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 Network software release version 8.0. The Version 8.0 release introduces the General Availability for Vectra AI Platform with Response UX, Instant Investigation for Network Accounts, Advanced Investigation extended metadata retention, triage for account groups, Vectra Match HostID enrichment, and coverage enhancements to M365 Risky Exchange and Disabling of Security Tools detections.

Release Schedule

8.0 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after Oct 31, 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 Nov 17, 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 Nov 17, 2023
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

General Availability of Vectra AI Platform with Respond UX — Vectra AI Platform

The Vectra AI Platform is the integrated signal powering XDR providing hybrid attack surface coverage across identity, public cloud, SaaS, and data center networks; AI-driven Attack Signal Intelligence that prioritizes real attacks in real-time; and integrated, automated, and managed response to move at the speed and scale of hybrid attackers. Click here for a copy of the Vectra AI Platform Overview and Migration Guide.

Please note: *If you would like to migrate to the Vectra AI Platform with Response UX, reach out to your account team.*

Instant Investigation for Network Accounts — Vectra AI Platform

In the September release we are expanding the Instant Investigation feature. In addition to the existing metadata available for Network Hosts, we are introducing a new section dedicated to providing metadata for RPC Calls, SMB access, and Services activities for Network Accounts. In situations where the same actor has both Azure AD and M365 accounts, we will link these accounts and offer metadata for activities in both domains. This enhancement aims to provide a more comprehensive view of specific actors in hybrid deployments.

Advanced Investigation Extended Metadata Retention — Vectra AI Platform

To facilitate investigations that span longer timeframes, we are introducing extended metadata retention options of either 14 or 30 days for Advanced Investigation. With this enhancement, users have the flexibility to select search periods of up to 14 or 30 days, depending on their subscription plan. It's important to note that this extended metadata retention period applies uniformly across all enabled data sources on a tenant, including Network, Azure AD & M365, and others. Also, please be aware that in this release, the extended metadata search period is exclusive to Advanced Investigation and does not apply to Instant Investigation.

Triage for Account Groups — Vectra AI Platform

To help our customers manage their detection workload effectively, we've added support for Triage by Account Group to our AI-driven Triage functionality. With release 8.0, you can specify account groups and triage detections against any member of those groups automatically. This will streamline your experience, for example by creating an account group for your IT admins and specifying behavior which it is expected they may perform, you can easily manage the addition of new IT admins through these account groups.

Please note: *Triage by Account Groups will only work with accounts which have been created in the Vectra AI Platform (either activity is seen or a detection has been fired). Please note also that triage is performed against the underlying accounts in reconciled accounts, so Azure AD & M365 detections are triaged only when the Azure AD accounts are in an account group. You should aim to add both the Network and the Azure AD account for a user to your account group if you are using triage for account groups across attack surfaces.*

Vectra Match HostID Enrichment — Vectra Match

Starting in 8.0, if you leverage Vectra Match and have the “Include Enhanced Details” configured for Vectra Match alerts, we will include additional Vectra proprietary information in the Vectra Match alerts sent to SIEM/SOAR. These fields include valuable HostID fields and Sensor information which is included in traditional Vectra Detections and Metadata and useful for more easily conducting investigation workflows. If you wish to turn off this enrichment, you can do so by disabling the “Included Enhanced Detail” option under the Syslog configuration for your respective destination.

Vectra CDR for Azure — Vectra AI Platform

Interested in learning about Vectra's upcoming Cloud Detection and Response for Azure product capabilities? We would like to ensure we are building what is important to you when identifying and responding to potential security threats across your Azure tenants. Share your views by taking this brief survey:

https://info.vectra.ai/azure-cdr-survey

Detections

M365 Coverage Enhancements — Vectra CDR for M365

The M365 Disabling of Security Tools and M365 Risky Exchange Operations detection have been enhanced to cover more attacker actions. These enhancements include techniques like license downgrade attacks, enabling powershell access, allowing email forwarding rules and impersonating users in emails.

Bug Fixes

PLAT-11659: Network metadata coherency is improved on KVM sensors

Release 8.0 introduces improvements to network metadata coherency on KVM sensors, however in some cases with KVM sensors operating at 8 cores or more may experience reduced bandwidth due to this fix. This is a known issue and will be addressed in the next patch release.

PLAT-11221: The first virtual NIC is the only NIC that receives traffic in Hyper-V

Addresses an issue where the second interface on a Hyper-V sensor does not process traffic.

CAT-2701: v2.5 /groups endpoint does not recognize page query param

Addresses an issue where the /api/v2.5/groups endpoint does not recognize the “page” query parameter.

CS-8132: “Cognito - Webex” group missing new IP subnets

Addresses an issue where the “Cognito - Webex” IP group was not updated to include recently published Webex IP subnets.

CS-8069: Vectra Match not logging detections shown in API

Addresses an issue where the Vectra Match forwarder does not log detections show in the API due to a time zone parsing error.

CS-7916: Host reports are not visible in the UI

Addresses an issue where Host reports created prior to the 7.7 release are not visible in the UI.

CS-7996: Missing “Last activity” in email alerts

Addresses an issue where detection alert emails are missing the “last activity” details.

CS-8025: Virtual Infrastructure page shows loading indefinitely

Addresses an issue where the Virtual Infrastructure page never loads and shows “Still trying to load Physical Hosts…” indefinitely.

CS-7899: PCAPs stuck in “transferring” status

Addresses an issue where PCAP status stuck in “transferring” due to error during the transfer process and does not retry the transfer.

CS-7820: Triage error during filter selection

Addresses an issue where “Device Name is any of” additional condition shows “This field contains invalid values” error even when valid characters are used.

CS-7999: Search API returns FieldNotFoundError

Addresses an issue where a null value for account.last_timestamp causes the Search API to return a FieldNotFoundError.

CS-8017: REST API not showing filtering options when using OPTIONS method

Addresses an issue where the /api/v2.x/detections endpoint returns a permissions error when attempting to use the OPTIONS method.

CS-7869: Account shows “disabled from outside Cognito” after lockdown from Vectra UI

Addresses an issue where a disabled AD account incorrectly shows “disabled from outside Cognito” despite being locked down from the Vectra UI.

CS-7881: Non-default session timeout not honored

Addresses an issue where systems with a non-default session expiry timer do not enforce session timeouts correctly.

CS-7931: Defender EDR ID filters may capture AAD/O365 traffic

Addresses an issue where hosts may be incorrectly marked as having Defender EDR installed due to incorrect filtering on O365 and AAD traffic.

CS-7791: Defender EDR incorrect handling of pending isolation state

Addresses an issue where attempting to lock/unlock an inactive host present in Defender EDR results in a failure condition due to incorrect handling of pending isolation status.

Appendix:

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

No, a reboot is not required as part of the 8.0 update.