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 8.3. The version 8.3 release introduces IPv6 Management Interface Support, Support for Private SSL keys in vsupport, and various detection enhancements to ICMP Tunnels and a new Azure AD detections. The 8.3 release also includes an end-of-life notice for the X80 and S2 hardware platforms.

Release Schedule

8.3 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on or after April 23, 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 May 2, 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 May 2, 2024
    - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Platform

Self-management of Private SSL Keys for GUI via CLI — Network

Vectra has introduced the ability for customers to upload their own private key with the HTTPS/SSL certificate through the CLI and API. This process can be executed through command line by leveraging *certificate add https --replace-key.* For more information, please see the SSL Certificate Installation document: https://support.vectra.ai/s/article/KB-VS-1015

Detections

ICMP Tunnel: Lateral Movement Client — Network

Vectra has introduced the ability to detect attacker behaviors where an attacker is leveraging the ICMP protocol to communicate between internal systems laterally within an environment which is not consistent with diagnostic use of the ICMP protocol. The Client Detection detects when the Client is using this technique to communicate in an environment. A new user interface for the ICMP Tunnel lateral movement 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

ICMP Tunnel: Lateral Movement Server — Network

Vectra has introduced the ability to detect attacker behaviors where an attacker is leveraging the ICMP protocol to communicate between internal systems laterally within an environment which is not consistent with diagnostic use of the ICMP protocol. The Server Detection detects when the Server is using this

technique to communicate in an environment. A new user interface for the ICMP Tunnel lateral movement 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

ICMP Tunnel: Command and Control — Network

Vectra has introduced the ability to detect attacker behaviors where an attacker is leveraging the ICMP protocol as a Command and Control channel between an internal and external system in a way that isn't consistent with the diagnostic use of the ICMP protocol. A new user interface for the ICMP Tunnel Command and Control 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

ICMP Tunnel: Exfiltration — Network

Vectra has introduced the ability to detect attacker behaviors where an attacker is leveraging the ICMP protocol for data exfiltration. When data is sent between an internal and external system in a way that isn't consistent with the diagnostic use of the ICMP protocol this new detection will trigger. A new user interface for the ICMP Tunnel Data Exfiltration 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

Suspicious Active Directory Operations Triage Enhancement — Network

Starting in 8.3, with the Suspicious Active Directory Operations detection, you will be able to add Internal Targets based upon IP addresses and groups in addition to the previously supported host / host-group objects.

Suspicious Remote Execution Performance Improvement — Network

Vectra has introduced a performance improvement for the Suspicious Remote Execution detection to handle more demanding environments. There is no action required for this feature, it is enabled in this release.

Suspicious Access from Cloud Provider — Azure AD

Vectra has introduced the ability to detect attackers who compromise an identity and accesses it from a public cloud provider, such as Amazon, Azure or GCP to attempt evade detection and hide their true location. The detection uses machine learning to identify whether a user normally accesses their account from the public cloud. Bening alerts may trigger when a user uses an application that routes through a public cloud or cloud hosted virtual machines. This new alert will prioritize an account when it occurs with other alerts in a similar manner to the Azure AD Suspicious Sign-On alert.

X80 and S2 Platform End-of-Life Notice

The X80 and S2 hardware platforms will be EOL on January 7th, 2025.

After the 7th of January 2025, Vectra will no longer support:

- Software upgrades for X80 and S2 appliances.
- Software upgrades for brain appliances where an S2 sensor is paired.
- Hardware replacements for X80 or S2 appliances or their components.

Please contact your Vectra account team to discuss future options for replacing affected X80 or S2 hardware prior to the 7th of January, 2025.

Bug Fixes

CS-8614: User Login Performance Issues

Resolves an intermittent issue where upon a user login an additional reload of the screen occurred which impacted system performance during logins.

CS-8428: Intermittent API Issue When Editing Threat Feed

Resolves an issue where upon deleting, editing, or creating new Threat Feeds caused issues in some scenarios where users were not able to perform their desired task due to the system believing there was already a Threat Feed with the same name.

CS-8404: X-Forwarded-For (XFF) Populating Second IP

Resolves an issue where the incorrect IP address is being displayed for XFF hosts on SQL Injection detections. The second IP address (WAF) was being displayed when the accurate IP address should be the first IP address that corresponds to the Client IP address.

CS-8536: Kerberoasting: SPN Sweep Detection URL Returns Error

Resolves an intermittent issue where the URL for a Kerberoasting: SPN Sweep detection returns an error.

APE-9241: Modal for Multiple Active Directories Displays Incorrect Value

Resolves an intermittent issue within Multiple Active Directories where the Autobind dropdown in modal incorrectly displays an internal backend value when selected. This issue has now been resolved and the Autobind dropdown in modal displays correctly.

CS-8579: Modal for Multiple Active Directories Displays Incorrect Value

Resolves an issue where the Triage Filter tab resulted in an error.

Appendix:

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

No, a reboot is not required as part of the 8.3 update.