Cognito Detect™ 4.4 Release Notes

X-series platform and S-series sensors software update

In August 2018, the Vectra® X-series appliances and S-series sensors were updated to Cognito Detect software release Version 4.4.

Cognito Detect software release Version 4.4 introduces host ID and navbar improvements, password rotation for local users, and improved HTTPS/HTTP tunnel and brute force detections.

Detections

Vectra constantly evaluates detection algorithm coverage and efficacy using opt-in metadata and direct user feedback. This feedback drives targeted enhancements in our algorithms and we encourage your continued feedback via the user community.

In this release, Vectra continues its focus on advanced attacker behaviors with several major detection enhancements in the command-and-control (C&C) and exfiltration categories.

Detection enhancement: Hidden HTTPS tunnel C&C and exfiltration

The hidden HTTPS tunnel detections have been enhanced by adding detection coverage for tunnels that consist of a single long TCP session. This coverage enhancement represents the expanded use of Deep Learning algorithms within Cognito Detect.

Additionally, hidden HTTPS tunnel detections now provide context on the type of tunnel that was observed. Possible tunnel types may include a single, long text-based session (for a shell type interaction), a single, long graphical session (for an RDP or VNC type interaction), or multiple short session. Customers should expect to see a slight increase in hidden HTTPS tunnel detections because of the coverage enhancement.

Detection enhancement: Hidden HTTP tunnel C&C and exfiltration

The efficacy of the hidden HTTP tunnel detection has been improved by suppressing detection events on single domains where DNS requests resolve to multiple IP addresses.

Single domains with IP clusters are highly unlikely to be part of an attacker's infrastructure. Coverage for the detection algorithm has been enhanced by relaxing duration requirements for the tunnel activity. Customers should expect a net decrease in the amount of hidden HTTP tunnel detections because of the enhancements.

Detection enhancement: Brute-force attack

The coverage of the brute-force attack algorithm has been enhanced. The algorithm now inspects traffic on the FTP, MongoDB and Telnet protocols. Negligible increases in detection counts are expected at most customer sites.

New features

Password rotation for local users

Cognito Detect administrators can now configure a password expiration time for UI users. Once the timer expires, an email notification is sent to the user, who will be required to change the Detect UI password. Password rotation is a general security best-practice and is mandated by compliance standards, such as PCI.

Platform enhancements

Notification emails

Improved descriptive text in the subject and body portions of notification emails for host and detection assignment/unassignment, alerts, key asset target/activity, and password expiration/changes.

Host ID improvements

Periodic query of host rDNS for a given IP address based on TTL now maintains an up-to-date IP:rDNS mapping when a host DNS change occurs.

Static navbar

Cognito Detect users can statically expand or collapse the left-side navigation bar and have the preferred state persist during the user session.

Modified timestamp added to REST APIs

Added note_modified_timestamp and note_modified_by to host, detection, campaign, and search REST APIs. This allows searching for note modifications on hosts, detections, and campaigns via the note_modified_timestamp_gte parameter.

Security updates

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

Bug fixes

CS-2416 – First and last seen times for Hosts incorrect in Campaigns

The Campaign page in the UI was showing an incorrect first-seen timestamp for Hosts.

CS-2373 – Hosts renamed in Cognito Detect not showing up in Cognito Recall searches

This addresses an issue where Named Hosts that have been renamed in Cognito Detect are not showing up in Cognito Recall searches.

CS-2410 – Incorrect permissions check

The Managed Proxies page in the UI was preventing users without View Traffic permissions to view proxies.

CS-2370 – Test email delay

The test email under the Settings page may take too long to timeout and display a failure message.

APP-6618 – Inactive hosts* and *detections missing Cognito Recall link
This addresses an issue in Cognito Detect where inactive hosts and detections are missing links to Cognito Recall.

CS-2384 – Carbon Black links on the Hosts page ignore custom port setting
Carbon Black links on the Hosts page redirect to Port 443, even when a custom port is defined.

PLAT-3904 – IEEE data reaching out to external IPs
This addresses an issue where a Cognito Detect system process was reaching out to external IP addresses.

CS-2433 – Triage filter CSV limitation
This fixes an issue where pasting a CSV list of IP addresses into a triage filter results in the input being truncated.