Cognito® Platform Software Update

In March 2021, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.5.

The Version 6.5 release introduces support for linked network and Azure AD accounts, Kerberos Cipher encryption in Recall and Stream metadata, additional saved searches for C2 behaviors, new Data Gathering, and Novel External Destination Port detections, enhancements to the Hidden HTTPS Tunnel detection and changes to Azure AD detection names. Cognito® platform enhancements and bug fixes are also included in this release.

New Features

Linked Network & Azure AD Accounts — Cognito Detect for Network, Detect for Office365

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 6.5 release, customer will now see all network & O365 accounts will be linked automatically where both accounts have been seen by Vectra and their Active Directory Integration is enabled.

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

In release 6.4, EDR agent information was reported on the Host details page and reports, even if the EDR has not been configured as an External Connector. In this release, coverage for EDR agents has been expanded for cases where hosts communicate through a proxy.

Ticket Encryption Type in Kerberos Metadata — Cognito Stream, Cognito Recall

Kerberos ticket requests can be made and responded to using a variety of different cipher algorithms to encrypt the data. Weak encryption types allow for attackers to capture and then crack credentials offline during attacks like Kerberoasting. In this release we have added the request and response ciphers, as fields req_ciphers and rep_cipher, into the Kerberos metadata to allow for analysts to understand the usage of weak ciphers in the environment. This knowledge can help teams make changes to how Kerberos is used in the environment and better investigate events during network attacks.

Potential Kerberoasting Dashboard — Cognito Recall

Following on from the new Metadata fields we've added, req_ciphers and rep_cipher, we have created a dashboard in Cognito Recall which you can use to find potential cases of kerberoasting happening on your Network. This Dashboard is available now on your Recall instance in the Dashboards section.

New Recall Saved Searches — Cognito Recall

Vectra's Security Research team are constantly looking to reduce your risk of breach by releasing Custom Models for new and emerging threats. In release 6.5, we have released 5 new custom models. 4 Custom Models relate to the Nettitude Posh C2 framework, which is used by red teams and malicious actors to gain control in your network. Our other custom model will alert on potential uses of the recently announced Centreon Systems PAS Webshell CVE (Reference: CERTFR-2021-CTI-005).

The searches are:

- Cognito - TTP - x509 - Posh C2 default Certificate Values
- Cognito - TTP - SMB - Potential Posh C2 Fcomm implant file (*)
- Cognito - TTP - SMB - Default Posh C2 PBind Named Pipe
- Cognito - TTP - HTTP - Default Posh C2 HTTP Beacon
- Cognito - TTP - HTTP - Potential PAS WebShell targeting Centreon Systems

We've deployed these custom models as enabled by default for all Cognito Recall Users as they have been tested at scale and will generate high fidelity detections, the searches above marked with (*) may cause a high number of false positives on some systems, so we would encourage investigating this search and enabling it if you think it will be valuable in your organization. If you would not like to receive these notifications, you can disable them easily by navigating to "Manage" -> "Custom Models", search for a specific model and then deactivate it from the edit dialog.

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.

New Detection: Data Gathering

The final goal of many advanced attackers is to exfiltrate high value business data. Prior to data leaving a monitored system, data is often gathered from other internal systems. In this release, coverage has been added for this early exfiltration stage with a new alert, Data Gathering. This alert will identify when an internal host is observed collecting an anomalous amount of data from other internal systems. Beyond providing earlier coverage for attacker behaviors, this alert also ensures visibility for exfiltration to remote workers where the final data movement to the attacker infrastructure is not visible.

New Info Detection: Novel External Destination Port

Most software leverages a standard set of external ports to communicate to the internet. When new ports are observed this can indicate the installation of a new specialty software in the environment or in some cases communication from a compromised host. In this release, Vectra has added a new info level detection which reports when novel external connections are observed in the environment. Analysts can leverage this alert to better understand new software being used and to provide additional context around anomalous command and control channels. This detection is not scored and does not impact host scoring.

Coverage Enhancement: Hidden HTTPS Tunnel

Hidden HTTPS tunnels are an effective way for an attacker to control a remote host. Coverage for short session tunnels has been expanded to alert on more novel attacker frameworks and configurations. In this release, a new approach to identify tunnels has been introduced that is driven by the observation of active beacons with anomalous TLS infrastructure and target destinations. Tunnels events identified with this behavior will be reported with a triagable Tunnel Type value of, *Multiple short TCP sessions - Abnormal Beacon.* Most teams can expect an increase in the number of Hidden HTTPS tunnel alerts of this type in their system.

Context Enhancement: O365 Ransomware and O365 Malware Stage: Upload

Attackers with compromised O365 credentials may directly target SharePoint shares to spread or monetize their stolen credentials. In this release two Vectra detections related to SharePoint behaviors: O365 Ransomware and O365 Malware Stage: Upload; have been updated to report details of the filenames impacted in the event. Note that if Detect for O365 has been configured to anonymize data these files names will not be visible to analysts.

Context Enhancement: Renaming Azure AD Detections

Attackers that compromise Azure AD credentials have access to O365 as well as any federated application. Detections for behaviors that pertain to Azure AD have been renamed to make their impact beyond just O365 clearer and to better represent the identified behavior. This name change will not impact triage or existing syslog integrations. The renamed detections are as follows:

Previous Name	**New Name**
O365 Account Brute-Force	Azure AD Successful Brute-Force
O365 Admin Account Creation	Azure AD Admin Account Creation
O365 Brute Force Attempt	Azure AD Brute-Force Attempt
O365 Change to Trusted IP Configuration	Azure AD Change to Trusted IP Configuration
O365 Login Attempt to Disabled Account	Azure AD Login Attempt to Disabled Account
O365 MFA Disabled	Azure AD MFA Disabled
O365 Newly Created Admin Account	Azure AD Newly Created Admin Account
O365 Redundant Access Creation	Azure AD Redundant Access Creation
O365 Suspicious Application Permissions	Azure AD Suspicious OAuth Application
O365 Suspicious Azure AD Operation	Azure AD Suspicious Operation
O365 Suspicious Sign-On	Azure AD Suspicious Sign-On
O365 TOR Activity	Azure AD TOR Activity
O365 Unusual Scripting Engine Usage	Azure AD Unusual Scripting Engine Usage
O365 Account Manipulation	O365 Suspicious Mailbox Manipulation

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.

Bug Fixes

CS-4615 – Alarm not sent correctly during system update

Resolves issue where host scoring change notifications may not be sent by system if hosts cross alert thresholds during a system update.

CS-4713 – Windows Event Log Ingestions error on Raw TCP save

Resolves issue where users may be unable to save Windows Event Log Ingestion configuration when Raw TCP type is used.

CS-4681 – Enabling enhanced details may cause sending of syslog to stop

Resolves issue where enabling ‘include enhanced detail’ may cause the brain to stop sending syslogs.

CS-4613 – Lateral Movement: Error parsing account name with detection

Resolves issue where account name may not be properly parsed in some Lateral Movement detections.

CS-4682 – Triage cannot be done and download of pcaps unavailable

Resolves issue where a process memory bug may prevent the creation of triage filters or pcaps unavailable for download.

CS-4652 – Cannot triage unusual keyboard layout: Unknown - 3489727497

Resolves issue where Suspicious Remote Desktop detection cannot be triaged due to Unusual keyboard layout: Unknown – 3489727497.

CS-4734 – O365 accounts in active state without active detections

Resolves issue where an O365 account may show up as active, even when it has no active detections.

CS-4672 – Stream syslog publishing metadata with newline character

Resolves issue where Stream metadata may contain a valid newline that is published within a quoted attribute that may cause downstream parsing issues.

CS-4710 – Migration of legacy CrowdStrike credentials to OAuth2does not refresh URL dropdown

Resolves issue where clicking a CrowdStrike URL does not refresh the selection from the dropdown when attempting migrate legacy credentials to OAuth2.

CS-4639 – Full group members not show on Hosts page

Resolves issue where Hosts page only shows active hosts irrespective of group or status filters whenever Elastic is indexing.

CS-4711 – SIEM configuration not rendering correctly in UI

Resolves issue where the SIEM configuration may show a log source configured, but it cannot be edited.

CS-4691 – REST API “Encountered an error running health check”

Resolves issue where a call to the /api/v2.1/health endpoint may return an error stating “Encountered an error running health check“.

CS-4704 – Sorting sensor list by location value returns 500 error

Resolves issue where attempting to sort sensor list by location/region values results in a 500 error.