to install a trojan application that provides the attacker future access to the tenant without passing MFA. Vectra's detection coverage for trojan applications in Azure AD and Teams has been expanded to include coverage for more application permission types that have been observed in use by attackers. Customers may see at most 1-2 more alerts of this type per Month.

Enhanced Signal for M365 Ransomware Activity — Vectra Detect for M365

Attackers deploying ransomware against cloud-linked shares can encrypt the files locally and sync them to the cloud. Vectra's detection signal for this type of attack has been improved, reducing overall alert volumes by considering common benign encryption mechanisms while maintaining coverage for real attacks.

Enhanced Coverage for Risky Exchange Operation — Vectra Detect for M365

Attackers will abuse the native SendAs functionality to send emails as a user to spearphish internal or external accounts and spread. The Suspicious Mailbox Operation will not report suspicious use of this operation by attacks. In most customers, there should be no increase in volumes, but in some cases, there may be close to 10 more alerts of this type per Month.

New Dashboards

Traffic Visibility & Event Breakdown Dashboard — Cognito Recall

Vectra have released 2 dashboards, to help customers understand what the source of their Recall log Volume might be.

To help customers understand the causes of their Recall Log Volume, a dashboard has been added with visualizations which offer a detailed breakdown of recall events, determining the data volume transferred from the Brain to the Recall infrastructure. It breaks down the events by Protocol and IPs, aiding the analysis of metadata production from monitored endpoints. This does not necessarily show what is causing the most network traffic in your environment, but what is causing the most recall log volumes, a factor of how your network traffic is parsed into Zeek formatted metadata.

To understand network traffic in your environment, the Network Traffic Visibility dashboard rapidly brings to light the machines contributing to heavy traffic volumes along with the ports and protocols utilized during those sessions. This is helpful when analyzing high Recall usage, as it allows you to narrow down traffic behaviors granularly, identifying spikes in usage, and presenting the loudest machines as they compare to the system-aggregate usage during that time. This has been helpful in identifying specific tools and services unhelpful to Vectra that may be candidates for traffic visibility exclusion. The volume of data sent does not correlate directly with Recall volumes but is clearly informative of where large volumes of network traffic are generated in your environment, which will help with both Recall management but also general Network traffic analysis.

These dashboards should hopefully give customers insights into what the cause of their Recall usage was.

ChatGPT Usage Dashboard — Cognito Recall

Vectra have released a new dashboard to give you insights into the usage of the OpenAI's service 'ChatGPT' on your network. This service, although legitimate, might pose a risk for security as the AI models process data being sent to its services to improve the user experience. This may result in

sensitive internal data being sent to and processed by the service eventually being exposed to 3rd parties.

Due to this concern numerous outlets have advised against allowing users to send data to these services for processing. This Dashboard will help you to identify when users are communicating with these services.

Vectra Match File Rotation — Vectra Match

Vectra Match has introduced a new 'rotate' option to the ruleset upload operation. When this option is enabled, if there is no more disk space available for the ruleset partition, the system will automatically remove the oldest ruleset file not assigned to a sensor. For additional information, please see our API guide or Postman collection.

Bug Fixes

CS-7758: Alerts from accounts with no recent detection activity

Addresses an issue where accounts with no recent detection activity may generate alerts.

CS-7766: Misaligned detection tag icon box

Addresses an issue where the detection tag icon box may be misaligned on the Detections page.

CS-7784: Not parsing the DHCP service from Infoblox

Addresses an issue where the DHCP metadata is not parsed when using Infoblox to deliver DHCP service.

CS-7076: Cybereason integration pulling multiple ID artifacts per host

Addresses an issue where the Cybereason EDR integration may pull in multiple ID artifacts per host due to a change from decimal to alphanumeric host IDs in the Cybereason API.

CS-7714: Suspicious Admin "end" time can be misleading

Addresses an issue where Suspicious Admin "start" and "end" time show the same timestamp when only a start time should be shown as this correlates to only the beginning of a suspicious connection.

PLAT-9930: Vectra Match Unhealthy State Timer Update

Previously, when Vectra Match was in an Unhealthy state and the issue is resolved, the status Endpoint would remain Unhealthy for 24 hours to ensure the condition didn't quickly return. This has been updated to remain in the Unhealthy state for 1 hour before returning to the Healthy state to ensure the system isn't flapping.

CS-8021: Host Session Processing Issue

Addresses an issue that was mitigated in the 7.8.1 patch, where some host sessions were potentially not processed. This has now been addressed permanently in 7.8.2.

SAASAPPS-4174: Sensor Default Password Issue

Addresses an issue with sensor passwords when the default password has not been changed. This has now been addressed.

Appendix:

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

No reboot is required as part of the 7.8 update.