Home
Sala/Modalidades
Editais e Processos
Editais Encerrados/Arquivados
Atas e Documentos
Recursos
Relatórios
Esclarecimentos
Impugnações
Apenados / Impedidos
Contratações - PNCP
Dados de Mercado

CONSULTAR ESCLARECIMENTO

Solicitação respondida

Nome do Usuário
Henrique Crema

Participante
Scansource Brasil Distribuidora de Tecnologias Ltda.

Solicitação

Solicitação criada às 23:05 em 02/02/2026, última edição às 09:33 em 04/02/2026

Como interessado, no uso do direito previsto na legislação vigente, venho solicitar esclarecimento acerca de disposições técnicas, nos termos abaixo: 1- "Deve permitir a funcionalidade de ARP bridging;" Entendemos que a finalidade técnica deste requisito é garantir a integridade e a segurança do domínio ARP da rede, prevenindo situações como ARP spoofing, “ARP storm” / Storm control, associações indevidas entre IP/MAC e possíveis cenários de bypass às políticas de segurança na camada 2. Está correto o entendimento a este requisito, podendo ser comprovado por meio de mecanismos que assegurem a proteção, o controle e a inspeção do protocolo ARP, preservando a visibilidade e a segurança do tráfego na rede, garantindo finalidade operacional prevista no item? 2- "Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar ‘ARP Storm;" Entendemos que a finalidade técnica deste requisito é prevenir situações de degradação da rede causadas por excesso de tráfego ARP, tais como instabilidade na comunicação da camada 2, sobrecargas de tabelas ARP e possíveis cenários de negação de serviço. Está correto o entendimento referente ao atendimento a este requisito podendo ser comprovado por meio de mecanismos que permitam detectar, controlar e mitigar comportamentos anômalos relacionados ao protocolo ARP, assegurando a estabilidade e a segurança operacional da rede conforme previsto no item? 3- "A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android" Entendemos que a finalidade técnica deste requisito é permitir que dispositivos móveis com sistemas operacionais Apple iOS e Android quando suportados pelo sistema operacional possam estabelecer conexões VPN seguras com a solução ofertada, utilizando recursos nativos dos sistemas operacionais, garantindo acesso remoto seguro sem a necessidade de aplicações adicionais. Está correto o entendimento deste requisito, podendo ser comprovado desde que a solução permita a conexão VPN nativa nesses dispositivos, sendo o suporte aos sistemas operacionais mencionados considerando as capacidades nativas de VPN disponibilizadas por cada fabricante, de modo que a conectividade segura seja viabilizada conforme os recursos suportados por cada sistema operacional, assegurando a mesma funcionalidade de acesso remoto seguro prevista no item? 4- "Deve possuir módulo de Anti-malware (Anti-Vírus e Anti-Bot) integrado ao próprio appliance de segurança" Entendemos que a finalidade técnica deste requisito é assegurar que o próprio appliance de segurança possua, de forma nativa e integrada, mecanismos capazes de identificar, bloquear e inspecionar ameaças relacionadas a malware, bem como detectar e impedir comunicações com infraestruturas de comando e controle (botnets/C2), sem a necessidade de soluções externas ou dispositivos adicionais. Está correto o entendimento de que o cumprimento a este requisito pode ser comprovado desde que a solução ofertada possua tais capacidades de proteção contra malware e comunicações maliciosas de forma integrada ao equipamento, independentemente da nomenclatura comercial utilizada para os mecanismos de detecção (como “Anti-Bot”, “C2 detection”, “Botnet protection” ou similares)? 5- "A solução deve ser capaz de inspecionar o tráfego criptografado TLS versão 1.2 no mínimo e SSH" Entendemos que a finalidade técnica deste requisito é garantir que a solução de segurança seja capaz de aplicar inspeção, controle e políticas de segurança sobre tráfego criptografado, evitando que tais protocolos sejam utilizados como meio de bypass às regras de segurança, garantindo visibilidade, controle de aplicações e prevenção de ameaças. Está correto o entendimento, que para o protocolo TLS, a inspeção se dá por meio de descriptografia e análise do conteúdo, e que, para o protocolo SSH, o atendimento ao requisito pode ser comprovado por mecanismos que permitam identificar, controlar, bloquear e aplicar políticas sobre sessões SSH, prevenindo seu uso indevido como túnel de evasão, ainda que não haja a descriptografia do conteúdo da sessão? 6- "Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware" Entendemos que a finalidade técnica deste requisito é garantir que arquivos contendo ameaças desconhecidas (dia zero) sejam analisados pela solução de segurança antes de sua entrega ao usuário final, de forma que conteúdos maliciosos sejam identificados, bloqueados ou neutralizados, impedindo que o usuário receba arquivos comprometidos. Está correto o entendimento em relação ao atendimento a este requisito pode ser comprovado por meio de mecanismos avançados de análise de ameaças, tais como sandboxing, emulação, análise comportamental, inteligência artificial ou técnicas equivalentes de detecção e bloqueio, que impeçam a entrega de arquivos maliciosos ao usuário? 7- "A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas" Entendemos que a finalidade técnica deste requisito é garantir que a solução utilize ambientes virtuais controlados, distintos para execução e análise comportamental de arquivos suspeitos, possibilitando a identificação de códigos maliciosos com base

Home
Sala/Modalidades
Editais e Processos
Editais Encerrados/Arquivados
Atas e Documentos
Recursos
Relatórios
Esclarecimentos
Impugnações
Apenados / Impedidos
Contratações - PNCP
Dados de Mercado

virtualização é apresentada ou administrada pela solução? 8- “A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo” Entendemos que a finalidade técnica deste requisito é permitir que arquivos identificados de forma inequívoca por seu hash criptográfico possam ser reconhecidos como confiáveis pela solução, possibilitando que não sejam bloqueados ou submetidos a análises adicionais após validação administrativa. Está correta a interpretação e entendimento de que este requisito pode ser comprovado desde que a solução identifique os arquivos por meio de seu hash, utilize esse identificador como critério de reputação e confiança, e permita ao administrador liberar e reconhecer arquivos legítimos com base nesse identificador, garantindo a mesma finalidade de controle prevista no item? 9- “Prover autenticação de usuários para os serviços Telnet, FTP, HTTP3 e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea” Entendemos que a finalidade técnica deste requisito é garantir que a solução seja capaz de identificar e autenticar os usuários que acessam serviços como Telnet, FTP, HTTP, HTTP3 e HTTPS através do equipamento, utilizando bases externas de usuários e grupos, permitindo a aplicação de políticas de segurança baseadas em identidade do usuário. Está correto o entendimento no qual o atendimento a este requisito pode ser comprovado desde que a solução permita a identificação e autenticação dos usuários por meio da integração simultânea com diretórios de usuários, por exemplo AD/LDAP, possibilitando a aplicação de políticas de acesso aos serviços mencionados com base nessa identidade? 10- “Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração” Entendemos que a finalidade técnica deste requisito é permitir a segregação de funções administrativas diretamente no equipamento NGFW, possibilitando a criação de diferentes perfis de acesso com permissões específicas, de modo que múltiplos administradores possam atuar com responsabilidades distintas e controladas. Está correto o entendimento a este requisito, podendo ser comprovado por meio dos mecanismos de controle de acesso administrativo disponíveis no próprio NGFW, assegurando a segregação de responsabilidades prevista no item? 11- “A solução poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre” Considerando que o item visa assegurar que a solução seja composta por appliances do próprio fabricante virtualizado ou físico, questiona-se se pode ser aceita a oferta de plataforma de gerenciamento centralizado disponibilizada em nuvem pelo mesmo fabricante dos firewalls, mantendo-se as características exigidas para os appliances de gerenciamento previstos no item. 12- “Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria” Está correta a interpretação bem como o atendimento a este requisito pode ser comprovado desde que as alterações realizadas por meio do gerenciamento centralizado tenham sua aplicação confirmada nos dispositivos gerenciados e que a rastreabilidade dessas mudanças para fins de auditoria possa ser evidenciada por meio dos registros disponíveis nos próprios equipamentos? 13- “Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente ;” Entendemos que a finalidade técnica deste requisito é assegurar a segregação de responsabilidades na administração da solução, permitindo que alterações realizadas sejam previamente validadas antes de sua aplicação efetiva no ambiente, de forma a mitigar erros operacionais e impactos negativos. Está correto o entendimento de que o atendimento a este requisito possa ser comprovado desde que a solução disponha de mecanismos que permitam controle administrativo, rastreabilidade das alterações realizadas e possibilidade de validação prévia à sua aplicação, garantindo a supervisão por responsável distinto conforme previsto no item? 14- Questionamentos sobre o ITEM 5 e subitens relacionados ao tema de acesso seguro. Considerando a complexidade técnica dos requisitos descritos no ITEM 5 e itens subsequentes, a necessidade do correto entendimento de sua finalidade operacional para a elaboração da proposta técnica, solicitamos a confirmação dos entendimentos a seguir, com o objetivo de assegurar aderência plena às exigências previstas no edital. Entendemos que a finalidade deste conjunto de requisitos é prover acesso seguro às aplicações privadas e públicas por meio de uma plataforma em nuvem do fabricante que integre controle por identidade, políticas granulares por aplicação, verificação de postura do dispositivo e navegação segura ao usuário, está correto o entendimento? TCP/UDP, SSH, RDP, SQL Entendemos que a menção a protocolos diversos como TCP e UDP visa assegurar que aplicações de diferentes naturezas possam ser acessadas de forma segura e controlada por identidade e políticas, sem caracterizar acesso irrestrito à rede da contratante, o entendimento está correto? Acesso sem agente / navegadores Está correto o entendimento de que o acesso às aplicações privadas pode ocorrer por meio de navegador Web compatível ou navegador seguro ofertado pelo fabricante da solução, sem necessidade de instalação de agentes, mantendo os requisitos de identidade, políticas de acesso e segurança previstos no item? ChromeOS / Ubuntu O entendimento está correto de que o suporte aos sistemas operacionais mencionados pode ser atendido por meio do acesso seguro às aplicações através de navegador compatível? Considerando a evolução contínua dos sistemas operacionais de mercado e das soluções de segurança, está correto o entendimento de que o suporte aos sistemas operacionais mencionados poderá ser atendido tanto pelas funcionalidades atuais da solução quanto por evoluções e atualizações disponibilizadas pelo fabricante durante o período contratual, mantendo a aderência aos requisitos do edital? Proxy reverso / IdP Entendemos que a menção a proxy reverso se refere à mediação do acesso às aplicações por um serviço em nuvem com validação prévia de identidade e aplicação de

Home
Sala/Modalidades
Editais e Processos
Editais Encerrados/Arquivados
Atas e Documentos
Recursos
Relatórios
Esclarecimentos
Impugnações
Apenados / Impedidos
Contratações - PNCP
Dados de Mercado

entendimento está correto? DNS / navegação segura Entendemos que a finalidade do requisito é proteger os usuários contra ameaças baseadas em DNS e navegação Web, por meio de filtragem de domínios e URLs aplicada conforme o contexto do dispositivo e do usuário, o entendimento está correto? CASB / SaaS Entendemos que a finalidade do requisito de proteção a aplicações SaaS é permitir visibilidade e controle de acesso baseados em identidade e contexto do dispositivo, preservando a experiência de logon único existente, está correto o entendimento? Invisibilidade de recursos não autorizados Está correto o entendimento de que o requisito visa assegurar que o usuário visualize e acesse apenas as aplicações explicitamente autorizadas pelas políticas definidas pelo administrador? Menu de aplicações Está correto o entendimento de que a disponibilização das aplicações ao usuário pode ocorrer por meio de interface segura provida pelo serviço em nuvem do fabricante, navegador compatível ou via navegador seguro ofertado pelo fabricante, não sendo obrigatória a presença de menu publicado diretamente no sistema operacional do dispositivo? Conectores em múltiplos pontos Está correto o entendimento de que a menção a múltiplos conectores visa permitir flexibilidade de acesso às aplicações privadas a partir de diferentes pontos da infraestrutura, não impondo obrigatoriedade de arquitetura específica, desde que o acesso seguro às aplicações seja garantido? Criptografia / Man-in-the-middle / criptografia dupla dentro dos tuneis encriptados Entendemos que o requisito visa garantir que toda comunicação entre o usuário, o serviço em nuvem do fabricante e as aplicações seja cifrada e protegida contra interceptações. Está correto o entendimento destes itens?

Documentos da Solicitação

DOCUMENTOS	
ESCLARECIMENTO PE 06 2026.pdf	⬇

Nome do Usuário
Danilo dos Santos Servilha

Participante
Prefeitura Municipal de Hortolândia

Resposta

Resposta criada às 09:33 em 04/02/2026

Prezado(s), Segue documento anexo contendo as Respostas relacionadas aos esclarecimentos solicitados.

Documentos da Resposta

DOCUMENTOS	
3 - RESPOSTA BBMNET 1.pdf	⬇

VOLTAR

Questão 1:
"Deve permitir a funcionalidade de ARP bridging;"

Entendemos que a finalidade técnica deste requisito é garantir a integridade e a segurança do domínio ARP da rede, prevenindo situações como ARP spoofing, "ARP storm" / Storm control, associações indevidas entre IP/MAC e possíveis cenários de bypass às políticas de segurança na camada 2.

Está correto o entendimento a este requisito, podendo ser comprovado por meio de mecanismos que assegurem a proteção, o controle e a inspeção do protocolo ARP, preservando a visibilidade e a segurança do tráfego na rede, garantindo finalidade operacional prevista no item?

Resposta:

Sim. O entendimento está correto.

A finalidade técnica do requisito está relacionada à proteção do domínio ARP da rede e à prevenção de cenários como ARP spoofing, ARP storm e associações indevidas entre endereços ip e mac na camada 2 em nosso ambiente.
Se a solução atender a este requisito por meio de mecanismos que permitem a inspeção, controle e limitação do tráfego ARP na interface é valido, possibilitando a mitigação de comportamentos anormais e preservando a integridade do domínio de broadcast

Questão 2:
"Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar 'ARP Storm'"

Entendemos que a finalidade técnica deste requisito é prevenir situações de degradação da rede causadas por excesso de tráfego ARP, tais como instabilidade na comunicação da camada 2, sobrecargas de tabelas ARP e possíveis cenários de negação de serviço.

Está correto o entendimento referente ao atendimento a este requisito podendo ser comprovado por meio de mecanismos que permitam detectar, controlar e mitigar comportamentos anômalos relacionados ao protocolo ARP, assegurando a estabilidade e a segurança operacional da rede conforme previsto no item?

Resposta:

Sim. O entendimento está correto.
A finalidade do requisito está relacionada à prevenção de degradações na rede causadas por excesso de tráfego ARP, que podem resultar em instabilidade na comunicação da camada 2, sobrecarga de tabelas ARP e potenciais cenários de negação de serviço.
Caso a solução ofertada atenda dessa forma, será válido

Questão 3:
"A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android"

Entendemos que a finalidade técnica deste requisito é permitir que dispositivos móveis com sistemas operacionais Apple iOS e Android quando suportados pelo sistema operacional possam estabelecer conexões VPN seguras com a solução ofertada, utilizando recursos nativos dos sistemas operacionais, garantindo acesso remoto seguro sem a necessidade de aplicações adicionais.

Está correto o entendimento deste requisito, podendo ser comprovado desde que a solução permita a conexão VPN nativa nesses dispositivos, sendo o suporte aos sistemas operacionais mencionados considerando as capacidades nativas de VPN disponibilizadas por cada fabricante, de modo que a conectividade segura seja viabilizada conforme os recursos suportados por cada sistema operacional, assegurando a mesma funcionalidade de acesso remoto seguro prevista no item?

Resposta:

Sim. O entendimento está correto.

A finalidade do requisito está relacionada a compatibilidade, caso a solução ofertada atenda com configurações nativa nos sistemas solicitados, será aceito

Questão 4:
"Deve possuir módulo de Anti-malware (Anti-Vírus e Anti-Bot) integrado ao próprio appliance de segurança"

Entendemos que a finalidade técnica deste requisito é assegurar que o próprio appliance de segurança possua, de forma nativa e integrada, mecanismos capazes de identificar, bloquear e inspecionar ameaças relacionadas a malware, bem como detectar e impedir comunicações com infraestruturas de comando e controle *(botnets/C2),* sem a necessidade de soluções externas ou dispositivos adicionais.

Está correto o entendimento de que o cumprimento a este requisito pode ser comprovado desde que a solução ofertada possua tais capacidades de proteção contra malware e comunicações maliciosas de forma integrada ao equipamento, independentemente da nomenclatura comercial utilizada para os mecanismos de detecção (como *"Anti-Bot", "C2 detection", "Botnet protection"* ou similares)?

Resposta:
Sim. O entendimento está correto.

A finalidade do requisito está relacionada a capacidade de proteção contra malware e comunicações maliciosas de forma integrada ao equipamento de proteção de vírus e botnets, poderá ser em um único componente ou um dedicado a tal função, desde que o objetivo seja cumprido.

Questão 5:
"A solução deve ser capaz de inspecionar o tráfego criptografado TLS versão 1.2 no mínimo e SSH"

Entendemos que a finalidade técnica deste requisito é garantir que a solução de segurança seja capaz de aplicar inspeção, controle e políticas de segurança sobre tráfego criptografado, evitando que tais protocolos sejam utilizados como meio de bypass às regras de segurança, garantindo visibilidade, controle de aplicações e prevenção de ameaças.

Está correto o entendimento, que para o protocolo TLS, a inspeção se dá por meio de descriptografia e análise do conteúdo, e que, para o protocolo SSH, o atendimento ao requisito pode ser comprovado por mecanismos que permitam identificar, controlar, bloquear e aplicar políticas sobre sessões SSH, prevenindo seu uso indevido como túnel de evasão, ainda que não haja a descriptografia do conteúdo da sessão?

Resposta:

Sim. O entendimento está correto, a finalidade do requisito é garantir que protocolos criptografados não sejam utilizados como meio de evasão às políticas de segurança,

garantindo visibilidade, controle de aplicações e prevenção de ameaças em nosso ambiente, caso a solução ofertada atenda por meio de mecanismos para o devido controle, será valido.

Questão 6:

"Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware"

Entendemos que a finalidade técnica deste requisito é garantir que arquivos contendo ameaças desconhecidas (dia zero) sejam analisados pela solução de segurança antes de sua entrega ao usuário final, de forma que conteúdos maliciosos sejam identificados, bloqueados ou neutralizados, impedindo que o usuário receba arquivos comprometidos.

Está correto o entendimento em relação ao atendimento a este requisito pode ser comprovado por meio de mecanismos avançados de análise de ameaças, tais como sandboxing, emulação, análise comportamental, inteligência artificial ou técnicas equivalentes de detecção e bloqueio, que impeçam a entrega de arquivos maliciosos ao usuário?

Resposta:

Sim. O entendimento está correto e válido.

Questão 7:

"A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas"

Entendemos que a finalidade técnica deste requisito é garantir que a solução utilize ambientes virtuais controlados, distintos para execução e análise comportamental de arquivos suspeitos, possibilitando a identificação de códigos maliciosos com base em seu comportamento, sem dependência de assinaturas.

Está correto o entendimento de que este requisito pode ser comprovado desde que a solução realize a análise comportamental de ameaças em ambientes virtuais variados, capazes de simular diferentes sistemas operacionais para fins de detecção, como por exemplo em nuvem do fabricante independentemente da forma como essa virtualização é apresentada ou administrada pela solução?

Resposta:

Sim. O entendimento está correto e válido, o termo de maquinas virtuais é a capacidade de execução do arquivo suspeito em sistemas operacionais em ambientes controlados do fabricante e não a disponibilidade de máquinas virtuais para o nosso ambiente.

Questão 8:

"A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo"

Entendemos que a finalidade técnica deste requisito é permitir que arquivos identificados de forma inequívoca por seu hash criptográfico possam ser reconhecidos como confiáveis pela solução, possibilitando que não sejam bloqueados ou submetidos a análises adicionais após validação administrativa.

Está correta a interpretação e entendimento de que este requisito pode ser comprovado desde que a solução identifique os arquivos por meio de seu hash, utilize esse identificador como critério de reputação e confiança, e permita ao administrador liberar e reconhecer arquivos legítimos com base nesse identificador, garantindo a mesma finalidade de controle prevista no item?

Resposta:

Sim, o entendimento é valido, nosso objetivo é garantir que os administradores possam ter a capacidade de liberar arquivos que estejam sob suspeita desde que a solução identifique os arquivos por meio de seu hash, seja em relatório ou na dashboard e utilize esse identificador como critério de reputação e confiança, será aceito.

Questão 9:
"Prover autenticação de usuários para os serviços Telnet, FTP, HTTP3 e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea"

Entendemos que a finalidade técnica deste requisito é garantir que a solução seja capaz de identificar e autenticar os usuários que acessam serviços como Telnet, FTP, HTTP, HTTP3 e HTTPS através do equipamento, utilizando bases externas de usuários e grupos, permitindo a aplicação de políticas de segurança baseadas em identidade do usuário.

Está correto o entendimento no qual o atendimento a este requisito pode ser comprovado desde que a solução permita a identificação e autenticação dos usuários por meio da integração simultânea com diretórios de usuários, por exemplo AD/LDAP, possibilitando a aplicação de políticas de acesso aos serviços mencionados com base nessa identidade?

Resposta:

Sim, o entendimento está correto.

Nosso objetivo é garantir que a solução ofertada, ofereça a capacidade de identificar e autenticar usuários, dessa forma permite os administradores aplicarem controle de políticas mais granulares.

Questão 10:
"Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração"

Entendemos que a finalidade técnica deste requisito é permitir a segregação de funções administrativas diretamente no equipamento NGFW, possibilitando a criação de diferentes perfis de acesso com permissões específicas, de modo que múltiplos administradores possam atuar com responsabilidades distintas e controladas.

Está correto o entendimento a este requisito, podendo ser comprovado por meio dos mecanismos de controle de acesso administrativo disponíveis no próprio NGFW, assegurando a segregação de responsabilidades prevista no item?

Resposta:

O entendimento está correto, será aceito a criação dos perfis de administração diretamente no equipamento ou na solução de gerenciamento, desde que cumpra o objetivo.

Questão 11:
"A solução poderá ser entregue como appliance físico ou appliance virtual, sendo todos do mesmo fabricante dos firewalls, não sendo aceita solução de software livre"

Considerando que o item visa assegurar que a solução seja composta por appliances do próprio fabricante virtualizado ou físico, questiona-se se pode ser aceita a oferta de plataforma de gerenciamento centralizado disponibilizada em nuvem pelo mesmo fabricante dos firewalls, mantendo-se as características exigidas para os appliances de gerenciamento previstos no item.

Resposta:

De acordo com a possibilidade de gerenciamento em nuvem, desde que cumpra o objetivo sem prejuízo aos requisitos deste item.

Questão 12:
"Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria"

Está correta a interpretação bem como o atendimento a este requisito pode ser comprovado desde que as alterações realizadas por meio do gerenciamento centralizado tenham sua aplicação confirmada nos dispositivos gerenciados e que a rastreabilidade dessas mudanças para fins de auditoria possa ser evidenciada por meio dos registros disponíveis nos próprios equipamentos?

Resposta:

Sim, a interpretação está valida, poderá ser aceito a validação dos registros no equipamento, o objetivo é ter visibilidade de atividades realizadas nos equipamentos em possíveis auditorias.

Questão 13:
"Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente ;"

Entendemos que a finalidade técnica deste requisito é assegurar a segregação de responsabilidades na administração da solução, permitindo que alterações realizadas sejam previamente validadas antes de sua aplicação efetiva no ambiente, de forma a mitigar erros operacionais e impactos negativos.

Está correto o entendimento de que o atendimento a este requisito possa ser comprovado desde que a solução disponha de mecanismos que permitam controle administrativo, rastreabilidade das alterações realizadas e possibilidade de validação prévia à sua aplicação, garantindo a supervisão por responsável distinto conforme previsto no item?

Resposta:

Sim, o entendimento está correto, caso a solução ofereça meios para validação da realização de atividades, juntamente com o controle de perfis de gerenciamento, será valido.

Questão 14:
Questionamentos sobre o ITEM 5 e subitens relacionados ao tema de acesso seguro.

Considerando a complexidade técnica dos requisitos descritos no ITEM 5 e itens subsequentes, a necessidade do correto entendimento de sua finalidade operacional para a elaboração da proposta técnica, solicitamos a confirmação dos entendimentos a seguir, com o objetivo de assegurar aderência plena às exigências previstas no edital.

Entendemos que a finalidade deste conjunto de requisitos é prover acesso seguro às aplicações privadas e públicas por meio de uma plataforma em nuvem do fabricante que integre controle por identidade, políticas granulares por aplicação, verificação de postura do dispositivo e navegação segura ao usuário, está correto o entendimento?

Resposta: Sim, o entendimento está correto.

Questão 15:
TCP/UDP, SSH, RDP, SQL

Entendemos que a menção a protocolos diversos como TCP e UDP visa assegurar que aplicações de diferentes naturezas possam ser acessadas de forma segura e controlada por identidade e políticas, sem caracterizar acesso irrestrito à rede da contratante, o entendimento está correto?

Resposta: Sim, o entendimento é correto

Questão 16:
Acesso sem agente / navegadores

Está correto o entendimento de que o acesso às aplicações privadas pode ocorrer por meio de navegador Web compatível ou navegador seguro ofertado pelo fabricante da solução, sem necessidade de instalação de agentes, mantendo os requisitos de identidade, políticas de acesso e segurança previstos no item?

Resposta: Sim, o entendimento está correto

Questão 17:
ChromeOS / Ubuntu

O entendimento está correto de que o suporte aos sistemas operacionais mencionados pode ser atendido por meio do acesso seguro às aplicações através de navegador compatível?

Considerando a evolução contínua dos sistemas operacionais de mercado e das soluções de segurança, está correto o entendimento de que o suporte aos sistemas operacionais mencionados poderá ser atendido tanto pelas funcionalidades atuais da solução quanto por evoluções e atualizações disponibilizadas pelo fabricante durante o período contratual, mantendo a aderência aos requisitos do edital?

Resposta: Sim, o entendimento é valido, serão aceitos acessos a aplicações correspondentes ao perfil inclusive via navegador.

Questão 18:
Proxy reverso / IdP

Entendemos que a menção a proxy reverso se refere à mediação do acesso às aplicações por um serviço em nuvem com validação prévia de identidade e aplicação de políticas de acesso. Está correto o entendimento?

Resposta: Sim, o entendimento está correto e válido

Questão 19:
Integração com NGAV / Postura dinâmica

Entendemos que a finalidade do requisito é permitir que o estado de segurança do dispositivo, avaliado por solução de proteção de endpoint, influencie dinamicamente as políticas de acesso às aplicações e não a obrigatoriedade do fornecimento do produto de endpoint NGAV neste processo, o entendimento está correto?

Resposta: Sim, o entendimento é valido, nosso objetivo é garantir que a solução ofertada seja compatível com soluções NGAV, não ofertada nesse processo.

Questão 20:
DNS / navegação segura

Entendemos que a finalidade do requisito é proteger os usuários contra ameaças baseadas em DNS e navegação Web, por meio de filtragem de domínios e URLs aplicada conforme o contexto do dispositivo e do usuário, o entendimento está correto?

Resposta: Sim, o entendimento está correto

Questão 21:
CASB / SaaS

Entendemos que a finalidade do requisito de proteção a aplicações SaaS é permitir visibilidade e controle de acesso baseados em identidade e contexto do dispositivo, preservando a experiência de logon único existente, está correto o entendimento?

Resposta: Sim, o entendimento é valido e correto.

Questão 22:
Invisibilidade de recursos não autorizados

Está correto o entendimento de que o requisito visa assegurar que o usuário visualize e acesse apenas as aplicações explicitamente autorizadas pelas políticas definidas pelo administrador?

Resposta: Sim, o entendimento está correto, o objetivo é garantir que os acessos sejam feitos por usuários com a devida permissão, caso não tenha, não poderá acessar o recurso.

Questão 23:
Menu de aplicações

Está correto o entendimento de que a disponibilização das aplicações ao usuário pode ocorrer por meio de interface segura provida pelo serviço em nuvem do fabricante, navegador compatível ou via navegador seguro ofertado pelo fabricante, não sendo obrigatória a presença de menu publicado diretamente no sistema operacional do dispositivo?

Resposta: Sim, o entendimento está correto e válido, desde que cumpra com o objetivo.

Questão 24:
Conectores em múltiplos pontos

Está correto o entendimento de que a menção a múltiplos conectores visa permitir flexibilidade de acesso às aplicações privadas a partir de diferentes pontos da infraestrutura, não impondo obrigatoriedade de arquitetura específica, desde que o acesso seguro às aplicações seja garantido?

Resposta: Sim, o entendimento está correto.

Questão 25:
Criptografia / Man-in-the-middle / criptografia dupla dentro dos tuneis encriptados

Entendemos que o requisito visa garantir que toda comunicação entre o usuário, o serviço em nuvem do fabricante e as aplicações seja cifrada e protegida contra interceptações. Está correto o entendimento destes itens?

Resposta: Sim, o entendimento é valido, nosso objetivo é garantir que a solução seja segura com proteções nativas da plataforma a fim de evitar possíveis comprometimentos com os dados.