Cognito® 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 Cognito® software release version 6.18

The Version 6.18 release introduces Lateral Movement Triage Filters for Destination IP/Host, SentinelOne Active Alerts Count, Detect API Created_Timestamp Attribute, and Remote Support Heartbeat Message in Audit Log.

Cognito® platform enhancements and bug fixes are also included in this release.

Release Schedule

6.18 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on 4/27/2022
    - 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 5/2/2022
    - 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 5/4/22.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Lateral Movement Triage Filters on Destination IP/Host — Cognito Detect for Network

Starting in 6.18, Detections in category Lateral will have a new Triage match criteria to enable the user to specify the destination address or host for all Triage filters of type Lateral. Prior to 6.18, only the Internal Stage Loader detection enabled the user to specify the destination address using the 'Internal Target IP is any of' or 'Internal Target Hostname is any of'.

If you would like to configure the destination, you can go to any Lateral Triage filter (existing or new) and under Additional Conditions specify the 'Internal Target IP is any of' or 'Internal Target Hostname is any of' conditions, with the IP or Hostname specified for the respective match criteria.

SentinelOne Active Alerts Count — Cognito Detect for Network

Starting in 6.18, a new statistic will be added to the Host Details page for customers who have SentinelOne integration to identify how many 'Active Alerts' are being reported by SentinelOne for a given host. You can view this information by going to the Host -> Details page, and looking under the SentinelOne Artifacts section.

IPv6 Dashboards in Recall — Cognito Detect for Network

Coinciding with the 6.18 release, we are introducing a new dashboard to highlight IPv6 activity in your environment. You can browse this dashboard by going into Recall -> Dashboards and looking for "TH - IPv6 Dashboard". This dashboard highlights IPv6 Hosts, Traffic Volumes, Directionality (Internal, Inbound/Outbound) per Protocol breakdowns, Multicast, and IPv6 tunneling. No action is required on the user to configure the dashboard to start using this feature.

Detect API Created_Timestamp Attribute — Cognito Detect for Network

Starting in 6.18, the Detect API will be enhanced to add a new attribute in the API for which identifies when a Detection was created. This is different from the First Seen attribute which may change if new information is identified that shifts the First Seen, as the Created Timestamp is simply when the detection was created. Please see https://support.vectra.ai/s/article/KB-VS-1174 for additional information.

Remote Support Heartbeat Message in Audit Log — Cognito Detect for Network

Starting in 6.18, Vectra when Remote Support is enabled, we will generate a daily heartbeat message in the Audit Log to indicate that Remote Support is enabled. This message is in addition to the existing Remote Support Enable/Disable messages that are already available. For more information see: https://support.vectra.ai/s/article/KB-VS-1045

EOL Announcements

VMWare ESXi 6.0 Support for vSensors and Stream

We are announcing 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.

X24 Appliance Support

As previously announced, the X24 appliance is End of Life, 6.17 was the last release to support the X24, and thus any X24 appliance will not upgrade to 6.18.

Bug Fixes

CS-5847: SentinelOne Host-ID Artifact Mismatch

This addresses a condition where some hosts which have SentinelOne integration may report the wrong Host-ID information when merging Hosts together. This has been addressed.

CS-5708: Host-ID not properly updated after new Static Address Added

When a new static address is added to the Static Address pool, Host-ID was not properly re-evaluating the existing assignments. This has been addressed.

CS-5932: vCenter Integration Removing Paired Sensors from Brain

Under some circumstances during network timeouts with vCenter integration is enabled, it may remove paired vSensors from the Brain even though this action was not performed by the user. This has been addressed.

CS-5593: SentinelOne Host-ID Artifacts Not Visible in UI

This addresses a condition where SentinelOne host artifacts may not show up in the UI under the Host Details page for hosts with Sentinel One enabled. This has been addressed.

CS-5750 Crowdstrike Host-ID Artfiacts Not Visible in UI

This addresses a condition where some hosts which have Crowdstrike integration may report the wrong Host-ID information when merging Hosts together. This has been addressed.

DS-3653: Proxy may impact C2 Detection

Under some complex circumstances where traffic is proxied, the presence of beaconing activity to popular destinations could prevent the presentation of concurrent C2 channels to the user. This has been addressed.

SEC-1488: OpenSSL Patched for CVE-2022-0778

This vulnerability has been patched in 6.17 for all Vectra Detect for Network platforms..

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.