

Informação nº 22/2021 – STI

Brasília, 15 de outubro de 2021.

Processo nº. 2682/2021

Interessados: Tribunal de Contas do Distrito Federal; BRINFOR SOLUÇÕES EM TI LTDA.

Assunto: Verificação quanto à aderência ou não aos requisitos solicitados no Edital do Pregão Eletrônico nº 13/2021, referente à contratação de empresa especializada para fornecimento, instalação e configuração, em lote único, de solução de proteção de estações de trabalho e servidores de aplicação, com suporte técnico e garantia *on site* por período de 48 meses e treinamento na solução.

Senhor(a) Pregoeiro(a),

1. Trata-se de Informação em resposta ao Despacho-SELIC presente na peça n.º 66 do Processo n.º 2682/2021. O referido despacho solicita, por parte da equipe técnica responsável pela contratação, manifestação quanto ao atendimento ou não da documentação técnica complementar apresentada pela BRINFOR SOLUÇÕES EM TI LTDA (peça n.º 65), solicitada na Informação n.º 20/2021 – STI/SI (peça n.º 64).

2. Após análise de todos os itens e respectivas referências, a equipe técnica chegou à conclusão de que a solução não está completamente aderente ao que foi solicitado em Edital. A análise realizada pode ser verificada em documento anexo à atual Informação.

3. Por fim, é importante ressaltar que as funcionalidades solicitadas pelo Tribunal, no Edital do Pregão Eletrônico nº 13/2021, devem ser comprovadas por documentação técnica, declaração da própria fabricante do software ou imagens do software que realmente evidenciem o que foi solicitado. Para fins comprobatórios, não será aceita a simples declaração do licitante.

[assinado digitalmente]

Leonardo Ramos Paz

Integrante Técnico

ANEXO I

ITEM	ANÁLISE
1.1.1.1.9. O antivírus de <i>web</i> deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador;	
1.1.1.1.9.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou	Atende , conforme documentação apresentada na primeira matriz de compatibilidade e complementada com informações na segunda matriz de compatibilidade.
1.1.1.1.9.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;	Documentação insuficiente . A documentação apresentada não foi suficiente para comprovar essa funcionalidade. A comprovação dessa funcionalidade é importante, pois alguns ataques podem sobrecarregar o buffer do endpoint, o que pode ocasionar congelamento ou o reinício da aplicação.
1.1.1.1.12. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;	Atende . Na primeira matriz de compatibilidade, para a comprovação do item em análise, o licitante apresentou o link < https://support.eset.com/pt/melhores-praticas-para-se-proteger-contra-o-malware-filecoder-ransomware >, que trata sobre melhores práticas para a proteção contra ransomware, e o link < https://help.eset.com/ees/7/en-US/idh_config_dmon.html >, que apresenta uma funcionalidade chamada "Document protection", que escaneia documentos do Microsoft Office antes de serem abertos. Porém, a documentação não é clara com relação à análise de macros VBA. Além disso, a imagem e descrição apresentadas na documentação complementar também não ajudam muito na elucidação do item. Porém, no link presente em < https://help.eset.com/eei/1.6/en-US/process_scripts.html >, para a comprovação de outro item (1.1.1.1.18), percebeu-se a comprovação dessa funcionalidade.
1.1.1.1.18. Capacidade de executar varreduras em tempo real contra-ataques dirigidos a vulnerabilidades do navegador;	Atende , conforme imagem e descrição apresentada.
1.1.1.1.23. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em base local ou na nuvem da reputação das URLs acessadas;	Atende , conforme imagem e descrição apresentada.
1.1.1.1.26. Controle de Aplicações em ambiente Windows (Application Control);	Não atende . A tela apresentada habilita o controle de dispositivos, não o controle de aplicações.

1.1.1.1.27. Proteção avançada contra ransomware, com capacidade de reverter o incidente;	Atende parcialmente - Conforme imagem e descrição apresentada, é possível verificar que a solução possui proteção contra ransomware, porém não foi apresentada documentação que comprove a capacidade de reverter o incidente, com, por exemplo, técnicas de reversão de criptografia ou outros mecanismos.
1.1.1.1.28. Solução que simule o ambiente real do Tribunal, criando armadilhas para permitir que o malware execute ações em um ambiente totalmente isolado e seja bloqueado antes de atingir qualquer computador;	Documentação insuficiente. A documentação apresentada na primeira matriz de compatibilidade e na matriz complementar não é suficiente para comprovar o que foi solicitado.
1.1.1.1.29. Mitigação de exploração de vulnerabilidades em aplicações conhecidas;	Atende, conforme imagem e descrição apresentada.
1.1.1.1.32. Impedir técnicas de manipulação de memória (Memory Exploit Mitigation);	Atende. Documentação em < https://help.eset.com/ees/8/pt-BR/idh_config_threat_sense.html?zoom_highlightsub=memoria >
1.1.1.1.47. Caso o servidor de gerenciamento seja appliance, será aceita apenas a modalidade virtual e deverá ser instalado em:	Atende, conforme compromisso do próprio licitante.
1.1.1.1.47.1. PROXMOX/KVM;	
1.1.1.1.47.2. Ambiente VMware, desde que a contratada implante todo o ambiente necessário para a execução, que deverá contemplar, no mínimo:	
1.1.1.1.47.2.1. Servidor de, no máximo 2U, a ser instalado no rack do TCDF, com especificações necessárias para a correta execução da aplicação;	
1.1.1.1.47.2.2. Licenciamento completo para execução do VMware e do appliance de gerenciamento, incluindo sistema operacional e demais softwares ou hardwares necessários;	
1.1.1.1.55. Permitir a instalação de servidores de gerenciamento adicionais;	Atende. Após reanálise da documentação encaminhada na primeira matriz de compatibilidade, percebeu-se que a solução

	permite que serviços possam ser separados em servidores adicionais.
1.1.1.1.64.2. Remediação de vulnerabilidades aplicando patches, de forma remota, via console de gerenciamento;	Não atende. De acordo com a documentação apresentada inicialmente, complementada pela tela apresentada, não fica clara a atualização de aplicativos já instalados. A documentação inicial trata de atualização do sistema operacional e instalação de software de terceiros, porém não faz referência à atualização de software de terceiros.
1.1.1.1.66. Suportar redirecionamentos dos logs para um servidor de log;	Atende, conforme imagem e descrição apresentada.
1.1.1.1.68. Atualização incremental, remota e em tempo real das vacinas da solução;	Documentação insuficiente. Apesar de o licitante declarar que a solução funciona como solicitado pelo Tribunal, não foi apresentada nova documentação, nem declaração do próprio fabricante.
1.1.1.1.71. As atualizações das configurações e das definições de vírus não poderão utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e deverá ser feito sem requerer reinicialização do computador ou serviço para aplicá-la;	Não atende. Segundo o item em análise, "(...) deverá ser feito sem requerer reinicialização do computador ou serviço para aplicá-la". Conforme imagem apresentada, em determinado momento, a atualização do produto pode requerer a reinicialização do computador. Inclusive, há uma opção que pode ser selecionada para permitir a reinicialização automática quando necessário. Por fim, segundo a própria imagem apresentada, para ser concluída, a instalação poderá esperar até a próxima reinicialização para ser concluída.
1.1.1.1.80. Deve exibir todos ou os principais detalhes do incidente em uma única página (EDR), contendo no mínimo: 1.1.1.1.80.1. Status do incidente; 1.1.1.1.80.2. Escopo impactado; 1.1.1.1.80.3. Quantidade de estações de trabalho impactadas; 1.1.1.1.80.4. Quantidade de servidores impactados; 1.1.1.1.80.5. Quantidade de usuários impactados; 1.1.1.1.80.6. Data e hora da detecção; 1.1.1.1.80.7. Modelo(s) de detecção acionado(s);	Não atende. A funcionalidade de EDR não ficou evidenciada nas documentações encaminhadas inicialmente nem na documentação complementar. Conforme apontado no item 1.1.1.1.82, poderia ter sido evidenciado com uma cena real de ataque, onde as informações solicitadas fossem apresentadas.
1.1.1.1.82. A solução deve ter capacidade de apresentar a visibilidade completa do vetor de ataque, disseminação e	Não atende. Apesar das imagens apresentadas, não foi demonstrada uma cena real de ataque, na qual seja possível visualizar, de forma completa, o vetor de ataque, disseminação e extensão do impacto de ameaças avançadas.

extensão do impacto de ameaças avançadas;	
1.1.1.1.83. Durante o processo de análise da cadeia de processos, deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante;	Atende , conforme imagem e descrição apresentada.
1.1.1.1.84. Após o vencimento das licenças, mesmo que sem atualizações, a solução deverá continuar funcionando;	Documentação insuficiente. Apesar de o licitante declarar que a solução funciona como solicitado pelo Tribunal, não foi apresentada nova documentação, nem declaração do próprio fabricante.
1.1.2.1.3. Possibilitar a criação de uma mídia (pendrive, CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;	Atende , conforme imagem e descrição apresentada.
1.1.2.1.9. Possibilitar que, caso o computador cliente saia da rede corporativa, seja ativada política alternativa na qual a estação de trabalho possa ser atualizar diretamente no site do fabricante;	Atende , conforme imagem e descrição apresentada.
1.1.3.1.2. A solução deverá ser compatível e homologada, no mínimo, para os seguintes sistemas operacionais e versões (64 bits): 1.1.3.1.2.1. Ubuntu Server 14.04 e superiores; 1.1.3.1.2.2. Windows Server 2008 e superiores; 1.1.3.1.2.3. CentOS 6.6 e superiores;	Não atende. De acordo com a documentação apresentada em < https://help.eset.com/efs/8.1/en-US/system_requirements.html >, a solução não foi testada para funcionar com Ubuntu 14.04 LTS e CentOS 6.6. Para atender a este item, deveria ter sido apresentada outra documentação que demonstrasse que a solução é aderente a essas versões de Sistemas Operacionais. A simples declaração do licitante não possui força comprobatória maior que uma documentação oficial ou declaração do próprio fabricante para este item. Essa compatibilidade é importante, pois o Tribunal possui sistemas legados instalados nessas versões de sistemas operacionais.
1.1.3.1.3. A solução deve possuir funcionalidade de realizar verificações de segurança em ambientes virtualizados por KVM ou PROXMOX;	Atende , conforme imagem e descrição apresentada.
1.1.3.1.6. Proteção de hosts docker e contêineres em ambiente Linux;	Não atende. A documentação apresentada não demonstra a funcionalidade de segurança em contêineres, com por exemplo, o scanning de contêineres docker e respectivas imagens. A documentação também não demonstra se o antivírus reconhece determinada VM como um host docker.

1.1.3.1.9. Deve ser capaz de executar rastreamento nos hosts e fornecer lista de recomendações de segurança para softwares que estiverem instalados, bem como para o sistema operacional;	Atende parcialmente - Na imagem apresentada, não é possível visualizar as recomendações de segurança para software, mas, tão somente, para o sistema operacional.
1.1.3.1.10. Permitir atuar no modo “em linha” para bloqueio de ataques ou modo “escuta” para monitoração e alertas;	Não respondido
1.1.3.1.14. Possuir a capacidade de criação de regras customizadas para proteger aplicações desenvolvidas pelo cliente;	Atende , conforme imagem e descrição apresentada.
1.1.3.1.15. Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;	Atende , conforme imagem e descrição apresentada.