Prezado Senhor (a),

Seguem nossos pedidos de esclarecimentos técnico acerca do Edital PE 1301017 000049/2018, para que os mesmos possam ser encaminhados ao Pregoeiro dentro do prazo máximo de 08 (oito) dias, conforme artigo 48, §3º da Lei Federal nº 8.666.

QUESTIONAMENTOS:

1.3. A console de monitoração e configuração deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas as fermentas para a monitoração e controle da proteção dos dispositivos;

1.7. Deve permitir sincronização com o Active Directory (AD), para gestão de usuários e grupos integrados às políticas de proteção;
Não encontrado referência da integração com o AD.

1.10. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;
Não encontrado referência da criação de regras para usuários.

1.13. A console de gerenciamento deve permitir a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs;
Não encontrado referência para a configuração de níveis de acesso a console.

1.19. Permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;
Não encontrado a opção de exportação dos relatórios em CSV e PDF.

1.42. Deverá permitir exportar o relatório de logs de auditoria nos formatos CSV e PDF;
Não encontrado a funcionalidade.

1.47.2. Atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
Não encontrada a lista de aplicativos e suas categorias. O controle é feito manualmente.

1.47.3. Verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
Não encontrado a funcionalidade.

1.47.6. Detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
Funcionalidade não encontrada.

1.47.7. Deve possuir a opção de customizar, uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
Funcionalidade não encontrada.

1.48.1. Possuir proteção a vazamento ou perda de dados sensíveis, considerando o seu conteúdo ou o seu tipo real, além da possibilidade de avaliar a extensão do arquivo e múltiplos destinos como colocado abaixo;
Funcionalidade não encontrada.

1.48.2. Permitir a identificação de informações confidenciais, como números de passaportes ou outras informações pessoais identificáveis e/ou informações confidenciais mesmo que os documentos não tenham sido corretamente classificados, utilizando CCLs (Lista de Controle de Conteúdo);
Não possuem CCLs.

1.48.3. Possibilitar o bloqueio, somente registrar o evento na Console de Administração, ou perguntar ao usuário se ele ou ela realmente quer transferir o arquivo identificado como sensível;

1.48.4. Deve possuir listas de CCLs pré-configuradas com no mínimo as seguintes identificações:
1.48.4.1. Números de cartões de crédito;
1.48.4.2. Números de contas bancárias;
1.48.4.3. Números de Passaportes;
1.48.4.4. Endereços;
1.48.4.5. Números de telefone;
1.48.4.6. Códigos postais definidas por países como França, Inglaterra, Alemanha, EUA, etc;
1.48.4.7. Lista de e-mails;
Não possuem nenhuma CCL, tudo deve ser incluído manualmente.

1.48.5. Suportar adicionar regras próprias de conteúdo com um assistente fornecido para essa finalidade;

1.48.6. Permitir criar regras de prevenção de perda de dados por tipo verdadeiro de arquivo;

1.48.7. Possuir a capacidade de autorizar, bloquear e confirmar a movimentação de dados sensíveis e em todos os casos, gravar a operação realizada com as principais informações da operação;
Funcionalidades não encontradas.

1.49.5. Capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
Não achei referência das técnicas de exploração de vulnerabilidades. Eles conseguem proteger?

3.1.13. Windows Server 2016;
Não encontrado a referência de compatibilidade.

3.1.18. Amazon Linux;
Não encontrado a referência de compatibilidade.

3.1.26. Deve possuir integração com as nuvens da Microsoft Azure e Amazon Web Services para identificar as informações dos servidores instanciados nas nuvens;
Não encontrado a referência de compatibilidade.

3.2.6. Capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
Não encontrado a referência de atendimento.

Quaisquer informações sobre os questionamentos poderão ser dirigidas ao Pregoeiro, Ricardo Miranda, através do e-mail aisi@transportes.mg.gov.br.

Belo Horizonte, 28 de setembro de 2018.

Ricardo Miranda
Pregoeiro