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 8.2. The version 8.2 release introduces multi-AD support and introduces the use of a new attribute for account lockdown. Detection updates include two new Kerberoasting detections for Network, Enhanced Coverage for Admin Persistence and Decreased Time-to-Detect for Azure AD Sign-on Alerts for Azure AD, and several new detections and coverage enhancements for AWS.

Release Schedule

8.2 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after Feb 5th, 2024
    - 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 Feb 13th, 2024
    - 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 Feb 13th, 2024
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Multi-AD Support — Network

Release 8.2 introduces support for integrating with more than one Active Directory server for host and account context enrichment and account Active Directory Lockdown. Host and account details now display context from multiple ADs and locking an account will disable that account across the multiple ADs.

More information on configuring Active Directory integration on the Vectra Platform can be found here: https://support.vectra.ai/s/article/KB-VS-1210

AD Integration Custom Configuration Options — Network

In cases where the UserAccountControl Active Directory attribute is not available to perform Account Lockdown, Vectra administrators now have the option to use the AccountExpires attribute for locking network accounts. Additionally, you now have the option to utilize the Info attribute for sending additional context, such as incident number, to your Active Directory when performing an Active Directory Lockdown on an account.

Please note: Both the AccountExpires and Info attributes are considered custom configurations and must be first enabled by Vectra Support. More information on using the AccountExpires and Info attributes with Account Lockdown can be found here: https://support.vectra.ai/s/article/KB-VS-1734

Detections

Kerberoasting: Targeted Weak Cipher Response — Network

In addition to the two existing Kerberoasting detections for Weak Cipher Downgrade and SPN Sweep, Vectra has introduced a new Kerberoasting detection when an attacker attempts to perform a very quiet Kerberoasting attack with as few as 1 single Weak Cipher attempt against a high privileged service. A new user interface for the Kerberoasting: Targeted Weak Cipher Response detection has been introduced in addition to the ability to configure triage rules for this detection. For more information, please see the Understanding Vectra AI document: https://support.vectra.ai/s/article/KB-VS-1285

Info: Single Weak Cipher Response — Network

Vectra has introduced a new Info detection called Info: Single Weak Cipher Response. This is similar to the new Kerberoasting Targeted Weak Cipher Response, but is designed to detect when the privilege of the Kerberoasting target is not privileged, and thus additional review by an analyst should be considered as this may be benign activity depending on your environment. A new user interface for the Info: Single Weak Cipher Response detection has been introduced in addition to the ability to configure triage rules for this detection. For more information, please see the Understanding Vectra AI document: https://support.vectra.ai/s/article/KB-VS-1285

Enhanced Coverage for Admin Persistence — Azure AD

Coverage for attackers adding admin persistence to Azure AD tenants has been expanded. Specifically, Azure AD Admin Account Creation, Azure AD Newly Created Admin Account and Azure AD Redundant Access, have been enhanced to alert on accounts being created with or granted additional types of admin permissions. No notable increase in the number of Vectra alerts is expected with this enhancement.

Decreased Time-to-Detect for Azure AD Sign-on Alerts — Azure AD

Time-to-detect has been further reduced for real time Azure AD alerts related to the initial access to Azure AD account from an attacker. Specifically, algorithm enhancements to Azure AD Suspicious Sign-on, Azure AD Suspicious Sign-On MFA Failed, and Azure AD compromised Access have enabled faster reporting of threats without impacting coverage.

New Coverage for AWS Relational Databases (RDS) — AWS

With this release, Vectra is introducing new coverage surrounding abuse of relational databases in AWS that house sensitive information. The AWS Suspect Public RDS Change detection is the first in a series of detections surrounding RDS and covers methods that an attacker may use to exfiltrate backups (snapshots) of RDS databases. Prompt detection of this behavior can curb exfiltration and impact stages of an AWS cloud attack.

New Coverage to Identify Malicious Traffic Mirroring — AWS

Vectra is introducing new coverage to surface malicious behaviors of setting up a traffic mirror to intercept sensitive information such as credentials. The new AWS Suspect Traffic Mirror Creation detection covers methods that an attacker may leverage to create an EC2 instance as a target for mirrored traffic. Surfacing behaviors surrounding the mirroring of traffic within VPCs where traffic is usually unencrypted allows SecOps to stop adversaries from progressing towards their objective of impact.

New Coverage to protect Amazon Machine Images (AMI) AWS

With this release, Vectra is introducing new coverage to stop malicious exfiltration of Amazon Machine Images (AMIs). These images are templates that hold valuable information and can be used to launch EC2 instances containing extract sensitive data. The new AWS Suspect Public AMI Change detection covers methods that an attacker may use to exfiltrate these AMIs. Prompt detection of this behavior can curb exfiltration and impact stages of an AWS cloud attack.

Deeper Protection for AWS Organizations AWS

Vectra is expanding the coverage provided for AWS Organizations. AWS Organizations is a compliance service that enables guardrails and central management for all member accounts within an organization. A common tactic leveraged by attackers is to remove a compromised account from its associated Organization to bypass these compliance guardrails. The new AWS Suspect Organization Exit detection surfaces this behavior allowing SecOps to thwart attempts to bypass defenses.

Enhanced Coverage for Logging Defense Evasion Techniques AWS

Coverage for attacker methods that involve compromising logging has been expanded. The AWS CloudTrail Logging Disabled detection has been enhanced to identify adversaries that use either Event Selectors or S3 Lifecycle rules to impair logging. This is a technique used by popular attack tools such as Stratus red team and allow an attacker to avoid detection as they move towards states of Impact. Volume of alerts is expected to remain the same.

Enhanced Coverage for Privilege Escalation Techniques AWS

Coverage for novel methods of privilege escalation have been added. Specifically, the techniques covered by the AWS Suspect Privilege Escalation detection have been expanded to include methods adversaries use to escalate permissions not just using policies, but also AWS services such as EC2 instances. These enhancements enable detection of methods found in attack tools such as CloudGoat. Environments that rely heavily on compute instances may say a minor increase in the volume of AWS Suspect Privilege Escalation alerts.

Bug Fixes

CS-8360: Unable to save Active Directory configuration

Resolves an issue where the system returns an error stating “Unable to save AD configuration” when attempting to save or modify the Active Directory external connector configuration.

CS-8491: Unable to set IPMI password on S11 sensor

Resolves and issue where the vscli returns a server error when attempting to set the IPMI password.

CS-8283: SSH key deprecated setting vulnerability

Removes SHA1 deprecated setting for SSH host key for brain and sensors.

CS-8469: SAML error when saving profile with accented letter

Resolves an issue when adding the Federation Metadata XML file and saving the SAML profile the UI gives the error "Unknow error occurred" when the XML file contain accented letters.

CS-8449: Manage Groups modal duplication and pasting errors

Resolves issues related to usability of the Manage Groups module that includes duplicate values not being returned as errors, and pasting of a valid group which is not already an existing member incorrectly returns an error.

CS-8361: GET request to retrieve notification settings does not work for super-admin

Resolves an issue a user with a super-admin role cannot perform a GET request to retrieve notification settings from the v2.5 API.

CS-8431: Detection filtering does not distinguish between “Filtered by AI” and “Marked as fixed”

Resolves and issue where detection filtering in the UI does not allow "Marked as fixed" to be filtered separated from “Filtered by AI”.

Appendix:

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

No, a reboot is not required as part of the 8.2 update.