Cognito® 6.0 Release Notes

Cognito® platform software update

In August 2020, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.0.

The Version 6.0 release introduces general availability of Cognito Detect for O365, new Targeted RPC Recon detection, Security insights, and other UI and platform features. Cognito® platform enhancements and bug fixes are also included in this release.

Cognito Detect for O365

COGNITO DETECT for Office 365

Excited to announce the General availability (GA) of Cognito Detect for O365. Detect for O365 provides deep coverage for attacker behaviors in O365 across multiple applications in the O365 suite – teams, sharepoint, exchange, onedrive, Azure AD and Office365. The accounts and detections observed are surfaced in the Cognito UI, eliminating the need for multiple dashboards to track attackers across on-prem and SaaS environments. To try it for free, navigate to the “Settings->Cognito SaaS” page in the Cognito UI and click on the “Free Trial” button. Details on how to self-onboard into the trial can be found here.

Security Insights

COGNITO DETECT

Security Insights are a new class of detections within the Cognito Detect portfolio. New and unusual events frequently occur in network environments. Independently these events do not indicate a clear security threat that should be prioritized for investigation for analysts. But being aware of new and unusual network events can provide additional context and support a deeper understanding of environment and lead to faster response to security events and better network management.

The new security insight detections are classified in the info category of detections and can be accessed from drop downs on the Detections Page and on individual Host pages. These detections are unscored and will not contribute to host scoring.

New Host

This Security Insight allows for greater visibility into when new hosts are entering the environment. An event will be generated for when artifacts for new hosts are identified.

Novel Mac Vendor

This Security Insight allows for greater visibility into when new types of hosts are enter the environment. An event is generated when a rarely see MAC vendor is observed entering the environment.

New features

Enhanced Notes

COGNITO DETECT

Version 6.0 introduces enhanced notes on hosts, detections and accounts page. The note now allows for formatting, markdown, hyper link and adding bullet points. This makes it easier for security analysts to add formatted text and external links as a part of investigations. Further, multiple notes can be added to any host, detection or account object. This allows for collaboration between analysts and chronological tracking of the investigation.

CrowdStrike OAuth2 Support

COGNITO DETECT

Version 6.0 adds support for OAuth2 authentication for the CrowdStrike integration. Both authentication methods (existing legacy and OAuth2) are supported starting 6.0, but the legacy authentication will be deprecated after October by CrowdStrike and thus by Vectra as well. The OAuth2 authentication will require a client id and a client secret from a new API client you create in the CrowdStrike Falcon UI. For more information on on obtaining your OAuth2 credentials or the credential migration process, please see the CrowdStrike OAuth2 Migration FAQ page on the Vectra support portal: https://support.vectranetworks.com/hc/en-us/articles/360052718994-CrowdStrike-OAuth2-Migration-FAQ

Enhanced details for detection syslog and kafka output

COGNITO DETECT

Syslog and kafka output for detections now have the option to include additional details about the events. This allows security teams consuming the alerts in their SIEM to have more context about the alerts thus reducing the need to pivot back to the Cognito UI for it. Please refer to the syslog reference guide for the description of the details for the detections. The additional details can be enabled by enabling ‘Include enhanced detail’ for the syslog or kafka setting.

Windows event log ingestion over syslog

COGNITO DETECT

Windows event log ingestion for driving Privileged Access Analytics (PAA) and host id has been extended to syslog format over TCP. Syslog formats supported are snare and RFC 5424. This enables additional SIEMs and agents which support syslog format to send windows event logs to Cognito UI.

Support for 10, 25 and 100G Interfaces for S101 sensor

S101 sensor is the largest physical sensor in the Cognito family with the ability to ingest up to 40 Gbps of sustained traffic. This now supports 2x10, 2x25 or 2x100 interfaces in lieu of 2x40 on the capture ports providing flexibility of deployment options. Customers desiring this can contact their local sales team to discuss their requirements for capturing traffic.

Certificate Expiry Dashboard

COGNITO RECALL

Cognito Recall tracks all certificates by extracting metadata from all network traffic.

We want to help you avoid that dreaded support ticket asking if your site has been hacked, with a confused customer worrying about the legitimacy of your site as their browser warns that your website is unsafe and to get “Back to safety.” Certificate outages can have a substantial business impact, so we've created a dashboard in Cognito Recall that shows you certificates in your network that are actively in use and are about to expire.

By focusing on the certificates that are being used you won’t ever need to worry about wasting time on old certificates that no one is accessing – only the key certificates that are used daily. This should enable you to deliver tangible value to network administrators by alerting them if widely used key certificates in your organization will expire soon and helping to prevent easily avoidable outages.

This dashboard is available by pivoting to Cognito Recall and clicking on “Certificate Expiry Dashboard”. By default, results are limited to external facing certificates, but this can easily be toggled to show internal certificates as well.

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 Suspicious Admin

Administrative accounts provide access to critical resources in the environment. These accounts are highly valuable to external and internal threats as they allow attackers to move laterally through the network to access high value resources. In this release we have enhanced the capabilities of the Suspicious Admin detection to provide better coverage for when SSH and RDP admin credentials are abused to move laterally in the network. The updated algorithm increases detection coverage for local credential abuse by insider threats and external actors.

RPC Targeted Recon detection

In this release we are releasing the Targeted RPC Recon detection. This detection enhances Vectra's detection capabilities for early stage targeted reconnaissance of another host or of the DC. The RPC commands support a wide range of operations that can allow for an attacker to gain access to information about the environment including details about who owns a host, what information resides on a host, what permissions a host has and what shares are available. Specific function calls are often leveraged when attackers want to dump credentials and escalate their privilege in the network. The new Vectra detection learns baselines for what clients and servers normally do in the network related to reconnaissance like RPC function calls and then alerts when anomalous calls are made by a host.

O365 Suspicious Sharing

Unauthorized sharing of large volume or breadth of files or folders may indicate that the organization is at increased risk of data theft or data loss, through either unintentional misconfiguration or intentionally malicious activities. Use of sharing enables attackers to maintain access to data after a compromised account is remediated. This detection looks for users sharing files and/or folders at a volume that is higher than is normal for both the environment and for the account.

O365 External Teams Access

Attackers may use a compromised account to add an external account to be a member of an existing O365 Teams account. This type of access enables an attacker to perform additional discovery or collection activities by exposing sensitive business information which may include shared files, meeting content, or chat transcripts without needing to use the internal account. This detection was designed to alert when suspicious external accounts are added to an environment.

O365 Suspicious Teams Application

Attackers may trick users into installing applications into Teams environments which may undermine existing security controls, such as multi-factor authentication (MFA), and enable malicious action on behalf of the authorizing user, increasing risk to enterprise system and data and increasing the likelihood of further attack progression. This detection was designed to alert when new applications are authorized within Teams which have high risk permissions.

O365 Newly Created Admin Account

Attackers will look to create fallback account after they gain a foothold in an O365 tenant in order to ensure continued access if their initial access is discovered and they are locked out. This detection was designed to alert on new accounts that have been designated as an admin.

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

Updated Terms of Service
Vectra has updated our standard Terms of Service, which can be found at https://www.vectra.ai/legal/terms-of-service. Please direct any questions or concerns to legal@vectra.ai.

Bug fixes
CS-4286 – Windows event log ingestion over xml from nxlog has errors
Fixed xml support for windows event logs to account for subtle changes in what nxlog sends out.

APP-11575 – Warning if password is blank / not entered for LDAP config
Added additional warnings when password is blank or not entered in the LDAP configuration. This prevents invalid configurations and surfaces such errors in the UI

CS-4236 – Account lockdown throws 500 error
LDAP CNs that contained commas and parentheses would cause an error when a user attempted to disable the account.

CS-4166 – vsupport restore list failing, getting auth failures
Fixed a scenario where the "vsupport restore brain" command may not include the backups received from another brain

CS-4260 – Offline updates has multiple entries
Fixed an edge case where offline update links may not have been generated properly

CS-4264 – Audit message syslog is not sent
Addresses an issue where audit notifications may not be forwarded to the syslog or Kafka destination when the “enhanced detail” option was selected