Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL

EXAME

DE ESCLARECIMENTOS

PREGÃO ELETRÔNICO Nº 90428/2024/SUPEL/RO

Processo Administrativo: 0035.003501/2023-45

Objeto: Aquisição de um software antivírus para atender a estação de trabalho (usuários), baseando- se no fato de que o antivírus corporativo é um software de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais. Antivírus para usuários finais são mais simples, focando na defesa contra sites maliciosos, spam e outras ameaças comuns. Já as soluções corporativas incluem pacotes de serviços exclusivos para empresas, capacitando-as a lidar com grandes volumes de dados e diversas variedades de ciberataques e Licença de Antivírus para equipamento do tipo servidor físico ou virtual para implementar os ativos do *Data Center* da SEPOG.

A Superintendência Estadual de Licitações – SUPEL, através do Pregoeiro Substituto nomeado na Portaria nº 29/2025/SUPEL/GAB**,** vem neste ato responder ao pedido de esclarecimento, enviado por e-mail por empresa interessada.

1 - DO PEDIDO DE ESCLARECIMENTO - 0059124416

''Prezados boa noite Segue pedido de esclarecimento do edital supracitado, processo Nº 0035.003501/2023-45. A empresa xxxx sediada em Porto Velho vem respeitosamente solicitar esclarecimentos dos seguintes itens que nos deixam fora do processo, o qual poderemos atender com melhor custo benefício em relação o que exige nas especificações técnicas do termo de referência sem prejuízo de entrega de solução inferior. Aliás, nossa oferta trata-se de solução que compete em características técnicas com a solução da Fortinet, o qual encontra-se bem avaliada por vários Órgãos de avaliações internacionais como os recentes Testes de MITRE. Segue quesonamentos: Em relação aos itens abaixo exige-se as especificações que estão fechados para um único fabricante:

1. Realizar um patch virtual, através da restrição de acessos nas aplicações vulneráveis;

2. O antivírus deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado;

3. O antivírus deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo e os destinos IP do tráfego gerado pelo aplicativo.

4. O antivírus de referência adotada nesta especificação técnica se baseia no modelo ForEDR;

5. A citação do modelo se pauta na necessidade da oferta dos licitantes ser totalmente integrada com os ativos FORTINET presentes em nosso ambiente, composto de diversas soluções da referida fabricante.

Verificamos que é solicitado no edital que o aplicativo deve incorporar as técnicas do MITRE ATT&CK. Conforme pode se observar na página deste orgão: hps://aackevals.mitre-engenuity.org/ não tem informações sobre o fabricante Fortinet. Isto implicaria uma grande lacuna de informação sob a Capacidade de Proteção de Ameaças como o menuPass + ALPHV BlackCat (2024) Seria aceitar em um orgão público uma ferramenta não testada em sua eficiência conforme pedido no edital A integração com Firewalls sempre será possível desde que o Firewall permita e isso deveria ser demandado a nível de Firewall e não dos EDRs Soluções de mercado altamente capacitadas como SentinelOne, Checkpoint, Crowdstrike e Capture Client (SonicWall) estariam impedidos de parciparem deste edital. Visto que a Fornet não ter parcipado dos recentes Testes de MITRE o que a qualificaria junto com Kaspesrky que também não parcipa a muitos anos dos testes do MITRE, invalidando assim sua capacidade de detecção a ataques de hackers reais Seguem os recentes testes e os resultados dos que se submeteram, que podemos ulizar na nossa argumentação

Fonte: https://attackevals.mitre-engenuity.org/

Black MITRE TESTS

menuPass + ALPHV BlackCat (2024)

SentinelOne

Checkpoint

Crowdstrike

Podemos verificar que a maioria dos Orgãos, inclusive Orgãos Estaduais de Rondonia, possuem anvirus de fabricantes diferentes do firewall o qual funciona em perfeita harmonia sem problema de compabilidade, inclusive é até mesmo recomendado em relação a segurança que seja de fabricantes disntos. Sendo assim perguntamos se é possível a oferta de fabricantes de soluções de anvírus que não seja o mesmo do firewall, o qual atende integralmente o que se pede no objeto que é antivírus corporativo de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais? Temos a certeza que o orgão em nenhum momento será prejudicado por abrir a competição para estes renomados fabricantes de cibersegurança. Agradecemos a atenção e ficamos a disposição para escalrecimentos.''

2 - ANÁLISE E CONCLUSÃO - Resposta 0059142563

Inicialmente, considerando a especificidade técnica dos questionamentos, informo que o pedido de esclarecimentos foi encaminhado para a Unidade Requisitante para manifestação por meio do Despacho 0059126655, tendo esta emitido a **Resposta 0059142563 SEPOG-ASTIC,** a qual cito:

*''**RESPOSTA AO PEDIDO DE ESCLARECIMENTO***

*Em atenção ao pedido de esclarecimento protocolado pela empresa **xxxx**, referente ao Pregão Eletrônico nº 90428/2025, informamos o seguinte:*

*As especificações técnicas constantes no Termo de Referência foram elaboradas com base na **infraestrutura tecnológica já existente na Secretaria de Estado do Planejamento, Orçamento e Gestão – SEPOG**, a qual adota um ecossistema de segurança da informação **padronizado na fabricante Fortinet**, incluindo soluções como **firewall, gerenciamento centralizado, monitoramento e resposta a incidentes**.*

*A **padronização e a integração nativa entre os componentes da arquitetura de segurança da informação são fatores imprescindíveis para a administração eficiente do ambiente da SEPOG**, considerando que **a Secretaria dispõe de uma equipe técnica enxuta, com recursos humanos limitados para operar e manter múltiplas plataformas de diferentes fabricantes**.*

*Portanto, a exigência de que a solução de proteção contra ameaças cibernéticas possua **integração com os ativos Fortinet já implantados** não configura direcionamento indevido, mas sim **uma exigência técnica motivada pela necessidade de compatibilidade, continuidade operacional, interoperabilidade, controle centralizado e mitigação de riscos.***

Destacamos ainda que:

- *Os requisitos funcionais descritos no edital (como aplicação de patch virtual, controle por versão de aplicativos e visibilidade de tráfego) são **características esperadas de soluções modernas de EDR/NGAV** e **não exclusivas de um único fabricante**;*

- *A citação ao modelo ForEDR é meramente **referencial**, com intuito de **exemplificar o nível de proteção esperado**;*
- *A **aderência à matriz MITRE ATT&CK** se refere ao uso das táticas e técnicas como base metodológica para detecção de ameaças, e **não exige participação formal nos testes públicos do MITRE Engenuity**;*
- *A participação de fabricantes distintos da Fortinet **é permitida**, desde que a solução ofertada **atenda integralmente às exigências funcionais do edital e comprove integração compatível com o ambiente atual da SEPOG**.*
  - *O produto somente será aceito se após a instalação for identificada a integração das plataformas. Caso contrário o objeto será recusado.*

*A administração pública tem o dever de buscar soluções que garantam **maior segurança, eficiência operacional e economicidade**. Nesse sentido, a escolha por uma arquitetura integrada e coerente com os sistemas atualmente em uso **assegura maior governança e controle do ambiente tecnológico**, sem prejuízo à ampla competitividade, desde que respeitadas as condições técnicas estabelecidas.*

Sem mais para o momento, colocamo-nos à disposição para eventuais esclarecimentos adicionais.''

À vista disso, considerando a manifestação técnica da Unidade Requisitante, no sentido de manter a exigência e o descritivo analisado, informo que o edital permanecerá inalterado.

3 - DO PEDIDO DE ESCLARECIMENTO - 0059164185

''Prezados, boa noite, Solicitamos esclarecimentos sobre o item 1 do edital de pregão em epígrafe.

1. Ambiente Atual de Segurança Qual é a solução anvírus atualmente ulizada pela SEPOG em estações e servidores? Existem outras ferramentas de segurança atualmente implementadas (como EDR, firewall, SIEM)? A SEPOG possui inventário atualizado das máquinas e estações que receberão a solução? Todas as máquinas estão integradas a um domínio Acve Directory? A infraestrutura da SEPOG conta com ambientes virtualizados? Se sim, qual o hipervisor ulizado? Onde está instalado o gerenciador do Kaspersky hoje? Em estrutura própria ou de terceiros? Quantos dispositivos existem no ambiente no total? Quais são os sistemas operacionais em uso? Quais versões? Quantos servidores físicos possui no ambiente? Qual a versão do sistema operacional dos servidores físicos? O ambiente conta com servidores virtuais? Se sim, quantos? Quantos desktops há na estrutura? Quantos dispositivos móveis precisam de proteção? Qual o sistema operacional dos dispositivos moveis? A empresa possui Active Directory (AD)? Há um Firewall em uso? Se sim, qual solução é utilizada? O acesso remoto à rede da empresa é permitido? Qual o tipo de conexão com a internet? Qual a velocidade da conexão com a internet?

2. Infraestrutura para Instalação A SEPOG dispõe de servidor (sico ou virtual) disponível para a instalação da console de gerenciamento da solução? A solução deverá obrigatoriamente ser instalada em ambiente on-premises ou aceita também console em nuvem? Há restrições de acesso à internet (proxy/firewall) que possam impactar a atualização das definições de segurança nos endpoints?

3. Escopo de Instalação e Licenciamento O escopo inclui a instalação da solução também em servidores (Windows Server, Linux), conforme mencionado no item 2? Caso afirmavo, é possível informar a quandade esmada de servidores e seus respecvos sistemas operacionais? Haverá endpoints fora da rede local (home office, unidades remotas)? Há expectava de proteção remota para esses disposivos? Existe necessidade de cobertura para estações com sistema operacional Linux?

4. Recursos e Funcionalidades Esperadas Há modelo padrão de relatórios exigido (HTML, PDF, CSV)? Existe periodicidade definida para emissão? Quais eventos de segurança devem obrigatoriamente gerar alertas por e-mail? Existe a necessidade de auditoria detalhada das ações administravas executadas via console? A SEPOG requer a funcionalidade de desinstalação automazada do anvírus atualmente instalado?

5. Suporte e Atendimento A solução deverá contar com suporte técnico em português durante todo o período contratual? Qual SLA, escopo e disponibilidade são esperados do suporte? Nosso suporte

está disponível por meio de abertura de chamados em uma plataforma online, com primeira resposta em oito horas úteis e apenas suporte nível 1. Isso atenderia vocês?''

4 - ANÁLISE E CONCLUSÃO - Resposta 0059228874

Considerando a especificidade técnica dos questionamentos, informo que o pedido de esclarecimentos foi encaminhado para a Unidade Requisitante para manifestação por meio do Despacho 0059164337, tendo esta emitido a **Resposta 0059228874 SEPOG-ASTIC,** a qual cito:

*'' **1. AMBIENTE ATUAL DE SEGURANÇA***

Qual é a solução antivírus atualmente utilizada pela SEPOG em estações e servidores?

Resposta: A SEPOG utiliza atualmente o Kaspersky (venceu em abril/2024)

Existem outras ferramentas de segurança atualmente implementadas (como EDR, firewall, SIEM)?

Resposta: A SEPOG utiliza Firewall Fortinet

A SEPOG possui inventário atualizado das máquinas e estações que receberão a solução?

Resposta: A solução de inventário está desatualizada

Todas as máquinas estão integradas a um domínio Active Directory?

Resposta: Todas as máquinas Windows.

A infraestrutura da SEPOG conta com ambientes virtualizados? Se sim, qual o hipervisor utilizado?

Resposta: AHV Nutanix

Onde está instalado o gerenciador do Kaspersky hoje? Em estrutura própria ou de terceiros?

Resposta: Máquina Virtual Estrutura própria

Quantos dispositivos existem no ambiente no total?

Resposta: Está no TR

Quais são os sistemas operacionais em uso? Quais versões?

Resposta: Está listado no TR a solução deve ser compatível com diversas versões.

Quantos servidores físicos possui no ambiente?

Resposta: Apenas os nó de hiperconvergencia e a Storage.

Qual a versão do sistema operacional dos servidores físicos?

Resposta: AHV Nuntanix

O ambiente conta com servidores virtuais? Se sim, quantos?

Resposta: Está no quantitativo. no processo

Quantos desktops há na estrutura?

Resposta: Está no quantitativo. no processo

Quantos dispositivos móveis precisam de proteção?

Resposta: Não se aplica

Qual o sistema operacional dos dispositivos moveis?

Resposta: Não se aplica

A empresa possui Active Directory (AD)?

Resposta: Sim

Há um Firewall em uso? Se sim, qual solução é utilizada?

Resposta: Sim, Fortinet

O acesso remoto à rede da empresa é permitido?

Resposta: Apenas se formalizado

Qual o tipo de conexão com a internet?

Rsposta: Fibra

Qual a velocidade da conexão com a internet?

Resposta: 500 Mb

2. INFRAESTRUTURA PARA INSTALAÇÃO

A SEPOG dispõe de servidor (físico ou virtual) disponível para a instalação da console de gerenciamento da solução?

Resposta: Já foi respondido, sim, possuí (virtual)

A solução deverá obrigatoriamente ser instalada em ambiente on-premises ou aceita também console em nuvem?

Resposta: Obrigatoriamente on-premises

Há restrições de acesso à internet (proxy/firewall) que possam impactar a atualização das definições de segurança nos endpoints

Resposta: Existe restrição, sua equipe deve fornecer as URLs para liberação.

3. ESCOPO DE INSTALAÇÃO E LICENCIAMENTO

O escopo inclui a instalação da solução também em servidores (Windows Server, Linux), conforme mencionado no item 2?

Resposta: sim

Caso afirmativo, é possível informar a quantidade estimada de servidores e seus respectivos sistemas operacionais?

Resposta: Já foi respondido

Haverá endpoints fora da rede local (home office, unidades remotas)? Há expectativa de proteção remota para esses dispositivos?

Resposta: Sim em home office

Existe necessidade de cobertura para estações com sistema operacional Linux?

Resposta: Sim existe a cobertura.

4. RECURSOS E FUNCIONALIDADES ESPERADAS

Há modelo padrão de relatórios exigido (HTML, PDF, CSV)? Existe periodicidade definida para emissão?

Resposta: No mínimo PDF e CSV. A periodicidade deve ser opcional definida em um painel de controle.

Quais eventos de segurança devem obrigatoriamente gerar alertas por e-mail?

Resposta: Deve ser opcional definidos em um painel de controle.

Existe a necessidade de auditoria detalhada das ações administrativas executadas via console?

Resposta: Se houver a opção sim

A SEPOG requer a funcionalidade de desinstalação automatizada do antivírus atualmente instalado?

Resposta: Se houver a opção sim

5. SUPORTE E ATENDIMENTO

A solução deverá contar com suporte técnico em português durante todo o período contratual?

Resposta: Sim, conforme Termo de Referência

Qual SLA, escopo e disponibilidade são esperados do suporte? Nosso suporte está disponível por meio de abertura de chamados em uma plataforma online, com primeira resposta em oito horas úteis e apenas suporte nível 1. Isso atenderia vocês?

Resposta: Desde que solucionem o problema apresentado, sim.

Porto Velho, 11 de abril de 2025.''

À vista disso, considerando a manifestação técnica da Unidade Requisitante, no sentido de manter a exigência e o descritivo analisado, informo que o edital permanecerá inalterado.

DA DECISÃO

Isto posto, **presto os ESCLARECIMENTOS solicitados e considerando que as informações não afetam a formulação das propostas de preços, registro que o prazo de abertura do certame fica mantido** para o dia **14 de abril de 2025, às 10h00min. (horário de Brasília - DF)**, no site: https://www.comprasgovernamentais.gov.br/, permanecendo os demais termos do edital inalterados.

Porto Velho - RO, 11 de abril de 2025.

Thales Silva Souza
Pregoeiro Substituto - SUPEL/RO

Documento assinado eletronicamente por **Thales Silva Souza**, **Pregoeiro(a)**, em 11/04/2025, às 13:59, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0059235686** e o código CRC **434032B6**.

Referência: Caso responda este(a) Exame, indicar expressamente o Processo nº 0035.003501/2023-45 SEI nº 0059235686