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 7.6

The Version 7.6 release introduces support for Vectra Match, REST API v2.5, 50 Gbps AWS brain, and faster detection reporting.

Vectra Detect platform enhancements and bug fixes are also included in this release.

Release Schedule

7.6 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after March 29th, 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 April 5th, 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 April 5th, 2023
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Vectra Match

Vectra Match

Version 7.6 introduces support for Vectra Match. Vectra Match delivers the ability for customers to provide Suricata compatible signatures to detect known Indicators of Compromise (IOCs) within the network. In this initial release, Vectra Match supports the following functionality:

- Vectra Match on all supported physical, virtual, and cloud sensors
- Bring your own ruleset, including customer defined, open source (ETOpen), and commercial (ETPro)
- Ability to define an IDS policy per Vectra sensor
- API Management
- Alerts generated in native Suricata EVE/Fast log formats
- Alerts sent to SIEM/SOAR via Syslog and Kafka

For more information, please see our Vectra Match Deployment Guide

50 Gbps AWS Brain

Vectra Detect for Network

With this release, customers can now deploy a Vectra Brain in AWS which would support up to ~50 Gbps of network traffic. This cloud appliance would be based on the r5d.16xlarge instance. The existing AWS CloudFormation template for the Vectra Brain would be updated to offer this new size. Deployment documentation is available at https://support.vectra.ai/s/article/KB-VS-1254 , backup and migration processes are the same as existing 5 Gbps and 15 Gbps options.

REST API v2.5 — Vectra Detect for Network

Release 7.6 introduces the v2.5 REST API. The v2.5 API provides support for programmatic access to Vectra Match via a new /api/v2.5/vectra-match endpoint. This endpoint allows you to list, create, modify, and delete IDS rules. More information can be found in the Vectra REST API Guide for v2.5. You can also find sample queries in the Vectra public Postman collection for v2.5.

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.

Faster Detection Reporting — Vectra Detect for M365 and Detect for Azure AD

The non-scored “Azure AD Account Brute Force Attempt” detection has been enhanced to report on brute force attempt activity in real-time.

Bug Fixes

CS-7479: Data Source Sensor page long load time

Addresses an issue where the Data Source Sensors page can take over a minute to load due to the network timeouts when retrieving sensor data from all regions.

CS-7415: Setting for FQDN-based email alert links does not save

Addresses an issue where changing the email alert link settings to use DNS Name instead of IP address setting does not get changed upon clicking "Save" button.

CS-7469: “Host Detail” does not link to correct device on M365 Defender dashboard

Addresses an issue where the "Host Detail" link for a given host links to the M365 home screen instead of the selected device on the M365 Defender dashboard.

CS-6689: /api/v2.2/settings/proxy endpoint returns HTTP 500 error

Addresses an issue where the /api/v2.2/settings/proxy endpoint returns an Internal Server Error message when attempting to retrieving the current proxy configuration.

CS-6187: Internal Stage Loader detection API does not include bytes sent/received

Addresses an issue where the /api/v2.3/detections/<detection_id> endpoint does not include bytes sent/received for the Internal Stage Loader detection.

CS-7033: Offline customers unable to generate Stream license

Addresses an issue where some offline customers may see an error “There was a problem with generating license key” when attempting to generate a Stream license.

CS-6287: AD username not recognized due to case sensitivity

Addresses an issue where case sensitivity is incorrectly enforced on a database column causing some AD usernames to not be recognized.

Appendix:

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

No reboot is required as part of the 7.6 update.