Resposta ao pedido de esclarecimento da **Empresa 5 INTITUTO TECNOLÓGICO**.

PEDIDO ESCLARECIMENTO 02

QUESTIONAMENTO 1

Em relação ao item: **"3.2.5. Análise de Malwares Modernos;",** entendemos que se a solução ofertada executar a análise de malwares modernos baseado em assinaturas e com uma equipe de laboratório de inteligência localizado no Brasil, capaz de identificar as ameaças modernas e em uma próxima atualização do produto, entregar ao SESI-DF a base de conhecimentos destes malwares, o item será considerado como atendido?
Está correto nosso entendimento?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto, pois o serviço pretendido requer uma resposta antecipada a possível infecção por *Malwares* de quaisquer naturezas, sobretudo os modernos, sendo este requisito essencial contra ameaças de dia zero em potencial. Ademais este item faz referência à licença de Sandbox que deve integrar a Solução de Segurança de Prevenção de Ameaças de Próxima Geração.

QUESTIONAMENTO 2

Em relação aos itens, fazemos o seguinte questionamento:

"3.7. Deve auxiliar e facilitar a sua administração através de ferramentas que forneçam recomendações e melhores práticas em segurança, inclusive com alertas de erros comuns de configuração nas políticas e também no sistema operacional da solução."
3.8. Deve ser possível também verificar se as recomendações fornecidas estão sendo seguidas ou não;
3.11.1. Visualização da situação atual e histórica da Segurança do ambiente;
3.11.2. Visualização e tomadas de decisão com base em referenciamento geográfico das informações de Segurança (ataques, invasões, conexões, etc.);
3.11.3. Relatórios de visões correlacionadas envolvendo as camadas de segurança da solução ofertada;
3.11.8. Detectar e alertar acessos de administradores em horários irregulares e possíveis tentativas de adivinhação de credenciais administrativas (password guessing attacks) da solução;
3.11.9. Análises e alertas de alterações em configurações da solução antes que elas sejam aplicadas, visando impedir erros humanos de configuração;
3.11.10. Análises de risco do ambiente em tempo real, com base em melhores práticas de segurança, regulamentações e também em padrões customizados pela CONTRATADA;
3.11.11. Notificações instantâneas sobre mudanças, eventos e acontecimentos que representem ou gerem impacto na segurança do ambiente;
3.11.12. Referência cruzada da base de assinaturas de detecção com os identificadores CVE (Common Vulnerabilities and Exposures).
4.5.13. Permitir auditoria e relatórios avançados das alterações realizadas;"

Entendemos que o contrato é para fornecimento de SOC com serviço de firewall, portanto, a execução de recomendações poderá ser executada por técnico especializado na ferramenta, onde este irá aplicar as melhores práticas em segurança, inclusive alertando por relatórios confeccionados pela equipe sobre os erros comuns. Portanto, não haverá perda na qualidade da solução contratada, caso o fornecedor opte por ofertar o serviço ao invés de ferramentas. Todos os itens acima são mais bem elaborados se for feito por um recurso técnico especialista. Baseando-se em análises de logs e relatórios para entender o comportamento da rede protegida e as mudanças que possam causar diminuição do nível de segurança da rede de TI. Por fim, se a LICITANTE atender todos itens acima pela execução de mão-de-obra técnica, estes, serão considerados como atendidos.
Está correto nosso entendimento?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto, pois o objeto contempla serviços de segurança de perímetro com fornecimento de equipamentos (2 firewalls NGFW), administração e monitoração de segurança, resposta a incidentes de segurança em conjunto com funcionalidades da solução de Segurança de Prevenção de Ameaças de Próxima Geração e ferramentas que atendam este conjunto, em regime 24x7x365. Os profissionais responsáveis pelo gerenciamento da solução da CONTRATADA realizarão o planejamento, elaboração de melhores práticas e emissão de relatórios visando a proteção do ambiente do Conselho Nacional do SESI e utilizarão os dados gerados através da emissão de relatórios mensais e sempre que solicitado pelo Conselho, visando a mensuração e qualidade do serviço conforme descrito no item 8.22 do Termo de Referência.

QUESTIONAMENTO 3

Em relação ao item: **“4.6.9.8. Suporte a, no mínimo, 3 (três) roteadores virtuais na mesma instância de firewall;”,** entendemos que, se a solução ofertada permitir que o recurso de SD-WAN gerencie a tabela de rotas e consiga redirecionar o tráfego de rede baseado em parâmetros de configuração de origem ou destino e ainda permitir verificar a latência, perda de pacotes, jitter e consumo de banda da rota de saída podemos considerar o item como atendido.
Está correto nosso entendimento?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto, pois o suporte mínimo a 3 (três) roteadores virtuais na mesma instância de firewall atende a necessidade do CN-SESI em realizar o isolamento do roteamento pela possibilidade de balanceamento da rede com diferentes níveis de segurança para as opções de conectividade da WAN (Internet), tornando necessário o isolamento de tabelas.

QUESTIONAMENTO 4

Em relação ao item**: “4.6.15. Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser**

acessíveis via SNMP;", a solução que representamos não possui suporte ao protocolo LLDP e esse item limita a participação de vários fabricantes de solução de segurança. Entendemos que o objeto do SESI-DF é permitir a maior participação de interessados no processo de compra e assim conseguir baixar o valor final de contrato. Baseado, no bom senso do órgão o item não será obrigatório e fator de eliminação de interessados na participação do pregão. Além do fato de não ser item de extrema necessidade técnica ou de segurança de rede.
Está correto nosso entendimento?

Resposta emitida pela Área Técnica (solicitante): A CTIC informa que o entendimento não está correto pois este protocolo é utilizado por diversos fabricantes, tais como:

1. Check Point
2. Fortinet
3. Palo Alto
4. Entre outros

Ademais o protocolo LLDP atende uma necessidade do CN-SESI sendo de suma importância para o troubleshooting, monitoramento e segurança efetiva do ambiente, facilitando a investigação de incidentes e descoberta de potenciais vulnerabilidades, além de sua função de reconhecimento de ativos de rede, sendo utilizado para identificar equipamentos diretamente conectados. Para obter o resultado esperado, serão aceitos acréscimos de outros produtos e serviços para plena execução do protocolo LLDP, mediante comprovação de marca e modelo na proposta técnica.

QUESTIONAMENTO 5

Em relação aos itens abaixo, enviamos o seguinte questionamento**:**

Após pesquisa técnica em sites de vários fabricantes (itens abaixo), constatamos que apenas um único fabricante atende a especificação técnica na sua plenitude.

Mediante a essa identificação, sugerimos que seja feita uma nova especificação técnica onde haja um número maior de participantes e consequentemente o melhor custo x benefício para o erário.

"4.6.18. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
4.6.20. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
4.6.22. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver descriptografia de SSL e SSH;
4.6.26. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
4.7.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
4.7.12. Controle de inspeção e descriptografia de SSH por política;

4.7.13. A descriptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
4.7.19. Deve suportar no mínino três tipos de negação de tráfego nas políticas: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
4.8.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
4.8.10. Deve permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, etc;
4.8.18. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
4.8.19. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da CONTRATANTE;
4.8.20. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:
4.8.20.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.
4.8.24.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando nas mesmas, o volume em bytes trafegado por cada aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra;
4.8.24.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da aplicação na determinada regra;
4.8.24.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias;
4.8.24.4. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos; 4.8.24.5. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;
4.9.9. Deve permitir o bloqueio de vulnerabilidades;
4.9.18. Possuir assinaturas para bloqueio de ataques de buffer overflow;
4.9.19. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
4.9.20. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
4.9.21. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
4.9.26. Deve suportar referência cruzada com CVE;
4.9.29. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;
4.9.30. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

4.10. ANÁLISE DE MALWARES MODERNOS

4.10.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

4.10.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

4.10.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

4.10.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características Documento assinado digitalmente. Verificação em: http://10.16.168.89:8080/docflow/digitalSignChecker.jsf. Utilize o código: ABXR-LLLA-GHM7-ZPZ9

4.10.5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

4.10.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional, Windows 7 (32 bits) e Windows 7 (64 bits), ou superior; 4.10.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;

4.10.8. Para ameaças trafegadas em protocolo SMTP ou POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

4.10.9. O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

4.10.10. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

4.10.11. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

4.10.12. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

4.10.13. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

4.10.14. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falsopositivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência.
4.10.15. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sandbox) independentes para execução simultânea de arquivos suspeitos;
4.10.16. Caso sejam necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sandbox), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;
4.10.17. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
4.10.18. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar), MacOS (mach-O, DMG e PKG), RAR e 7-ZIP no ambiente de sandbox;
4.10.19. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox com frequência de, pelo menos, 5 minutos
4.10.20. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.
4.10.21. Deve permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus da solução;

4.14. FILTRO DE DADOS

4.14.1. **Permite a criação de filtros para arquivos e dados pré-definidos;**
4.14.2. **Os arquivos devem ser identificados por extensão e assinaturas;**
4.14.3. **Permite identificar e opcionalmente prevenir a transferência de vários tipos de a rquivos (MS Office, PDF, etc) identificados sobre protocolos HTTP, HTTPs, FTP, SMTP e S MB;**
4.14.4. **Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;**
4.14.5. **Permitir identificar e opcionalmente prevenir a transferência de informações sensí veis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criaçã o de novos tipos de dados via expressão regular;**
4.14.6. **Permitir listar o número de aplicações suportadas para controle de dados;**
4.14.7. **Permitir listar o número de tipos de arquivos suportados para controle de dados;**

4.16.12. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
4.16.13. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
4.16.14. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

Resposta emitida pela Área Técnica (solicitante): A CTIC esclarece que o CN-SESI pretende contratar empresa especializada para fornecimento de Solução Integrada de Serviços

Gerenciados de Segurança que contemplem serviços de segurança de perímetro com fornecimento de equipamentos, administração e monitoração de segurança, resposta a incidentes de segurança. Dessa forma, todas as funcionalidades pedidas, poderão ser atendidas por um ou mais produtos, devidamente combinados com atividades e expertise da proponente. Dessa forma, não há o que se dizer em restrição de competitividade, pois o objetivo do CN-SESI é o resultado da composição de produtos e serviços. Visando as necessidades do CN-SESI, tais funcionalidades foram pensadas e qualificadas para a segurança e efetiva contenção contra ataques cibernéticos que sofremos no ano passado, conforme descrito no item 2 (Justificativa) do Termo de Referência. O Termo de Referência deste edital foi baseado em editais disponíveis no mercado e visam atender as necessidades deste Conselho.

***Resposta enviada no e-mail** [redacted]@5it.com.br

Brasília, 29 de abril de 2021.

Comissão de Licitação Serviço Social da Indústria – Conselho Nacional