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 7.4

The Version 7.4 release introduces Account Groups, an update to the REST API, page load performance improvements, faster detection reporting for some M365 and Azure AD detections and support for CrowdStrike v2 device details endpoint.

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

Please note that the 7.4 update will upgrade the system BIOS on all non-S11 platforms and will perform a reboot of Brain and sensor appliances immediately following the 7.4 update.

Additionally, the 7.4 update includes minor changes to CEF syslog output which may require updates to syslog parsers. See CS-5993 in the Bug Fix list and "CEF Syslog changes" in the Appendix for additional information.

Release Schedule

7.4 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on January 26th, 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 January 26th, 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 February 1st, 2023
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Account Groups — Vectra Detect for Network

Version 7.4 introduces support for the grouping of accounts. Account groups help to simplify the triage workflow, when you have multiple accounts that need to be triaged in a similar manner, by allowing triage filters to be applied directly to an account group instead of individual accounts. Account can be added to groups from the Manage Groups page or directly from the individual account page. Accounts can also be added to groups from the all accounts page. An account can be a member of one or more groups. If an account is added to a group that has a triage filter assigned to it, the triage will automatically apply to detections on the account without the need for additional action.

REST API v2.4 — Vectra Detect for Network

Release 7.4 introduces the v2.4 REST API. The v2.4 API provides support for programmatic account group management via a new /api/v2.4/groups endpoint. This endpoint allows you to list, create, modify, and delete account groups. More information can be found in the Vectra REST API Guide for v2.4. You can also find sample queries in the Vectra public Postman collection for v2.4.

Page Load Performance Improvements — Vectra Detect for Network

As Vectra works to deliver efficient analyst workflows, we also are working to improve performance of our User Interface. In the 7.4 release, a number of significant performance improvements have been delivered which should result in significantly improved page load times, especially for customers with large data sets.

CrowdStrike v2 Get Device Details Endpoint — Vectra Detect for Network

CrowdStrike will deprecate support for the v1 Get device details endpoint in February 2023. The Get device details endpoint is used by Vectra for host context whenever the CrowdStrike EDR integration is enabled. Release 7.4 will automatically migrate from the v1 to the v2 endpoint with no configuration changes required.

Sensor and System Settings UI Changes — Vectra Detect for Network

In preparation for upcoming changes to the Vectra Detect platform, the location of some system settings will change as part of release 7.4, as follows:

- Platform wide settings are still located at *Settings > General*
- Brain specific settings are now under *Data Sources > Network > Brain Setup*
- Sensor management is now under *Data Sources > Network > Sensors*
- Detect for Azure AD & M365 management is now under *Data Sources > Azure AD & M365*

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

Several Vectra M365 and Azure AD detections have been enhanced to report threats within less than an hour of Vectra receiving and processing the relevant logs from Microsoft. Specifically, Azure AD Brute Force Successful and M365 Malicious Mailbox Rule.

Bug Fixes

PLAT-8920: Upgrade FIPS Kernel

Resolves a potential stability issue on all Dell platforms, except the S11. The system BIOS will be upgraded and will reboot immediately following the 7.4 update.

PLAT-8829: CVE-2022-21797

Addresses Critical CVE-2022-21797 where joblib could be vulnerable to Arbitrary Code Execution. More information on CVE-2022-21797 can be found here.

PLAT-9904: CVE-2022-24422

Addresses Critical CVE-2022-24422 where a remote unauthenticated attacker may potentially gain access to the console. More information on CVE-2022-24422 can be found here.

Please note: This fix requires customers who log into iDRAC with a hostname to configure a manual DNS entry in their iDRAC configuration. The ability to set a manual DNS hostname can now be done via the appliance CLI. For more information, please see IPMI / iDRAC Configuration (IP Address, Hostname, Certificates) on the Vectra Support site.

CS-6812: Static Host reset to generic host

Resolves an issue where a static IP host is continuously reset to generic host even after being added to the static host list.

CS-5993: CEF syslog messages may include non-machine parseable components

Resolves an issue where CEF messages may include non-machine parseable components. All CEF message attributes are now JSON encoded where applicable. See “CEF Syslog Changes” in Appendix for detailed information.

CS-6470: Read-only account can generate Host Severity reports

Resolves an issue where a read-only user may still generate a Host Severity report by sending direct HTTP request to the reporting endpoint.

CS-6637: Mixed mode backups restored to Brain only mode shows capture ports

Resolves an issue where health data restored as part of a backup never expires and persists in the health dashboard even after the health issue has cleared.

CS-6407: Advanced Search on Host Page unavailable

Resolves an issue where slow queue fetches cause low replication rate making Advanced Search unavailable.

CS-6156: Selecting “Raw JSON” as Stream destination requires multiple ports

Resolves an issue where multiple ports are presented as required settings to save the configuration, whenever selecting “Raw JSON” as Stream destination settings.

CS-6798: API query does not return value when filtering some hosts

Resolves an issue where the v2.2 API does not return the same results as UI search when filtering hosts by mac addresses.

DATA-3327: Re-enabling TLS metadata on sessions atop HTTP CONNECT proxying

Resolves an issue where TLS metadata on sessions that are established atop HTTP CONNECT proxying is not enabled.

CS-6755: DHCP service from Infoblox not parsed correctly

Resolves an issue where some DHCP fields are not parsed correctly when using Infoblox DHCP service.

Appendix:

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

Yes. As outlined in PLAT-8920 above, this update will perform a reboot of the Brain and sensor appliances immediately following the 7.4 update.

CEF Syslog changes

The following changes have been made to CEF syslog output for improved handling and consistency:

- None objects are now encoded as empty strings.
- Quotes have been added where previously missing (v2 CEF).
- Single quotes have been converted to double quotes.

Previously	`msg="{'sensor':probe1,'detectionProfile': None}"`
Now	`msg="{"sensor":"probe1","detectionProfile": null}"`