Pregão Eletrônico

- **Visualização de Recursos, Contrarrazões e Decisões**

CONTRARRAZÃO :

A ILUSTRÍSSIMA SENHORA PRESIDENTE DA COMISSÃO PERMANENTE DE LICITAÇÃO

PREGÃO ELETRÔNICO Nº 19/2020
Processo Administrativo n° 25100.000.191/2020-64
À Comissão Permanente de Licitação – CPL
Sra. Pregoeira

GLOBAL IP TECNOLOGIA INN TECNOLOGIA DA INFORMAÇÃO LTDA, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº 08366661-0001/47, estabelecida no endereço SCN SETOR COMERCIAL NORTE, QD. 04, BLOCO B, N. 100, SALA 1402, Cobertura, EDIFÍCIO VARIG, ASA NORTE, BRASÍLIA – DF, CEP: 70.714-900, neste ato representada por seu Representante Legal, Ronaldo de Albuquerque Ribeiro, já devidamente qualificado nos Autos do certame em referência, vem respeitosamente à presença de Vossa Senhoria, tempestivamente, com fulcro no Artigo 109, inciso I, alínea "a", §3º, da Lei 8.666/93, a fim de interpor:

CONTRARRAZÕES AO RECURSO ADMINISTRATIVO

Interposto pela concorrente/licitante ALL TECH, irresignada com a decisão da Comissão de Licitação que a inabilitou/desclassificou, consoante as razões de fato e de direito a seguir apontadas de forma detalhada que demonstram e ratificam a decisão tomada pela Comissão pelas razões a seguir:

DA TEMPESTIVIDADE

Diante da comunicação do recurso, o prazo para impugnação/contrarrazões finda-se na data de 27 de janeiro de 2021, Quarta-feira.

DOS FATOS

A FUNASA, publicou o Edital no. 19/2020, tornando público o Pregão Eletrônico do tipo menor preço, tendo por objeto o Registro de Preço para contratação de licenciamento de solução de segurança para proteção de estações de trabalho ("Endpoint") e redes, com serviços de suporte técnico e atualização, serviço de migração e serviço de treinamento para atender às necessidades da Funasa, pelo período de 36 (trinta e seis) meses.
Com a inabilitação da licitante anterior, a GLOBAL IP passou a ser classificada, posto que atende todos os requisitos do edital convocatório.

Irresignada, a empresa ALL TECH apresentou recurso pela inabilitação.
A presente contrarrazões têm o intuito de ratificar a classificação e habilitação da licitante GLOBAL IP TECNOLOGIA DA INFORMAÇÃO, com fatos contrários às informações contidas no recurso impetrado pela licitante ALL TECH a qual solicita a desclassificação da GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA de forma equivocada, uma vez que a empresa atende todas as exigências do edital, conforme será demonstrado.

DAS CONTRARRAZÕES

DA ESTRITA OBSERVÂNCIA AOS PRINCÍPIOS QUE REGEM O PROCESSO LICITATÓRIO

É consabido que todo e qualquer processo licitatório deve ser norteado pelos Princípios básicos estampados no caput do Artigo 3º, da Lei nº 8.666/93.

Significa dizer que a Administração Pública só pode fazer o que a Lei permite. Logo, se a Lei permite que a Administração Pública contrate com o ente privado e estabelece um meio formal para isso (que é a Licitação), as Partes envolvidas (licitantes e Administração Pública) devem se pautar pelas diretrizes e regramentos do edital aprovado para a finalidade específica, eis que se submetem de forma subordinada ao certame.

Por isso, caso a Comissão Permanente de Licitação ao analisar toda a documentação enviada pela GLOBAL IP TECNOLOGIA DA INFORMAÇÃO, concluiu pela sua c, acertadamente, pela sua habilitação, diante de cumprimento ao Princípio da Legalidade e Princípio da Vinculação ao Instrumento Convocatório, o qual vincula a Administração Pública.

Nessa perspectiva, passamos a corroborar a decisão de habilitação, elencamos ponto a ponto as considerações:

QUANTO AO ITEM 1 do Recurso:

1) Em atenção ao item sub item 1.1, item 1 do Anexo I do Termo de Referência, onde se lê "A solução de gerenciamento deverá ser feita através de uma central única, baseada em web e em nuvem, que deverá conter todas a ferramentas para a monitoração e controle da proteção dos dispositivos;", resta claro, em análise da documentação proposta como comprovatória (documento "5-Endpoint Security Administration Guide R80.30.pdf") que não há a funcionalidade de gerência centralizada e única dos produtos propostos, uma vez que o a referia documentação fala apenas em alta disponibilidade (o título consta como "Management High Availability" – "Alta disponibilidade de gerenciamento" em tradução livre) e o texto introdutório deixa claro que se fala de alta disponibilidade do banco e redundância. Desta forma, a existência de múltiplas consoles dificulta visualização de logs e eventos de segurança pelo time da FUNASA, dificultando o entendimento holístico de eventos de segurança;

Resposta a alegação: Informamos que a documentação apresentada para comprovação do sub item 1.1 trata, também, sobre redundância da gerência centralizada da solução SandBlast Agent do fabricante Check Point. Ainda sim é possível comprovar o atendimento ao item em questão com o documento público abaixo:
https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf
Visualizando a página 1 do documento "endpoint-security-datasheet.pdf" é possível verificar o parágrafo:

SOLUTION
(...)A comprehensive management dashboard gives administrators maximum visibility on security areas important to your organization. Manage our full suite of Endpoint Security Software Blades for PCs and Mac under one console.
Ainda no referenciando o mesmo documento podemos verificar na página 1 o parágrafo:
FEATURES
(...)Single console manages endpoint threat prevention, data security, network access, and compliance(...)
Seguindo a comprovação, ainda podemos referenciar o documento público do fabricante abaixo:
https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf

Visualizando a página 3 do documento "sandblast-agent-datasheet.pdf" é possível verificar o parágrafo:
Endpoint Security Management
SandBlast Agent endpoint security management is available via a simple, easy-to-use managed cloud service. Manage endpoints from any location, including office, home, or when on the road. The service is deployed, maintained, and optimized by Check Point and offers these benefits: (...)

Sendo assim, fica claro o total atendimento ao sub item em questão.

2) Em atenção ao item 5 do Anexo I do Termo de Referência, onde se lê "Módulo para proteção de vulnerabilidades e Host IPS (HIPS)", não fica claro nas documentações comprobatórias o atendimento dos itens 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.9, 5.10 e 5.11, constando apenas um comparativo entre versões comerciais (há de se observar a diversos tópicos propondo a demonstração bem como links para páginas de caráter comercial). Consta-se ainda a ausência de comprovação técnica propriamente dita para cada um dos sub itens listados anteriormente.

A presença da funcionalidade para proteção de vulnerabilidades é essencial, visto que a maioria dos ataques ciber criminosos utiliza-se da exploração de vulnerabilidades para a execução de artefatos maliciosos, exploração e elevação de credenciais e outras técnicas maliciosas;

Resposta a alegação : Em diligência técnica realizada pela FUNASA em 14/01/2021 junto a Global IP Tecnologia, foram solicitadas informações detalhadas do atendimento ao item 5 (subitens 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, 5.10 e 5.11), na oportunidade foram enviadas as informações detalhadas que comprovam plenamente o atendimento ao que foi solicitado no termo de referência nos itens.

Primeiramente devemos apresentar, também, resposta a um dos questionamentos feitos nesse processo, em que:

"8. Esclarecimento 06/01/2021 14:44:38
Questionamento item 3.30 , 3.31 e item 5 "3.30. IPS/IDS integrado à solução de antivírus e gerenciado de forma centralizada; 3.31. O IPS/IDS deverá proteger contra exploração de vulnerabilidades de softwares; 5. Módulo para proteção de vulnerabilidades e Host IPS (HIPS) 5.1. Todas as regras das funcionalidades de Host IPS ……." Conforme edital os item 3.30 e 3.31 descrevem funcionalidades de IPS/IDS, essas soluções são focadas em combater ameaças com assinaturas reconhecidas, entretanto a nova geração de Endpoint está baseada em ameaças com assinaturas reconhecidas e não reconhecidas, realizadas através de análise comportamental e inteligência artificial, o que por sua vez proporciona maior segurança aos dispositivos. A solução baseada em políticas para detectar e impedir a comunicação por processos com comandos maliciosos, monitorando todo o tráfego da rede vindo de todos os processos executados no endpoint ações baseadas em assinaturas conhecidas e não conhecidas. A solução de endpoint EDR acrescenta ao modelo tradicional uma análise comportamental e inteligência artificial , além das assinaturas reconhecidas e não conhecidas, a qual é superior a solução de IPS/IDS nos endpoints. Desta forma podemos entender que uma solução que execute funcionalidades superior à solicitada nos itens será aceita ?
Resposta 06/01/2021 14:44:38
O entendimento está correto."

Antes de tudo deixamos claro que a funcionalidade de "Anti-Exploit" trata exatamente sobre a proteção contra exploração de vulnerabilidades (em texto livre "anti-exploração").
A solução de Anti-exploit não trata apenas vulnerabilidades conhecidas utilizando CVEs (Common Vulnerabilities Exposures" já existentes no mercado. A mesma, também, executa detecções com base em comportamentos suspeitos.

Ainda sim, podemos referenciar o documento público do fabricante:
https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf

Visualizando a página 2 do documento, podemos verificar a parágrafo:

Anti-Exploit
"Protects against application threats that exploit memory vulnerabilities. Anti-Exploit protects widely targeted applications such as Microsoft Office, Adobe PDF Reader, Browsers, and Adobe Flash. Anti-Exploit uses four technologies to protect against existing and new exploits:
• Import – Export Address Table Parsing
• Return Oriented Programming
• Stack Pivoting
• VB Script God Mode"
E também na página 4, no seguinte parágrafo:

"Anti-Exploit
• Provides protection against exploit based attacks compromising legitimate applications
• Detects exploits by identifying suspicious memory manipulations in runtime
• On detection, shuts down the exploited process and remediates the full attack chain"

Ainda sim, é possível verificar várias informações de conteúdo público onde exemplos de detecções de explorações de vulnerabilidades são demonstradas, utilizando a solução SandBlast Agent. Como exemplo apresentamos um vídeo exposto no canal oficial do fabricante "Check Point":
https://www.youtube.com/watch?v=M9NtnK4gDNQ

Sendo assim, fica claro o total atendimento aos itens em questão.

3) Em atenção ao item 6 do Anexo 1 do Termo de Referência, onde consta "Módulo para Controle de Aplicações", na documentação entregue ("2-CP_R80.30_GA_EndpointSecurity_AdminGuide") não fica comprovada a possibilidade de aplicação da política de Controle de Aplicações para os alvos desejados, conforme descrito no Termo de Referência nos sub itens 6.1, 6.2 e 6.3. A não presença de comprovação do referido item gera dúvidas quanto à real possibilidade de seleção de destinos a este tipo de política de segurança;

Resposta a alegação: Em diligência técnica realizada pela FUNASA em 14/01/2021 junto a Global IP Tecnologia, foram solicitadas informações detalhadas do atendimento aos subitens 6.1, 6.2 e 6.3, na oportunidade foram enviadas as informações detalhadas que comprovam plenamente o atendimento ao que foi solicitado no termo de referência nos itens.

Ainda, em documentos oficiais apresentados, fica clara a possibilidade de aplicação de políticas, não só para controle de aplicação mas também para todas as funcionalidades da solução para alvos desejados, tanto grupo de máquinas e usuários, estações de trabalho individuais e/ou usuários específicos.

Em referência ao documento público oficial do fabricante:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_EndpointSecurity_AdminGuide/html_frameset.htm

Pesquisando por "Working with virtual groups", é possível verificar o parágrafo:

"Virtual Groups let you manage groups of users and computers with SmartEndpoint. You can use Virtual Groups with Active Directory for added flexibility or as an alternative to Active Directory.(...)"

"Adding Objects with an Installation Package
When you distribute a new Endpoint Security client installation package, you can assign users and computers to a destination group. Computers and users that use this package are automatically assigned to the group when they connect to the server for the first time. (...)"

Adicionalmente podemos verificar o documento público do fabricante:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_EndpointSecurity_AdminGuide/html_frameset.htm

Pesquisando pelo tópico "Working with the Application Control Policy", podemos verificar o parágrafo (aqui é detalhado como as políticas de controle de aplicação são criadas):

"Working with the Application Control Policy

Configure which applications are allowed, blocked, or terminated and what happens when applications are not identified. (...)"

Sendo assim, fica claro o total atendimento aos itens 6.1, 6.2 e 6.3 em questão.

4) Ainda sobre o item 6, sub item 6.4, do Anexo 1 do Termo de Referência, não há presença na documentação apontada a possibilidade de verificação de logs do referido módulo de proteção, impossibilitando assim a visualização dos eventos e consequente entendimento de eventos de segurança que eventualmente venham a acontecer.

A necessidade de módulo de controle de aplicações se deve ao fato de que nem sempre aplicações indesejadas são consideradas vírus/malwares/artefatos maliciosos, como por exemplo mineradores de cripto moedas, aplicações de jogos, P2P (peer-to-peer) e outras indesejadas ao ambiente corporativo, permitindo um maior controle do parque computacional;

Resposta a alegação: Em diligência técnica realizada pela FUNASA em 14/01/2021 junto a Global IP Tecnologia, foram solicitadas informações detalhadas do atendimento ao item 6 (subitens 6.4), na oportunidade foram enviadas as informações detalhadas que comprovam plenamente o atendimento ao que foi solicitado no termo de referência nos itens.

Utilizamos, também, telas da própria solução, no intuito de melhor demonstrar tais funcionalidades solicitadas.

Ainda sim deixamos claro a possibilidade de total visualização de logs e eventos detectados por todas as funcionalidades da solução.

Podemos referenciar o documento público do fabricante:
https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf

Referenciando a página 3 do documento "sandblast-agent-datasheet.pdf", podemos verificar o parágrafo:
"(...)Event logs and incident reports are accessed through SmartEvent and SmartLog, providing deep insights into the nature of the most advanced attacks. Each package offers non-intrusive, low-overhead deployment using a SandBlast remote sandbox as a service or placed on your own private appliances."
Observando, também, o documento público do fabricante: https://www.checkpoint.com/downloads/products/endpoint-security-datasheet.pdf
Referenciando a página 1 do documento "endpoint-security-datasheet.pdf", podemos verificar o parágrafo:
"ACTIONALABLE INCIDENT ANALYSIS
SandBlast Agent provides full visibility with its forensics capabilities, monitoring and recording all endpoint events: files affected, processes launched, system registry changes, and network activity."
Fica claro a possibilidade de total visualização de todos os eventos detectados pela ferramenta (não apenas de controle de aplicação, mas de todas as funcionalidades). Não apenas visualização dos logs, mas também o correlacionamento desses eventos/logs possibilitando a criação de relatórios detalhados e específicos"
Complementando, podemos verificar em documento público do fabricante:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_EndpointSecurity_AdminGuide/html_frameset.htm
Pesquisando por "Application Control" no documento "CP_R80.30_EndpointSecurity_AdminGuide", podemos verificar o parágrafo:

"Application Control

The Application Control component restricts network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes. Only applications that try to get network access can be blocked or terminated. If specified in an Application Control rule, an alert shows which application was blocked or terminated.
You can also enable the Reputation Service (previously called the Program Advisor) to recommend applications to allow or block."
Aqui fica clara a funcionalidade de controle de aplicação já integrada à solução SandBlast Agent.

Sendo assim, fica claro o total atendimento ao item em questão.

5) Ainda em atenção ao item 6, sub item 6.7, não há na documentação a possibilidade de execução de aplicações desejadas apenas como coleta de evento sem a efetiva aplicação da regra, uma vez que a documentação resta clara em que as possibilidades são "Allowed applications" e "blocked applications" ("aplicações permitidas" e "aplicações bloqueadas" em tradução livre).

Este tipo de execução de regra é essencial quando há o desconhecimento do analista responsável dos tipos de aplicações existentes no parque (cenário comum em início de operações de novas ferramentas, por exemplo), o que reduz o impacto ao usuário final de

bloqueios indevidos, mas também permite que alguns usuários possam executar determinadas aplicações com conhecimento do administrador através dos logs gerados;

Resposta a alegação: Assim como apresentado em documentação de comprovação e também no documento público do fabricante:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_EndpointSecurity_AdminGuide/html_frameset.htm

Pesquisando pelo tópico "Application Control" podemos verificar o parágrafo:
"Application Control
The Application Control component restricts network access for specified applications. The Endpoint Security
administrator defines policies and rules that allow, block or terminate applications and processes. Only applications that try to get network access can be blocked or terminated. If specified in an Application Control rule, an alert shows which application was blocked or terminated.

You can also enable the Reputation Service (previously called the Program Advisor) to recommend applications to allow or block. (...)"

Fica claro aqui a possibilidade de monitoramento de uma aplicação pela solução SandBlast Agent. Toda aplicação que toma ação de "allow" é logada no sistema, ou seja, eventos são gerados para essa aplicação, sem qualquer ação preventiva seja tomada.

No decorrer da sessão, é possível detectar diversas possibilidades de políticas para o controle de aplicação.

Adicionalmente, podemos citar a ferramenta "Appscan".
Observando o documento público do fabricante:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_EndpointSecurity_AdminGuide/html_frameset.htm
Pesquisando pelo tópico "Importing Program References", temos o parágrafo:

"Importing Program References

The Appscan command lets you automatically create Application Control rules for common applications and operating system files on endpoint computers network. This is especially useful when you have a clean standard image. (...)
(...)Create an Appscan for each disk image used in your environment. You can then create rules that will apply to those applications(...)"

Sendo assim, fica claro o atendimento ao item 6.7.

6) No item 7 e seus sub itens 7.2 e 7.5 do Anexo I do Termo de Referência, fica, além de não comprovada a existência de funcionalidade de Endpoint Detection and Response (EDR), a dúvida se este módulo de fato existe na solução ofertada, uma vez que as documentações apontadas como comprobatórias se referem à soluções de "Media Encryption & Port Protection", e "Application Control" conforme se observa no canto superior direito das páginas apontadas, onde indica-se o assunto de que trata-se a seção. Como comprovação adicional, também apontamos que a própria especificação desejada nestes sub itens não consta comprovada nas páginas indicadas;

Resposta a alegação: Conforme documentação técnica apresentada não só para comprovação deste item, mas para os demais itens, fica claro que a solução ofertada trata-se de um Endpoint Detection and Response.
Adicionalmente apresentaremos maiores informações que comprovam tal característica, ainda comprovando os itens 7.2 e 7.5.

Como pode ser verificado em documento público oficial do fabricante:
https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf

Quando observamos a página 2, mais especificamente o parágrafo:

"Endpoint Detection and Response
Uses signature-based protection against known malware."
Seguimos ainda com o mesmo documento público "sandblast-agent-datasheet.pdf", verificamos ainda na página 2 o parágrafo:
"Robust Incident Detection and Response
The SandBlast forensics analysis process starts automatically when a malware event occurs. Advanced algorithms and a deep analysis of the raw forensic data helps build a comprehensive incident summary with actionable attack information, including: (...)"
Abaixo um exemplo de detecção e resposta executada pela solução, com toda a análise forense:
https://forensics.checkpoint.com/wannacryptor2_1/

Sobre o monitoramento ou exclusão (white list) de determinadas aplicações, podemos comprovar tal funcionalidade com o documento público d fabricante:
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_EndpointSecurity_AdminGuide/html_frameset.htm

Pesquisando pelo tópico "Monitoring and Exclusions", podemos verificar:
"Define which processes are monitored by the Forensics component.
In the default monitoring settings, processes with certificates from some trusted companies are excluded.
You can Add, Edit, and Remove exclusions from the list. (...)"

Fica claro o atendimento ao item 7 e subitens 7.2 e 7.5.

7) Ainda em se tratando do item 7 do Anexo I do Termo de Referência, mas desta vez sobre o sub item 7.3, não resta claro na documentação que o relatório forense coletará todos os dados dos artefatos analisados.

A coleta destes dados se faz necessário para que o administrador tenha em mãos todas as informações sobre o evento de segurança para que possa entender com precisão os artefatos envolvidos no incidente, e possa tomar decisões acertadas. A falta destas informações prejudica, gerando lacunas de conhecimento;

Resposta a alegação: Conforme demonstrado com documentações oficiais do fabricante, fica claro a existência de relatórios forenses.
Ainda sim podemos comprovar tal funcionalidade com os documentos públicos do fabricante:
https://www.checkpoint.com/downloads/products/sandblast-agent-datasheet.pdf

Quando observamos a página 2, mais especificamente o parágrafo:
"Robust Incident Detection and Response

The SandBlast forensics analysis process starts automatically when a malware event occurs. Advanced algorithms and a deep analysis of the raw forensic data helps build a comprehensive incident summary with actionable attack information, including: (...)"
Abaixo um exemplo de detecção e resposta executada pela solução, com toda a análise forense:
https://forensics.checkpoint.com/wannacryptor2_1/

Sendo assim fica claro o atendimento ao item 7.3.

8) Em atenção ao item 8, sub itens 8.2 e 8.7.41 do Anexo I do Termo de Referência, que comporta o seguinte título "Solução De Proteção Contra Ameaças Avançadas", não fica comprovada a possibilidade de personalização/customização da sandbox, muito pelo contrário, visto que tal documento deixa claro na tabela apresentada "Emulation Specifications" ("Especificações de Emulação" em tradução livre) as possibilidade de apenas se utilizar os sitemas operacionais Microsoft Windows XP e Windows 7, além de uma pequena compatibilidade de tipos de arquivos.

Pesa ainda o fato de que a comprovação do sub item 8.7.41 faz referência apenas à "Centralized Monitoring" ("Monitoramento Centralizado" em tradução livre), não constando informações sobre sandbox, que pertence à um componente totalmente diferente.

Entendemos que uma sandbox customizável deve oferecer a possibilidade de suportar diversos sistemas operacionais a escolha do usuário, papel de parede, hora, língua, programas instalados, bem como diversos tipos de arquivos e extensões, entre outros fatores. Isto se faz necessário para que haja a mitigação de técnicas de evasão de sandbox, onde o artefato suspeito percebe que está sendo testado em um ambiente controlado e permanece inerte, gerando um falso negativo, e consequentemente, a liberação deste para o usuário, expondo assim o ambiente corporativo a um artefato potencialmente muito danoso, visto que este já foi testado por outras camadas de segurança antes de sua submissão à sandbox;

Resposta a alegação: Em diligência técnica realizada pela FUNASA em 14/01/2021 junto a Global IP Tecnologia, foram solicitadas informações detalhadas do atendimento ao item 8 (subitens 8.2 e 8.7.41), na oportunidade foram enviadas as informações que atenderam plenamente o que foi solicitado no termo de referência.
Foram utilizadas, também, telas da própria solução para melhor entendimento.
Podemos constatar a comprovação de tais itens com as documentações públicas oficiais do fabricante:
https://www.checkfirewalls.com/datasheets/ds-sandblast-appliances.pdf

Verificando a página 1 do documento "ds-sandblast-appliances.pdf", podemos verificar os parágrafos:

"Product Features

Identify new malware hidden in over 40 files types, including: Adobe PDF, Microsoft Office, Java, Flash, executables, and archives
Protect against attacks targeting multiple Windows OS environments (...)"

Vale deixar claro que em momento algum no edital foi solicitado quantidades específicas de compatibilidade de tipos de arquivos, ainda assim demonstramos quantidade superior a concorrentes de mercado.
Também referente às máquinas virtuais disponíveis para emulação em ambiente virtual não é verdade quando se diz que existem apenas 2 sistemas operacionais para emulação na solução apresentada. A compatibilidade com múltiplos sistemas operacionais Windows foi demonstrada em diligência, utilizando telas da própria solução ofertada.

Adicionalmente, conforme documentação pública oficial do fabricante:
https://www.checkfirewalls.com/datasheets/ds-sandblast-appliances.pdf

Observando a página 3 do documento "ds-sandblast-appliances.pdf", na especificação técnica do appliance ofertado (TE1000X), podemos verificar a capacidade do equipamento:

"Number of virtual machines : 28"

Tecnologias avançadas são utilizadas pelo Sandbox On-premise da Check Point. A detecção é feita não somente através de emulações a nível de sistemas operacionais, mas antes disso através de tecnologias de detecção a nível de CPU, o que agiliza a emulação e aumenta o nível de acuracidade da funcionalidade.

Tal característica é possível ser identificada no documento público do fabricante:
https://www.checkfirewalls.com/datasheets/ds-sandblast-appliances.pdf

Visualizando a página 1 do documento "ds-sandblast-appliances.pdf", podemos verificar o parágrafo:

"Product Features

Unique CPU-Level technology catches malware before it has an opportunity to deploy and evade detection"

Fica claro, conforme informações apresentadas, que a solução de Sandbox, denominada Sandblast, do fabricante Check Point não é uma solução engessada, sendo possível customizações tanto a nível de implementação quanto a nível de emulação, sendo possível definir sistemas operacionais específicos para emulação, versões do sistema operacional e do pacote Office, adobe, etc.

Sendo assim fica claro o atendimento ao item 8, subitens 8.2 e 8.7.41.

9) Ainda em atenção ao item 8 do Anexo I do Termo de Referência, apontamos que a documentação entregue não comprova o atendimento dos itens 8.7.16, 8.7.20 e 8.7.25, não havendo descrição de análise dos protocolos e tipos de arquivos solicitados. Destacamos ainda que a documentação "7-CP_R80.40_EndpointSecurity_AdminGuide", apresentada para o item 8.7.16, em sua seção apontada na documentação comprovatória (página 121), consta como "External Endpoint Policy Servers", que conforme ela própria explica na página 119, funciona como replicador de políticas de segurança, e não como sandbox, como assim desejado na especificação do Item;

Resposta a alegação: Em diligência técnica realizada pela FUNASA em 14/01/2021 junto a Global IP Tecnologia, foram solicitadas informações detalhadas do atendimento ao item 8 (subitens 8.7.16, 8.7.20 e 8.7.25), na oportunidade foram enviadas as informações que atenderam plenamente o que foi solicitado no termo de referência.

Foram utilizadas, também, telas da própria ferramenta para auxiliar o entendimento e comprovação dos itens 8.7.16, 8.7.20 e 8.725, além de documento interno intitulado "SK106123 - File types supported by SandBlast Threat Emulation".
Parte do documento apresentado:

Complementarmente, abaixo temos site oficial da Check Point onde são listados mais de 255 mil aplicações e protocolos detectados pela solução, nativamente:
https://appwiki.checkpoint.com/appwikisdb/public.htm

Sendo assim, fica claro o atendimento aos itens 8.7.16, 8.7.20, 8.7.25 e 8.7.16.

10) Ainda em referência ao item 8, mais especificamente ao sub item ao 8.7.25, não há menção alguma à detecção baseada no verdadeiro tipo de arquivo (True File Type), conforme solicitado.

Esta diferenciação do verdadeiro tipo de arquivo é importante visto que uma técnica comum por atacantes é mascarar a real extensão do artefato malicioso com outra extensão, visando enganar e burlar agentes de segurança (por exemplo, um arquivo executável com extensão .exe é maquiado para parecer um arquivo de texto com extensão .docx);

Resposta a alegação: Tal funcionalidade foi comprovada com documento oficial do fabricante.
Para que fique claro o atendimento a tal funcionalidade, podemos verificar o documento público oficial da Check Point:
https://www.checkfirewalls.com/datasheets/ds-sandblast-appliances.pdf

Referenciando a página 1, parágrafo:

"Product Features
Identify new malware hidden in over 40 files types, including: Adobe PDF, Microsoft Office, Java, Flash, executables, and archives"

Fazendo referência, também, à tecnologia de sandbox em nuvem, que utiliza a mesma tecnologia on-premise, podemos verificar o documento público:
https://www.checkpoint.com/downloads/products/sandblast-cloud-datasheet.pdf
Onde na página 1, temos o parágrafo:

"Deep malware inspection at the CPU- level, where exploits cannot hide
Inspects broad range of documents and common file-types"

Também foi apresentado ao licitante em diligência, documento interno da Check Point intitulado "SK106123 - File types supported by SandBlast Threat Emulation"

Parte do documento apresentado:

Em exemplos de detecções feitas na ferramenta, também é possível detectar vários exemplos que demonstram detecção de arquivos com extensões não verdadeiras, ou seja, arquivos .EXE com extensões .DOC. A detecção de arquivos já pré conhecidos (Common File Types) é feita pela característica do arquivo, não pela extensão que acompanha o nome do mesmo.
Diante do exposto, fica claro o atendimento ao item 8.7.25.
11) Em atenção ao item 8, sub item 8.7.42, não resta comprovado a identificação de comunicação maliciosas em dispositivos móveis. Tal identificação é de suma importância, visto que a existência de tais dispositivos em redes corporativas é natural na era em que vivemos, sejam eles dispositivos de propriedade da FUNASA ou do próprio individuo, visto que o advento da consumerização de Tecnologia trouxe este fenômeno consigo. A não identificação gera um vácuo na detecção de ameaças, expondo e aumentando a superfície de ataque disponível à um atacante;

Resposta a alegação:

Tal funcionalidade foi comprovada com documentação oficial do fabricante.
Adicionalmente é possível verificar o atendimento ao item 8.7.42 acessando ao link público do fabricante:
https://threatwiki.checkpoint.com/threatwiki/public.htm

No link basta procurar por ameaças para mobile (ex: Android.Xbot):

Todas as ameaças descritas no "threatwiki" são identificadas pela solução SandBlast Agent.

Ainda, mostramos abaixo uma detecção de um artefato malicioso direcionado para dispositivos móveis rodando o sistema operacional Android (abaixo report forense da detecção):

Abaixo link do VirusTotal.com com informações da ameaça detectada:
https://www.virustotal.com/gui/file/aa4d888798843c953bfd3f061e48be3cd4e6f70becb14f360b37605060ef7588/details

Sendo assim, fica claro o atendimento ao item 8.7.42.

12) No sub item 8.7.46 do item 8 do Anexo I do Termo de Referência, em consonância com o descrito no tópico 8 deste documento, a descrição comprobatória se refere à Centralized Monitoring" ("Monitoramento Centralizado" em tradução livre), o que não condiz com a especificação técnica solicitada, que é a detecção de tentativas de ataque do tipo brute-force, uma metodologia muito comum em ataques cibernéticos, onde é realizada uma abordagem de tentativa e erro massiva até que se encontre, em algum momento a combinação desejada;

Resposta a alegação: Conforme comprovado em documentação oficial do fabricante, a solução SandBlast Agent é capaz de detectar uma grande diversidade de ataques conhecidos e desconhecidos, isso inclui ataques de força bruta (brute force) conhecidos e desconhecidos, utilizando a funcionalidade de "behavioral guard".

Adicionalmente, conseguimos comprovar tal funcionalidade com documentação interna do fabricante, intitulada "SK163578 - Enterprise Endpoint Security E82.10 Windows Clients":
https://supportcenter.checkpoint.com/supportcenter/portal?
eventSubmit_doGoviewsolutiondetails=&solutionid=sk163578#What's%20New%20in%20E82.10

Abaixo imagem com parte do documento interno onde é possível verificar uma atualização para o cliente Windows, melhorando a detecção de ataques de força bruta desconhecidos:

Abaixo temos link público do fabricante com exemplo de assinaturas já conhecidas de Brute-Force utilizadas pela gama de soluções Check Point:

https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0754.html

Fica claro que a solução SandBlast Agent protege não apenas tentativas de Brute-Force conhecidas, mas também desconhecidas, utilizando a funcionalidade de Behavioral-Guard (comportamento).

Sendo assim, fica claro o atendimento ao item 8.7.46.

13) Consta ainda no sub item 8.7.59. do mesmo item 8 do Anexo I do Termo de Referência, a necessidade de encaminhamento dos logs gerados à ferramentas de syslog, algo indispensável às administrações de ativos computacionais. No entanto, não resta provado na documentação "2-CP_R80.30_GA_EndpointSecurity_AdminGuide" a existência de envio à este tipo de ferramenta externa. Salientamos ainda que a documentação se refere à um produto de segurança para endpoint e não para Ameaças Avançadas conforme solicitado em especificação técnica (isto pode ser notado no rodapé da página apontada onde lê-se "Endpoint Security Administration Guide" e no canto superior direito, indicativo da seção do documento, "Using SmartEndpoint";

Resposta a alegação: Primeiramente devemos salientar que tal funcionalidade foi comprovada com a documentação apresentada.
Tanto a solução de Endpoint Security quanto o SandBlast Agent utilizam as mesmas tecnologias, o que mudará entre elas é a quantidade de funcionalidades existentes em cada uma, sendo uma mais completa que a outra.
Adicionalmente, apresentamos documento público oficial do fabricante que demonstra o atendimento a tal funcionalidade:
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/SandBlast-Agent-Admin-Guide/Topics-SBA-AG/Log-Exporter.htm?Highlight=syslog

Pesquisando pelo tópico "Exporting Logs", podemos verificar o parágrafo:
Check Point Log Exporter is an easy and secure method to export Check Point logs over syslog. Log Exporter is a multi-threaded daemon service which runs on a log server. Each log that is written on the log server is read by the Log Exporter daemon. It is then transformed into the applicable format and mapping and sent to the end target.

Sendo assim, fica claro o atendimento ao item 8.7.59.

b) - Não atendimento aos requisitos de qualificação técnica exigidos pelo Edital;

Diante da documentação de habilitação anexada pela empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA, em momento prévio ao certame, verifica-se que a mesma não atende aos requisitos de qualificação técnica mínimos exigidos pelo Edital.
De acordo com o Edital, item 9.11 "Qualificação Técnica":

9.11.1. Comprovação de aptidão para a prestação dos serviços em características,
quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.
9.11.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:
9.11.1.1.1. Comprovação de aptidão para a prestação dos serviços em características e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por período não inferior a um ano, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.
9.11.1.1.2. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MPDG n. 5, de 2017;
9.11.1.1.3. Para a comprovação da experiência mínima de 1 (um) ano, é admitida a apresentação de atestados referentes a períodos sucessivos não contínuos, não havendo a obrigatoriedade do um ano ser ininterrupto, conforme item 10.6.1 do Anexo VII-A da IN SEGES/MPDG n.5/2017;
[...]
9.11.1.1.6. O atestado de capacidade técnica deve atender no mínimo 20% do quantitativo exigido para os itens do Termo de Referência.

De acordo com os itens de habilitação técnica especificados em Edital, o licitante deveria anexar atestados de capacidade técnica comprovando que forneceu solução centralizada de segurança do tipo Endpoint Protection (Item 1), bem como solução de proteção contra ameaças avançadas(Item 2) em quantidade mínima de 20% ao exigido para os itens do Termo de Referência.
Ao analisarmos os documentos anexados pela empresa Global IP, identificam-se dois atestados de capacidade técnica nomeados como "Atestado ANTT endpoint.pdf" e "Atestado banco do brasil Endpoint.pdf", respectivamente.

Em referência ao primeiro documento mencionado, verifica-se que a empresa em questão forneceu à ANTT no ano de 2012, soluções de segurança para endpoint e para e-mails (anti-spam) da fabricante SYMANTEC, em quantidade superior aos 20% exigidos. No segundo atestado apresentado, a empresa forneceu ao Banco do Brasil em 2010, licenças para proteção de endpoint da marca CHECKPOINT, com funcionalidades similares ao primeiro atestado apresentado. Tais confirmações se dão com base em consulta ao portal dos fabricantes, citados abaixo:

1) https://www.broadcom.com/products/cyber-security/endpoint
2) https://docs.broadcom.com/docs/mail-security-for-microsoft-exchange-en
3) https://www.checkpoint.com/products/media-encryption/
4) https://sc1.checkpoint.com/documents/R80.40/SmartEndpoint_OLH/EN/Content/Topics-EPSG/FDE-CPFDE-intro.htm

Ao analisarmos os atestados apresentados frente à exigência do edital, o qual trata de duas soluções distintas, segurança para endpoint(Item 1) e segurança para ameaças avançadas(Item 2), verifica-se uma lacuna na documentação enviada para qualificação técnica da empresa GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA.

Ambos atestados apresentados, trata-se especificamente de soluções RESTRITAS à segurança para endpoints. Assim, confirma-se que a empresa em questão não comprou capacidade técnica anterior e, portanto, não está apta a fornecer os produtos e serviços relacionados à solução de ameaças avançadas.
Assim posto, a recorrida GLOBAL IP TECNOLOGIA DA INFORMACAO LTDA deve ser desclassificada do presente Pregão, considerando que além da solução ofertada não atender os mínimos requisitos técnicos contidos no Anexo ao Termo de Referência, a mesma não comprovou capacidade técnica para fornecer a solução para ameaças avançadas nos termos do subitem 9.11 do Edital.

Resposta a alegação:
Conforme exigido em Edital a qualificação técnica busca identificar se a licitante já prestou serviços em características, quantidades e prazos compatíveis com o objeto da licitação, os atestados de capacidade técnica apresentados demonstram claramente características similares ao solicitado no Edital e atendem o mínimo 20% do exigido em edital, no caso ter atendido no mínimo 712 dispositivo com solução de endpoint, que se trata da principal função da solução, que em suma é proteger os 3560 dispositivos do órgão. O exposto pela licitante ALL TECH, que os atestados apresentados pela Global IP Tecnologia não atendem especificamente ao item 2, sendo incoerente essa alegação, uma vez que foi comprovado ter prestado serviço em características e quantidades

semelhantes.

Não há de se falar em atestado específico para cada funcionalidade constante no Edital, porque se assim fosse, todas as licitantes deveriam entregar atestados para atender os 223 requisitos exigidos no termo de referência do Edital 19/2020, por esse motivo são solicitados atestados com características e quantidades compatíveis.

Vale ressaltar que no atestado da ANTT , onde consta a solução symantec Endpoint Protection a solução ofertada atende os requisitos de Edital visto que possui a funcionalidade de detecção de ameaças avançadas realizadas através de detecção heurística tecnologia denominada pela Symantec como Bloodhound heuristic, desta forma demonstrando que essa funcionalidade já foi prestada em serviço anterior, mesmo não sendo necessário a comprovação de todos os 223 requisitos técnicos do termo de referência deste Edital.

Claro está que as exigências constantes no Edital são ilegais pois comprometem a isonomia no certame, além de malferir o princípio da motivação dos atos administrativos, uma vez que não há qualquer justificativa para as necessidades apontadas nos itens impugnados.

Sendo assim os atestados apresentados pela GLOBAL IP TECNOLOGIA atendem plenamente o exigido em Edital em característica e quantidades compatíveis com o serviço a ser prestado.

Em face do exposto, solicitamos que seja mantida a classificação e habilitação da licitante GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA baseado nos princípios administrativos que regem a ampla defesa nos certames públicos, uma vez que todos os itens elencados no recurso da ALL TECH foram demostrados de forma equivocadas e todos os itens foram devidamente detalhados nas respostas às alegações.

Vale ressaltar que a empresa EVERY TI TECNOLOGIA & INOVAÇÃO EIRELI manifestou intenção de recurso e após decorrido o prazo administrativo e analisado a documentação da licitante GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA , se pronunciou em seu recurso a desistência declarando " Não encontramos inconsistências." o que ratifica a decisão da equipe técnica da FUNASA e as justificativas inseridas no bojo das contrarrazões.

DO PEDIDO:
Por todo o exposto, REQUER seja julgado provido as contrarrazões apresentadas, mantendo-se a HABILITAÇÃO E CLASSIFICAÇÃO da licitante GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA decorrente do atendimento dos requisitos de Edital, prevalecendo o exposto pela equipe técnica da FUNASA na análise dos documentos e justificativas enviadas a FUNASA.
Outrossim, lastreada nas contra razões recursais, requer-se que essa Comissão de Licitação ratifique a decisão de Habilitação e classificação da licitante GLOBAL IP TECNOLOGIA DA INFORMAÇÃO LTDA em conformidade com o § 4°, do art. 109, da Lei n° 8666/93, para que surtam os devidos fins de direito.

Nesses Termos,
Pede Deferimento.

Atenciosamente,

Ronaldo de Albuquerque Ribeiro
Representante Legal
Global IP Tecnologia da Informação LTDA.

OBS.: POR SE TRATAR DE CONTRARRAZÃO COM IMAGENS, DOCUMENTO TAMBÉM ENVIADO POR E-MAIL.

Fechar