Esclarecimento 10/02/2016 18:47:51

Empresa VERT Tecnologia Performance Resultados
Seguem pedidos de esclarecimento para o pregão supra. 1 -Com relação ao Anexo I do edital item 1.1.10. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): d) Por linha-de-comando, parametrizável, com opção de limpeza; Entendemos que se a varredura já estiver determinada por padrão da solução como Limpeza, atendemos o item, esta correto o nosso entendimento?
2 -Com relação ao Anexo I do edital item 1.1.10. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): e) Automáticos do sistema com as seguintes opções: Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); Entendemos que a solução que por padrão execute ao mesmo tempo a movimentação do arquivo infectado para a Quarentena, renomeie o arquivo e negue o acesso ao mesmo, está atendendo ao item. Está correto nosso entendimento?
3 - Com relação ao Anexo I do edital itens 1.1.13, 1.1.14 e 1.1.15, onde são destacadas a reputação de URL. Entendemos que uma solução que atenda de forma mais granular a este requisito, fazendo a reputação de arquivos dentro de um site / domínio, evitando que um domínio inteiro seja bloqueado apenas por uma interpretação macro da reputação de uma de suas páginas atende ao item, está correto o entendimento?
4 - Com relação ao Anexo I do edital, item 1.1.17. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante; Entendemos que a partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal-intencionado, atenderemos ao item. Está correto nosso entendimento?
5 - Com relação ao Anexo I do edital, item 1.1.19. Deve permitir a adição automática às listas de exclusão/arquivos conhecidos de modo a evitar novas detecções dos arquivos no ambiente de gestão da solução de endpoint; Entendemos que a adição de arquivos, diretórios, tipos de arquivos sendo realizada pelo administrador da ferramenta atende ao item. Está correto nosso entendimento?
6 - Com relação ao Anexo I do edital, item 1.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: a) Suse Linux Enterprise 9, 10 e 11; b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0; c) Centos 4.0, 5.0 e 6.0. Entendemos que com o End Of Life de vários sistemas operacionais solicitados o suporte fica prejudicado pela falta de continuidade de seu desenvolvimento, conforme pode ser visto no seu link abaixo, desta forma, entendemos que o atendimento aos sistemas operacionais em linha de produção e atualização atende ao requisito. Está correto nosso entendimento?
http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00003.html
https://access.redhat.com/support/policy/updates/errata
http://stephane.lesimple.fr/fedora/packages-search/ Comprovação MAC OS
https://support.symantec.com/en_US/article.tech195325.html
https://en.wikipedia.org/wiki/History_of_Mac_OS Release Notes:
https://support.symantec.com/en_US/article.TECH163829.html
https://support.symantec.com/en_US/article.TECH231877.html LINUX
https://support.symantec.com/en_US/article.TECH101598.html
https://support.symantec.com/en_US/article.TECH223240.html
7 - Com relação ao Anexo I do edital, item 1.2.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação; Entendemos que a proteção não será exercida pela capacidade de análise em profundidade dos arquivos compactados, pois, antes de ser verificado o último nível de compactação obrigatoriamente todos os níveis anteriores já foram verificados, desta forma, entendemos que a verificação em até 10 níveis de compactação atende ao requisito. Está correto nosso entendimento?
8 - Com relação ao Anexo I do edital, item 1.3.3. A solução anti-malware deverá possuir a capacidade de negar acesso aos arquivos contaminados; Entendemos que a solução que por padrão execute ao mesmo tempo a movimentação do arquivo infectado para a Quarentena,

renomeie o arquivo e negue o acesso ao mesmo, está atendendo ao item. Está correto nosso entendimento?
##
########## 9 - Com relação ao Anexo I do edital, item 1.3.16. Caso a solução anti-malware necessite de um servidor dedicado, a mesma deverá possuir no mínimo os seguintes requisitos: ... b) Deverá permitir o escalonamento Round Robin, isto é, se o primeiro servidor estiver ocupado, a solicitação é enviada ao próximo servidor disponível; Entendemos que a solução deverá ser capaz de entregar a alta disponibilidade de comunicação entre os clientes e os servidores da solução onde quando um servidor estiver muito ocupado ou parado, as requisições deverão ser encaminhadas automaticamente para o próximo servidor disponível da solução, esta configuração pode ser facilmente configurada em uma lista de servidores e prioridades de conexão. Está correto nosso entendimento?
##
########## 10 - Com relação ao Anexo I do edital, item 1.3.17. A solução anti-malware deverá suportar, no mínimo, 4 (quatro) conexões de, no mínimo, 10 Gbps (dez gigabit por segundo) e o acesso simultâneo de, no mínimo, 50 usuários; O atendimento a este item dependera do sizing realizado da solução para o ambiente computacional do CJF e também da arquitetura de rede e dados do mesmo, está correto o nosso entendimento?
##
########## 11 - Com relação ao Anexo I do edital, item 1.3.40. Da remoção: … c) Proteção contra desinstalação e desativação não autorizada do produto. Entendemos que uma solução para proteção de repositórios de dados (storage) deverá somente ser administrada por administradores de redes ou analistas de segurança do CJF, não havendo nenhuma intervenção ou contado dos usuários finais com a console de gerencia da solução. Por este motivo entendemos que a característica de Proteção contra desinstalação e desativação não autorizada do produto é desnecessária, uma vez que apenas os administradores do ambiente computacional do CJF terão acesso ás consoles de gerencia da solução, está correto o nosso entendimento?
##
########## 12 - Com relação ao Anexo I do edital, item 1.6.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente; Conseguimos a partir de ferramentas da própria solução desinstalar clientes de terceiros e entendemos que este procedimento atende ao item em questão, está correto o nosso entendimento?
##
########## 13 - Com relação ao Anexo I do edital, item 1.6.19. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; 14 - A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal intencionado, atenderemos ao item. Está correto nosso entendimento?
##
########## 15 - Com relação ao Anexo I do edital, item 1.6.23. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal-intencionado, atenderemos ao item. Está correto nosso entendimento?
##
########## 16 - Com relação ao Anexo I do edital, item 1.6.38. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto. A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal intencionado, atenderemos ao item. Está correto nosso entendimento?
##
########## 17 - Com relação ao Anexo I do edital, item 1.8.12. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente; Entendemos que a proteção contínua do endpoint é determinada pelas assinaturas existentes em sua base e tais regras específicas são inerentes a cada ambiente de produção cabendo ao administrador da solução determinar sua necessidade ou não, está correto o nosso entendimento?
##
########## 18 - Com relação ao Anexo I do edital, item 1.8.23. Deve permitir a

emissão de alertas via smtp e snmp; Entendemos que o envio dos Logs para um Syslog, possibilitando vários níveis de detalhamento chegando a níveis de auditoria juntamente com o envio de alertar em SMTP, atende ao item. Assim como a possibilidade de validar a saúde do Servidor de gerencia a partir da própria console, possibilitando a notificação conforme desejar. Está correto o nosso entendimento?
##
################ 19 - Com relação ao Anexo I do edital, item Em atenção aos itens 1.8.32, 1.8.33, 1.8.34, 1.9.17, 1.9.18, 1.9.19, entendemos que o acesso a console de administração limitada a partir de vários níveis de acesso, impossibilitando que usuários interfiram nas configurações estabelecidas pelo ADM da solução, possibilitando acesso somente de leitura e visualização de relatórios, assim como, a possibilidade de entrega de relatórios WEB para acompanhamento e check da saúde do ambiente atende aos itens. Está correto nosso entendimento?
##
################ 20 - Com relação ao Anexo I do edital, item 1.9.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: … b) Atributos do certificado utilizado para assinatura digital do executável; … d) Base de assinaturas de certificados digitais válidos e seguros. Entendemos que uma solução que tenha tais proteções verificadas a partir de assinaturas recebidas diretamente do site do fabricante, atende aos requisitos solicitados. Está correto nosso entendimento?
##
################ 21 - Com relação ao Anexo I do edital, item 1.10.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão: … s) Infravermelho; t) Bluetooth; Entendemos que uma solução que se apresente protegendo a manipulação das informações enviadas aos dispositivos USB, atende ao requisito, uma vez que os dispositivos trabalhando sob Infravermelho e Bluetooth, apresentam-se ao sistema operacional como um drive USB. Está correto nosso entendimento?
##
################ 22 - Com relação ao Anexo I do edital, item 2.2.26. Deve ser compatível com IPV6; Entendemos que por se tratar de um software instalado e integrado ao Software de Mensageria Exchange, onde a proteção é executada sob as caixas postais dos usuários, desta forma, tal funcionalidade é implementada no Software de mensageira. Entendemos que atendemos ao item, está correto nosso entendimento?
##
################ 23 - Com relação ao Anexo I do edital, item 2.3.18. Deve permitir verificar mailbox stores e public foldes; e 2.3.19. Deve permitir definir a "idade mínima" das mensagens a serem verificadas; Entendemos que por se tratar de um software instalado e integrado ao Software de Mensageria Exchange, onde a proteção é executada sob as caixas postais dos usuários, desta forma, tal funcionalidade é implementada no Software de mensageira. Entendemos que atendemos ao item, está correto nosso entendimento?
##
################ 24 - Com relação ao Anexo I do edital, item 2.3.74. A solução de anti-spam deverá submeter e-mails suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na análise das informações: a) Processos de autostart; b) Modificações de arquivos de sistema; c) Serviços criados e modificados; d) Atividade de rede suspeita; e) Modificações de registros. Entendemos que estes subitens não se aplicam a esta aplicação, uma vez que sua funcionalidade primária é proteção ao tráfego de mensagens, nada relacionado ao endpoint. Em contra partida durante a implantação da solução em um hardware é feito um hardening do sistema operacional. Entendemos que desta forma estamos atendendo ao item, nosso entendimento está correto?
##
################ 25 - Com relação ao Anexo I do edital, item 2.3.81. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro; Entendemos que a criação de área de suspeitos de virus quarentenados no gateway, juntamente com área de quarentena por usuários, assim como, um folder de incidentes de quarentena, atendem ao item. Está correto nosso entendimento?
##
################ 26 - Com relação ao Anexo I do edital, item 2.3.125. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio; Entendemos que as diversas possibilidades como SPF, Sender ID Authentication, Good e Bad Sender, DNS-based IP reputation. Atendemos aos requisitos, está correto nosso entendimento?
##
################ 27 - Com relação ao Anexo I do edital, item 2.3.176. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual; Entendemos que as limitações de uso de CPU não fazem parte deste software, uma vez que o appliance é dedicado e sem interferência direta ao usuário final. Está correto nosso entendimento?
##

################ 28 - Com relação ao Anexo I do edital, item 3 e seus subitens, entendemos que os itens direcionados como Bloqueio pela solução contra ataques de APT, uma fez que tais funcionalidades sejam executadas pelo módulo de Endpoint, o qual faz uso e é o mesmo agente de proteção dos Endpoints podem ser alertadas pela solução de APT, mas efetivamente executadas a partir da solução de Endpoint. Encontra-se em roadmap a execução das tarefas de bloqueio a partir da console de gerenciamento da Solução contra APTs, com previsão para lançamento da nova versão para o mês de março de 2016, no entanto, hoje já é possível inserir um equipamento em quarentena, colocando-o isolado dos demais quando verificado seu comprometimento. Entendemos que conforme descrito acima, atendemos o item 3 e seus subitens, está correto o nosso entendimento?
##
################ 29 - 3.23. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS, Messenger, eBuddy,ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP; Entendemos que determinados aplicativos são muito específicos e com particularidades das mais diversas, desta forma, detectando-se a tecnologia na qual se baseiam os aplicativos e aplicações, estaremos atendendo ao item. Está correto nosso entendimento?
##
################ 30 - Com relação ao Anexo I do edital, item 3.70. Capacidade de salvar uma investigação antes de ser finalizada; 3.71. Capacidade de restaurar uma investigação para continuá-la ou consultá-la; Entendemos que será possível entregar a solução de forma virtualizada, em conjunto com o hardware dimensionado para a execução da proteção, entendemos ainda que uma vez entregue a solução virtualizada, não existe limite na quantidade de servidores scanners a serem implementados e sem custo extra para o CJF, possibilitando um ganho de escalabilidade e proteção. Está correto nosso entendimento?
##
################ 31 - Com relação ao Anexo I do edital, itens itens 3.108.8., 3.109.8, 3.110.8 Entendemos que o acesso a console de administração limitada a partir de vários níveis de acesso, impossibilitando que usuários interfiram nas configurações estabelecidas pelo ADM da solução, possibilitando acesso somente de leitura e visualização de relatórios, assim como, a possibilidade de entrega de relatórios WEB para acompanhamento e check da saúde do ambiente atende aos itens. Está correto nosso entendimento?
##
################ 32 - Com relação ao Anexo I do edital, item 3.108.16. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações: a) Uso de CPU b) Uso de Disco; c) Uso de Memória; d) Tráfego malicioso analisado; e) Todo o tráfego analisado. Entendemos que a funcionalidade de verificação da saúde da solução atende ao requisito, uma vez que se trata de uma solução dedicada e para cada fabricante os ponteiros de validação podem ser diferentes ou até mesmo com pesos distintos. Está correto nosso entendimento?
##
################ 33 - Com relação ao Anexo I do edital, item 3.110.5. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de health-check e log da base de dados; Entendemos que a entrega das informações em gráficos e relatórios distintos a partir do módulo de relatórios da solução atende ao item. Está correto nosso entendimento?

Resposta 10/02/2016 18:47:51

1 -Com relação ao Anexo I do edital item 1.1.10. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): d) Por linha-de-comando, parametrizável, com opção de limpeza; Entendemos que se a varredura já estiver determinada por padrão da solução como Limpeza, atendemos o item, esta correto o nosso entendimento? RESPOSTA: Não está correto. 2 -Com relação ao Anexo I do edital item 1.1.10. Deve permitir diferentes configurações de detecção (varredura ou

rastreamento): e) Automáticos do sistema com as seguintes opções: Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); Entendemos que a solução que por padrão execute ao mesmo tempo a movimentação do arquivo infectado para a Quarentena, renomeie o arquivo e negue o acesso ao mesmo, está atendendo ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 3 - Com relação ao Anexo I do edital itens 1.1.13, 1.1.14 e 1.1.15, onde são destacadas a reputação de URL. Entendemos que uma solução que atenda de forma mais granular a este requisito, fazendo a reputação de arquivos dentro de um site / domínio, evitando que um domínio inteiro seja bloqueado apenas por uma interpretação macro da reputação de uma de suas páginas atende ao item, está correto o entendimento? RESPOSTA: Conforme o edital. 4 - Com relação ao Anexo I do edital, item 1.1.17. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante; Entendemos que a partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal-intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 5 - Com relação ao Anexo I do edital, item 1.1.19. Deve permitir a adição automática às listas de exclusão/arquivos conhecidos de modo a evitar novas detecções dos arquivos no ambiente de gestão da solução de endpoint; Entendemos que a adição de arquivos, diretórios, tipos de arquivos sendo realizada pelo administrador da ferramenta atende ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 6 - Com relação ao Anexo I do edital, item 1.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: a) Suse Linux Enterprise 9, 10 e 11; b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0; c) Centos 4.0, 5.0 e 6.0. Entendemos que com o End Of Life de vários sistemas operacionais solicitados o suporte fica prejudicado pela falta de continuidade de seu desenvolvimento, conforme pode ser visto no seu link abaixo, desta forma, entendemos que o atendimento aos sistemas operacionais em linha de produção e atualização atende ao requisito. Está correto nosso entendimento? http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00003.html https://access.redhat.com/support/policy/updates/errata http://stephane.lesimple.fr/fedora/packages-search/ Comprovação MAC OS https://support.symantec.com/en_US/article.tech195325.html https://en.wikipedia.org/wiki/History_of_Mac_OS Release Notes: https://support.symantec.com/en_US/article.TECH163829.html https://support.symantec.com/en_US/article.TECH231877.html LINUX https://support.symantec.com/en_US/article.TECH101598.html https://support.symantec.com/en_US/article.TECH223240.html RESPOSTA: Conforme o edital. 7 - Com relação ao Anexo I do edital, item 1.2.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação; Entendemos que a proteção não será exercida pela capacidade de análise em profundidade dos arquivos compactados, pois, antes de ser verificado o último nível de compactação obrigatoriamente todos os níveis anteriores já foram verificados, desta forma, entendemos que a verificação em até 10 níveis de compactação atende ao requisito. Está correto nosso entendimento? RESPOSTA: Não está correto. 8 - Com relação ao Anexo I do edital, item 1.3.3. A solução anti-malware deverá possuir a capacidade de negar acesso aos arquivos contaminados; Entendemos que a solução que por padrão execute ao mesmo tempo a movimentação do arquivo infectado para a Quarentena, renomeie o arquivo e negue o acesso ao mesmo, está atendendo ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 9 - Com relação ao Anexo I do edital, item 1.3.16. Caso a solução anti-malware necessite de um servidor dedicado, a mesma deverá possuir no mínimo os seguintes requisitos: ... b) Deverá permitir o escalonamento Round Robin, isto é, se o primeiro servidor estiver ocupado, a solicitação é enviada ao próximo servidor disponível; Entendemos que a solução deverá ser capaz de entregar a alta disponibilidade de comunicação entre os clientes e os servidores da solução onde quando um servidor estiver muito ocupado ou parado, as requisições deverão ser encaminhadas automaticamente para o próximo servidor disponível da solução, esta configuração pode ser facilmente configurada em uma lista de servidores e prioridades de conexão. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 10 - Com relação ao Anexo I do edital, item 1.3.17. A solução anti-malware deverá suportar, no mínimo, 4 (quatro) conexões de, no mínimo, 10 Gbps (dez gigabit por segundo) e o acesso simultâneo de, no mínimo, 50 usuários; O atendimento a este item dependera do sizing realizado da solução para o ambiente computacional do CJF e também da arquitetura de rede e dados do mesmo, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 11 - Com relação ao Anexo I do edital, item 1.3.40. Da remoção: … c) Proteção contra desinstalação e desativação não autorizada do produto. Entendemos que uma solução para proteção de repositórios de dados (storage) deverá somente ser administrada por administradores de redes ou analistas de segurança do CJF, não havendo nenhuma intervenção ou contado dos usuários finais com a console de gerencia da solução. Por este motivo entendemos que a característica de Proteção contra desinstalação e desativação não autorizada do produto é desnecessária, uma vez que apenas os administradores do ambiente computacional do CJF terão acesso ás consoles de gerencia da solução, está correto o nosso entendimento? RESPOSTA: Não está correto. 12 - Com relação ao

Anexo I do edital, item 1.6.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente; Conseguimos a partir de ferramentas da própria solução desinstalar clientes de terceiros e entendemos que este procedimento atende ao item em questão, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 13 - Com relação ao Anexo I do edital, item 1.6.19. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; 14 - A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 15 - Com relação ao Anexo I do edital, item 1.6.23. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal-intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 16 - Com relação ao Anexo I do edital, item 1.6.38. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto. A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 17 - Com relação ao Anexo I do edital, item 1.8.12. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente; Entendemos que a proteção contínua do endpoint é determinada pelas assinaturas existentes em sua base e tais regras específicas são inerentes a cada ambiente de produção cabendo ao administrador da solução determinar sua necessidade ou não, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 18 - Com relação ao Anexo I do edital, item 1.8.23. Deve permitir a emissão de alertas via smtp e snmp; Entendemos que o envio dos Logs para um Syslog, possibilitando vários níveis de detalhamento chegando a níveis de auditoria juntamente com o envio de alertar em SMTP, atende ao item. Assim como a possibilidade de validar a saúde do Servidor de gerencia a partir da própria console, possibilitando a notificação conforme desejar. Está correto o nosso entendimento? RESPOSTA: Conforme o edital. 19 - Com relação ao Anexo I do edital, item Em atenção aos itens 1.8.32, 1.8.33, 1.8.34, 1.9.17, 1.9.18, 1.9.19, entendemos que o acesso a console de administração limitada a partir de vários níveis de acesso, impossibilitando que usuários interfiram nas configurações estabelecidas pelo ADM da solução, possibilitando acesso somente de leitura e visualização de relatórios, assim como, a possibilidade de entrega de relatórios WEB para acompanhamento e check da saúde do ambiente atende aos itens. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 20 - Com relação ao Anexo I do edital, item 1.9.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: … b) Atributos do certificado utilizado para assinatura digital do executável; … d) Base de assinaturas de certificados digitais válidos e seguros. Entendemos que uma solução que tenha tais proteções verificadas a partir de assinaturas recebidas diretamente do site do fabricante, atende aos requisitos solicitados. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 21 - Com relação ao Anexo I do edital, item 1.10.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão: … s) Infravermelho; t) Bluetooth; Entendemos que uma solução que se apresente protegendo a manipulação das informações enviadas aos dispositivos USB, atende ao requisito, uma vez que os dispositivos trabalhando sob Infravermelho e Bluetooth, apresentam-se ao sistema operacional como um drive USB. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 22 - Com relação ao Anexo I do edital, item 2.2.26. Deve ser compatível com IPV6; Entendemos que por se tratar de um software instalado e integrado ao Software de Mensageria Exchange, onde a proteção é executada sob as caixas postais dos usuários, desta forma, tal funcionalidade é implementada no Software de mensageira. Entendemos que atendemos ao item, está correto nosso entendimento? RESPOSTA: Conforme o edital. 23 - Com relação ao Anexo I do edital, item 2.3.18. Deve permitir verificar mailbox stores e public foldes; e 2.3.19. Deve permitir definir a "idade mínima" das mensagens a serem verificadas; Entendemos que por se tratar de um software instalado e integrado ao Software de Mensageria Exchange, onde a proteção é executada sob as caixas postais dos usuários, desta forma, tal funcionalidade é implementada no Software de mensageira. Entendemos que atendemos ao item, está correto nosso entendimento? RESPOSTA: Conforme o edital. 24 - Com relação ao Anexo I do edital, item 2.3.74. A solução de anti-spam deverá submeter e-mails suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na análise das informações: a) Processos de autostart; b) Modificações de arquivos de sistema; c) Serviços criados e

modificados; d) Atividade de rede suspeita; e) Modificações de registros. Entendemos que estes subitens não se aplicam a esta aplicação, uma vez que sua funcionalidade primária é proteção ao tráfego de mensagens, nada relacionado ao endpoint. Em contra partida durante a implantação da solução em um hardware é feito um hardening do sistema operacional. Entendemos que desta forma estamos atendendo ao item, nosso entendimento está correto? RESPOSTA: Conforme o edital. 25 - Com relação ao Anexo I do edital, item 2.3.81. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro; Entendemos que a criação de área de suspeitos de virus quarentenados no gateway, juntamente com área de quarentena por usuários, assim como, um folder de incidentes de quarentena, atendem ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 26 - Com relação ao Anexo I do edital, item 2.3.125. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio; Entendemos que as diversas possibilidades como SPF, Sender ID Authentication, Good e Bad Sender, DNS-based IP reputation. Atendemos aos requisitos, está correto nosso entendimento? RESPOSTA: Conforme o edital. 27 - Com relação ao Anexo I do edital, item 2.3.176. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual; Entendemos que as limitações de uso de CPU não fazem parte deste software, uma vez que o appliance é dedicado e sem interferência direta ao usuário final. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 28 - Com relação ao Anexo I do edital, item 3 e seus subitens, entendemos que os itens direcionados como Bloqueio pela solução contra ataques de APT, uma fez que tais funcionalidades sejam executadas pelo módulo de Endpoint, o qual faz uso e é o mesmo agente de proteção dos Endpoints podem ser alertadas pela solução de APT, mas efetivamente executadas a partir da solução de Endpoint. Encontra-se em roadmap a execução das tarefas de bloqueio a partir da console de gerenciamento da Solução contra APTs, com previsão para lançamento da nova versão para o mês de março de 2016, no entanto, hoje já é possível inserir um equipamento em quarentena, colocando-o isolado dos demais quando verificado seu comprometimento. Entendemos que conforme descrito acima, atendemos o item 3 e seus subitens, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 29 - 3.23. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS, Messenger, eBuddy,ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP; Entendemos que determinados aplicativos são muito específicos e com particularidades das mais diversas, desta forma, detectando-se a tecnologia na qual se baseiam os aplicativos e aplicações, estaremos atendendo ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 30 - Com relação ao Anexo I do edital, item 3.70. Capacidade de salvar uma investigação antes de ser finalizada; 3.71. Capacidade de restaurar uma investigação para continuá-la ou consultá-la; Entendemos que será possível entregar a solução de forma virtualizada, em conjunto com o hardware dimensionado para a execução da proteção, entendemos ainda que uma vez entregue a solução virtualizada, não existe limite na quantidade de servidores scanners a serem implementados e sem custo extra para o CJF, possibilitando um ganho de escalabilidade e proteção. Está correto nosso entendimento? RESPOSTA: Conforme o edital 31 - Com relação ao Anexo I do edital, itens itens 3.108.8., 3.109.8, 3.110.8 Entendemos que o acesso a console de administração limitada a partir de vários níveis de acesso, impossibilitando que usuários interfiram nas configurações estabelecidas pelo ADM da solução, possibilitando acesso somente de leitura e visualização de relatórios, assim como, a possibilidade de entrega de relatórios WEB para acompanhamento e check da saúde do ambiente atende aos itens. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 32 - Com relação ao Anexo I do edital, item 3.108.16. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações: a) Uso de CPU b) Uso de Disco; c) Uso de Memória; d) Tráfego malicioso analisado; e) Todo o tráfego analisado. Entendemos que a funcionalidade de verificação da saúde da solução atende ao requisito, uma vez que se trata de uma solução dedicada e para cada fabricante os ponteiros de validação podem ser diferentes ou até mesmo com pesos distintos. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 33 - Com relação ao Anexo I do edital, item 3.110.5. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de health-check e log da base de dados; Entendemos que a entrega das informações em gráficos e relatórios distintos a partir do módulo de relatórios da solução atende ao item. Está correto nosso entendimento?

Resposta 10/02/2016 18:47:51

1 -Com relação ao Anexo I do edital item 1.1.10. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): d) Por linha-de-comando, parametrizável, com opção de limpeza; Entendemos que se a varredura já estiver determinada por padrão da solução como Limpeza, atendemos o item, esta correto o nosso entendimento? RESPOSTA: Não está correto. 2 -Com relação ao Anexo I do edital item 1.1.10. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): e) Automáticos do sistema com as seguintes opções: Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena); Entendemos que a solução que por padrão execute ao mesmo tempo a movimentação do arquivo infectado para a Quarentena, renomeie o arquivo e negue o acesso ao mesmo, está atendendo ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 3 - Com relação ao Anexo I do edital itens 1.1.13, 1.1.14 e 1.1.15, onde são destacadas a reputação de URL. Entendemos que uma solução que atenda de forma mais granular a este requisito, fazendo a reputação de arquivos dentro de um site / domínio, evitando que um domínio inteiro seja bloqueado apenas por uma interpretação macro da reputação de uma de suas páginas atende ao item, está correto o entendimento? RESPOSTA: Conforme o edital. 4 - Com relação ao Anexo I do edital, item 1.1.17. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante; Entendemos que a partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal-intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 5 - Com relação ao Anexo I do edital, item 1.1.19. Deve permitir a adição automática às listas de exclusão/arquivos conhecidos de modo a evitar novas detecções dos arquivos no ambiente de gestão da solução de endpoint; Entendemos que a adição de arquivos, diretórios, tipos de arquivos sendo realizada pelo administrador da ferramenta atende ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 6 - Com relação ao Anexo I do edital, item 1.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: a) Suse Linux Enterprise 9, 10 e 11; b) Red Hat Enterprise Linux 4.0, 5.0 e 6.0; c) Centos 4.0, 5.0 e 6.0. Entendemos que com o End Of Life de vários sistemas operacionais solicitados o suporte fica prejudicado pela falta de continuidade de seu desenvolvimento, conforme pode ser visto no seu link abaixo, desta forma, entendemos que o atendimento aos sistemas operacionais em linha de produção e atualização atende ao requisito. Está correto nosso entendimento? http://lists.opensuse.org/opensuse-security-announce/2011-09/msg00003.html https://access.redhat.com/support/policy/updates/errata http://stephane.lesimple.fr/fedora/packages-search/ Comprovação MAC OS https://support.symantec.com/en_US/article.tech195325.html https://en.wikipedia.org/wiki/History_of_Mac_OS Release Notes: https://support.symantec.com/en_US/article.TECH163829.html https://support.symantec.com/en_US/article.TECH231877.html LINUX https://support.symantec.com/en_US/article.TECH101598.html https://support.symantec.com/en_US/article.TECH223240.html RESPOSTA: Conforme o edital. 7 - Com relação ao Anexo I do edital, item 1.2.10. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação; Entendemos que a proteção não será exercida pela capacidade de análise em profundidade dos arquivos compactados, pois, antes de ser verificado o último nível de compactação obrigatoriamente todos os níveis anteriores já foram verificados, desta forma, entendemos que a verificação em até 10 níveis de compactação atende ao requisito. Está correto nosso entendimento? RESPOSTA: Não está correto. 8 - Com relação ao Anexo I do edital, item 1.3.3. A solução anti-malware deverá possuir a capacidade de negar acesso aos arquivos contaminados; Entendemos que a solução que por padrão execute ao mesmo tempo a movimentação do arquivo infectado para a Quarentena, renomeie o arquivo e negue o acesso ao mesmo, está atendendo ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 9 - Com relação ao Anexo I do edital, item 1.3.16. Caso a solução anti-malware necessite de um servidor dedicado, a mesma deverá possuir no mínimo os seguintes requisitos: ... b) Deverá permitir o escalonamento Round Robin, isto é, se o primeiro servidor estiver ocupado, a solicitação é enviada ao próximo servidor disponível; Entendemos que a solução deverá ser capaz de entregar a alta disponibilidade de comunicação entre os clientes e os servidores da solução onde quando um servidor estiver muito ocupado ou parado, as requisições deverão ser encaminhadas automaticamente para o próximo servidor disponível da solução, esta configuração pode ser facilmente configurada em uma lista de servidores e prioridades de conexão. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 10 - Com relação ao Anexo I do edital, item 1.3.17. A solução anti-

malware deverá suportar, no mínimo, 4 (quatro) conexões de, no mínimo, 10 Gbps (dez gigabit por segundo) e o acesso simultâneo de, no mínimo, 50 usuários; O atendimento a este item dependera do sizing realizado da solução para o ambiente computacional do CJF e também da arquitetura de rede e dados do mesmo, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 11 - Com relação ao Anexo I do edital, item 1.3.40. Da remoção: … c) Proteção contra desinstalação e desativação não autorizada do produto. Entendemos que uma solução para proteção de repositórios de dados (storage) deverá somente ser administrada por administradores de redes ou analistas de segurança do CJF, não havendo nenhuma intervenção ou contado dos usuários finais com a console de gerencia da solução. Por este motivo entendemos que a característica de Proteção contra desinstalação e desativação não autorizada do produto é desnecessária, uma vez que apenas os administradores do ambiente computacional do CJF terão acesso ás consoles de gerencia da solução, está correto o nosso entendimento? RESPOSTA: Não está correto. 12 - Com relação ao Anexo I do edital, item 1.6.9. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente; Conseguimos a partir de ferramentas da própria solução desinstalar clientes de terceiros e entendemos que este procedimento atende ao item em questão, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 13 - Com relação ao Anexo I do edital, item 1.6.19. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; 14 - A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 15 - Com relação ao Anexo I do edital, item 1.6.23. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante; A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal-intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 16 - Com relação ao Anexo I do edital, item 1.6.38. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto. A partir de uma categorização da reputação baseada de forma mais granular, onde são analisados os arquivos que o usuário acessa em cada site / domínio, a proteção propiciada é muito mais precisa e eficaz sem a necessidade de bloqueio de um domínio por completo, mas sim bloqueado o acesso ao determinado arquivo mal intencionado, atenderemos ao item. Está correto nosso entendimento? RESPOSTA: Não está correto. 17 - Com relação ao Anexo I do edital, item 1.8.12. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente; Entendemos que a proteção contínua do endpoint é determinada pelas assinaturas existentes em sua base e tais regras específicas são inerentes a cada ambiente de produção cabendo ao administrador da solução determinar sua necessidade ou não, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 18 - Com relação ao Anexo I do edital, item 1.8.23. Deve permitir a emissão de alertas via smtp e snmp; Entendemos que o envio dos Logs para um Syslog, possibilitando vários níveis de detalhamento chegando a níveis de auditoria juntamente com o envio de alertar em SMTP, atende ao item. Assim como a possibilidade de validar a saúde do Servidor de gerencia a partir da própria console, possibilitando a notificação conforme desejar. Está correto o nosso entendimento? RESPOSTA: Conforme o edital. 19 - Com relação ao Anexo I do edital, item Em atenção aos itens 1.8.32, 1.8.33, 1.8.34, 1.9.17, 1.9.18, 1.9.19, entendemos que o acesso a console de administração limitada a partir de vários níveis de acesso, impossibilitando que usuários interfiram nas configurações estabelecidas pelo ADM da solução, possibilitando acesso somente de leitura e visualização de relatórios, assim como, a possibilidade de entrega de relatórios WEB para acompanhamento e check da saúde do ambiente atende aos itens. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 20 - Com relação ao Anexo I do edital, item 1.9.14. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: … b) Atributos do certificado utilizado para assinatura digital do executável; … d) Base de assinaturas de certificados digitais válidos e seguros. Entendemos que uma solução que tenha tais proteções verificadas a partir de assinaturas recebidas diretamente do site do fabricante, atende aos requisitos solicitados. Está correto nosso

entendimento? RESPOSTA: Conforme o edital. 21 - Com relação ao Anexo I do edital, item 1.10.15. Deve ser capaz de identificar e bloquear informações nos meios de transmissão: … s) Infravermelho; t) Bluetooth; Entendemos que uma solução que se apresente protegendo a manipulação das informações enviadas aos dispositivos USB, atende ao requisito, uma vez que os dispositivos trabalhando sob Infravermelho e Bluetooth, apresentam-se ao sistema operacional como um drive USB. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 22 - Com relação ao Anexo I do edital, item 2.2.26. Deve ser compatível com IPV6; Entendemos que por se tratar de um software instalado e integrado ao Software de Mensageria Exchange, onde a proteção é executada sob as caixas postais dos usuários, desta forma, tal funcionalidade é implementada no Software de mensageira. Entendemos que atendemos ao item, está correto nosso entendimento? RESPOSTA: Conforme o edital. 23 - Com relação ao Anexo I do edital, item 2.3.18. Deve permitir verificar mailbox stores e public foldes; e 2.3.19. Deve permitir definir a "idade mínima" das mensagens a serem verificadas; Entendemos que por se tratar de um software instalado e integrado ao Software de Mensageria Exchange, onde a proteção é executada sob as caixas postais dos usuários, desta forma, tal funcionalidade é implementada no Software de mensageira. Entendemos que atendemos ao item, está correto nosso entendimento? RESPOSTA: Conforme o edital. 24 - Com relação ao Anexo I do edital, item 2.3.74. A solução de anti-spam deverá submeter e-mails suspeitos a solução de análise de ameaças avançadas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado na análise das informações: a) Processos de autostart; b) Modificações de arquivos de sistema; c) Serviços criados e modificados; d) Atividade de rede suspeita; e) Modificações de registros. Entendemos que estes subitens não se aplicam a esta aplicação, uma vez que sua funcionalidade primária é proteção ao tráfego de mensagens, nada relacionado ao endpoint. Em contra partida durante a implantação da solução em um hardware é feito um hardening do sistema operacional. Entendemos que desta forma estamos atendendo ao item, nosso entendimento está correto? RESPOSTA: Conforme o edital. 25 - Com relação ao Anexo I do edital, item 2.3.81. Possibilitar a criação de áreas de quarentenas separadas para cada tipo de filtro; Entendemos que a criação de área de suspeitos de virus quarentenados no gateway, juntamente com área de quarentena por usuários, assim como, um folder de incidentes de quarentena, atendem ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 26 - Com relação ao Anexo I do edital, item 2.3.125. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio; Entendemos que as diversas possibilidades como SPF, Sender ID Authentication, Good e Bad Sender, DNS-based IP reputation. Atendemos aos requisitos, está correto nosso entendimento? RESPOSTA: Conforme o edital. 27 - Com relação ao Anexo I do edital, item 2.3.176. Deve limitar uso de CPU em agendamento de rastreamento ou rastreamento manual; Entendemos que as limitações de uso de CPU não fazem parte deste software, uma vez que o appliance é dedicado e sem interferência direta ao usuário final. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 28 - Com relação ao Anexo I do edital, item 3 e seus subitens, entendemos que os itens direcionados como Bloqueio pela solução contra ataques de APT, uma fez que tais funcionalidades sejam executadas pelo módulo de Endpoint, o qual faz uso e é o mesmo agente de proteção dos Endpoints podem ser alertadas pela solução de APT, mas efetivamente executadas a partir da solução de Endpoint. Encontra-se em roadmap a execução das tarefas de bloqueio a partir da console de gerenciamento da Solução contra APTs, com previsão para lançamento da nova versão para o mês de março de 2016, no entanto, hoje já é possível inserir um equipamento em quarentena, colocando-o isolado dos demais quando verificado seu comprometimento. Entendemos que conforme descrito acima, atendemos o item 3 e seus subitens, está correto o nosso entendimento? RESPOSTA: Conforme o edital. 29 - 3.23. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT UDP, RTSP/RDT-TCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS, Messenger, eBuddy,ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP; Entendemos que determinados aplicativos são muito específicos e com particularidades das mais diversas, desta forma, detectando-se a tecnologia na qual se baseiam os aplicativos e aplicações, estaremos atendendo ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 30 - Com relação ao Anexo I do edital, item 3.70. Capacidade de salvar uma investigação

antes de ser finalizada; 3.71. Capacidade de restaurar uma investigação para continuá-la ou consultá-la; Entendemos que será possível entregar a solução de forma virtualizada, em conjunto com o hardware dimensionado para a execução da proteção, entendemos ainda que uma vez entregue a solução virtualizada, não existe limite na quantidade de servidores scanners a serem implementados e sem custo extra para o CJF, possibilitando um ganho de escalabilidade e proteção. Está correto nosso entendimento? RESPOSTA: Conforme o edital 31 - Com relação ao Anexo I do edital, itens itens 3.108.8., 3.109.8, 3.110.8 Entendemos que o acesso a console de administração limitada a partir de vários níveis de acesso, impossibilitando que usuários interfiram nas configurações estabelecidas pelo ADM da solução, possibilitando acesso somente de leitura e visualização de relatórios, assim como, a possibilidade de entrega de relatórios WEB para acompanhamento e check da saúde do ambiente atende aos itens. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 32 - Com relação ao Anexo I do edital, item 3.108.16. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações: a) Uso de CPU b) Uso de Disco; c) Uso de Memória; d) Tráfego malicioso analisado; e) Todo o tráfego analisado. Entendemos que a funcionalidade de verificação da saúde da solução atende ao requisito, uma vez que se trata de uma solução dedicada e para cada fabricante os ponteiros de validação podem ser diferentes ou até mesmo com pesos distintos. Está correto nosso entendimento? RESPOSTA: Conforme o edital. 33 - Com relação ao Anexo I do edital, item 3.110.5. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de health-check e log da base de dados; Entendemos que a entrega das informações em gráficos e relatórios distintos a partir do módulo de relatórios da solução atende ao item. Está correto nosso entendimento? RESPOSTA: Conforme o edital.

Complementando a Resposta 4.

Houve um erro material. Onde se lê: "Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e de terceiros ...", leia-se

"Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e/ou de terceiros ..."

Esclarecimento 10/02/2016 18:53:39

Referente ao item de proteção para Storage, devido ao número de total de dispositivo ser 1062, entendemos que a solução ofertada deverá atender plenamente ao número de 1062 dispositivos licenciados, tendo em vista que alguns fabricantes trabalham com licenciamento por usuários/dispositivo ao invés de licença por Storage. Está correto nosso entendimento?

Resposta 10/02/2016 18:53:39

Entendo que a solicitação é intempestiva. No entanto, o Termo de Referência, no seu anexo IV, define o número de dispositivos a serem cobertos pela solução de proteção para endpoint em 1062 dispositivos. O entendimento está correto.

Esclarecimento 11/02/2016 12:16:33

Questionamento 1: Com relação ao item 2 "SOLUÇÃO PARA PROTEÇÃO DE E-MAIL", subitem 2.1, "A solução deve ser oferecida em alta disponibilidade, sendo que pelo menos dos nós do cluster deve ser appliance físico, suficientemente dimensionada para suportar a, no mínimo, 650 (seiscentos e cinquenta) caixas postais, não considerando grupos ou listas de distribuição como caixas postais e ao processamento de 200.000 (duzentos mil) mensagens por hora;". Entendemos que, poderá ser oferecida uma máquina física e uma segunda máquina, que será utilizada para

cluster, poderá ser virtual, e será fornecida pelo Conselho da Justiça Federal. Sendo assim, não seria necessária à entrega de um segundo servidor físico para alta disponibilidade, para este ítem. Está correto nosso entendimento sobre o item? Questionamento 2: Conforme nosso entendimento, a nossa solução utiliza servidores Microsoft, estes S.Os serão fornecidos pelo Conselho de Justiça Federal, podendo ser virtualizados ou físicos, dispensando a contratada vencedora do certame, da aquisição de licenças Microsoft Server e entregando somete as licenças para solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados. Está correto nosso entendimento? Questionamento 3: Conforme nosso entendimento, a nossa solução utiliza licenças Microsoft SQL, estes servidores serão fornecidos pelo Conselho de Justiça Federal, podendo ser virtualizados ou físicos, dispensando a contatada vencedora do certame, da aquisição de licenças Microsoft SQL Server e entregando somete às licenças para solução unificada de segurança para proteção de e-mail, proteção de endpoint e proteção contra ataques avançados. Está correto nosso entendimento? Questionamento 4: Com relação ao ítem 1.12.36, "Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e de terceiros, possibilitando a coleta de logs de gerenciamento e correlação em "real-time";" Entendemos que empresas renomadas de mercado estão descontinuando seus produtos SIEM e são muito raras as que tem sua própria fabricação de SIEM. Isto torna o certame limitado podendo ter somente um fabricante participando. Sendo assim a palavra e de fabricação própria limita a uma única empresa do mercado. No nosso entendimento esta deveria ser substituída por e/ou ficando assim o item "1.12.36. Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e/ou de terceiros, possibilitando a coleta de logs de gerenciamento e correlação em "real-time";

Resposta 11/02/2016 12:16:33

Entendo que o questionamento é intempestivo. No entanto: Resposta 1: Conforme o TR, pelo menos um dos nós do cluster deverá ser físico. Resposta 2: O produto deverá ser entregue com todo o licenciamento necessário. O CJF mantém contrato de licenciamento para SO apenas para seu ambiente de virtualização. Resposta 3: O produto deverá ser entregue com todo o licenciamento necessário. O CJF possui contrato de licenciamento apenas para seu SGBD Microsoft em ambiente de virtualização. Conforme os itens 2.1, 2.3.142 e 3.6.11, e 3.6.11 a solução deverá operar em alta disponibilidade. A solução não deverá depender do funcionamento do ambiente de virtualização para sua operação continuada. Resposta 4: O entendimento está correto. Houve um erro material. Onde se lê: "Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e de terceiros ...", leia-se "Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e/ou de terceiros ..."