Cognito® platform software update

In December 2020, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.3.

The Version 6.3 release introduces an enhancement to host scoring based on detection profiles, contextual documentation links, role identification for hosts, proxy support for External Connectors and SASL basic authentication for Windows Event Log ingestion and Cognito Stream. On the detection front, there are enhancements to O365 Suspicious Sign-On Activity and the Hidden HTTP(S) Tunnel alerts. Cognito® platform enhancements and bug fixes are also included in this release.

New features

Enhancement to Host Scoring

COGNITO **DETECT**

How host threat and certainty are determined has been enhanced to better prioritize modern attackers and increase the efficiency of security teams. Vectra tracks individual hosts over long periods of time and attributes detections to any host that behaves suspiciously. An AI model of attacker behaviors is used to correlate the individual detections seen on a host and report its threat and certainty. In this release, the AI model has been enhanced to better prioritize true attacker progression and behavior.

Scores for host are now directly related to detection profile of the host. Detection Profiles map to priority quadrants in the following way:

Quadrant	Detection Profiles
Critical	External Adversary, Ransomware, Botnet, Worm
High	Insider Threat: Admin, Insider Threat: User
Medium	IT Services, Vulnerability Discovery
Low	Cloud Services, Potentially Unwanted Program, IT Discovery

Users can expect to see fewer benign hosts in the high and critical quadrants allowing truly malicious actors to be clearly prioritized. We encourage reviewing any procedures related to escalation to ensure that they consider both high and critical quadrant hosts.

In-App Documentation Links

COGNITO **DETECT**

Beginning in Release 6.3, Cognito Detect will include hyperlinks to supplementary documentation alongside common configurable elements in the UI. In-app documentation links may include one or more of the following:

- Support articles
- Demo videos
- External reference material

Please note that not all configurable elements have in-app links in Release 6.3. Additional links and content will be added with each subsequent release.

Role identification for Hosts

COGNITO **DETECT**

Hosts observed operating in a functional role such as a DNS server or database server will now be labeled with their respective roles on the Host page of the Cognito UI. Functional roles may include:

- DC server
- DNS server
- DHCP server
- Web server
- Print server
- Proxy server
- File server
- Database server

What's on my network?: Host Roles

COGNITO **DETECT**

With the addition of role information for hosts, Cognito Detect now includes a summary of host roles observed in the *What's on my network?* section of the Executive Report.

EDR External Connectors Use Proxy Setting

COGNITO **DETECT**

The External Connectors for CrowdStrike, Carbon Black and Microsoft Defender ATP now have the configuration option to honor the system proxy setting. To enable, select the "Use the configured proxy in Services" checkbox under each individual External Connector.

SASL for Windows Event Log Ingestion

COGNITO **DETECT**

Cognito Detect now supports the use of SASL/PLAIN (username and password) with Kafka for Windows Security Event Log ingestion. To enable this, navigate to Settings > External Connectors. There you can enable Windows Event Log Ingestion and choose SASL from the Authentication dropdown. Once filling out the username and password, choosing SSL as the protocol allows you to authenticate using SASL/PLAIN, removing the complexity of managing certificates.

SASL for Cognito Stream

COGNITO **STREAM**

Cognito Stream now supports the use of SASL/PLAIN (username and password) for Stream outbound via Kafka. To enable this, navigate to Settings > Cognito Stream. There clicking on edit allows you to choose SASL Plain as the authentication method. Once filling out the username and password, choosing SSL as the protocol allows you to authenticate using SASL/PLAIN, removing the complexity of managing certificates.

Flash EOL Dashboard

COGNITO **RECALL**

On January 1st, 2021, Flash will be officially marked as End of Life. This means that any new CVEs found in Flash will not be patched, and so Flash will quickly become even more of an attack surface for malicious actors than it is widely recognized as today.

Network metadata is an excellent tool in your arsenal to lockdown usage of flash, letting you find usage of Flash on your system, even where you were sure you had uninstalled it. To make it easier for you to track usage of Flash on your network, we have created the Flash EOL Dashboard. This data is pulled from unencrypted HTTP traffic exclusively, and so it is not an exhaustive list of Flash usage, but should help you find systems which are still hosting Flash content, and clients on your network which are running Flash.

New Cognito Recall Saved Searches

COGNITO **RECALL**

Vectra Security Research continued their efforts to help secure your networks by creating the following Cognito Recall Saved Searches. Using these Saved Searches, you can search for and find suspect or malicious behavior within your network using Cognito Recall. Additionally, these Saved Searches can be converted to Custom Models if you wish to be automatically alerted should these items appear on your network in the future.

New Saved Search Name	Description
Cognito TTP - HTTP - Potential Weblogic exploit CVE-2020-14882	This search is designed to catch the encoded Directory traversal and targeting of the Weblogic admin panel as seen in the RCE exploit.

Detections

COGNITO DETECT COGNITO DETECT for Office 365

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.

Detection Enhancement - O365 Suspicious Sign-On Activity

The O365 Suspicious Sign-On Activity detection alerts on the initial sign-on by an attacker to an infected account. This alert allows analysts to see when an attacker first gains access to an account so that they can stop the attacker before any progression occurs. This release expands the coverage and context of the alert to include and details related to geolocation, device type, and baselined history. Events are generated when anomalous sign-on related to unusual devices and geolocations are observed.

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.

O365 Download Logs Disabled

The download logs feature for O365 detections introduced in Release 6.2 has been disabled due to performance considerations. The functionality will be reenabled in a subsequent release.

Security updates

During an internal audit Vectra Engineering discovered some X29v2 and S101 systems were provisioned with the same equivalent set of SSH host identification keys. To improve security, Vectra has initiated SSH host key rotation for all such systems as part of the Version 6.3 software update. As a result of this change, when logging in to the Cognito Detect Brain as the "vectra" user via SSH, users may see a warning similar to the following. This warning is due to the rotation of the ssh keys.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:Oh/jCQM1/yCnd+7jeQdXxfv4p8RYX+yYy7gR9ieWr5Q.
Please contact your system administrator.
Add correct host key in /Users/jsmith/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/jsmith/.ssh/known_hosts:754
ECDSA host key for 192.168.50.18 has changed and you have requested strict checking.
Host key verification failed.
```

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-4477 - Custom triage filter rule "invalid values" error for Threat Intel match
Resolves issue where attempting to match on anything but <host>.domain format returns an error for "Match Domain is any of" additional condition when creating a custom triage filter for Vectra Threat Intelligence Match.

CS-4557 - Linked account errors
Resolves account linking and locking/unlocking errors related to the account linking feature introduced in release 6.2.

CS-4464 - Slow Accounts page graph after 6.2 upgrade
Resolves issue where the Accounts page graph is very slow to load after the 6.2 upgrade.

CS-4371 - Issue with report number totals
Resolves issue where "Detection Breakdown" count does not match the "Detections by Category" breakdown.

CS-4569 - Detection learning details repeated
Resolves issue Targeted RPC Recon detection shows duplicate hosts and network details.

CS-4549 – Account Links in Host Details broken
Resolves issue where links to the accounts seen on a host were not linking to the account page correctly.

CS-4544 - NTLM username not being extracted from some SMB transactions
Resolves issue where some NTLM usernames are not being extracted and placed in SMB Brute-Force detections, nor is metadata generated for the NTLM authentication request in SMB.

CS-4341 - Report filtering errors
Resolves issue with report filtering where a report cannot be created if Custom Model detection type is included and filtering by sensor does not impact output.

CS-4518 - External Connectors page does not load
Resolves issue where the External Connectors Settings page does not load due to AWS settings timeout.

CS-4499 – Incorrect offline update links
Resolves issue where Updater system may generate incomplete list of offline update download links for air gapped systems.