Vectra Detect Platform Software Update

The Vectra® X-series appliances, B-series appliances, S-series sensors, Cloud Brain, and Cloud Sensors, are scheduled to be updated to Vectra Detect for Network software release version 7.0

The Version 7.0 release introduces Ai-Triage on by Default, Algorithm Performance Improvement, Host-ID Conflict Resolution Improvement, Nutanix AHV vSensor Certification, and Recall Metadata Forwarder Update.

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

Release Schedule

7.0 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on August 29th, 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 Sept 6th, 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 Sept 6th, 2022
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

AI-Triage Enabled by Default

Vectra Detect for Network

AI-Triage was originally introduced in 6.17 for C2/Exfil detections, and then extended to support Lateral Movement detections in 6.19. Due to the great success and customer benefits of the feature, in 7.0 we will be enabling this feature by default, with two exceptions. If you have previously disabled AI-Triage or if you are deployed in Offline Mode, we will not enable the feature. You can review the status of the feature under Settings-AI-Triage. For more information about AI-Triage, please see our KB article: https://support.vectra.ai/s/article/KB-VS-1582

Algorithm Performance Improvements

Vectra Detect for Network

Vectra has made performance improvements to the Suspicious Remote Execution, Hidden HTTPS Tunnel, DNS Hidden Tunnel (C2) and DNS Hidden Tunnel (Exfil) algorithms. There should not be any noticeable change in functionality, and no action required by the user, but the algorithms will perform better when the system is busy than previous releases.

Host-ID Conflict Resolution improvement

Vectra Detect for Network

Starting in 7.0, Vectra is making an improvement to the Host-ID subsystem. Host-ID plays an important role in the Vectra platform by following the movement of Hosts throughout their lifecycle on the network, regardless of what IP address the Host may have at any point. As part of the 7.0 release, we are enhancing Host-ID to better handle scenarios where we receive conflicting Host-ID artifacts from the network and integrations. Starting in this release, if there is conflict between Host-ID sources for a given host, we will choose the Host that best matches the set of artifacts observed. Prior to 7.0 when there was conflict the system would choose the Host to assign artifacts based on the first artifact the system observed in a host session. There is no action required by

the user. To view what artifacts the system knows about a Host, you can go to any Host in the system, click the Details tab, and review the Host-ID Artifacts. Please understand this change to Host artifact assignment logic does not change the logic behind Host naming. That logic remains as described in the Understanding Vectra Detect Host Naming article on the support website.

Nutanix AHV vSensor Certification — Vectra Detect for Network

Vectra has achieved formal certification of the vSensor from Nutanix running on their AHV platform. The image is now available for download directly within the platform under Manage -> Sensors -> Download Virtual Image. For more information, please see our Nutanix Deployment Guide: https://support.vectra.ai/s/article/KB-VS-1603

Recall Metadata Forwarder Update — Vectra Detect for Network

Vectra has improved the Recall Metadata Forwarding Service. The update improves Recall's ability to recover from network or system disruptions. There is no action required by the user, nor any changes in Recall's specifications, metadata, or behavior; simply that Recall will now be more resilient to disruptions.

Bug Fixes

EC-1208, EC-1209: Scheduling Selective PCAPs does not work as expected when Timezone for Brain doesn't match Sensor

This addresses an issue that occurs then the Sensor and the Brain have different timezones, and the user schedules a future PCAP job in Selective PCAP. This has now been addressed.

Data-1985: SMB messages are not correctly parsed when full session is not observed

This addresses an issue where SMB metadata would not be produced if Vectra did not see the full SMB transaction from the beginning. This could be due to a system restart, mapped network drive that SMB previously negotiated, or due to traffic mirroring issues. Now, Vectra will correctly parse SMB messages even if we did not see the initial SMB session setup.

Data-1980, CS-6000: TLS misidentified when session begins as HTTP in Proxy Scenarios

This addresses an issue where when a session begins as HTTP and then performs a CONNECT to a proxy using TLS/SSL, we still identify the session as HTTP. We will now properly recognize this session as HTTPS and inspect it/generate metadata accordingly.

CS-6350: Stream Kafka Unable to Publish Metadata to Azure EventHub

This addresses an issue where Stream Kafka was unable to publish metadata to Azure Eventhub due to a limitation on the supported password length to 128 characters. This has been addressed.

CS-6265: Browsing to the index.html URL redirects to NGINX landing page.

This addresses an issue a user browsing to the index.html file will be redirected to the NGINX landing page rather than the Login page.

CS-6263: EDR Artifacts not showing up in Host Detail Page after Host Merge.

This addresses a rare scenario when Host-ID determines that two systems are the same Host (typically after IP address changes) and the EDR artifacts are not merged properly so the new host does not display the EDR artifacts under the Host Detail page. This has been addressed.

CS-6153: Error received when trying to reorder Triage Filters

This addresses an issue where a user may receive an error message when trying to reorder the Triage Filter priority order. This has been addressed.

CS-6202: System Health Page Not Auto-Updating

This addresses an issue where the System Health page does not auto-update as expected. This has been addressed.

CS-6108: Windows Event Log Kafka Configuration not properly updating

This addresses an issue where when editing the Windows Event Log integration when using Kafka. If the user switches between Plaintext, SSL, and SAML, the system does not properly update. This has been addressed.

CS-6085: Port Scan Incorrectly lists port 80 in Syslog message when multiple ports are listed

This addresses an issue where when there is a port scan detection that has multiple ports, the dst_port field lists port 80, which is incorrect because there is multiple ports, which are correctly listed in the ports field. Going forward if there is multiple ports, a 0 will be listed in the dst_port to indicate that there are multiple ports (since this field can only accept one as part of the standard message) and the ports field will continue to list out all of the ports in the syslog message.

CS-6023: Security Analyst is able to set Google GCP Connector

This addresses an issue where when a Security Analyst user is able to setup the GCP connector, even though as a security analyst they should not be able to. This issue has been addressed.

CS-5719: Invalid STIX Document Caused Threat Intel Service Restart

This addresses an issue where an invalid STIX document could cause the Threat Intel Service to restart. This has been addressed so that it is gracefully handled with an error message.

CS-5746: UI Allowed Invalid Subnet to be Submitted

This addresses an issue where an invalid subnet could be submitted to the Internal Networks page. This has been addressed so an error message will be displayed to the user if there is an invalid submission.

PLAT-8411: 8-Core vSensor at 100% CPU

This addresses an issue where the 8 core vSensor shows it is at 100% CPU due to flow threads being configured for hot polling. This has been addressed.

PLAT-8089: FIPS Mode does not pass STIG 2 Check

This addresses an issue where Vectra deployments running in FIPS Mode will not pass the STIG 2 Check. This has been addressed.

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.