Cognito® Platform Software Update

In January 2021, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.4.

The Version 6.4 release introduces support for ZScaler Private Access (ZPA), extended EDR identification and API access for Enhanced Notes. On the Recall side there is now a direct link to Recall form the Detect Dashboard for easier access, the addition of Beacon and SMB Activity in the Recall Host Dashboard, table views to see key information in Metadata Streams, and new saved search content for APT29 Solar Storm campaigns. Cognito® platform enhancements and bug fixes are also included in this release.

New Features

Support for ZScaler Private Access (ZPA) — Cognito Detect for Network

Cognito Detect can now ingest logs from ZScaler Private Access (ZPA), further extending the detection and response capabilities of the platform to remote workers. The logs, in conjunction with traffic analysis, allows Cognito to detect attacker behaviors that may be exhibited by attackers abusing user sessions of remote workers over ZPA. The surfaced detections will be attributed to the specific user who is logging in over ZPA and prioritized on Host page. To setup ZPA log ingestion, navigate to 'Settings->External Connectors' and enter the ZPA connector IPs and log forwarder IP into the Cognito UI. Details on how to setup log forwarding from ZScaler can be found here. Note that when ZPA accounts are observed authenticating for the first time Cognito will report a New Host info detection.

Enhanced Notes via v2.2 API — Cognito Detect for Network

The ability to create, read, update and delete Enhanced Notes is now available in the Detect API. The following methods are supported when working with Enhanced Notes via the v2.2 API:

- GET
- POST
- PATCH
- DELETE

Additional details and examples of working with the Enhanced Notes endpoints can be found here.

Extended EDR identification on Hosts page and Reporting — Cognito Detect for Network

Cognito Detect can now identify hosts running security agents based on network traffic behaviors associated with popular endpoint detection and response (EDR) security agents. The Host details page will now display EDR agent information, whenever available, even if the EDR has not been configured as an External Connector. The "What's on my network?" section of the Executive report has also been expanded to display hosts observed running EDR agents. The following EDR security agents are currently supported on both the Host page and in reporting:

- BitDefender
- Carbon Black
- CrowdStrike
- Cylance Endpoint
- FireEye
- FortiEDR
- McAfee
- McAfee ePO

- Microsoft Windows Defender
- Palo Alto Networks EDR
- SentinelOne
- Sophos
- Symantec
- Tanium
- Trend Micro

Direct Recall Link from your Dashboard — Cognito Recall

As we focus on making it easier to use our products, we've added a feature to help you jump to Recall in one simple click straight after logging into your Detect Brain. You should now see an "Investigate in Cognito Recall" link in the top right corner of the dashboard.

This link will take you directly into the iSession table view which will shows the most important fields in your iSession metadata stream/conn_log. You'll be able to quickly see IPs, hostnames, port used, and bytes sent & received, and quickly get to the information you need.

Beacon & SMB Activity in the Host Dashboard — Cognito Recall

The Recall Host Dashboard is the landing page when you pivot from Detect to Recall and offers a great in-depth insight into your Host. We have added 2 new tables to this Dashboard so that you can quickly zero in on noteworthy events quickly.

Beacons are a sequence of periodic sessions that can underpin the communication system present in Hidden HTTP and HTTPS tunnels use by attacker for command and control. We will now show any beacons we spot involving this host in a data table.

SMB activity can expose what files a host has been accessing, so you are quickly able to see what the scope of a compromise might be, or to see if any important files have been accessed by the host.

Table Views to see key information in Metadata Streams — Cognito Recall

Cognito Recall exposes a huge volume of valuable metadata, but some fields are only valuable in certain situations, while others are key information. So, we have created a “table view” for every Metadata Stream which will quickly show the key fields for a given metadata stream. By using these table views, you can very easily see key information in an uncluttered way.

You can access a table view by clicking “open” in the top right navbar of the Discover view in Recall, and then typing “Table View” and selecting the metadata stream you want to investigate. You can bookmark these pages to quickly access them in future.

New Saved Search Content — Cognito Recall

After the FireEye incident, Vectra's Security Research team immediately released 2 Custom Models designed to match the signatures seen in the APT29 Solar Storm Campaign, these have been active and monitoring your Recall instances from shortly after the announcement of this breach.

The searches are:

- Cognito TTP - iSession - APT29 Solar Storm Campaign C2 Domains

- Cognito TTP - iSession - APT29 Solar Storm Campaign C2 IP Addresses

We've deployed these custom models as enabled by default for all Cognito Recall Users as they track known bad IPs & Domains associated with the attack and should only generate high fidelity detections.

You can also use these models as saved searches in Recall to see if any historical activity matches these signatures by opening these saved searches in the discover view.

Detections — Cognito Detect for Network, Cognito Detect for Office365

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.

Hidden HTTPS Detection JA3 and JA3s Context

Hidden HTTPS tunnels are an effective way for an attacker to control a remote host. In order to help analysts with their investigations into active tunnels and to support information sharing between security organizations, the SSL/TLS client and server fingerprints known as the JA3 and JA3s hashes are reported with each alert. Team's can use this information to consult with external threat intel sources and identify other systems leveraging the same SSL/TLS stacks in other recall and stream. Both the JA3 and JA3s fields can be used to create triage rules.

Text Wrapping for Long Values on Detection Pages

Enhancements were made to multiple detection pages to allow for long values to appear on multiple lines instead of truncate. This change supports easier day-to-day interaction with detection page information.

Detection Deprecation

Attackers may attempt to create a rogue DC server to progress their attack. Historically, this behavior was covered in Cognito Detect by the Kerberos Server detection. In the recently released RPC Targeted Recon coverage for this type of attack was expanded. The Targeted RPC Recon monitors for anomalous usage of DC data replication commands that would allow an attacker to create a rogue DC server. Given the marked improvement of the Targeted RPC Recon approach the Kerberos Server detection was deprecated in the 6.2 release.

X24 Platform End-of-Life Notice

The X24 hardware platform will be EOL on 30th September 2021.

After the 30th September 2021, Vectra will no longer support:

- Software upgrades for X24 appliances.
- Software upgrades for brain appliances where an X24 sensor is paired.
- Hardware replacements for X24 appliances or their components.

Please contact your Vectra account team to discuss future options for replacing affected X24 hardware prior to the 30th September 2021 date.

Vectra Community

For more information on this product release, its features, best practices and more, please register for our Customer Community. You'll find product demos, feature videos and discussions with other Vectra users on the platform!

You can login or create an account on the Customer Community here.

Bug Fixes

CS-4556 – Advanced search not available due to indexing

Resolves issue where Advanced search may become unavailable due to Elasticsearch indexing.

CS-4615 – Alarm not sent correctly during system update

Resolves issue where hosts may cross scoring thresholds, but no notifications are sent from the system after the 6.3 update.

CS-4590 – Custom model filter not working correctly

Resolves issue where a Recall Custom Model may trigger a detection with hosts outside of the configured filter.

CS-4597 – O365 logs download does not honor proxy settings

Resolves issue where O365 logs cannot be downloaded due to timeout because the Proxy Config settings are not being honored.

CS-4589 – POC Report returns 500 error when selecting tags

Resolves issue where filtering on Host tags in the POC report may return a 500 error.

CS-4607 – Syslog test is broken with JSON output

Resolves issue where the syslog test button does not function properly when the JSON message output format is selected.

CS-4614 – Data Smuggler triggering detection on multicast address

Resolves issue where Data Smuggler detections may be triggered by multicast addresses.

CS-4629 – Data Smuggler: Duplicate Pull entries

Resolves issue where the Data Smuggler detection may show duplicated exfiltration events.

CS-4634 – Syslog event missing threat intel name

Resolves issue where the threat intel name show in UI is omitted from the corresponding syslog events for a Threat Intelligence Match detection.

CS-4575 – Unable to save passwords due to unsupported characters

Resolves issue where some integration passwords cannot be saved due to the use of unsupported Unicode or extended Ascii Unicode characters.

CS-4587 – Windows Event Log Ingestion “others” stat reporting incorrect value

Resolves issue where the “other” count for Windows Event Log Ingestion is reporting the total events instead of other events.

CS-4633 – AWS External Connector add credentials fails to save

Resolves issue where adding credentials to the AWS External Connector fails to save new settings.

CS-4633 – AWS External Connector add credentials fails to save

Resolves issue where adding credentials to the AWS External Connector fails to save new settings.

CS-4576 – Vsupport command “set ipmi_password” fails on Stream M29

Resolves issue where Vsupport “set ipmi_password” fails to complete on Stream M29 with “vsupport_api failed” error.

CS-4610 – SSO Integration gives 500 error upon login

Resolves issue where SSO user may receive 500 error when user’s original domain does not match the SAML redirection domain.

CS-4625 – Sensors lose interface setting on reboot

Resolves issue sensors may lose interface settings after reboot.

CS-4169 – REST API does not return health status timely

Resolves issue where responses from the /api/v2.1/health endpoint may be excessively delayed.