Cognito® Platform Software Update

In April 2021, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.7.

The Version 6.7 release introduces two new O365 and Azure AD detections, enhancements to multiple existing O365 and Azure AD detections and a new native integration for SentinelOne endpoint. Cognito® platform enhancements and bug fixes are also included in this release.

New Features

SentinelOne Endpoint Integration — Cognito Detect for Network

Release 6.7 introduces native integration support for SentinelOne Endpoint. This includes improved host identification via SentinelOne 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 SentinelOne Endpoint hosts. Analysts can one-click pivot directly from Detect host pages to SentinelOne Endpoint host pages for seamless investigation of hosts activity. SentinelOne 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.

Enhancement to EDR Identification — Cognito Detect for Network

The service that automatically identifies endpoint protection agents running on hosts has been enhanced to identify CISCO AMP agents. Hosts which were previously reported as having Windows Defender ATP present will now be reported as having Windows Defender present, referencing both Defender ATP and Defender AV.

Traffic Parsing of SGT Headers — Cognito Detect for Network

Traffic parsing has been enhanced to support parsing for traffic with Cisco Security Group Tag headers.

Assignments on Detection Deprecation — Cognito Detect for Network

In future release 6.8, Cognito Detect will no longer support assignments for detections from the detection page. This change is to support a planned enhancement to the analyst workflow in an upcoming release. In release 6.8, an analyst or manager can assign a host to an analyst. This will assign all the detections under the host to the analyst.

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.

New Detection: Azure AD Privilege Operation Anomaly — Cognito Detect for O365

Vectra is releasing a new Azure AD detection to detect when privilege accounts are abused in the Azure AD environment by either external attackers or insider threats. Provisioning accounts with the proper permissions remains a challenge for security teams. This is why Vectra developed a way to automatically identify the lowest privilege needed by an account in an environment to perform its job by passively observing the behavior of the account. This approach allows Vectra to detect when granted privileges are abused beyond what has been seen in

the past. The new Azure AD Privilege Operation Anomaly model protects against attacker actions on the Azure AD backend and alerts on advanced attacker tactics that span lateral movement, persistence, defensive evasion and impact. Alerts trigger on the anomalous usage of privilege operations like setting federated trusts, modifying certificates or changing application permissions.

New Detection: O365 Suspicious Compliance Search — Cognito Detect for O365

Vectra is releasing a new O365 detection to detect when an attacker abuses native O365 compliance search technology to search exchange data in the O365 environment. Teams will be alerted on scenarios like attackers using compliance search to survey exchange conversations to find if they have been found by defenders or attackers using compliance search looking to find valuable data for exfiltration. Alerts trigger when compliance search functionality is used by an account that does not normally use this functionality.

Multiple O365 and Azure AD Detection Enhancements — Cognito Detect for O365

Vectra is releasing enhancements to several O365 and Azure AD that increase their coverage for different ways attackers are abusing stolen accounts. These enhancements impact Azure AD Unusual Scripting Engine Usage, Azure AD Redundant Access Creation, O365 Suspicious Mail Forwarding, Azure AD TOR Activity, Azure AD Successful Brute-Force, Azure AD Brute-Force Attempt, O365 Unusual eDiscovery Search.

X24 Platform End-of-Life Notice

The X24 hardware platform will be EOL on 30th September 2021.

After the 30th September 2021, Vectra will no longer support:

- Software upgrades for X24 appliances.
- Software upgrades for brain appliances where an X24 sensor is paired.
- Hardware replacements for X24 appliances or their components.

Please contact your Vectra account team to discuss future options for replacing affected X24 hardware prior to the 30th September 2021 date.

Bug Fixes

CS-4865: Addresses an issue that impacted the ability modifying VPN connectivity

CS-4818: Addresses an issue that impacted the ability to collect sensor topology information

CS-4811: Addresses an issue that impacted the ability to search on AD context

CS-4794: Addresses an issue that impacted the ability to view SAML profiles