JUSTIÇA FEDERAL
Tribunal Regional Federal da 1ª Região

CIRCULAR/NULIT N. 029 **Brasília, 01 de outubro de 2018.**

REFERÊNCIA: PREGÃO ELETRÔNICO N. 47/2018 - **PROCESSO:** 0004190-38.2016

Senhores Licitantes,

Em atenção às solicitações de esclarecimentos apresentadas, à Pregoeira, com base nas informações prestadas pelo Setor Requisitante, esclarece:

Pergunta 1:

Temos descrito no item 5.1.3. DO AGENTE DE PROTEÇÃO, especificamente nos subitens 5.1.3.1.8. e 5.1.3.1.9. as distribuições LINUX(Red Hat (x86/x64) e CentOS (x86/x64) respectivamente) que deverão ser suportadas pela solução ofertada. Nesse sentido, no item 5.1.3.3. é exigido que a solução deverá possuir IPS e Firewall de host. Entendemos que a solução ofertada deverá contemplar IPS e Firewall de host para proteção das máquinas LINUX, está correto o nosso entendimento?

Relacionado ao questionamento anterior, caso a resposta seja positiva, solicitamos o quantitativo de Servidores LINUX para o correto dimensionamento da solução a ser ofertada.

Resposta:

Devem ser observados os requisitos de compatibilidade descritos nos subitens 5.1.3.1.8, 5.1.3.1.9 e de funcionalidade descrito no subitem 5.1.3.3, aplicável aos sistemas operacionais previstos no item 5.1.3.1, quesitos válidos tanto para estações de trabalho quanto servidores.

O quantitativo atual de Servidores Linux ativos em 28/09 é de 539 unidades virtuais, aproximadamente 25 servidores físicos e aproximadamente 30 estações de trabalho Linux.

Cabe destacar que eventuais fornecimentos posteriores, decorrentes da ARP, deverão contemplar, nos preços a serem ofertados, quaisquer dos SOs listados em 5.1.3.1.

Pergunta 2:

O Item 5.1.3 DO AGENTE DE PROTEÇÃO em seu subitem 5.1.3.1 requisita o seguinte:

"5.1.3.1. Deverá ser plenamente compatível com as seguintes tecnologias de sistema operacional:

5.1.3.1.1. Windows Server 2003 sp2 (32/64-bit).

5.1.3.1.4. Windows XP sp2 / sp3 (x86/x64)."

Questionamento: Os itens 5.1.3.1.1 ao 5.1.3.1.4 se referem a plataformas com suporte já descontinuado pela Microsoft. Entendemos que por se tratarem de sistemas legados, a solução de antivirus a ser entregue em sua última versão possua limitações, o que também compromete a funcionalidade de Machine Learning, a qual fica impossibilitada de rodar em sistemas legados. Apenas para esses casos pontuais, entendemos que poderá ser entregue uma versão de software que não esteja em sua última versão e que não possua o módulo Machine Learning, desde que ainda possua atualizações constantes de vacinas do fabricante.

Está correto nosso entendimento?

Resposta:

Havendo limitação da versão mais atualizada do AGENTE DE PROTEÇÃO com relação à funcionalidade Machine Learning, em especial com relação a versões de SO com suporte descontinuado pelos respectivos fabricantes, a CONTRATADA poderá fornecer a versão mais atualizada do agente que mantenha compatibilidade com as plataformas previstas no subitem 5.1.3.1, garantindo ainda total compatibilidade com a solução de gerenciamento e atualização de vacinas e sem prejuízo das demais características de proteção contra vírus e agentes maliciosos.

Neste caso, alinhado ao subitem 3.1.30 das Obrigações da Contratada – Anexo VI do Edital, deverá ser garantido o fornecimento do upgrade do agente quando da atualização das plataformas, sem ônus para o contratante ou qualquer necessidade de licenciamento adicional.

Pergunta 3:

Para o subitem 1.3.3.7, o mesmo traz: "Deverá ser capaz de prover proteção contra invasão que explorem vulnerabilidades do sistema operacional do host ou dos aplicativos de terceiros instalados no mesmo."

Entendemos que a solução de proteção de endpoint deve oferecer mecanismos de prevenção contra as principais ameaças e vulnerabilidades. Embora a maioria das tecnologias de segurança sejam projetadas para identificar e parar os

estágios iniciais de um ataque é extremamente necessário mecanismos que possam identificar possíveis movimentações laterais no ambiente. Entendemos que a solução deva adicionar uma camada complementar de proteção que permita a descoberta de um atacante dentro do ambiente. Entendemos que a solução de proteção de endpoint deva contar com mecanismos capazes de distribuir iscas no ambiente que possam revelar a presença de um invasor dentro do ambiente como uma camada extra para a detecção do ataque. Está correto o nosso entendimento?

Resposta:

Devem ser observados os requisitos da solução descritos no Edital.

Pergunta 4:

Para o subitem 1.3.3.5.2, o mesmo traz: "Deverá ser capaz de monitorar tentativas de exploração de vulnerabilidades conhecidas, oferecendo blindagem dessas ações, para os casos de impossibilidade de atualização de Sistema Operacional ou Aplicativo relacionado;"

Entendemos que a solução de proteção de endpoint, para prover a blindagem das tentativas de exploração, deve disponibilizar de uma ferramenta que complemente as funcionalidades de antivírus, detectando e remediando ameaças persistentes avançadas. Está correto nosso entendimento?

Resposta:

A ferramenta deve prover recursos de monitoramento e bloqueio de vulnerabilidades conhecidas, mormente aquelas descritas no item 1.3.3 e seus subitens, seja por meio de recursos nativos ou complementares a esses.

Atenciosamente,

Assinado de forma digital por ELIZETE FERREIRA COSTA:80452809191
Dados: 2018.10.01 14:31:06 -03'00'

Elizete Ferreira Costa
Pregoeira