Version 2.120.1.151
Release Date: April 11, 2025
CYRISMA Version 2.120.1.151 feature releases and updates

New Features

Patch Management - Introduced advanced patch control settings under Admin > System Config, allowing users to define Blackout Hours, restrict patching on specific machines, and exclude selected 3rd-party applications from auto or manual patching.

Report Builder - Optional Password Protection for Reports - Users can now choose to enable password protection for generated reports via Admin > Config. When enabled, reports are delivered as password-protected ZIP files to enhance security. All reports expire 24 hours after generation.

Fixes in User Experience and Functions

Dark Web

Setup Dark Web Monitor - Resolved an issue that prevented users from creating monitors using domain names with top-level domains longer than six characters.

Patch Manager

Central Vulnerability Manager - Added host vulnerability summary modals to the Root Cause Breakdown table for workstations and servers. These modals include suppression capabilities, allowing users to review and manage vulnerabilities at the host level more efficiently.

Windows KB article numbers are now automatically linked to their corresponding Microsoft Support pages, streamlining access to patch information and eliminating the need for manual lookups.

Windows KB article numbers are now automatically linked to their corresponding Microsoft Support pages, streamlining access to patch information and eliminating the need for manual lookups.

Improved patch classification by separating Linux and macOS root causes into distinct tables. For Windows, patching is now displayed in two dedicated tables: one for KB Article Patching and another for Root Causes & Vulnerabilities.

Vulnerability Scan

History - Fixed an issue with the "Scan Again" function for internal authenticated scans. Scan details are now properly recalled when rescheduling, restoring expected functionality.