ESCLARECIMENTO PREGÃO PRESENCIAL Nº 38/2018
Processo nº 04766/2018 - SC 034919

Objeto: Contratação de empresa especializada para prestação de serviço continuado de Solução Integrada de Serviços Gerenciados de Segurança, composta por: solução de WAF (Web Application Firewall); solução APT (Advanced Persistent Threat); gestão de vulnerabilidades; visibilidade total de logs, redes e informações; monitoramento e resposta a incidentes de segurança da informação através de Centro de Operações; e treinamento, tudo de acordo e conforme Termo de Referência (Anexo I) do Instrumento Convocatório.

Pergunta 1: Para fins de habilitação no certame, é exigida de cada empresa licitante a realização de vistoria técnica nas instalações dos CONTRATANTES em Brasília e em São Paulo, para conhecimento do ambiente computacional e verificação de eventuais requisitos físicos para o devido provimento dos serviços.
Questionamos se a visita técnica será realizada somente nas instalações de Brasília, ou também nas instalações do Estado de São Paulo?

Resposta 1: A vistoria deverá ocorrer nas instalações de Brasília.

Pergunta 2: Solicitamos mais um pedido de esclarecimento com o intuito de retiradas dos itens abaixo/alteração, com o intuito de ampliar a competição desse certame, visto que esses pontos são uma cópia da solução do fabricante McAfee e podem facilmente localizados no documento abaixo:

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26801/pt_BR/emg_1050_mg_0-12_pt-br.pdf

O fabricante que trabalhamos é um dos líderes do GARTNER para esse tipo de solução e apenas aqui em Brasília possui sua solução instalada no INSS, AGU, PETROBRAS, DATAPREV, PGR, Banco Central, CJF, CADE, entre outros

Os itens que solicitamos a retirada/alteração pois da forma como está apena a McAfee atende são:

1.*1.3.1 Windows 10, Windows 8.1, Windows 8, Windows 7, Sierra 10.12.x, El Captain 10.11.x, Yosemite 10.10.x.*

1.1.4.1 Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Storage Server 2012, Windows 2008 R2 (Standard/Datacenter/Enterprise/Web), Deve inclusive suportar o modo Server Core, Sierra 10.12.x, El Captain 10.11.x, Yosemite 10.10.x;

1.1.6 Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais para a composição do pacote.

1.1.8 Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de: Relatórios, Dashboards, Políticas, Configuração, Instalação/Desinstalação;

1.1.8.8 Este módulo deve estar público para o desenvolvimento da comunidade via Github;

1.1.14 Deve ser possível incluir exclusões por: Processo, Nome, Caminho do Arquivo, Hash MD5. E Em Módulo chamador: Nome, Caminho, Hash MD5, Signatário Digital e Proteção de acesso.

1.1.15 Deve fornecer regras de proteção nativamente, ou seja, definida pelo fabricante da solução, no mínimo, para: Acesso remoto a pastas locais, Alteração políticas de direitos dos usuários, Alterar os registros de extensão dos arquivos, Criação de novos arquivos na pasta Arquivo de Programas, Criação de novos executáveis na pasta Windows, Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema, Criar ou Modificar remotamente arquivos ou pastas, Desativar o editor de registro e o gerenciador de tarefas, Executar arquivos das pastas do usuário, Execução de scripts pelo host de script do Windows, Instalar objetos de ajuda a navegação ou extensões de shell, Instalar novos CLSIDs, APPIDs e TYPELIBs, Modificar configurações de rede, Modificar configurações do Internet Explorer, Modificar processos principais do Windows, Navegadores iniciando programas da pasta de downloads e Registrar programas para execução automática;

1.1.16 As regras especificadas devem permitir o seu: Bloqueio, ou, Informação, ou, Bloqueio e Informação;

1.1.17 Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros: Processos, Nome do processo, Hash MD5, Assinatura Digital, Usuário, Arquivos, Criação, Deletar, Executar, Alteração de permissão, Leitura, Renomear, Escrever, Chave de Registro, Escrever, Criar, Deletar, Ler, Enumerar, Carregar, Substituir, Restaurar, Alterar permissão, Valor de Registro, Ler, Criar, Deletar, Processo, Qualquer acesso, Criar thread, Modificar, Terminar, Executar e deve permitir a criação de exclusões;

1.1.26 Deve permitir a configuração do nível de agressividade da análise entre: Muito Baixo, Baixo, Médio, Alto e Muito Alto;

1.1.55 O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros: Ação; bloquear, permitir, direção, ambas, entrada, saída, protocolo, qualquer protocolo, protocolo IP, Ipv4, Ipv6, protocolo não-IP, tipo de conexão, rede sem fio, rede cabeada, rede virtual, especificação da rede, endereço IP, subnet, range, FQDN, protocolo de transporte, todos, ICMP, ICMPv6, TCP, UDP, STP, GRE, IGMP, IPSEC AH, IPSEC ESP, Ipv6 in Ipv4, ISIS over Ipv4, L2TP, agendamento, dias da semana, hora inicio, hora fim e aplicações;

1.1.55.1 Deve possuir as seguintes proteções: Generic Buffer Overflow Protection, Suspicious Caller and Caller Validation, Exploit Prevention, Access Protection, Data Execution Protection, Generic Privilege Escalation Protection e Proteção Web;

1.1.56 O módulo de Controle Web deve possuir as funcionalidades de permitir o bloqueio de browsers não suportados, dentre eles: Opera, Safari for Windows, Netscape, Maxthon, Flock, Avant Browser, Deepnet Explorer e PhaseOut;

1.1.59 Deve possuir, no mínimo, as seguintes categorias: Browser Exploits, download maliciosos, sites maliciosos, Phishing, pornografia, Hacking/Computer Crime, Spyware/Adware/Keyloggers, Anonymizer, Anonymizer Utilities, Alcohol, Blogs/Wiki, Business, Chat, Content Server, Dating, Dating/Social Networking, Digital Postcards, Discrimination, Drugs, Education, Entertainment, Extreme, Fashion, Finance, For Kids, Forum, Gambling, Game/Cartoon Violence, Games, General News, Government/Military, Gruesome Content, Health, Historical Revisionism, History, Humor/Comics, Illegal UK, Incidental Nudity, Information Security, Instant Messaging, Interactive Web Applications, Internet Radio/TV, Internet Services, Job Search, Major Global Religions, Marketing/Merchandising, Media Downloads, Media Sharing, Messaging, Mobile Phone, Moderated, Motor Vehicles, Non-Profit/Advocacy/NGO, Nudity, Online Shopping, P2P/File Sharing, Parked Domain, Personal Network Storage, Personal Pages, Pharmacy, Politics/Opinion, Portal Sites, Potential Criminal Activities, Potential Illegal Software, Potentially Unwanted Programs, Profanity, Professional Networking, Provocative Attire, Public, Information, Real Estate, Recreation/Hobbies, Religion/Ideology, Remote Access, Residential IP Addresses, Resource Sharing, Restaurants, School Cheating Information, Search Engines, Sexual Materials, Shareware/Freeware, Social Networking, Software/Hardware, Spam URLs, Sports, Stock Trading, Streaming Media, Technical Information, Technical/Business, Forums, Text Translators, Text/Spoken Only, Tobacco, Travel, Uncategorized, Usenet News, Violence, Visual Search Engine, Weapons, Web Ads, Web Mail, Web Meetings, Web Phone.

1.1.68 Caso o módulo detecte que exista um McAfee Web Gateway na rede, deverá deixar a análise a cargo deste último.

1.1.75 Dentre os comportamentos maliciosos, deve ser capaz de BLOQUEAR: acesso local a partir de cookies, a criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs, a riação de arquivos em qualquer local de rede, a criação de novos CLSIDs, APPIDs e TYPELIBs, a criação de threads em outro processo, a desativação de executáveis críticos do sistema operacional, Leitura/Exclusão/Gravação de arquivos visados por Ransomwares, Gravação e Leitura na memória de outro processo Modificação da política de firewall do Windows, Modificação da pasta de tarefas do Windows, Modificação de arquivos críticos do Windows e Locais do Registro, Modificação de arquivos executáveis portáteis, Modificação de bit de atributo oculto, Modificação de bit de atributo somente leitura, Modificação de entradas de registro de DLL AppInit, Modificação de locais do registro de inicialização, Modificação de pastas de dados de usuários, Modificação do local do Registro de Serviços, Suspensão de um processo, Término de outro processo;

1.1.85 Deve permitir integração com base global de virus – VirusTotal – para comparação e se o arquivo sob análise já foi detectado por outro fabricante;

1.1.101 Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca: Endereço IP Local; Hash do processo em execução; ID do processo; Status da transação TCP; Número da porta que originou o pacote de rede; Nome do arquivo; última data de gravação do arquivo; Data de Criação do arquivo; Data de deleção do arquivo; Versão do Sistema Operacional; Nome do Grupo de usuários; Se o grupo é local; SID do grupo; MAC de origem; MAC de destino; FLAGS TCP (ACK, SYN, RST e FIN); Número de transação TCP; Kernel Time; User Time; Comando que iniciou o processo; Quantidade de RAM utilizada pelo processo; Quantidade de Threads criadas pelo processo; MD5 do processo; SHA-1 do processo; Valor da chave de registro; Caminho da chave de registro;

1.1.114 Deve realizar análise heurística (IE-FFx-Acrobat Emulation) baseado em análise estatística comportamental da geometria do arquivo, semântica e comportamento do código.

1.1.165 Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura.

Resposta 2: *Favor desconsiderar o item 1.1.6, porém para as demais clausulas, estão de acordo com a necessidade da CNI, e que existem outras tecnologias (não só da MacAfee) que atendem a demanda.*

Para todos os efeitos este documento passa a integrar o edital em referência.

Brasília, 14 de dezembro de 2018.

Comissão Permanente de Licitação - CPL