Cognito® Platform Software Update

In June 2021, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.8.

The Version 6.8 release introduces a new native integration for Cybereason endpoint, enhancements to the Assignment workflow and an update to the Data Staging detection. Cognito® platform enhancements and bug fixes are also included in this release.

New Features

Cybereason EDR Support — Cognito Detect for Network

Release 6.8 introduces native integration support for Cybereason Endpoint. This includes improved host identification via Cybereason host artifacts such as OS version, mac address, hostname, last seen timestamp, containment state, patch level, EDR id, and IP address. This integration also includes native support for Host Lockdown of Cybereason's Endpoint hosts. Analysts can one-click pivot directly from Detect host pages to Cybereason Endpoint host pages for seamless investigation of hosts activity. Cybereason Endpoint settings can be found in Detect under Settings > EDR integrations. Host Lockdown is now a global setting and is configured under Settings > EDR Integrations > Host Lockdown.

Assignment Workflow Enhancement — Cognito Detect for Network

The Cognito platform will now have the ability to resolve assignments with an outcome. This means that members of the organization can now label investigations with their outcomes allowing for the ability to gain better visibility into the events occurring in their network. By default, the outcomes will be defined as Malicious True Positive, Benign True Positive, and False Positive. Malicious True Positive events are those who were judged to be potentially dangerous and were investigated to be dangerous. Benign True Positive events are those that were judged were to be dangerous, but the behavior was allowed. Finally, False Positive are events which were misidentified. More outcomes can be added via API support.

These resolutions will be used for reporting purposes which will come out in a later release. Using the Enhanced Assignment Workflow will allow for the collection of various high-level metrics which can be used to judge how well the organization is performing. This enhancement will no longer support assignments for detections from the detection page. If you are using assignments on detections, you will now have to make the assignment on the entity which will assign all the detections within it to you. However, investigations will now have to be closed with a resolution on an entity level.

Pingback Malware Custom Model — 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 6.8, Pingback Malware Search has been deployed to aid in the investigation and possible alerting of use of the Pingback Malware. The search is:

- Cognito – TTP iSession – ICMP Pingback Malware

This Malware has been seen used in recent breaches as part of a Command and Control suite of tools. It uses set commands in the ICMP data section as part of the communication. The search looks for these commands using the First 16 Bytes of the ICMP Data in Recall.

Detections

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: Data Gathering — Cognito Detect for Network

Attackers looking to exfiltrate data may first collect and stage that data on an internal machine. The Data Gathering detection can identify this behavior enabling analysts visibility into data collection prior to exfiltration. In this release the Data Gathering algorithm has been enhanced to better recognize benign gathering behavior associated with multiple machines gathering data from the same systems during events like software updates. This change will result in a decrease in benign detection volumes for all environments.

Bug Fixes

CS-4756: Fixed issue to support special characters in AD Connector

CS-4726: Included support for Crowdstrike in EDR counts in reports

CS-4780: Fixed Crowdstrike integration to not produce 500 errors when there are more than 10000 hosts