Vectra Detect Platform Software Update

The Vectra® X-series appliances, B-series appliances, S-series sensors, VM and Cloud Brain, VM and Cloud Sensors, are scheduled to be updated to Vectra Detect for Network software release version 7.5

The Version 7.5 release introduces support for Detect for AWS, a new Suspicious Active Directory Operations detection and faster detection reporting for some M365 and Azure AD detections.

Vectra Detect platform enhancements and bug fixes are also included in this release.

Please note that starting with the 7.5 release the Vectra Brain will connect to the Vectra cloud for remote support services using a DNS name instead of IP address.

Prior to the 7.5 release	After the 7.5 release
The Vectra Brain creates an outbound connection to destination 74.201.86.229 (TCP/443 or UDP/9970) for Remote Support services.	The Vectra Brain creates an outbound connection to rs.vectranetworks.com* (TCP/443 or UDP/9970) for Remote Support services.
* The rs.vectranetworks.com DNS name will continue to resolve to the 74.201.86.229 IP address. Please see Firewall requirements for Vectra appliances for additional information.	

Release Schedule

7.5 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after March 1st, 2023
  - 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 or after March 8th, 2023
  - 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 or after March 8th, 2023
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Detect for AWS in Vectra Brain UI

Vectra Detect for AWS

Starting this release, you can provision the ingestion of AWS CloudTrail logs into the Vectra cloud, from the Vectra Brain UI. This workflow is identical to the existing workflow for Azure AD and Office 365. Following this, Vectra will analyze your AWS control plane activity for threats, and you will see scored accounts and detections in the Brain UI. With this feature, your SOC can analyze threats in the network, Azure AD, Microsoft 365, and AWS, all in one place.

New MDR User and Role — Vectra Managed Detection and Response

Vectra MDR customers will see a new vectra_mdr user and a Vectra MDR role. This new user is used exclusively for programmatic system access when investigating assignments by the Vectra MDR team. Please note that Vectra MDR analysts cannot use the vectra_mdr user for logging into customer systems.

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.

Suspicious Active Directory Operations Detection — Vectra Detect for Network

Starting in 7.5, Vectra has introduced a new detection to identify the abuse of native Active Directory infrastructure components. This detection compliments existing detections like Targeted RPC Recon but looks for specific techniques like DCSync and DCShadow to escalate access within an environment. This detection is on by default and no user action is required.

Faster Detection Reporting — Vectra Detect for M365 and Detect for Azure AD

Several Vectra M365 and Azure AD detections have been enhanced to report threats within less than an hour of Vectra receiving and processing the relevant logs from Microsoft. Specifically, M365 Suspect eDiscovery Usage, M365 Suspicious Compliance Search, Azure AD Admin Account Creation, Azure AD Newly Created Admin Account, Azure AD Unusual Scripting Engine Usage, M365 External Teams Access, M365 Suspicious Power Automate Flow Creation and M365 Unusual eDiscovery Search.

Azure AD Scripting Engine Coverage — Vectra Detect for M365 and Detect for Azure AD

Expanded coverage for recently observed scripting engines associated with attacker automation, including PowerShell variants and Microsoft management APIs. This change improves the detection signal of Azure AD Unusual Scripting Engine Usage with a minimal increase in the overall detection volume.

Azure AD Admin Creation Coverage — Vectra Detect for M365 and Detect for Azure AD

Expanded coverage for the recently observed new admin types variants generated by attackers for creating redundant access channels. This change improves the detection signal of both the Azure AD Admin Account Creation and Azure AD Newly Created Admin Account with a minimal increase in the overall detection volume.

Bug Fixes

DP-2372: M365 Suspicious Mail Forwarding case sensitivity

Addresses an issue where the detection algorithm would treat mixed case forwarding addresses and user domains differently, resulting in benign alerts.

CS-7039: Incompatible SFP sys_check not displayed in user system-health report

Addresses an issue where the “show system-health” vscli command output does not include details of an unsupported SFP failure message when ran as the ‘vectra’ user.

CS-7287: SAML authentication loop

Addresses an issue where SAML authentication may cause a redirect loop between the Vectra brain and customer IdP when a user with a valid SAML token, but mismatched app permissions, attempts to access the Vectra UI.

CS-7411: Increase in NTP connectivity system alerts

Addresses an issue introduced in release 7.4 where the sensitivity of NTP connectivity checks were increased, leading to an increase in NTP connectivity alerts even under normal fluctuations.

CS-6801: Automatic updates toggle switch disabled

Addresses an issue introduced in release 7.2.1 where the Automatic updates toggle switch is disabled.

CS-6561: Campaign last activity shows incorrect age

Addresses an issue where the last activity of a campaign may show an incorrect age.

CS-6401: EDR artifacts missing from some hosts

Addresses an issue where caching of EDR artifacts may result in out-of-date data and some artifacts not linking to hosts. This fix will provide more accurate EDR artifact processing as Detect will only accept artifacts that are seen within two hours of processing.

CS-6214: Alarms not triggered for INFO-level Custom Models

Addresses an issue where INFO-level custom model detections do not send email alerts despite being configured to do so.

Appendix:

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

No reboot is required as part of the 7.5 update.