Release Notes: 2.41

Version 2.41 Release Date: November 1, 2023

The CYRISMA 2.41 release includes multiple bug fixes and feature enhancements including a new Debian-based Linux Agent, the ability to multi-decommission agents and targets, multiple enhancements in the patch management capability, and the option for CSV download of the target risk matrix.

Admin

- **Targets** - When on the 'Add A New Target' form, the 'Submit Updates' button is now 'Submit'
- **Scan Agents - Multi Decommission** - This is the ability to Decommission the agent with Uninstall bit in the database. Also, added the Edit icon in the agent status table
- **Scan Agents** – Debian-based kernel distribution based Linux Agent has been released
- **Targets - Multi Decommission** - Function to delete multiple targets

Header

- **User Settings - Access Events** - Time and dates are localized

Compliance

- **AD Monitor Results** - Fixed crashes
- **Microsoft Secure Score** - Some items in the 'Recommended Actions' table were missing their implementation - Next Steps' information.
- **Microsoft Secure Score** - Fixed an issue in the "Recommended Actions" table - When a row was expanded that had more than one paragraph of text in the 'Description' section, the paragraphs made several narrow columns of text that were side by side within the 'Description' column, making it difficult to read.

Dashboard

- **Compliance Tracker** - The cursor now turns into a hand pointer when the percentage bars are hovered over
- **CSV download** for The target risk matrix

Data Scan

- **History** - Clicking on locations no longer opens the sub-row
- **Data scan - Schedule a scan** - Office 365 scans and Google scans can no longer be scheduled with no categories selected.

Log In

- **Recover Password** - Changed input field background color to white
- **Forgot Username/Password** screen now has a button to move back to login page
- **One-Time Pass Code modal** - No longer showing HTML tags

Mitigation

- **Dashboard - Mitigation Key Performance Indicators** - When the page is loaded, the default time span filter is now highlighted. (M,Q,Y)
- **My mitigation plans** - Review and perform action. Click on Copy path icon. On paste, it's no longer pasting two entries of path
- **Scan Histories** - The '...' button can be used to create a mitigation plan from a scan.

Secure Baseline

- **Schedule a scan** - After selecting an agent other than an agent group, fixed an issue causing the target list not to appear,
- **Schedule a scan** - When editing a secure Baseline scan, now just targets that have agents are shown.

Site-Wide

- Table sections that show **vulnerability severity levels** with number/letter ratings and colors no longer appear to be clickable in Vulnerability- Scan History -'Top 5 Vulnerabilities Found' table, Vulnerability - Patch Manager- Root cause breakdown- Servers/Workstations modal, and Admin - Targets- 'Target Scan Summary' modal.
- **Internal Unauthenticated scan**, Admin-Targets-Network Discovery scan. When scheduling a scan and using CIDR notation, fixed an issue where anything could be entered after the CIDR notation and the scan could be submitted.
- For most scans, added feature to scan Bi-Weekly recurrence
- For most scan types, increased max recurrence from 26 to 52.
- Replaced checkbox components with formcheckbox
- Removed moment.js usage across the code base and replace with timeH functions
- Replaced direct usage of ProgressBar with ChartProgressBar component
- **Schedule a scan** - When a secure baseline scan with a future scan date was edited and the page was refreshed, fixed an issue where trying to edit the same scan again would show the scan has not saved the initial scan selections

Vulnerability Scan

- **Compare** - Added reset button to reset the target and scans selection
- **Dashboard** - The Scans in Progress are now accurately showing the scans in progress
- **Dashboard** - Targets with the Most Vulnerabilities - Clicking on target now shows details on modal similar to Top Vulnerabilities table
- **Dashboard - Top Vulnerabilities** - "Patch" action button now shows against respective root cause in table on Target modal
- **History - Expand scan**, in Vulnerabilities Breakdown chart click IP, fixed an issue where HTML tags were showing in the root cause section
- **In Progress** - Expand paused scan in progress, from vulnerability breakdown chart- in table expand the row. Fixed an issue where 'Failed Case Description' contained HTML tags
- **Schedule a scan** - Internal Unauthenticated scan- fixed an issue where the following IP range: 172.32.0.1-172.32.255.255 was able to be used for internal scans.
- **Schedule a scan** - When creating an Internal Unauthenticated scan- fixed an issue where CIDR /8-/24 did not work
- **Patch Manager** - All and 3rd party images are now clickable to filter the root cause table.
- **Patch Manager- Patch History,** Pending Patches can be Deleted/Canceled
- **Patch Manager- Root Cause Breakdown** - "Patch" action button now shows against respective root cause in table on Workstation and Server modals.