Vectra Detect Platform Software Update

The Vectra® X-series appliances, B-series appliances, S-series sensors, Cloud Brain, and Cloud Sensors, are scheduled to be updated to Vectra Detect for Network software release version 7.1

The Version 7.1 release introduces Kerberoasting Weak Cipher and SPN Sweep Detections and Entity Quadrant in Syslog Notifications.

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

Release Schedule

7.1 will have the following release schedule:

- **Customers with Remote Support Enabled:** Customers who have remote support enabled will receive the update on September 28th 2022
  - 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 October 5th, 2022
  - 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 October 5th, 2022
  - *Note: This does not impact customers that have requested they be pinned to a specific release from support.

Kerberoasting Weak Cipher and SPN Sweep Detections

Vectra Detect for Network

Detect for Network 7.1 introduces two new detections to detect the Kerberoasting attack behavior. Kerberoasting is an attack which takes advantages of the design of Kerberos, combined with encryption that can be broken with modern computing to gain access to other accounts in the Active Directory domain. The Kerberoasting Weak Cipher detection identifies the anomalous use of ciphers that are known to be susceptible to offline cracking, while Kerberoasting SPN Sweep identifies the technique of requesting a large number of SPN tickets from Kerberos which is often associated with this attack. Prior to 7.1, Kerberoasting could sometimes be detected with Privileged Anomaly detections, but the dedicated detection introduced into 7.1 will make detecting this attack much more robust.

Entity Quadrant in Syslog Notifications

Vectra Detect for Network

Starting in 7.1, Detect for Network introduces a new field to syslog messages to identify the “Quadrant” of a host or account as part of the Host Scoring syslog messages. The values for this field are Low, Medium, High, or Critical, and reflect the status of the given host or account in the UI. This field was introduced to the syslog message to make it easier for SIEM and other integrations to directly know what the status of a given host or account is, rather than having to calculate it from the Threat and Certainty scores. This new field is automatically included in the syslog messages if the Enhanced Detail option is checked under: Settings -> Notifications -> Syslog -> Destination: Include enhanced detail and Settings -> Notifications -> Kafka -> Destination: Include enhanced detail.

Bug Fixes

Detections-285: Hidden HTTP/HTTPS Tunnel Not Detected when used in large scale, multitenant hosts

This addresses an issue when C2 was hosted by large scale hosting environments that put large numbers of hosts on the same IP address. Prior to 7.1, some of these detection would be filtered out to avoid false positive detections. In 7.1, this process has been removed, now that AI-Triage is available and more accurate. Under rare conditions, there may be a temporary uptick in C2 detections until AI-Triage identifies these as benign, customers are also welcome to use standard triage filters to eliminate such detections manually.

Data-1969: Selective PCAP Match on Decapsulated Traffic does not honor capture filter

This addresses an issue with Selective PCAP when the Match on Decapsulated Traffic does not properly match on the decapsulated traffic. This has been addressed.

CS-6580: API Pagination falls back to IP rather than FQDN

This addresses an issue with the API when paginating results where the API link will fall back to using the Brain IP rather than the FQDN. This has been addressed

PLAT-8617: BIOS Upgrade on X29 and S101 to address Dell CVE-2022-22558

This release contains an upgrade for the BIOS on X29 and S101 systems to address a vulnerability in Dell BIOS. This has been addressed.

PLAT-8368: iDrac Update to address OpenSSL CVE-2022-0778

This release contains an upgrade to address OpenSSL Vulnerability CVE-2022-0778 in the iDrac interface. This has been addressed

Appendix:

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

This upgrade includes a BIOS fix for the X29 and S101 systems, per PLAT-8617. These systems will automatically be rebooted for the upgrade to take effect. All other systems will not require an upgrade.