Middleware (Servidores REST)

Middleware 01.23

Recursos

- Implementado controlador para licenças de treinamento e adicionado um serviço de expiração de licença de treinamento.
- Atualizado cada endpoint para considerar o novo recurso de modo de treinamento da aplicação web, juntamente com testes para cada endpoint no modo de treinamento.
- Adicionado um endpoint para redefinir todos os dados de treinamento de um grupo pai ao seu estado original.
- Implementados endpoints para a nova configuração de política de expiração de senha para grupos.
- Adicionando documentação para os endpoints Reactive Springboot.

Middleware 04.23

Funcionalidades

- Atualizações do Portal de Parceiros:
  - Implementados endpoints para o novo processo de Registro de Negócio (Register Deal) com aprovação de negócios pela Cyber Crucible
  - Atualizado o modelo PartnerDeal para ter um tipo associado aos negócios, cada um com um percentual de desconto associado
    - Também foi atualizado o modelo PartnerDeal para negócios do tipo Referral, de forma a armazenar a Conta de Usuário do Dashboard a ser associada às licenças do negócio
  - Atualizado o modelo PartnerDeal para poder separar a cobrança Mensal versus Anual para pagamento dos negócios
    - Inclui a atualização dos endpoints existentes para considerar a cobrança Mensal versus Anual no Stripe
  - Implementados endpoints para permitir o envio de orçamentos (quotes) através do Stripe para um negócio
  - Implementado endpoint para reenviar a fatura do Stripe de um negócio
  - Implementado endpoint para editar múltiplos campos de um negócio ao mesmo tempo, associado ao modal de edição de negócio na Aplicação Web
- Gerenciamento de Agentes/Licenças:
  - Implementado endpoint para atribuir licenças em massa a agentes
  - Implementado endpoint para alterar a configuração de relicenciamento automático de um determinado agente
  - Implementado endpoint para liberar uma licença de um agente informando o agentId na requisição
- Implementados endpoints para recuperar e salvar a configuração do usuário que exibe o ícone de configuração do script instalador na grade de Grupos
- Implementado endpoint para recuperar o valor de Autenticação de Cliente do Script Instalador do Agente para um grupo
- Atualizado nosso Serviço de Scanner de AV para pesquisar também na coleção de incidentes de identidade, além da coleção de criação de processos
- Diversas atualizações em nossa lista de listas brancas (whitelists) padrão de dados e identidade para AVs.
- Implementado novo endpoint de change stream para monitorar novas inserções de Extortion Response
- Implementado endpoint para copiar listas brancas (whitelists) para outro grupo
- Implementado endpoint para baixar o Arquivo de Diferença de Memória (Memory Diff File) de um incidente
- Implementada a categorização de programas de incidentes de identidade em aplicações

- Implementado o salvamento dos modos de coluna para cada grade de página web e o salvamento das configurações de visibilidade dos gráficos

Middleware 08.23

Funcionalidades

- Atualizações do Portal de Parceiros:
  - Implementados endpoints para permitir a criação de uma POC para negócios de parceiros aprovados
  - Implementados endpoints para a página de Gestão de Grupos de Distribuidores na Aplicação Web
  - Implementado endpoint para devolver os dados da grelha de Gestão de Pagamentos na Aplicação Web
  - Implementada a capacidade de alterar o proprietário de um negócio de parceiro
  - Implementada a capacidade de definir uma nota personalizada para negócios de parceiros que aparecem nas faturas e orçamentos do Stripe
- Implementado endpoint para permitir o reenvio de convites de conta de utilizador
- Adicionadas mais opções de etiquetagem de aplicações para objetos de Acesso à Identidade
- Atualização do modelo de Grupo para grupos de parceiros, de forma a incluir novos campos booleanos para o tipo de parceiro
- Atualização do modelo de Grupo para incluir uma lista de configurações de extensão canário
- Várias atualizações à nossa lista predefinida de listas brancas de dados + identidade + certificados para antivírus
- Ativação do suporte para HTTP/2
- Atualização do nosso Spring Boot para a versão mais recente, juntamente com várias outras dependências
- Implementados alertas de notificação para Acessos de Identidade Anómalos
- Ativada a compressão de respostas do servidor para os agentes
- Implementação de filtragem para a coluna "Sem Certificado de Confiança" da grelha de Acesso à Identidade na Aplicação Web, para as opções "Desconectado ao Obter Informações do Certificado" e "Tempo Esgotado ao Obter Informações do Certificado"
- Corrigido problema no nosso serviço de notificação de expiração de negócios de parceiros, para não enviar e-mails de expiração relativos a negócios já concluídos

Middleware 11.23

Recursos

- Atualizações da Lista de Permissões
  - Implementada a capacidade de criar uma exceção com o caminho e os argumentos do programa pai
  - Implementada a capacidade de criar uma exceção para corresponder a respostas de extorsão quando há apenas certificados confiáveis, corresponder apenas quando não há injeções relacionadas e corresponder apenas quando não há memória modificada
  - Implementada a capacidade de criar uma exceção para corresponder a gatilhos específicos de acesso a arquivos
- Implementada a configuração de grupo para liberar automaticamente licenças de agentes inativos
  - Atualizado o modelo de Grupo para ter uma configuração de quando liberar licenças de agentes inativos no grupo. As opções são 30/60/90 dias, ou desativar essa configuração
  - Atualizado o modelo de Agente para ter um novo status de inativo
  - Implementado serviço para liberar automaticamente as licenças de agentes inativos de acordo com a configuração de grupo
- Atualizado o endpoint para recuperação de respostas de extorsão para incluir o caminho e os argumentos do programa pai
  - O caminho e os argumentos do programa pai agora também estão incluídos nas contagens únicas de respostas de extorsão para a Aplicação Web, alertas de Notificação de Segurança e Resumos Executivos
- Atualizados nossos Relatórios de Resumo Executivo para separar o slide de Licenças em slides individuais de Licenças de Desktop e de Servidor
- Atualizado o modelo de Notificação de E-mail de Segurança e o serviço de Notificação de Segurança para incluir dois novos tipos de alerta
  - Modelo Comportamental Ajustado
  - Nova Versão do Agente
    - Quando as configurações de atualização gerenciada de um grupo são alteradas para desativar a atualização automática, uma notificação de Nova Versão do Agente é criada automaticamente para o grupo
- Atualizações de Função/Permissão de Usuário
  - Atualizadas as permissões de Gerente de Incidentes no modelo de Função para agora ter apenas visualização/edição de listas de permissões e regras de resposta silenciosa
  - Os grupos agora têm 3 funções padrão que não são editáveis pelo usuário:
    - Admin

    - Somente Leitura
    - Convidado
  - Usuários adicionados a um grupo por padrão recebem a Função de Convidado
- Implementados endpoints para o Modal de Ajuste do Processo de Utilitário do Navegador da Aplicação Web para gerenciar facilmente como os agentes em grupos devem responder aos processos utilitários do chrome
- Atualizado o endpoint do gráfico da página de Agentes para poder limitar as contagens aos agentes que se comunicaram nos últimos 30/60/90 dias
- Atualizado o alerta de e-mail de Atividade de Ransomware da Notificação de Segurança para incluir um link que redirecionará automaticamente os usuários para a página de Respostas de Extorsão com um filtro para mostrar as respostas às quais o alerta se referia
- Implementada a configuração de grupo para que os agentes de um grupo sejam executados ou não em modo de segurança
- Implementada uma opção de script powershell para instalação de agentes
- Atualização do nosso Spring Boot para a versão mais recente
- Diversas atualizações em nossa lista padrão de listas de permissões de dados + identidade + certificados para antivírus

Middleware 04.24

Funcionalidades

- Implementada a configuração de grupo e os endpoints relacionados para a configuração e gestão de configurações de proxy, de forma a auxiliar na implementação de agentes
- Atualizados os nossos endpoints de dados de telemetria para permitir visualizar todos os dados de telemetria ou apenas os dados diretamente relacionados com uma resposta a extorsão
- Implementada a configuração de grupo para ocultar automaticamente agentes em grupos quando uma licença é libertada de um agente, um agente é marcado como inativo, ou um agente conclui uma desinstalação
- Atualizados os links para o nosso painel nos nossos e-mails de notificação, de forma a incluir um parâmetro de URL utilizado para filtrar automaticamente os dados na grelha frontend relacionada, de modo a mostrar o que despoletou a notificação
- Atualizado o endpoint utilizado para o gráfico de Licenças de Agentes no frontend, de forma a incluir contagens para licenças de Desktop e de Servidor
- Implementados endpoints para a nova página frontend de Estado de Implementação do Cliente
- Atualizada a nossa afinação de processos para contemplar o Microsoft Edge WebView

Middleware 09.24

Recursos

- Implementados os endpoints para a nova configuração do Modo DMZ de Grupo
- Atualizados os endpoints de Registro de Negócio para permitir o registro de negócios multianuais com a possibilidade de pagamento antecipado ou pagamento anual para negócios multianuais
- Adicionada a capacidade de visualizar a análise de causa raiz para Acessos de Identidade
- Implementados Comportamentos Temporários Personalizados
- Atualizado o modelo de Usuário para salvar a configuração de ocultar ou exibir Licenças de Agente expiradas por padrão na grade de Licenças de Agente
- Atualizado o modelo de Notificação de Segurança e os endpoints/serviços relacionados para as novas opções de alerta de agente offline para agentes Parcialmente e Totalmente Offline
- Atualizações nos endpoints relacionados à adição das novas colunas no frontend, na grade de Agentes, para mostrar quando a licença atribuída expira e quando a licença foi atribuída ao agente
- Adicionada configuração ao Modelo de Grupo para que os agentes do grupo exibam o ícone do agente na bandeja do sistema da máquina do agente relacionado
- Atualizadas as consultas de grade no lado do servidor para permitir a inclusão de filtros com múltiplas condições para a mesma chave/coluna

Middleware 05.25

Funcionalidades

- Atualizado o modelo de Notificação de Vendas com novos tipos:
  - Os Parceiros Distribuidores podem receber alertas quando os seus subgrupos revendedores criarem um novo Registo de Negócio
  - Atividade de POC de Negócio de Parceiro
- Atualizado o processo de autenticação para permitir integração de SSO com o Microsoft Entra ID (Azure Active Directory)
- Atualizado o endpoint do instalador do agente para permitir um novo tipo de instalador para Native Cli
- Atualizados os endpoints para as novas atualizações do Parceiro Distribuidor
  - Adicionado um novo modelo de Partner in Motion
  - Atualizado o modelo de Registo de Negócio de Parceiro para adicionar a capacidade de os distribuidores aprovarem os negócios dos seus subgrupos revendedores
  - Adicionada a capacidade de os Parceiros Distribuidores editarem os descontos plurianuais dos seus subgrupos revendedores
  - Adicionada a capacidade de os distribuidores enviarem para si próprios orçamentos com o seu preço de distribuidor para o negócio de um subgrupo revendedor
  - Adicionado o requisito de, quando um subgrupo revendedor regista um negócio, ser necessário que o Acordo de Subgrupo Revendedor seja carregado pelo seu distribuidor principal na página de Gestão de Grupos de Distribuidores
- Atualizado o modelo de Função (Role) com um novo Gestor de Negócios de Parceiro para operações de registo de negócios, e atualizado cada endpoint relacionado para verificar as permissões
- Adicionado o endpoint para editar as definições de um grupo em massa
- Atualizado o nosso Spring Boot para a versão mais recente
- Melhoradas as consultas utilizadas na geração de relatórios executivos para reduzir o tempo necessário para gerar o relatório
- Movidas as nossas coleções de telemetria na base de dados para utilizar sharding
- Atualizada a consulta de agentes utilizada na grelha do painel para incluir se o agente é ou não um servidor
- Atualizado o endpoint /updateGroupAutomaticallyHideAgentsReactive para aplicar a atualização retroativamente aos agentes existentes
- Grandes atualizações de autenticação para permitir que os agentes chamem os nossos servidores REST através da nova autenticação OAuth alojada
- Adicionados novos endpoints para submissão de telemetria de DLL pelos agentes

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.