Cognito® platform software update

In November 2020, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.2.

The Version 6.2 release introduces a Unified view of Network & O365 accounts, a new Executive Report, support for CrowdStrike's EU and US Commercial 2 cloud environments, downloadable O365 logs, anonymization of sensitive data for O365, longer limited time share links, a number of new Detect for O365 detections and two new Security Insights. Cognito® platform enhancements and bug fixes are also included in this release.

New features

Link Your Network & O365 Accounts into a Unified View

COGNITO DETECT for Office 365

Compromising an account is a high value target for an attacker, whether on premise or in the cloud. Account Credentials offer an access point to progress deeper. Cognito Detect for O365 will allow you to track attack progression across the cloud and network, in 1 simple, unified, view of an account in Cognito.

It's clear from reviewing some recent attacks that attacker do not see the cloud network as even the slightest barrier in the progression of their attack. Attackers have been recently tracked beginning an attack by brute forcing weak credentials and then leveraged email rules to pivot to the endpoint. Once on the endpoint the credentials can be leveraged to move laterally and progress an attack. If your network & cloud detection portfolios are unlinked, then the scale of the attack can be completely missed.

With the 6.2 release, customers will be able to link accounts using a manual mapping system which will let them map their Cloud domains to their Kerberos realms. AD based automatic mapping is in progress for a future release.

Download the O365 Logs that Fired the Detection

COGNITO DETECT for Office 365

With the 6.2 release, we have exposed the raw log data which drove a detection to be fired within your detection page. Think of it as a PCAP for O365.

This log file will show you the context of the user's activity before the detection fired, and should save analysts from having to note the account involved, and the time range, pivot to a SIEM or another O365 log source, filter by the account, filter by the time range, and then see exactly what happened. Now it's just 1 click. The log file can be downloaded from all O365 detection pages created after the 6.2 release, and data within the log file will be anonymized unless you have specifically disabled anonymization.

Disable Anonymization in Detect for O365

COGNITO DETECT for Office 365

From Version 6.2, it will now be possible for customers to disable the anonymization of O365 data that is exposed through Cognito Detect. This will expose filenames and email content on detection pages and in the downloadable logs that is related to incidents. This information can speed the time it takes for analysts to investigate O365 alerts.

To disable anonymization, you will need to navigate to the Sensor Management page and untick “Anonymize sensitive data”.

Note that when “Anonymize sensitive data” is set to true, anonymized information will appear as Vectra-Anonymized:xxx. The anonymization results in a unique hash of the string value in the logs and is not a file hash.

New Executive Report: What’s on my Network?

COGNITO DETECT

Version 6.2 introduces the first of several reporting updates to come. This new executive-style report will focus on demonstrating system value by helping you answer the question “What’s on my network?” which will include:

- *Privileged Entities* report to quickly identify high-privilege admin or service accounts in your network.
- *Endpoint Coverage* report to find hosts with missing or disabled endpoint agents.
- *Devices by MAC OUI* report to discover new or rogue devices by MAC address vendor and the subnets where they’ve been observed.

CrowdStrike EU Cloud and US Commercial Cloud 2 support

COGNITO DETECT

Cognito Detect now provides support for two additional CrowdStrike cloud environments for External Connector integration:

- EU Cloud (https://api.eu-1.crowdstrike.com)
- US Commercial Cloud 2 (https://api.us-2.crowdstrike.com)

To determine which cloud environment your CrowdStrike External Connector integration should be using, please refer to the following table.

If you log into CrowdStrike Falcon via…	Select this URL when setting up your External Connector:
https://falcon.crowdstrike.com	api.crowdstrike.com
https://falcon.us-2.crowdstrike.com	api.us-2.crowdstrike.com

https://falcon.laggar.gcw.crowdstrike.com	api.laggar.gcw.crowdstrike.com
https://falcon.eu-1.crowdstrike.com	api.eu-1.crowdstrike.com

Share link maximum duration increased to 30 days

COGNITO **DETECT**

The maximum duration of limited time share links has been increased from 7 days up to 30 days. Share links are used for sharing detection pages between analysts. A list of shared links created by a user is available under the user's 'My Profile' page in Cognito Detect.

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 Emotet C2 Communication	Catches known Emotet C2 communications as of October 2020 based on a regex match.
Cognito – TTP – HTTP – Potential WordPress RCE Exploit	

User configured static hosts

COGNITO **DETECT**

Vectra users now have the ability to improve detection quality, host attribution and host context by directly inputting the IPs and CIDR blocks associated with static hosts in their environment. Configuring static hosts allows for better long-term baselining by Vectra's detections and the ability to better identify contextual information associated with a configured host. Static hosts can be added from the Settings page and will result in the creation of hosts with the naming convention of *Static-X.X.X.X*.

Additional syslog format support for Windows event log ingestion

COGNITO **DETECT**

Windows event log ingestion now supports ISC formatted syslog and JSON inside RFC 5424 syslog under the 'syslog' option. This allows for PAA detections and host id based

on Windows event logs in those formats. The previous 'SIEM' setting in the UI need not be used for Windows event log ingestion and existing customers utilizing it to send windows event logs can now send it to the new setting / port. The 'SIEM' setting can continue to be used for sending DHCP logs into Vectra. In release 6.3, the 'SIEM' setting will be renamed to 'DHCP Log ingestion'.

SAML 2.0-based Single Sign-On to Vectra Detect UI

COGNITO DETECT

Customers can now set up SSO federation to a SAML 2.0-based identity provider. In the 6.2 release, Vectra has validated Azure Active Directory, others will follow. Once federated, already authenticated users will get automatically logged in when they load the Vectra Detect URL. Unauthenticated users will get redirected to their identity provider's login portal. Features like password policies and multi-factor authentication will be enforced by the identity provider. Once authenticated, the user is assigned the Application Role defined in the identity provider, and mapping to a role (and permissions) defined on the Vectra Brain.

Note that API tokens can only be generated by local users, not SAML users.

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.

New Info Detection - New Host Role

The New Host Roles detection reports when Vectra observes a host operating in new functional role like that of a DNS server, DHCP server or database server. This alert is unscored and does not impact host or account scoring. Knowing when new functional roles comes online allows analysts to better understand their changing network environment. An event is generated whenever a host begins to show traffic indicators associated with a new functional role.

Note that a spike in New Host Role events may occur in the 6.2 release as roles are first identified.

New Info Detection - Novel Admin Protocol Usage

The Novel Admin Protocol Usage detection gives visibility into hosts using administrative protocols like SSH, RDP or WinRM for the first time. This alert is unscored and does not impact host or account scoring. While admin protocols are critical for normal business operations, understanding new usage gives analysts better situational awareness into what systems have direct access to other machines in the environment. New usage of admin protocols in an attack can also help provide context

into attacker's progression. Events are generated when an admin protocol that is rarely used by a host is used to connect to another machine.

Note that a spike in Novel Admin Protocol Usage events may occur soon after deployment while normal usage is identified.

New Info Detection - O365 Brute Force Attempt
The O365 Brute Force Attempt detection showcases accounts in the Azure AD and O365 environment that are being targeted for account takeover by an external attacker. This alert is unscored and does not impact host or account scoring. This alert allows for security teams to see early indicators of a concerted attack and take preventative actions that stop the attack from being successful. Events are generated when an excessive number of failures are observed connecting to one or more accounts from the same IP.

New Detection - O365 Suspicious Download Activity
The O365 Suspicious Download Activity detection reports when an account is seen downloading data an anomalous amount of data from SharePoint or OneDrive. Alerting on anomalous downloads allows for analysts to respond when compromised accounts or insider threats download data with malicious intent. Events are generated when an account is seen downloading an anomalous number of objects compared to the account's baseline or the baseline of other SharePoint and OneDrive users.

New Detection - O365 Login Attempt to Disabled Account
The O365 Login Attempt to a Disabled Account detection alerts when an IP tries to access a disabled account. Former employees with malicious intent may look to access old accounts to find if they still have access to valuable company resources. This alert gives analysts the opportunity to prevent any malicious actions by the former employee by ensuring that all previously accessible company resources and accounts are also no longer accessible.

New Detection - O365 Change to Trusted IP Configuration
The O365 Change to Trusted IP Configuration alerts when an account is seen making changes to the Trust IP configuration settings that impact where MFA and other conditional access policies are enforced. Attackers will look to modify the trusted IP space setting in order to allow themselves easier access to compromised accounts in the future.

New Detection - O365 MFA Disabled
The O365 MFA Disabled alerts when an account is seen disabling MFA for another account. Attackers will look to disabled MFA for accounts in order to allow themselves easier access to compromised accounts in the future.

New Detection - O365 Suspicious Exchange Transport Rule
The O365 Suspicious Exchange Transport Rule alerts when an account creates a new Exchange transport rule with a potentially risky set of parameters that may provide email collection, exfiltration, or deletion capabilities. Transport Rules are able to manipulate emails in transit to their destination making them more powerful than Inbox Rules which are only applied mail reaches an Inbox. Alerting on the creation of these rules by attackers or insider threats allows analysts to prevent potential data theft or data destruction by responding before the rules are ever run.

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 is 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.

Security updates
This release contains several software updates to harden the security of X-series appliances and S-series sensors.

Bug fixes
CS-4277 – Data Smuggler does not triage when destination is IP through proxy
Resolves issue where Data Smuggler detection does not triage correctly when destination IP is through proxy.

CS-4241 – Hosts containers created with generic IP name when artifacts available
Resolves issue where hosts may be created with generic IP address name even when host naming artifacts are available.

CS-4460 – Stream low throughput after 6.1 update
Resolves issue where Cognito Stream may experience low throughput after the 6.1 update.

CS-4314 – PAA infographic pins wrong item
Resolves issue where PAA infographic incorrectly highlights account when host is displaying the abnormality.

CS-4319 – Traffic notification for application in brain mode
Resolves issue where a system alert indicating "Not enough data available. Not enough traffic captured" may be sent when appliance is set to brain mode.

CS-4389 – "Check Settings" link results in a 500 Internal Server Error
Resolves issue when browsing to Settings > Services when there is no connectivity to the Vectra cloud, the "Check Settings" link results in a 500 Internal Server Error message.

CS-4446 – Host Severity Summary missing arrows
Resolves issue when the Host Severity Summary in the Security Dashboard does not display directional arrows next to host counts.

CS-4402 – Email alert has the wrong host information
Resolves issue where detection email alerts may reference incorrect hosts.

CS-4353 – IP address missing from CSV download on Network Stats page
Resolves issue where IP addresses from subnets lists on the Network Stats page may not show up in the "Download Current IPs (CS)" list.

CS-4376 – Custom models not alerting or generating detections
Resolves issue where custom models may trigger, but do not generate any subsequent detections or alerts.

CS-4485 – O365 Exfiltration Before Termination shows repeat admin action
Resolves issue where a single admin action in *O365 Exfiltration Before Termination* was shown multiple times.

SAAS-899 – O365 Exfiltration Before Termination wrong timestamp
Resolves issue where the timestamp of the admin action was incorrectly reported in the O365 Exfiltration Before Termination detection.

APP-12132 – Issue in O365 detection reporting
Resolves an issue where some O365 detections may not appear in the console.