MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS

PROCURADORIA-GERAL DE JUSTIÇA

DIRETORIA DE GESTÃO DE COMPRAS E LICITAÇÕES

Assunto: Resposta de Pedido de Esclarecimentos

Processo Licitatório nº 22/2025

Consulente: CH Tecnologia.
Solicitação nº 0010 - SIAD

Prezado(a) senhor(a),

Seguem respostas da unidade técnica Diretoria de Suporte e Manutenção (DSMT/PGJ) aos questionamentos apresentados por essa empresa:

QUESTIONAMENTO 1:

Solicitação de Esclarecimento - Controle de dispositivos - Com relação ao item 1.2.1.12, entendemos que a solução de segurança deve permitir a criação de políticas que possibilitem tanto o bloqueio quanto a varredura automática de dispositivos de armazenamento externos, quando aplicável. Para isso, assumimos que a solução deve incluir funcionalidades de controle de dispositivos USB, garantindo a identificação e mitigação de possíveis ameaças presentes nesses dispositivos antes de sua utilização em aplicações corporativas. Poderiam confirmar se esse entendimento está correto?

RESPOSTA: Não está correto o entendimento.

QUESTIONAMENTO 2:

Solicitação de Esclarecimento - Proteção contra Ransomware Com relação ao item 35, entendemos que a solução de segurança deve oferecer proteção avançada contra ransomware, incluindo a capacidade de monitorar e analisar processos criptográficos em execução no sistema, detectar tentativas de exclusão de backups e identificar padrões anômalos de alto volume de operações de I/O no sistema de arquivos. Além disso, compreendemos que a solução deve garantir a integridade dos arquivos ao identificar um ataque de ransomware, realizando automaticamente cópias de segurança antes da criptografia maliciosa. Assumimos também que essa funcionalidade deve ser implementada de forma independente do sistema operacional, impedindo a desativação do mecanismo de proteção por meio da remoção ou manipulação

do Shadow Copy ou outras tecnologias nativas do SO. Poderiam confirmar se nosso entendimento está correto e se há requisitos adicionais para essa proteção?

RESPOSTA: Não está correto o entendimento.

QUESTIONAMENTO 3:

Solicitação de Esclarecimento - Proteção Contra Ransomware, Exploits e Ferramentas de Ataque Com relação ao item 65, entendemos que a solução de segurança para endpoints deve ser capaz de detectar e bloquear atividades maliciosas associadas a ransomwares, exploits e outras ameaças avançadas, incluindo a identificação e neutralização de ferramentas amplamente utilizadas em ataques, como Metasploit, Mimikatz, entre outras. Além disso, compreendemos que, para oferecer proteção eficaz contra ransomware, a solução deve ser capaz de monitorar e identificar tentativas de criptografia maliciosa, garantindo a preservação dos arquivos por meio de cópias de segurança automáticas antes da modificação. Assumimos também que essa funcionalidade deve ser resistente a tentativas de desativação, utilizando um mecanismo independente do sistema operacional para impedir a manipulação ou remoção do Shadow Copy ou de outras tecnologias de proteção nativas. Poderiam confirmar se nosso entendimento está correto?

RESPOSTA: Não está correto o entendimento.

QUESTIONAMENTO 4:

Solicitação de Esclarecimento – Mecanismos de Proteção Contra Ransomware No que concerne ao item 33, compreendemos que a solução de segurança para endpoints deve incorporar mecanismos avançados de proteção contra ransomware, incluindo a análise heurística e comportamental de processos criptográficos em execução, a identificação de tentativas de exclusão de backups e a detecção de padrões anômalos de alta taxa de operações de I/O no sistema de arquivos, indicando potenciais ataques em andamento. Além disso, assumimos que a solução deve adotar estratégias proativas de mitigação, garantindo a integridade dos dados mediante a criação automática de cópias de segurança antes da criptografia maliciosa. Para assegurar a resiliência contra técnicas de evasão, entendemos que esse mecanismo de proteção deve ser imune à desativação do Shadow Copy ou de quaisquer outros sistemas nativos de recuperação, por meio de uma

abordagem independente do sistema operacional, evitando assim a manipulação por agentes mal-intencionados. Poderiam confirmar se esse entendimento está correto? Caso existam diretrizes adicionais ou requisitos específicos para a implementação dessa funcionalidade, solicitamos maiores esclarecimentos.

RESPOSTA: Não está correto o entendimento.

QUESTIONAMENTO 5:

Solicitação de Esclarecimento – Processos de Triagem, Investigação e Comunicação no Serviço de MDR Em relação ao item 106, entendemos que o serviço de MDR (Managed Detection and Response) deve incluir um processo contínuo e proativo de triagem, investigação e análise de incidentes de segurança, com a comunicação imediata e sem a necessidade de solicitação formal ou abertura de “ticket” por parte da CONTRATANTE. Além disso, compreendemos que a solução deverá possibilitar a comunicação direta entre a equipe de segurança da CONTRATADA e o fabricante da solução, utilizando a própria console da solução para tal interação, garantindo assim um fluxo eficiente e ágil de informações críticas. Poderiam confirmar se o nosso entendimento está correto? Caso haja requisitos específicos adicionais ou um processo distinto para a comunicação entre as partes, solicitamos maiores esclarecimentos.

RESPOSTA: Não está correto o entendimento; sem requisitos adicionais.

QUESTIONAMENTO 6:

Solicitação de Esclarecimento – Explicação e Comunicação Sobre Eventos e Incidentes Em relação ao item 109, entendemos que o serviço de Managed Detection and Response (MDR) deve fornecer, sempre que solicitado pela CONTRATANTE, explicações detalhadas sobre os eventos de segurança detectados pela solução, bem como esclarecimentos técnicos referentes aos relatórios de incidentes enviados. Além disso, compreendemos que a solução deve disponibilizar um canal de comunicação direto entre a equipe de segurança da CONTRATADA e o fabricante da solução, garantindo que essa interação ocorra de forma nativa por meio da console da plataforma. Essa funcionalidade visa assegurar uma resposta ágil e eficiente na investigação e mitigação de ameaças, permitindo uma análise aprofundada dos eventos de segurança e facilitando a tomada de decisão com base em informações

precisas e contextualizadas. Poderiam confirmar se o nosso entendimento está correto? Caso existam requisitos adicionais ou um fluxo de comunicação diferenciado, solicitamos gentilmente mais detalhes.

RESPOSTA: Não está correto o entendimento; sem requisitos adicionais.