



RESPOSTA AO PEDIDO DE ESCLARECIMENTO

Ref.: Pregão Eletrônico nº 72/2026

Processo nº P204663/2026

Assunto: Pedido de Esclarecimento – Solução Antivírus Endpoint Detection and Response – EDR

Veio a este setor Célula de Gestão de Tecnologia da Informação e Comunicação – CETEC, pedido de esclarecimento.

Em atenção ao pedido de esclarecimento apresentado, referente aos requisitos técnicos previstos no Termo de Referência e no Estudo Técnico Preliminar, especialmente quanto às funcionalidades de Firewall de Host e integração com outras soluções de segurança, apresentam-se os seguintes esclarecimentos:

1. Quanto ao Firewall de Host

1.1. Serão aceitas soluções EDR/NGAV que realizem controle de tráfego e proteção de rede por meio de integração nativa com o firewall do sistema operacional, desde que o gerenciamento das regras seja efetuado de forma centralizada pela solução ofertada?

Resposta:

Não.

Para fins de atendimento ao requisito, a solução EDR/NGAV deverá disponibilizar funcionalidade própria e integrada de Firewall de Host, contemplando os recursos necessários para controle e proteção do tráfego de rede, bem como a criação, aplicação e gerenciamento centralizado das respectivas políticas por meio da solução ofertada.

Não será considerado suficiente o simples aproveitamento, integração ou gerenciamento do firewall nativo do sistema operacional, ainda que este possibilite a criação e aplicação de regras de tráfego.

A solução deverá atender integralmente às funcionalidades estabelecidas no item 10 dos requisitos funcionais, incluindo o controle bidirecional de tráfego por aplicação, porta, protocolo e endereço IP, com políticas baseadas em localização (rede interna, externa e Wi-Fi).

1.2. O requisito será considerado atendido quando a solução possibilitar a criação, aplicação e gerenciamento centralizado de regras por aplicação, porta, protocolo e endereço IP, ainda que utilize mecanismos nativos do sistema operacional?

Resposta:

Não.



O requisito será considerado atendido somente quando a solução EDR/NGAV ofertada disponibilizar Firewall de Host como funcionalidade integrante da própria solução, permitindo a criação, aplicação, gerenciamento e administração centralizada das políticas de segurança. A utilização de mecanismos nativos do sistema operacional, isoladamente ou como recurso principal para atendimento ao requisito, não será considerada suficiente, ainda que tais mecanismos possam ser administrados de forma centralizada.

A solução deverá disponibilizar os recursos de Firewall de Host necessários ao atendimento integral das funcionalidades previstas no item 10 dos requisitos funcionais, incluindo o controle bidirecional de tráfego por aplicação, porta, protocolo e endereço IP, bem como políticas baseadas na localização da rede.

1.3. Existe a obrigatoriedade de que o Firewall Host seja um módulo proprietário do fabricante da solução ofertada ou serão aceitas soluções equivalentes que entreguem as funcionalidades requeridas e o mesmo resultado operacional?

Resposta:

Não necessariamente.

Não se estabelece a obrigatoriedade de que o Firewall de Host seja desenvolvido exclusivamente pelo próprio fabricante da solução EDR/NGAV. Entretanto, o mecanismo ofertado deverá constituir funcionalidade integrante e devidamente integrada à solução EDR/NGAV, possibilitando sua configuração, aplicação e gerenciamento de forma centralizada por meio da própria solução.

Não será considerado suficiente o simples aproveitamento ou gerenciamento do firewall nativo do sistema operacional, conforme esclarecido nos itens 1.1 e 1.2.

Serão aceitas diferentes arquiteturas tecnológicas, desde que a solução ofertada disponibilize efetivamente a funcionalidade de Firewall de Host e atenda integralmente aos requisitos estabelecidos no item 10 do Termo de Referência, independentemente da forma de implementação adotada pelo fabricante.

1.4. Serão aceitos datasheets, documentação técnica e declaração do fabricante ou distribuidor autorizado?

Resposta:

Sim.

Serão aceitos, para fins de comprovação das características técnicas, documentos oficiais do fabricante, incluindo datasheets, manuais, documentação técnica, matriz de funcionalidades e declarações formais emitidas pelo fabricante ou representante/distribuidor autorizado, desde que permitam verificar objetivamente o atendimento aos requisitos estabelecidos no Termo de Referência.



A Administração poderá solicitar documentação técnica complementar quando a documentação apresentada não for suficiente para comprovar o atendimento ao requisito específico.

2. Quanto ao SIEM e SOAR

2.1. Qual SIEM/SOAR está atualmente em uso?

Resposta:

Esclarece-se que o Termo de Referência não estabelece a integração imediata com uma plataforma SIEM ou SOAR específica como requisito obrigatório da contratação.

O item 11 dos requisitos funcionais estabelece a necessidade de "Integração com outras soluções de segurança, quando aplicável", devendo tal requisito ser interpretado como capacidade de interoperabilidade da solução ofertada.

A referência à integração com SIEM e SOAR constante do levantamento de mercado do Estudo Técnico Preliminar representa característica associada às soluções EDR avaliadas no levantamento, não constituindo, por si só, exigência de integração imediata com plataforma SIEM ou SOAR específica.

2.2. E se não existir SIEM/SOAR atualmente?

Resposta:

Considerando que não foi estabelecida no Termo de Referência uma plataforma SIEM ou SOAR específica para integração imediata, serão aceitas soluções EDR que disponibilizem mecanismos de interoperabilidade com outras soluções de segurança, tais como APIs, Syslog, Webhooks, CEF, conectores nativos ou mecanismos equivalentes.

O objetivo é assegurar que a solução contratada possua capacidade técnica de disponibilizar eventos, alertas, logs e demais informações de segurança para eventual integração presente ou futura com plataformas de segurança adotadas pela Administração.

2.3. Caso exista SIEM/SOAR implantado, qual é o fabricante?

Resposta:

Não há, para esta contratação, exigência de integração imediata com uma plataforma SIEM ou SOAR específica.

Consequentemente, não se estabelece fabricante, versão ou modelo específico de plataforma SIEM/SOAR como requisito para formulação da proposta.

2.4. APIs, Syslog, CEF, Webhooks e conectores nativos serão suficientes?

Resposta:



Sim, desde que tais mecanismos possibilitem efetivamente o envio, compartilhamento ou disponibilização dos eventos, alertas, logs e demais informações de segurança necessárias à interoperabilidade com outras soluções.

Serão aceitos APIs, Syslog, CEF, Webhooks, conectores nativos ou mecanismos tecnicamente equivalentes, desde que comprovada a capacidade de integração da solução ofertada.

3. Considerações finais

Os esclarecimentos acima têm por finalidade objetivar a interpretação dos requisitos técnicos já estabelecidos no Termo de Referência, sem alteração do objeto ou criação de exigências adicionais.

A Administração busca contratar solução de segurança de endpoints do tipo Antivírus Endpoint Detection and Response (EDR), contemplando os recursos de prevenção, detecção e resposta a incidentes, gerenciamento centralizado, proteção de rede por meio de Firewall de Host, aplicação de políticas de segurança, geração de relatórios, registro de logs e demais funcionalidades estabelecidas no instrumento convocatório.

Serão admitidas soluções tecnicamente equivalentes, independentemente da arquitetura ou implementação tecnológica adotada pelo fabricante, desde que atendam integralmente às funcionalidades e condições estabelecidas no Termo de Referência.

FRANCISCO ULISSE
LIMA
JUNIOR:04065059348

Assinado de forma digital por FRANCISCO ULISSE LIMA
JUNIOR:04065059348
DN: c=BR, o=ICP-Brasil, ou=Secretaria da Receita
Federal do Brasil - RFB, ou=RFB e-CPF A3, ou=(EM
BRANCO), ou=23035197000108, ou=presencial,
cn=FRANCISCO ULISSE LIMA JUNIOR:04065059348
Dados: 2026.10.02 16:59:01 -03'00'

FRANCISCO ULISSE LIMA JUNIOR

Gerente

Célula de Gestão de Tecnologia da Informação e Comunicação – CETEC