Cognito Detect™ 4.5 Release Notes

X-series appliances and S-series sensors software update

In September 2018, the Vectra® X-series appliances and S-series sensors were updated to Cognito Detect™ software release Version 4.5.

Cognito Detect software release Version 4.5 introduces TACACS+ authentication to externally authenticate users to the web UI and easily view assignments on *Hosts* and *Detections* pages using basic filtering and the improved *Hidden DNS Tunnel* detection. Cognito® platform enhancements and bug fixes are also included.

New features

TACACS+ authentication

Cognito Detect now supports TACACS+ for external user authentication. Customers can now create users in Cognito that authenticate against external TACACS+ servers, such as Cisco ACS or Windows TACACS+ server. TACACS+ authentication supports both PAP and CHAP authentication protocols.

Customers can create a TACACS+ authentication profile and assign it to a user. Roles must still be defined locally in the Cognito settings and assigned locally to users by the administrator. Once set up, users can log-in to Cognito using their corporate credentials.

Assignments basic filtering

Users can now see assignments on *Hosts* and *Detections* pages. The basic search bar on both pages now includes the ability to filter host and detection results by assigned user and see aggregate assignment counts for each. This makes it very easy for users to view hosts or detections assigned to them and also to identify unassigned hosts and 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 a new detection enhancement in the command-and-control (C&C) category.

Detection enhancement: Hidden DNS tunnel C&C

The coverage of the *Hidden DNS Tunnel* detection has been significantly enhanced by leveraging a new multicomponent model that looks at a variety of factors related to DNS session lookups, including:

- TTL
- Name size
- Interaction and data rate
- Structure of the names in a sequence
- Unusual use of record types

Since the coverage for tunneling behaviors has increased, customers should expect the volume of detection events to increase as well. Customers may see *DNS Tunnel C2* detections against domains like *sophosxl.com* and *E5.sk*, which leverage the DNS protocol to send data and fetch instructions. Behaviorally, these interactions are similar to malicious C&C traffic over the DNS protocol. If such services are sanctioned, Vectra recommends using triage filters to suppress detections against these events.

Platform enhancements

Inside/outside network configuration
The settings to configure inside (trusted) or outside (untrusted) the network have been enhanced. There is no implicit assumption of RFC 1918 addresses always being the inside the network. Customers can define the inside of their network using a combination of RFC 1918 addresses and addresses from the public IP address space. The new setting also allows for exclusion of IPs to allow for granular definition.

Report on failed backup rotation
A notification is now written to audit logs whenever backup file rotations have failed, allowing admins to act if a failure occurs.

Security updates

This release contains several software updates to harden the security of X-series appliances and S-series sensors. This release requires an update to the system kernel in order to apply recent security fixes and to provide logging improvements. **Please note that this update will trigger a system reboot that may result in downtime for up to a half hour.**

Deprecated feature

Removal of GeoIP feeds
GeoIP feeds are being deprecated in Cognito Detect. New detection events that contain external destinations where clicking the IP or domain for geographic context will no longer render a map in the context overlay window. Previous detection events with geographic data will continue to render a map in the context overlay window.

Below spec vSensors unsupported in future release
As outlined in the *Campus Sensor Installation Guide*, Vectra vSensors require the CPU of the ESX host to be one of the following:

- Intel Silvermont processors
- Intel Goldmont processors
- Intel Nehalem processors and newer
- Intel Haswell processors and newer
- AMD Barcelona-based processors and newer AMD Bulldozer-based processors and newer AMD Bobcat-based processors
- AMD Jaguar-based processors and newer AMD Piledriver-based processors and newer

Failure to meet the minimum vSensor CPU requirements will result in the loss of ability to upgrade vSensors to future versions of Cognito Detect. **Please ensure that the ESX hosts on which virtual sensors are deployed meet the above requirements.** Further information can be found in the *Campus Sensor Installation Guide* located under the *Resources* tab in Cognito Detect. Please contact Vectra support for additional assistance.

Bug fixes

CS-2353 – "Bandwidth drop" alerts for sensors
This addresses an issue where very low traffic levels may trigger sensor fault emails.

CS-2400 – Brute Force detections missing PCAP and mislabeled
Brute Force detections on UDP Port 427 were mislabeled and missing PCAPs.

CS-2434 – Bad values shown on "detections" curve
Addressed an issue where data values in tooltip did not match the cursor position on the detections curve.

CS-2435 – Change help text for set interface to remove "mode" prompt
Removal of superfluous word "mode" in "set interface" CLI command help text.

CS-2448 – No autofocus on Notes

This addresses a UI issue where the *Notes* entry box is not autofocused, requiring users to perform an extra click when entering notes on a host/detection page.

CS-2466 – Badly formatted header on Bandwidth Drop email alert
Corrects incorrectly formatted email text for *Bandwidth Drop* alerts.

CS-2474 – SQL injection XFF triage ambiguity
Updated SQL injection detection to make triaging XFF Host clearer. The address (IP address or FQDN) shown under recent activity for *X-Forwarded-For* value should be used for triage of XFF Host.

CS-2498 – Vcli local restore does not restore PCAPs
Corrects issue of missing PCAPs after a brain-to-brain restore via vcli.

APP-6731 – Negative detection counts in PDF reports
Corrects an issue where the *Detections Breakdown* PDF report may show negative numbers for the *"Threat Detections"* count.