Middleware 12.25

Recursos

- Adicionados novos endpoints para Visualização de DLL no painel para visualizar carregamentos de módulos não confiáveis relacionados a Extortion Responses, Process Creations, Process Injections e Identity Accesses
- Atualizados os endpoints de Extortion Response e Identity Access para as consultas do painel retornarem campos adicionais para Visualização de DLL, incluindo memória de módulo modificada, caminho de módulo modificado, etc
- Atualizado o modelo do Agent para incluir novos campos indicando se o agente está totalmente configurado e a data em que o agente foi totalmente configurado pela primeira vez
- Adicionados novos endpoints e controlador para a página de Gerenciamento do AI Firewall
- Atualizado o endpoint que retorna a lista de agentes para o painel, incluindo novos campos indicando para qual servidor REST e servidor OAuth o agente está se comunicando, além do IPv4 e IPv6 WAN do agente
- Adicionado um novo endpoint para a página de Extortion Responses que permite aos usuários visualizar todos os campos de um Extortion Response nesse endpoint, em vez de usar o endpoint existente que oferece uma visão condensada dos campos e exige uma chamada de API adicional para obter mais detalhes.
  - Os usuários no painel podem usar a alternância na página de Extortion Responses para usar a opção de grade anterior ou a nova opção de grade que retorna todos os campos em uma única grade
- Adicionada uma nova opção nas Notificações de Segurança para incluir um arquivo CSV no alerta por e-mail para Alertas de Ransomware e Identity Access, contendo informações sobre o motivo do disparo do alerta.

Revision #1
Created 2026-07-24 05:26:22 UTC by Dennis Underwood
Updated 2026-07-24 05:26:22 UTC by Dennis Underwood