Middleware (servidores REST)

- Middleware 01.23
- Middleware 04.23
- Middleware 08.23
- Middleware 11.23
- Middleware 04.24
- Middleware 09.24
- Middleware 05.25
- Middleware 12.25

Middleware 01.23

Funcionalidades

- Se implementó el controlador para las licencias de formación y se agregó un servicio de vencimiento de licencias de formación.
- Se actualizó cada endpoint para tener en cuenta la nueva funcionalidad de modo de formación de la aplicación web, junto con pruebas para cada endpoint en el modo de formación.
- Se agregó un endpoint para restablecer todos los datos de formación de un grupo principal a su estado original.
- Se implementaron los endpoints para la nueva configuración de política de vencimiento de contraseñas para grupos.
- Se está agregando documentación para los endpoints de Reactive Springboot.

Middleware 04.23

Características

- Actualizaciones del Portal de Socios:
  - Se implementaron los endpoints para el nuevo proceso de Registro de Acuerdos (Register Deal) con aprobación de acuerdos por parte de Cyber Crucible
  - Se actualizó el modelo PartnerDeal para que tenga un tipo asociado a los acuerdos, cada uno con un porcentaje de descuento asociado
    - También se actualizó el modelo PartnerDeal para los acuerdos de tipo Referido, a fin de almacenar la Cuenta de Usuario del Dashboard que se asociará con las licencias del acuerdo
  - Se actualizó el modelo PartnerDeal para poder separar la facturación Mensual frente a la Anual en el pago de los acuerdos
    - Incluye la actualización de los endpoints existentes para tener en cuenta la facturación Mensual frente a la Anual en Stripe
  - Se implementaron endpoints para poder enviar cotizaciones a través de Stripe para un acuerdo
  - Se implementó un endpoint para reenviar la factura de Stripe de un acuerdo
  - Se implementó un endpoint para editar múltiples campos de un acuerdo al mismo tiempo, asociado con el modal de edición de acuerdos en la Aplicación Web
- Gestión de Agentes/Licencias:
  - Se implementó un endpoint para asignar licencias de forma masiva a los agentes
  - Se implementó un endpoint para cambiar la configuración de re-licenciamiento automático para un agente determinado
  - Se implementó un endpoint para liberar una licencia de un agente pasando el agentId en la solicitud
- Se implementaron endpoints para recuperar y guardar la configuración de usuario que muestra el ícono de configuración del script del instalador en la cuadrícula de Grupos
- Se implementó un endpoint para recuperar el valor de Autenticación de Cliente del Script del Instalador del Agente para un grupo
- Se actualizó nuestro Servicio de Escaneo de AV para buscar también en la colección de incidentes de identidad, además de la colección de creación de procesos
- Varias actualizaciones a nuestra lista de datos predeterminados + listas blancas de identidad para los AV.
- Se implementó un nuevo endpoint de flujo de cambios (change stream) para detectar nuevas inserciones de Respuesta a Extorsión
- Se implementó un endpoint para copiar listas blancas a otro grupo
- Se implementó un endpoint para descargar el Archivo de Diferencia de Memoria (Memory Diff File) de un incidente

- Se implementó la categorización de los programas de incidentes de identidad en aplicaciones
- Se implementó el guardado de los modos de columna para cada cuadrícula de página web y el guardado de la configuración de visibilidad de los gráficos

Middleware 08.23

Características

- Actualizaciones del Portal de Socios:
  - Se implementaron endpoints para poder crear un POC para acuerdos de socios aprobados
  - Se implementaron endpoints para la página de Gestión de Grupos de Distribuidores en la Aplicación Web
  - Se implementó un endpoint para devolver los datos de la cuadrícula de Gestión de Pagos en la Aplicación Web
  - Se implementó la capacidad de cambiar el propietario de un acuerdo de socio
  - Se implementó la capacidad de establecer una nota personalizada para los acuerdos de socios que aparecen en las facturas y cotizaciones de Stripe
- Se implementó un endpoint para poder reenviar invitaciones de cuentas de usuario
- Se agregaron más opciones de etiquetado de aplicaciones para objetos de Acceso de Identidad
- Se actualizó el modelo de Grupo para grupos de socios para tener nuevos campos booleanos según el tipo de socio
- Se actualizó el modelo de Grupo para tener una lista de configuraciones de extensión canary
- Diversas actualizaciones a nuestra lista de listas blancas predeterminadas de datos + identidad + certificados para antivirus
- Habilitación del soporte HTTP/2
- Actualización de nuestro Spring Boot a la última versión, junto con otras diversas dependencias
- Se implementaron alertas de notificación para Accesos de Identidad Anómalos
- Se habilitó la compresión de respuestas del servidor para los agentes
- Se implementó el filtrado para la columna Sin Certificado Confiable de la cuadrícula de Acceso de Identidad en la Aplicación Web para las opciones "Desconectado al Recuperar Información del Certificado" y "Tiempo de Espera Agotado al Recuperar Información del Certificado"
- Se corrigió un problema en nuestro servicio de notificación de vencimiento de acuerdos de socios para no enviar correos de vencimiento para acuerdos completados

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

Middleware 04.24

Funciones

- Se implementó la configuración de grupo y los endpoints relacionados para la configuración y gestión de configuraciones de proxy, con el fin de facilitar la implementación de agentes
- Se actualizaron nuestros endpoints de datos de telemetría para poder visualizar todos los datos de telemetría o solo los datos directamente relacionados con una respuesta a extorsión
- Se implementó la configuración de grupo para ocultar automáticamente los agentes en grupos cuando se libera una licencia de un agente, un agente se marca como inactivo o un agente completa una desinstalación
- Se actualizaron los enlaces a nuestro panel en nuestros correos electrónicos de notificación para incluir un parámetro de URL utilizado para filtrar automáticamente los datos en la cuadrícula del frontend relacionada, mostrando lo que activó la notificación
- Se actualizó el endpoint utilizado para el gráfico de Licencias de Agentes del frontend para incluir los recuentos tanto de licencias de Escritorio como de Servidor
- Se implementaron endpoints para la nueva página del frontend de Estado de Implementación del Cliente
- Se actualizó nuestro ajuste de procesos para tener en cuenta Microsoft Edge WebView

Middleware 09.24

Funcionalidades

- Se implementaron los endpoints para la nueva configuración del Modo DMZ de Grupo
- Se actualizaron los endpoints de Registro de Operaciones para poder registrar acuerdos plurianuales con la posibilidad de pagar por adelantado o pagar anualmente para acuerdos plurianuales
- Se agregó la capacidad de ver el análisis de causa raíz para los Accesos de Identidad
- Se implementaron Comportamientos Personalizados Temporales
- Se actualizó el modelo de Usuario para guardar la configuración de ocultar o mostrar las Licencias de Agente vencidas de forma predeterminada en la cuadrícula de Licencias de Agente
- Se actualizaron el modelo de Notificación de Seguridad y los endpoints/servicios relacionados para las nuevas opciones de alerta de agente sin conexión de agentes Parcialmente y Totalmente sin conexión
- Actualizaciones a los endpoints relacionados con la incorporación de las nuevas columnas en el frontend en la cuadrícula de Agentes para mostrar cuándo vence la licencia asignada y cuándo se asignó la licencia al agente
- Se agregó una configuración al Modelo de Grupo para que los agentes del grupo muestren el ícono del agente en la bandeja del sistema de la máquina del agente correspondiente
- Se actualizaron las consultas de cuadrícula del lado del servidor para poder aceptar filtros de múltiples condiciones para la misma clave/columna

Middleware 05.25

Características

- Se actualizó el modelo de Notificación de Ventas con nuevos tipos:
  - Los Distributor Partners pueden recibir alertas cuando sus subgrupos de revendedores crean un nuevo Registro de Oportunidad (Deal Registration)
  - Actividad del POC de Oportunidad del Partner (Partner Deal POC)
- Se actualizó el proceso de autenticación para permitir la integración de SSO con Microsoft Entra ID (Azure Active Directory)
- Se actualizó el endpoint del instalador del agente para permitir un nuevo tipo de instalador para Native Cli
- Se actualizaron los endpoints para las nuevas actualizaciones de Distributor Partner
  - Se agregó un nuevo modelo de Partner in Motion
  - Se actualizó el modelo de Registro de Oportunidad del Partner (Partner Deal Registration) para agregar la capacidad de que los distribuidores aprueben las oportunidades de sus subgrupos de revendedores
  - Se agregó la capacidad de que los Distributor Partners editen los descuentos multianuales de sus subgrupos de revendedores
  - Se agregó la capacidad de que los distribuidores se envíen a sí mismos cotizaciones con sus precios de distribuidor para la oportunidad de un subgrupo de revendedores
  - Se agregó el requisito de que, cuando un subgrupo de revendedores registre una oportunidad, se requiera que el Acuerdo de Subgrupo de Revendedores (Subgroup Reseller Agreement) sea cargado por su distribuidor principal en la página de Gestión de Grupos de Distribuidores
- Se actualizó el modelo de Roles con un nuevo rol de Partner Deal Manager para las operaciones de registro de oportunidades, y se actualizó cada endpoint relacionado para verificar el permiso correspondiente
- Se agregó el endpoint para editar la configuración de un grupo de forma masiva
- Se actualizó nuestro Spring Boot a la última versión
- Se mejoraron las consultas utilizadas para generar informes ejecutivos, reduciendo el tiempo necesario para generar el informe
- Se migraron nuestras colecciones de telemetría en la base de datos para utilizar sharding
- Se actualizó la consulta de agentes utilizada para la cuadrícula del panel de control (dashboard grid) para incluir si el agente es un servidor o no
- Se actualizó el endpoint /updateGroupAutomaticallyHideAgentsReactive para aplicar retroactivamente la actualización a los agentes existentes
- Actualizaciones importantes de autenticación para permitir que los agentes se comuniquen con nuestros servidores REST mediante la nueva autenticación OAuth alojada
- Se agregaron nuevos endpoints para el envío de telemetría de DLL por parte de los agentes

Middleware 12.25

Funciones

- Se agregaron nuevos endpoints para la Visualización de DLL en el panel para ver las cargas de módulos no confiables relacionadas con Respuestas de Extorsión, Creaciones de Procesos, Inyecciones de Procesos y Accesos de Identidad
- Se actualizaron los endpoints de Respuesta de Extorsión y Acceso de Identidad para las consultas del panel a fin de devolver campos adicionales para la Visualización de DLL, incluyendo memoria de módulo modificada, ruta de módulo modificada, etc.
- Se actualizó el modelo de Agente para incluir nuevos campos que indican si el agente está completamente configurado y la fecha en que el agente fue completamente configurado por primera vez
- Se agregaron nuevos endpoints y un controlador para la página de Administración del Firewall de IA
- Se actualizó el endpoint que devuelve la lista de agentes para el panel a fin de incluir nuevos campos que indican a qué servidor REST y servidor OAuth está llamando el agente, así como la IPv4 y la IPv6 WAN del agente
- Se agregó un nuevo endpoint para la página de Respuestas de Extorsión que permite a los usuarios ver todos los campos de una Respuesta de Extorsión en este endpoint, en lugar de usar el endpoint existente que ofrece una vista condensada de los campos y requiere una llamada adicional a la API para obtener más detalles.
  - Los usuarios del panel pueden usar el interruptor en la página de Respuestas de Extorsión para alternar entre la opción de cuadrícula anterior y la nueva opción de cuadrícula que devuelve todos los campos en una sola cuadrícula
- Se agregó una nueva opción en Notificaciones de Seguridad para incluir un archivo CSV en la alerta por correo electrónico para Alertas de Ransomware y Acceso de Identidad, que contiene información sobre el motivo por el cual se activó la alerta.