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 7.3

The Version 7.3 release introduces Hyper-V VHDX format support, a host scoring enhancement based on detection velocity, Detection Profiles for accounts, and an enhancement to the Port Sweep detection.

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

Release Schedule

7.3 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on December 18th, 2022
  - 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 December 27th, 2022
  - 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 December 27th, 2022
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Hyper-V VHDX Format & Second Capture Interface Vectra Detect for Network

Starting in 7.3, Vectra will introduce support for Microsoft Hyper-V VHDX format for vSensor virtual machines. The VHDX format provides several advantages related to scale, reliability, and will help streamline deployments where the VHDX format is already in use. Additionally, moving to the VHDX format will introduce support for the use of a second capture interface. Vectra will continue to support vSensors running on existing VHD images, but all new deployments will use the new VHDX format.

Host Velocity Scoring Enhancement Vectra Detect for Network

Release 7.3 introduces a scoring enhancement based on the velocity of detection activity occurring on a host. Seeing different detections in quick succession on a host can provide an early indication of suspicious activity prior to an attack. Detection velocity now impacts host scoring and aids in driving hosts into the High and Critical quadrants faster for earlier detection.

Account Detection Profiles Vectra Detect for Network

Introduced in release 5.5, Detection Profiles aid in characterizing the nature of detection activity found on hosts, based on the active detections they have exhibited. Release 7.3 brings that same concept to Accounts, to help analysts gain a better understanding of the overall behavior of account detections. Profile types include:

- Compromised Credentials
- External Adversary
- Ransomware

- Insider Threat: Privileged
- Insider Threat: Non-Privileged
- Services Management
- Service Enumeration and Access
- Risky Services Utilization

The profiles are presented as a left-hand widget on the individual account and host pages.

Low Volume Port Sweep Enhancement Vectra Detect for Network

Starting in 7.3, Vectra is introducing an enhancement to the Port Sweep detection to identify evasive port sweep behaviors when an attacker my attempt to evade detection by performing low and slow port sweep techniques. This is part of the existing Port Sweep detection and compliments the Low Volume Port Scan detection introduced in 6.11. Low Volume Port Sweep will leverage the same UI and Triage filters as the existing Port Sweep detection.

Bug Fixes

CS-6757: System Health Dashboard displaying incorrect status for network interfaces

Resolves an issue where health warnings may be displayed for the brain management interface when the interface is running normally.

CS-6684: Brain-to-Brain backups may fail when using B101 as target

Resolves an issue where a brain-to-brain backup is not automatically copied to the target brain when that brain is a B101 model.

CS-6550: Invalid hyperlink to metadata sharing agreement

This addresses an issue that occurs when a user attempts to access the Vectra Metadata Sharing Agreement but cannot access the document due to invalid hyperlink. This has now been addressed.

CS-6420: Unable to select any region when creating O365 sensor

This addresses an issue that occurs when a user is unable to select any valid region when attempting to create an O365 cloud sensor. This has now been addressed.

CS-6352: Account Threat and/or Certainty Scores different between API and UI

This addresses an issue that occurs when different Threat and/or Certainty Scores are shown between the v2.2 API and UI for the same account. This has now been addressed.

CS-6263: Crowdstrike missing from host page

This addresses an issue that occurs when hosts known to be running the Crowdstrike EDR agent may not display Crowdstrike EDR artifacts on the host page. This has now been addressed.

CS-6262: Additional condition in triage filter not applied properly

This addresses an issue that occurs when additional conditions do not match correctly for Suspicious Relay triage filters. This has now been addressed.

CS-6006: Network Statistics page for Stream not showing data

This addresses an issue that occurs when the Network Statistics page for Stream does not show any data. This has now been addressed.

CS-5485: UI error / gateway timeout when disabling Account Lockdown

Resolves an issue where account lockdown inconsistently failed for some user accounts.

Appendix:

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

This update will not perform any reboot of the Brain or Sensor appliances, nor is any user interaction required.