Middleware 11.23

Funciones

- Actualizaciones de la lista blanca
  - Se implementó la capacidad de crear una excepción con la ruta y los argumentos del programa principal
  - Se implementó la capacidad de crear una excepción para coincidir con respuestas de extorsión cuando solo hay certificados de confianza, coincidir solo cuando no hay inyecciones relacionadas, y coincidir solo cuando no hay memoria modificada
  - Se implementó la capacidad de crear una excepción para coincidir con desencadenantes de acceso a archivos específicos
- Se implementó la configuración de grupo para liberar automáticamente las licencias de los agentes inactivos
  - Se actualizó el modelo de Grupo para tener una configuración sobre cuándo liberar las licencias de los agentes inactivos en el grupo. Las opciones son 30/60/90 días, o desactivar esta configuración
  - Se actualizó el modelo de Agente para tener un nuevo estado inactivo
  - Se implementó un servicio para liberar automáticamente las licencias de los agentes inactivos según la configuración de su grupo
- Se actualizó el endpoint para la recuperación de respuestas de extorsión para incluir la ruta y los argumentos del programa principal
  - La ruta y los argumentos del programa principal ahora también se incluyen en los recuentos de respuestas de extorsión únicas para la Aplicación Web, las alertas de Notificación de Seguridad y los Resúmenes Ejecutivos
- Se actualizaron nuestros Informes de Resumen Ejecutivo para separar la diapositiva de Licencias en diapositivas individuales de Licencias de Escritorio y de Servidor
- Se actualizó el modelo de Notificación de Seguridad por Correo Electrónico y el servicio de Notificación de Seguridad para incluir dos nuevos tipos de alerta
  - Modelo de Comportamiento Ajustado
  - Nueva Versión del Agente
    - Cuando se cambia la configuración de actualizaciones administradas de un grupo para desactivar la actualización automática, se crea automáticamente una notificación de Nueva Versión del Agente para el grupo
- Actualizaciones de Roles/Permisos de Usuario
  - Se actualizaron los permisos del modelo de Rol de Gestor de Incidentes para que ahora solo tenga visualización/edición para listas blancas y reglas de respuesta silenciosa
  - Los grupos ahora tienen 3 roles predeterminados que no son editables por el usuario:
    - Administrador

    - Solo lectura
    - Invitado
  - Los usuarios agregados a un grupo se asignan por defecto al Rol de Invitado
- Se implementaron endpoints para el Modal de Ajuste del Proceso de Utilidad del Navegador de la Aplicación Web para gestionar fácilmente cómo deben responder los agentes en los grupos a los procesos de utilidad de chrome
- Se actualizó el endpoint para el gráfico de la página de Agentes para poder limitar los recuentos a los agentes que se han conectado en los últimos 30/60/90 días
- Se actualizó la alerta por correo electrónico de Notificación de Seguridad de Actividad de Ransomware para incluir un enlace que redirigirá automáticamente a los usuarios a la página de Respuestas de Extorsión con un filtro para mostrar las respuestas a las que se refería la alerta
- Se implementó la configuración de grupo para que los agentes de un grupo se ejecuten o no en modo seguro
- Se implementó una opción de script de powershell para la instalación de agentes
- Actualización de nuestro Spring Boot a la última versión
- Diversas actualizaciones a nuestra lista de listas blancas predeterminadas de datos + identidad + certificados para los antivirus

---

Revision #1
Created 2026-07-24 01:24:51 UTC by Dennis Underwood
Updated 2026-07-24 01:24:51 UTC by Dennis Underwood