A
FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS – SEADE
PREGÃO ELETRÔNICO 009/2025
Processo Administrativo nº SEI 270.00000015/2025-91
UASG 201201
Data da sessão: 01/07/2025
Horário: 10h

Prezados membros desta comissão, boa tarde!

A NTSEC TECNOLOGIA E SOLUÇÕES LTDA inscrita no CNPJ nº 09.137.728/0001-34, vem por meio desta, solicitar esclarecimentos abaixo, respeitando os prazos e exigências deste referido edital e seus anexos.

- **3.1. Firewall - Solução de Segurança de perímetro (NGFW) Item 1 - TERMO DE REFERÊNCIA**

Itens 7 e 12 (Throughput com funcionalidades de segurança habilitadas)

Com base na análise técnica dos requisitos apresentados nos itens 7 e 12 do edital, gostaríamos de confirmar nosso entendimento quanto à forma de aferição do throughput exigido para o appliance de firewall.

Item 7:

“Suportar Throughput de, no mínimo, 20 Gbps com a funcionalidade de firewall (UTM/NGFW, IPS, Controle de Aplicação, Filtro de URL e Antivírus) habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote.”

Item 12:

“Suportar Throughput de, no mínimo, 1 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.”

Nosso entendimento técnico é o seguinte:

- O throughput de **20 Gbps mencionado no item 7** refere-se ao desempenho do equipamento com as funcionalidades típicas de **NGFW** habilitadas, ou seja, **firewall de nova geração (NGFW), IPS, controle de aplicação** mas **sem todas as assinaturas e engines de proteção avançada ativadas simultaneamente**;
- Já o **throughput de 1 Gbps mencionado no item 12** se refere ao desempenho com **todas as assinaturas e mecanismos de inspeção profunda habilitados e atuantes simultaneamente**, incluindo **controle de aplicação, IPS, antivírus, antispyware, filtro URL** e entendemos também que este throughput corresponde ao que o mercado normalmente chama de **Threat Protection Throughput** (ou Full Inspection / Deep Inspection), o qual pode incluir ainda **inspeção SSL, sandboxing e análise comportamental**, conforme o escopo da solução ofertada.

Dessa forma:

Podemos considerar que o item 7 se refere ao throughput de NGFW e o item 12 ao throughput de Threat Protection, conforme as definições mais comuns de mercado e medições técnicas padronizadas?
Está correto o nosso entendimento?

- **3.5. Solução de XDR (400 (quatrocentas) licenças - ITEM 5 - TERMO DE REFERÊNCIA**

1. *A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows (versões 32 e 64 bits) XP SP2 / SP3, 7, 8, 8.1 e 10*
2. *A solução proposta deve ser compatível com os seguintes sistemas operacionais: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022;*
3. *A solução proposta deve ser compatível com os seguintes sistemas operacionais: versões macOS: Yosemite (10.10), El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) e Catalina (10.15)*
4. *A solução proposta deve ser compatível com os seguintes sistemas operacionais: Versões do Linux: RedHat Enterprise Linux e CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 e 7.7 e Ubuntu LTS 16.04.5, 16.04.6, servidor 18.04.1 e 18.04.2, 64 bits"*
5. *A solução proposta deve ser compatível com os seguintes sistemas operacionais: Ambientes de Virtual Desktop Infrastructure (VDI) em VMware E Citrix. VMware Horizons 6 e 7 e Citrix XenDesktop 7*
6. *A solução proposta deve ser compatível com os seguintes sistemas operacionais: Oracle Linux OL (antigo OEL)*

O edital exige compatibilidade com diversos sistemas operacionais antigos e descontinuados, tais como:

- **Windows XP SP2/SP3, Windows Server 2003/2008, macOS Yosemite até Catalina, e distribuições Linux como Red Hat e CentOS 6.x, Ubuntu 16.04,** entre outros.

Entendemos que tais sistemas encontram-se **fora do ciclo de suporte oficial dos próprios fabricantes** (EOL – End of Life), não recebendo atualizações de segurança, o que compromete sua estabilidade e coloca em risco a segurança da rede. Além disso, tecnologias de XDR atuais não operam com agentes compatíveis nesses ambientes por razões técnicas e de segurança.

Dessa forma, entendemos que:

Questionamento 1: É possível considerar que os requisitos de compatibilidade com sistemas operacionais legados (itens 1 a 6) sejam classificados como **não eliminatórios**, ou que seja aceita compatibilidade apenas com **sistemas em suporte oficial** por seus fabricantes?
Está correto o nosso entendimento?

- **3.5. Solução de XDR (400 (quatrocentas) licenças - ITEM 5 - TERMO DE REFERÊNCIA**

Os itens 7 a 9 do edital determinam que o agente da solução tenha um consumo:

7. A solução proposta deve ter um consumo máximo de 120 MB de memória RAM
8. A solução proposta deve ter um consumo médio de menos de 2% do uso da CPU
9. A solução proposta deve consumir menos de 20 MB de espaço em disco

Entendemos que esses parâmetros não refletem o comportamento real de agentes XDR modernos, que utilizam mecanismos avançados como **análise comportamental, machine learning, e inspeção contínua** para identificar ameaças sofisticadas. Em tais cenários, o consumo de recursos pode variar dinamicamente, especialmente durante eventos de escaneamento, mitigação ou resposta a incidentes.

Além disso, é importante considerar que **o desempenho do agente também dependerá das características técnicas da máquina onde ele será instalado**, como arquitetura do processador, quantidade de memória RAM disponível, utilização de disco, e outros fatores de ambiente. Dessa forma, **não é tecnicamente viável garantir um consumo fixo e padronizado de CPU, RAM e disco em todos os cenários possíveis**, dada a heterogeneidade da infraestrutura computacional nos ambientes corporativos.

Por isso, compreendemos que:

Questionamento 2: Os limites estabelecidos para consumo de recursos referem-se ao estado **ocioso** do agente, e não durante atividades intensivas como escaneamento ou resposta ativa, sendo aceitável variação conforme o contexto do endpoint?

Está correto o nosso entendimento?

Desde já agradecemos e ficamos no aguardo do retorno.

Atenciosamente

Prezados Senhores,

Em atenção ao Pedido de Esclarecimento referente ao Pregão Eletrônico N° 009/2025, esta Fundação SEADE manifesta-se nos seguintes termos:

“Podemos considerar que o item 7 se refere ao throughput de NGFW e o item 12 ao throughput de Threat Protection, conforme as definições mais comuns de mercado e medições técnicas padronizadas?

Está correto o nosso entendimento?”

ESCLARECIMENTO: A referência do item 7 do 3. ESPECIFICAÇÕES DAS CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS (pg 86) deve ser atendida, é sobre Throughput de Firewall, IPv4 e IPv6, UDP 1518 / 512 / 64 byte.

“**Questionamento 1:** É possível considerar que os requisitos de compatibilidade com sistemas operacionais legados (itens 1 a 6) sejam classificados como **não eliminatórios**, ou que seja aceita compatibilidade apenas com **sistemas em suporte oficial** por seus fabricantes?

Está correto o nosso entendimento?”

ESCLARECIMENTO:

A Fundação Seade possui equipamentos com sistemas legados, não em produção, mas que eventualmente podem ser conectados à rede para recuperação de dados/informações/sistemas antigos, tais equipamentos podem possuir Windows XP, Windows 7, Windows Server 2003 e 2008 e nesses casos precisam de cobertura, são críticos, justamente por não possuir mais atualizações e/ou suporte do fabricante. A dificuldade na cobertura dos legados é compreendida, havendo flexibilização, neste contexto e conforme esclarecimento prestado em questionamento anterior:

Flexibilização da Exigência – Condições e Abrangência: Com o objetivo de assegurar a plena funcionalidade, a segurança e a aderência da solução ofertada ao ambiente existente, seguem as seguintes condições:

a) A regra de fornecimento da **versão mais atual do software agente (coletor) permanece integralmente válida para todos os sistemas operacionais que a Fundação SEADE considera em fase de suporte ativo por seus respectivos fabricantes e para os quais a versão mais recente do agente XDR seja compatível**. Isso inclui, mas não se limita a, Windows 10 Professional e superiores, Windows Server 2012 R2 e superiores (2016, 2019, 2022), e as versões de macOS e Linux que ainda recebam atualizações de segurança de seus fornecedores originais.

b) Será **permitido o fornecimento de uma versão de software agente (coletor) que não seja a mais recente disponibilizada pelo fabricante da solução XDR, mas que seja compatível, com suporte ativo do fabricante da solução XDR e receba atualizações de segurança**, para os sistemas operacionais listados no edital que se enquadrem nas seguintes condições de

"legado": * Sistemas operacionais que já atingiram o **status de "End-of-Life" (EOL)** ou "fim de suporte de segurança" por seus respectivos fabricantes (ex: Windows XP SP2/SP3, Windows Server 2003 R2 SP2, Red Hat Enterprise Linux e CentOS 6.x, Ubuntu LTS 16.04.x).

Requisitos:

a) A versão exata do software agente (coletor) da solução XDR que será instalada para cada sistema operacional legado específico (ex: Windows XP SP3, CentOS 6.10, etc.) deverá ser identificada.

b) A versão do agente XDR ofertada para os sistemas legados deve ainda **receber patches e atualizações de segurança** para ser executada no sistema operacional legado declarado.

c) Devem ser destacados eventuais impactos ou limitações conhecidas do uso de versões não mais recentes do agente XDR em comparação com a versão mais atual, especialmente no que tange a funcionalidades e desempenho, mesmo que para sistemas legados.

A flexibilização visa garantir a abrangência e eficácia da solução em todo o parque computacional da Fundação SEADE, sem comprometer a segurança, independentemente da versão, receba suas atualizações pertinentes.

“Questionamento 2: Os limites estabelecidos para consumo de recursos referem-se ao estado **ocioso** do agente, e não durante atividades intensivas como escaneamento ou resposta ativa, sendo aceitável variação conforme o contexto do endpoint?
Está correto o nosso entendimento?”

ESCLARECIMENTO: Devido a dinâmica operacional das soluções XDR modernas. Temos o seguinte:

- **Comportamento de Agentes XDR Modernos:** Reconhecemos que as soluções XDR atuais utilizam mecanismos avançados como análise comportamental, machine learning e inspeção contínua. Essas tecnologias são fundamentais para a identificação de ameaças sofisticadas, mas, por sua natureza, demandam um uso de recursos que varia dinamicamente. É, de fato, esperado que durante eventos de escaneamento, mitigação ou resposta a incidentes, o consumo de CPU, RAM e disco possa superar os limites (dentro do razoável) estabelecidos para um estado ocioso.
- **Variação Conforme o Contexto do Endpoint:** Além disso, a heterogeneidade da infraestrutura computacional nos ambientes corporativos é um fator crucial. O desempenho do agente é, sem dúvida, influenciado pelas características técnicas da máquina onde será instalado (arquitetura do processador, RAM disponível, utilização de disco, etc.). Dessa forma, pode não ser preciso garantir um consumo fixo e padronizado de CPU, RAM e disco em todos os cenários possíveis de operação.

Portanto, reafirmamos que os limites estabelecidos para o consumo de recursos (120 MB de memória RAM, menos de 2% de uso da CPU e menos de 20 MB de espaço em disco) referem-se ao estado ocioso estimado do agente.

É aceitável que haja variação no consumo conforme o contexto do endpoint, especialmente durante atividades intensivas como escaneamento, detecção ativa ou resposta a incidentes. O que buscamos é um desempenho otimizado em condições normais de operação, sem que isso impeça a capacidade da solução de atuar de forma eficaz em momentos críticos, sendo, portanto, neste contexto, são aceitos os valores sugeridos.