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 6.19

The Version 6.19 release introduces *AI-Triage Lateral Movement Support, Selective PCAP, and X29/M29 10Gbps Management Interface Support*

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

Release Schedule

6.19 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on 6/13/2022
    - 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 6/20/2022
    - 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 6/20/22.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

AI-Triage Lateral Movement Support — Vectra Detect for Network

Starting in 6.19, AI-Triage has been extended to support detections in the Lateral category. If the customer has enabled AI-Triage, no action will be required to take advantage of this new detection type. For more information, please see our Knowledge Base articles: KB Article: https://support.vectra.ai/s/article/KB-VS-1582

Selective PCAP — Vectra Detect for Network

Vectra Detect 6.19 introduces an important new capability for network operators called Selective PCAP. Selective PCAP provides the customer with the ability to trigger their own packet captures on sensor traffic interfaces directly from the Detect UI. This feature is valuable for troubleshooting scenarios where the customer would like to capture traffic which is being received on the network sensor for viewing in a PCAP viewing tools like Wireshark. Customers can schedule or create on demand packet captures, and create traffic filters to select the packets of interest. For additional information please see KB Article: https://support.vectra.ai/s/article/KB-VS-1579

X29/M29 10Gbps Management Interface Support — Vectra Detect for Network

In 6.19, Vectra is extending the ability for customers to leverage the 10Gbps interfaces on the X29/M29 as management interfaces. The X29/M29 traditionally has leveraged the two built in 1Gbps interfaces as the Mgt1 and Mgt2 interfaces, but with the introduction of the "set management speed 10G" command on the Vectra CLI for the respective Brain or Sensor. The first 10Gbps traffic interface can be dedicated as the Mgt1 interface.

Notices

Detection Name Change — Vectra Detect for O365

The detection name pre-fix “O365” used to denote attacker activity in Microsoft 365 will be changed to “M365” in the 6.21 release. This change allows Vectra to better match Microsoft’s product naming.

Customers can continue to use the same naming convention when interacting with these detections in the API. All requests returned from the API will include the updated alert name. Detection events logged via syslog will appear with the new detection name.

EOL Announcements

VMWare ESXi 6.0 Support for vSensors and Stream

In Detect 6.18, Vectra announced the EOL of VMWare 6.0 support in vSensors and vStream. 6.19 will be the last release to support VMWare 6.0 for vSensors and Stream. After 6.19, we will still support VMWare 6.5, 6.7, and VMWare 7 for vSensor and Stream. Customers are encouraged to upgrade their VMWare vSphere Host or migrate vSensors and Stream to VMWare 6.5 or later for continued support after 6.19.

Internet Explorer 11 EOL

Microsoft has announced the End of Life of Internet Explorer 11 on 6/15/22. Detect 6.20 will be the last release to support Internet Explorer 11 as a client web browser. Vectra will continue to support the latest versions of

- Chrome (and any browsers based upon the Chromium Engine, like MSFT Edge)
- Firefox
- Safari

Bug Fixes

CS-6044: Cannot change names of Triage filters

This addresses an issue where triage rule names cannot be edited after they have been created in 6.18. This issue has been addressed.

CS-6046: SSH Metadata Not Parsed

This addresses an issue where some non-standard implementations of SSH may not be parsed, and thus the metadata would not be present in Recall or Stream. This has been addressed.

CS-5886: Stream Metadata Interruption

This addresses an issue where the Brain to Stream metadata flow can be interrupted in rare cases when too much data is queued between Brain and Stream appliances. This has been addressed

CS-6002: Threat Intel Detection Match on Wrong Hostname

This addresses an issue where Vectra may create a detection on an IP address matched to a Domain name on the Threat Intelligence list. This happens when multiple IP addresses are returned when resolving a Domain on the Threat Intelligence list, most often when the IP’s exist in multi-tenant cloud environments. Vectra has improved the resolution logic in these complex scenarios to identify the best IP match in this release.

Known Issues:

Selecting Brain Appliance in Selective PCAP will result in Error.

Selective PCAP is only supported on Sensors, setting the Sensor to a Brain appliance is not supported. Brain appliances will be removed from the Sensor drop down list in an upcoming release.

Deleting Stopped Capture in Selective PCAP does not work

If a user stops a Packet Capture, the capture stops successfully, but the user is unable to delete the capture from the list. This will be addressed in an upcoming release.

Setting Duration in Selective PCAP does not work if Sensor/Brain is not in same time zone

Setting the duration in Selective PCAP does not work as expected when Sensor and Brain are in different time zones. All filtering works properly, including capture duration, but the duration does not work as expected. This will be addressed in an upcoming release

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.