Middleware 12.25

Features

- Added new endpoints for DLL Visualization on the dashboard for viewing related untrusted module loads for Extortion Responses, Process Creations, Process Injections, and Identity Accesses
- Updated the Extortion Response and Identity Access endpoints for the dashboard queries to return additional fields for DLL Visualization including modified module memory, modified module path, etc
- Updated the Agent model to have new fields for if the agent is fully configured and the date the agent was first fully configured
- Added new endpoints and controller for the AI Firewall Management page
- Updated the endpoint that returns the list of agents for the dashboard to include new fields for which rest server and OAuth server the agent is calling to, and the WAN IPv4 and IPv6 of the agent
- Added new endpoint for the Extortion Responses page that allows users to view all fields for an Extortion Response in this endpoint rather than using the existing endpoint that offers a condensed view of the fields and requires an additional api call to get more details.
  - Users on the dashboard can use the toggle on the Extortion Responses page to use the previous grid option and the new grid option that returns all fields in one grid
- Added a new option to Security Notifications to include a CSV file in the email alert for Ransomware and Identity Access Alerts containing information on why the alert was triggered.

Revision #1
Created 2026-07-13 18:50:16 UTC by Dennis Underwood
Updated 2026-07-13 18:50:16 UTC by Dennis Underwood