

Manaus, 04 de setembro de 2024.

Ofício circular nº 48/2024 – COLIC/CIGÁS.

(Referente ao Edital Pregão Eletrônico nº 90030/2024 – COLIC/CIGÁS).

Senhores Licitantes,

Em resposta ao Pedido de Esclarecimento recebido por esta Companhia de Gás do Amazonas - CIGÁS, referente a **Pregão Eletrônico nº 90030/302024 – COLIC/CIGÁS - Contratação de empresa especializada na prestação de serviço de Centro de Operações de Segurança (SOC), conforme condições e especificações técnicas constantes neste Edital e seus Anexos**, informamos que:

Através do DESPACHO N. 109/2024 - GETIN/CIGÁS, segue a devida resposta.

Pergunta 1: Para uma correta implementação de uma solução de SIEM/XDR, é necessária a instalação de componentes coletores próximos as fontes geradoras de logs. Neste sentido, a nossa solução possui um modulo específico que deve ser instalado na infraestrutura do cliente, proporcionando não somente a coleta de logs, mas também a lógica necessária para a compactação e criptografia dos dados que serão enviados ao SOC. Entendemos que a infraestrutura de virtualização necessária para a instalação deste coletor (appliance virtual), no formato de máquina virtual, será prevista pela CIGÁS. Caso o nosso entendimento esteja errado, solicitamos a CIGÁS especificar as características físicas disponíveis no seu Datacenter para a instalação de um coletor físico, devendo a CIGÁS disponibilizar conectividade, energia, espaço em rack, refrigeração, etc.

Resposta ao questionamento 1: Sim, está correto o entendimento. A CIGÁS fornecerá a infraestrutura de virtualização necessária para a instalação do coletor de logs em formato de máquina virtual. Ressaltamos a importância de que a Contratada atenda ao item 3.1.6.

Pergunta 2: No item 3.1.22 do edital é informada a infraestrutura objeto da monitoração. Para um melhor entendimento, solicitamos especificar os fabricantes e modelos das tecnologias mencionadas. Também solicitamos especificar se existem serviços em nuvem pública que devam ser considerados como fonte geradora de eventos.

Resposta ao questionamento 2: Os modelos e fabricantes que integram o nosso parque tecnológico são amplamente disponíveis e comercializados no mercado. Devido à confidencialidade, as características dos dispositivos serão divulgadas exclusivamente através de cláusulas contratuais, sem comprometer o andamento do certame. Em relação aos serviços de nuvem pública, utilizamos os players de mercado. No Termo de Referência, tal ação ocorrerá na fase de Levantamento e Planejamento, conforme item 3.2.1.

Pergunta 3: Os itens 3.1.24 e 3.1.25 mencionam os escalonamentos e tratativas de incidentes. Não identificamos no edital indicação de se a CIGAS possui atualmente ferramenta de gestão de chamados/tickets, ou se a CONTRATADA deverá incluir na prestação do serviço este tipo de solução. Caso a CIGAS possua solução, solicitamos indicar fabricante para avaliar a integrabilidade da mesma com o serviço solicitado.

Resposta 3: O acionamento para eventos de alta criticidade deve seguir rigorosamente a hierarquia estabelecida na tabela do item 3.1.24. Com relação a gestão de chamados, possuímos o Mildesk e o GLPI.

Pergunta 4: A tabela do ponto 3.5.2 indica para o ITEM 1 (Análise inicial do incidente) um prazo de notificação de 5 minutos. Esse prazo não considera a criticidade do incidente analisado. Entendemos que este item se refere ao output da ferramenta com a caracterização do evento detectado, informando - por exemplo - se e um caso de DDoS ou Malware. Caso o nosso entendimento esteja errado, solicitamos explicar a que se refere "Análise Inicial do Incidente".

Resposta ao questionamento 4: Sim, o entendimento está correto. O prazo refere-se ao tempo de resposta da equipe de SOC após a análise preliminar do evento detectado, indicando o tipo de incidente (ex: DDoS, Malware) e o nível de criticidade.

Pergunta 5: A tabela do ponto 3.5.2 indica para o ITEM 6 e 7 um prazo de notificação em dias. Solicitamos indicar se esta referido a dias corridos, ou dias uteis.

Resposta ao questionamento 5: Dias úteis

Informamos que essas respostas estarão disponíveis no endereço eletrônico da CIGÁS e se tornarão parte integrante do Edital e seus anexos.

Por fim, como o presente expediente não acrescenta novas informações e exigências ao Edital e nem afeta a formulação da proposta de preços, a data designada para abertura do certame permanecerá inalterada.

Atenciosamente,

DANIEL SILVA DOS SANTOS

Pregoeiro da Comissão Permanente de Licitação – CPL/CIGÁS

Visto:

ODÍLIO MENDONÇA DA SILVA

Coordenador de Licitação – COLIC/CIGÁS