ESCLARECIMENTO 1

CHAMAMENTO PÚBLICO

SELEÇÃO COM DISPUTA NA FORMA ABERTA PELO PROCEDIMENTO REMOTO Nº 49/2024

Processo nº PRO-02696/2024/2024 –SC 063765	**Critério: Econômico pelo Menor Preço**
Abertura: 04/10/2024	**Horário: 10h**
Local: SBN, Quadra 1, Bloco C, Edifício Roberto Simonsen, 2º andar, CEP 70040-903 Brasília (DF). Fone: (61) 3317-9609 – E-mail: processodeselecao@cni.com.br	

Considerando o que estabelece os artigos que compõem o TÍTULO I – DISPOSIÇÕES GERAIS do vosso Regulamento para Contratação e Alienação, em especial o seu objetivo em buscar proposta mais vantajosa a partir de suas necessidades, da observação do padrão de mercado e busca pela eficiência, eficácia e economicidade das atividades institucionais. Além disso, amparados pelos princípios da transparência, equidade, ética e integridade, e ainda, na certeza do zelo e apreço por tais determinações, apresentamos os questionamentos a seguir:

Ref: ANEXO I (TERMO DE REFERÊNCIA)

PERGUNTA 1.: Compreendemos que o ambiente a ser monitorado já está 100% implementado, de modo que a contratada não precisará adicionar nenhum outro equipamento ao ambiente durante o período de vigência do contrato. Está correto o nosso entendimento?

RESPOSTA 1: Sim, está correto o entendimento.

PERGUNTA 2 - Para que possamos realizado o dimensionamento do esforço necessário para atender as atividades com excelência, é necessário que seja respondido os questionamentos, abaixo referente ao SOC:

1.2.1 Qual a quantidade mensal de incidentes de segurança nos últimos 6 (seis) meses?

RESPOSTA 2.1: Entendemos que para dimensionamento da proposta favor considerar a métrica de 2000 eventos por segundo (EPS).

1.2.2 Qual a quantidade de incidentes mensais relacionados aos níveis de criticidade (Alto, Médio e Baixo) dos últimos de 6 (seis) meses?

RESPOSTA 2.2: Entendemos que para dimensionamento da proposta favor considerar a métrica de 2000 eventos por segundo (EPS).

1.2.3 Qual a quantidade de incidentes avaliados como falso positivos dos últimos de 6 meses? 1.2.4 Qual o tempo médio exigido para resolução dos incidentes relacionados aos níveis de criticidade (Alto, Médio e Baixo) do período de 6 meses?

RESPOSTA 2.3: Entendemos que para dimensionamento da proposta favor considerar a métrica de 2000 eventos por segundo (EPS).

Ref: ANEXO I (Termo de Referência), Item 3.1.1.8.1.4

PERGUNTA 3 - Ref: ANEXO I (Termo de Referência), Item 3.1.1.8.1.4

Naquele Item, é definido:

"A CONTRATADA deve armazenar as informações de desempenho do ambiente por um período mínimo de 24 meses, mantendo estas informações disponíveis para o CONTRATANTE. O intervalo mínimo de coleta de informações dos elementos gerenciados deverá ser definido no momento da implantação dos recursos, podendo ser alterado durante o decorrer do contrato. A CONTRATADA deve permitir a configuração de perfis de serviços que possibilitem a configuração de limiares (thresholds) para as variáveis monitoradas e níveis de serviço acordados."

Uma vez que no **Item 2.1.2** é destacado que as ferramentas de segurança necessárias para a prestação dos serviços são SIEM XDR, SOAR, SSE e Darktrace, serão providas pela CONTRATANTE.

Entendemos que, para que possamos armazenar as informações e promover insights de desempenho, precisamos considerar o direcionamento dos eventos do ambiente do **CONTRATANTE** para o ambiente de SIEM da **CONTRATADA**. Está correto o nosso entendimento? Caso NÃO por gentileza repassar um caso de uso.

RESPOSTA 3: A Contratada deve manter somente os dados que foram usados para gerar os relatórios e gravação das reuniões.

PERGUNTA 4 - Ref: ANEXO I (Termo de Referência), Item 3.1.1.8.1.6

Naquele item é definido:

"Ao detectar alguma falha, os responsáveis pela monitoração devem executar procedimentos pré-estabelecidos de aviso aos analistas do elemento de rede com problema e, se possível, já estabilizar o serviço afetado."

Entendemos que a **CONTRATADA** terá acesso administrativo total no ambiente do **CONTRATANTE** para que seja possível tomar ações administrativas para estabilizar serviços que possam estar sendo afetados. Está correto o nosso entendimento?

RESPOSTA 4: A CONTRATADA não terá acesso ao ambiente, existem playbooks dentro da solução de SOAR, para contingenciamento do ambiente, toda a execução será feita pela plataforma.

PERGUNTA – 5 - Ref: ANEXO I (Termo de Referência), Item 5.12

Naquele Item, é definido: "A CONTRATADA deverá possuir a capacidade de gerar, distribuir e arquivar relatórios, reportes e sumários sob demanda ou automaticamente." Solicitamos esclarecer se aqueles relatórios serão gerados nas ferramentas consideradas no Item 2.1.2? Caso não, favor exemplificar através de um caso de uso.

RESPOSTA 5: As ferramentas (SIEM XDR, SOAR, SSE e Darktrace), estão integradas a solução ao SIEM e os dados para gerar os relatórios deverão ser coletados no SIEM.

PERGUNTA – 6 Ref: ANEXO I (Termo de Referência), Item 5.15

Naquele Item, é definido:

"Quando utilizar softwares de sua propriedade, a CONTRATADA deverá adotar versões e tecnologias compatíveis às adotadas pelo CONTRATANTE. Serviços prestados com ferramentas incompatíveis facultam a recusa de recebimento do serviço pelo CONTRATANTE."

Com base no requisito daquele Item solicitamos:

i. Favor fornecer alguns exemplos de softwares.

ii. ii. Considerando que, conforme o **Item 2.1.2**, a prestação de serviços ocorre em ferramentas que já estão implementadas no ambiente do **CONTRATANTE**, e não está sendo solicitada a implementação ou sustentação de nenhuma outra ferramenta adicional, em qual cenário precisamos considerar ferramentas compatíveis?

RESPOSTA – 6: A CONTRATADA deverá informar quando for usar qualquer software que não fornecido pela CONTRATANTE.

PERGUNTA -7 Ref: ANEXO I (Termo de Referência), Item 12.3.2.4.1, Item 8 da Tabela

Naquele Item 8 da Tabela é definido:

"Testes de Intrusão ou "PenTest a cada 3 meses do tipo "caixa-preta" e "caixa-branca;"

Entendemos que está sendo solicitado Pentest no ambiente, porém não está sendo relacionado em nenhum outro item do documento, para que seja possível dimensionar este item. Dessa forma, solicitamos os seguintes esclarecimentos:

i. Qual é a quantidade de usuários que deverão ser testados?

ii. O serviço de Pentest é relacionado ao ambiente interno e/ou externo?
iii. O serviço de Pentest está relacionado a infraestrutura e/ou aplicações Web também?
iv. Quantas aplicações web estão disponibilizadas na Internet?
v. Existem APIs a serem testadas? Caso sim, quantas?
vi. Quantos servidores Windows?
vii. Do total acima, quantos servidores estão acessíveis externamente, a partir da Internet?
viii. Quantos servidores Unix/Linux?
ix. Do total acima, quantos servidores estão acessíveis externamente, a partir da Internet?
x. Qual o número total de estações de trabalho da rede interna?
xi. Caso exista algum serviço da sua rede hospedado em provedor ou datacenter externo, responda abaixo:
    a. Qual o nome do provedor ou datacenter?
    b. Quais os serviços hospedados nele?
    c. Quanto aos roteadores da sua rede, quantos são?
    d. Quais as principais marcas dos roteadores instalados?
    e. Quantos são os links para a Internet?
xii. Caso utilizem os bancos de dados, quais são os bancos (Oracle, MS-SQL, MySQL, Firebird, outros)?

RESPOSTA 7: Conforme errata publicada em 01/10/2024, foram retirados os itens 8,9 e 10 da tabela do item 12.3.2.4.1.

Brasília - DF, 01 de outubro de 2024.

Comissão Permanente de Contratação e Alienação