Cognito® Platform Software Update

In March 2022, the Vectra® X-series appliances, B-series appliances, S-series sensors, Cloud Brain, and Cloud Sensors, will be updated to Cognito® software release Version 6.17

The Version 6.17 release introduces AI-Triage, AI-Triage support for C2/Exfil Detections, and Recall IPv6 Support.

Cognito® platform enhancements and bug fixes are also included in this release.

Release Schedule

6.17 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on 3/30/22.
    - You can check if you have remote support enabled under Settings -> Services with Remote Support set to Enabled.
- **Customers Connected to Updater**: Customers who do not have remote support enabled but are connected to Updater will receive updates on 4/4/22
    - You can check if you are connected to Updater under Settings->Services and see that Updater Destination shows as connected, while Remote Support shows disabled.
- **All Other Customers***: Will be able to download the update on 4/6/22.
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

AI-Triage

Cognito Detect for Network

Starting in 6.17, Vectra has introduced AI-Triage. AI-Triage helps Security Analysts focus on the most important threats by identifying benign detections that are likely to be caused by traditional infrastructure and applications and automatically creating Triage rules for these detections so that they are not prioritized within the system.

In 6.17, for existing deployments, AI-Triage can be manually enabled by going to Settings -> AI-Triage -> AI Triage Enable. AI-Triage will be enabled by default for new deployments. For more information please see our Knowledge Base articles: KB Article: https://support.vectra.ai/s/article/KB-VS-1582

AI-Triage C2/Exfil Support

Cognito Detect for Network

Starting in 6.17, AI-Triage will support automatically creating rules for benign activity that is detected as C2/Exfil when AI-Triage is enabled. This system works by profiling the detections in the system to identify non-malicious C2/Exfil detections and create Triage rules automatically so these detections will not be prioritized by the system.

There is no user configuration required for this capability, if AI-Triage is enabled, which can be performed under Settings -> AI-Triage -> AI Triage Enable.

Recall IPv6 Support

Cognito Recall

Starting in 6.17, Vectra will officially support IPv6 for Cognito Recall. If IPv6 traffic is observed on the network, its metadata will be recorded to Recall, just like IPv4.

There is no action required for the user to enable this capability, and all logs maintain the same indexes and fields for IPv6 as IPv4. Note that IPv6 metadata logging is already supported in Cognito Stream, and there will be no changes to Stream as part of this feature release.

© 2022 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

Note: At this time, Recall IPv6 supports all of the Recall functionality supported for IPv4, with the exception of IPv6 Beacons and Custom Models which are not supported at this time.

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.

Enhanced Time-to-Report — Cognito Detect for O365

The underlying detection engine that generates Detect for O365 alerts has been enhanced. Ten high-impact Azure AD and M365 detections will now be run in a new streaming framework that enables reporting soon after Vectra receives and processes the relevant logs. This change is part of a greater effort to enhance the time-to-report of the Detect for Azure AD and M365 detection portfolio.

The ten Azure AD and M365 detections running in the streaming framework are:

Azure AD Detections	M365 Detections
Azure AD MFA Disabled	O365 eDiscovery Exfil
Azure AD TOR Activity	O365 Suspicious Exchange Transport Rule
Azure AD Redundant Access Creation	O365 Suspicious Mail Forwarding
Azure AD Login Attempt to Disabled Account	O365 Power Automate HTTP Flow Creation
	O365 Attacker Tool: Ruler
	O365 Risky Exchange Operation

New Detection: Azure AD Suspected Compromised Access — Cognito Detect for O365

The new Azure AD Suspected Compromised Access detection identifies when an attacker has successfully gained control of an Azure AD account and starts accessing internal resources. This detection is similar to Vectra’s existing Azure AD Suspicious Sign-on detection but is focused on the access events that have the highest alignment with attacker access events and warrant immediate prioritization absent seeing other behaviors. This detection uses a machine-learning algorithm that tracks 20+ different aspects of sign-in events relative to a long-running baseline to identify potential attacker access events. The high confidence focus of this alert means customers can expect to see one or zero alerts in a given month.

Bug Fixes

CS-5728: Detections Missing in UI

This addresses a rare condition when detections will be sent via Syslog/Email but will not be visible in the Cognito UI. This has been resolved.

CS-5894: GCP vSensor Performance Limited

© 2022 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.

This addresses a performance issue in the GCP vSensor that limited its performance below the specified rate. This has been resolved.

CS-5846: Advanced Search Timing Out

This addresses an issue where the Advanced Search may not complete and result in a time out message displayed in the UI. This has been resolved.

CS-5497 Dhost Field is Blank

This addresses an issue where after 6.1, the dhost field is blank when a proxy is present in the detection rather than containing the IP of the destination. This is because the dhost field is used for DNS names, not IP addresses. As a result a new field called proxied_dst has been created to include the IP address of the proxy (in the extended syslog).

CS-5710 Wrong Direction for Suspicious Remote Desktop

This addresses a scenario where the Suspicious Remote Desktop may infer the wrong client to server direction in the detection details. This has been resolved.

CS-5837 Unable to enable Stream after reboot

This addresses a scenario when Stream cannot be enabled or disabled in the UI after a reboot. This has been addressed. This has been resolved.

Appendix:

Will this upgrade perform a reboot of the Brain or Sensors?

This update will not perform any reboot of the Brain or Sensor appliances, nor is any user interaction required.

© 2022 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, Cognito and Security that thinks are registered trademarks and Cognito Detect, Cognito Recall, Cognito Stream, the Vectra Threat Labs and the Threat Certainty Index are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders.