OFÍCIO N. 159/2023
ASSUNTO: Pedido de esclarecimentos ao Pregão Eletrônico nº 19/2023.
PROCESSO N. 8521639-33.2023.8.06.0000

Fortaleza, 30 de novembro de 2023.

Prezado(s) Senhor(es),

Em resposta aos questionamentos enviados ao endereço eletrônico da Comissão Permanente de Contratação do TJCE, por empresas interessadas em participar do Pregão Eletrônico n. 19/2023, informo os esclarecimentos que seguem:

Pergunta 01:

Gostaríamos de entender melhor suas necessidades de segurança cibernética e apresentar uma solução tailor-made que acreditamos ser ideal para fortalecer a postura de segurança da infraestrutura de TI do TJ. Considerando a importância do Blue Team, propomos um Atestado de Habilitação Técnica com serviço de resposta a incidentes, e aqui estão alguns motivos pelos quais justificamos nossa proposta:

1. Compreensão da Necessidade: O TJ-CE já percebeu a necessidade crescente de uma estratégia de segurança cibernética robusta na organização. O Blue Team é crucial para prevenir, detectar e responder eficientemente a incidentes de segurança.

2. Especialização Técnica: Nossa equipe técnica possui certificações e experiência comprovada em segurança cibernética, garantindo que o atestado de habilitação técnica seja mais do que uma formalidade, sendo um reflexo tangível do nosso compromisso com a excelência.

3. Abordagem Proativa: Vemos a resposta a incidentes não apenas como uma reação, mas como uma ação proativa. Estamos constantemente atualizados sobre as últimas ameaças e empregamos medidas preventivas para evitar ataques.

4. Personalização do Serviço: Reconhecemos a singularidade de cada organização. Nosso serviço de resposta a incidentes é adaptável, podendo ser moldado para atender às necessidades específicas da sua empresa.

5. Conformidade com Normativas: Além de fortalecer a segurança, nossa oferta ajuda na conformidade com regulamentações governamentais e do setor, evitando penalidades associadas à não conformidade.

Diante desses pontos, gostaríamos de questionar se um atestado que explicita Resposta à Incidentes de Segurança pode ser utilizado para comprovar a habilitação técnica referente ao serviço 01 - Serviço de gestão de incidentes de segurança (Blue Team).

Resposta 01:

Não, o entendimento está errado. A CONTRATADA deverá apresentar documentação comprovatória solicitada nos itens dos documentos “Termo de Referência – TR” e “TRF ANEXO I”. Todavia, atestados podem ser utilizados para reforçar a comprovação de requisitos.

Pergunta 02:

De forma similar, possuímos alguns atestados de Testes de Intrusão, com atividades bastante similares a um serviço de Red Team, que basicamente utiliza-se de um Teste de Intrusão focado em Mitre Att&ck, para testar a eficácia de um ambiente, de forma controlada, bem como os controles de detecção das ferramentas de segurança. Desta forma, gostaríamos de confirmar a possibilidade da utilização de atestados de capacidade técnica de Testes de Intrusão para comprovar a habilitação técnica referente ao serviço 02 - Serviço de gestão testes de invasão (Red Team).

Resposta 02:

Não, o entendimento está errado. A CONTRATADA deverá apresentar documentação comprovatória solicitada nos itens dos documentos “Termo de Referência – TR” e “TRF ANEXO I”. Todavia, atestados podem ser utilizados para reforçar a comprovação de requisitos.

Pergunta 03:

Sobre o a execução do serviço de Pentest.
Quanto Pentest serão realizados o período de 36 meses ?

Resposta 03:

Não existe quantidade estabelecida/definida para a realização dos pentests. Os quantitativos e alvos dos testes de invasão, assim como as premissas e condições para realização dos mesmos serão, necessariamente, definidos e aprovados pela equipe de segurança da informação do TJCE.

Pergunta 04:

Em relação ao Item 4. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS GERENCIADOS DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO do TRF ANEXO I. – Relativos AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação, temos o seguinte subitem:

> *"4.3.1.A solução deverá oferecer a possibilidade da utilização de quantos coletores de eventos forem necessários de acordo com sua arquitetura de preferência (network appliance ou virtualização), desde que não gere impacto no desempenho (processamento, uso de memória, uso de armazenamento) nos ativos do TJCE."*

Entende-se que em relação aos coletores de eventos, será a CONTRATADA que deverá fornecer o hardware necessário para a instalação deles, dito isso, para um correto dimensionamento de servidores para abarcar os coletores virtuais, perguntamos: As fontes dos logs (firewalls, servidores, switches, etc) estão em uma única localidade ou poderão estar em mais de uma localidade? Se estiverem em mais de uma localidade, poderiam esclarecer a o desenho de arquitetura de rede e informar se essas localidades se comunicam entre si e com o Datacenter principal do TJ-CE e assim identificarmos se deverá ser alocado 1 ou mais coletores por localidade remota.

Resposta 04:

Sim, o entendimento está correto. As fontes dos logs (firewalls, servidores, switches, etc) estão em duas localidades na cidade de Fortaleza – CE.

Pergunta 05:

Em relação ao Item 4. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS GERENCIADOS DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO do TRF ANEXO I. – Relativos AQSETIN2022010 – Serviços Gerenciados de Segurança da Informação, temos o seguinte subitem:

> *"4.4.17. A solução deve ser capaz de correlacionar eventos e fluxos de rede, como NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou componentes adicionais ao licenciamento da solução."*

Entende-se que a solução deverá não só fazer a análise de logs e eventos, coma também de fluxos de rede. O TJ-CE tem o quantitativo de FPM (Flows per minute) que deverá ser contratado?

Resposta 05:

Não, o entendimento está errado. Conforme o item 4.6.3 do documento TRF ANEXO I, a CONTRATANTE somente usará a métrica de EPS como referência de contratação.

Pergunta 06:

Em relação ao Item 4. REQUISITOS TÉCNICOS MÍNIMOS DOS SERVIÇOS GERENCIADOS DE MONITORAMENTO E CORRELAÇÃO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO do EDITAL, temos o seguinte subitem:

"4.2.4. A CONTRATADA deverá implantar coletores (virtualizados ou em hardware) no ambiente do TJCE, a fim de realizar a coleta de logs localmente no ambiente do TJCE, absorvendo toda a responsabilidade de implantação dos coletores (Servidores, Máquinas Virtuais, Processamento, Sistema Operacional, etc). O TJCE somente fornecerá energia e link de conexão para o funcionamento da implantação dos coletores."

Entende-se que para o atendimento pleno do objeto a CONTRADA deverá realizar a instalação de um servidor hardware para realizar a coleta de logs nas instalações físicas do TJCE. Para melhor posicionamento das soluções, solicita-se que seja respondida as seguintes perguntas:

Qual o padrão de tomada utilizada no data center para o fornecimento dos cabos de força?

Para a comunicação de rede, qual o tipo de conexão deve ser ofertado? (ex.: ETH, SFP).

Qual a velocidade das portas do switch? Qual o modelo e marca do Switch ao qual o servidor vai ser conectado?

Deverá ser fornecido Cabo DAC, ETH ou Transceiver para esta comunicação? Se sim qual o modelo?

Resposta 06:

As especificações necessárias podem variar em função da ferramenta e do hardware da contratada. Essas dúvidas técnicas devem ser esclarecidas na vistoria técnica.

Pergunta 07:

DO PRAZO DE EXECUÇÃO DO OBJETO

O edital e seus ANEXOS definem que:

"5.2. A execução do objeto seguirá a seguinte dinâmica:

5.2.1. A CONTRATADA deverá implantar os serviços, no prazo máximo de 30 dias corridos após assinatura de contrato e Ordem de Serviço das soluções contratadas com, pelo menos, os seguintes requisitos atendidos e documentados em um relatório de implantação:

5.2.1.1. Lotação de todos os profissionais alocados por perfil (com a devida documentação comprobatória conforme itens 2.4, 3.4 e 4.8 do documento TRF ANEXO I) para os horários de expediente regular e de plantão contínuo.

5.2.1.2. Comprovação da disponibilidade de uso dos recursos de TI descritos no item 1.3.6 do documento TRF ANEXO I para viabilização de imediata prestação de serviços"

Em se tratando de um prazo exíguo para implantação das soluções exigidas neste certame, bem como a disponibilização de recursos humanos e seus materiais de trabalho, recursos estes que estarão dedicados para atuar/atender ao escopo disposto no edital e termos de referência, estamos entendendo que este prazo de 30 dias corridos poderá sofrer dilação, desde que alinhado previamente entre Contratada e Contratante, justificado e aprovado pelo TJCE.

Nosso entendimento está correto?

Resposta 07:

O Entendimento esta errado. A dilatação do prazo somente poderá ocorrer para casos efetivamente inesperados, fortuitos e imprevisíveis.

Pergunta 08:

DO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

O edital e seus ANEXOS definem que:

"4.7.14.6 Toda a mão de obra especializada necessária para a instalação e configuração da solução de SIEM deve ser fornecida pela CONTRATADA." Estamos entendendo que para atendimento do item de instalação, esta atividade poderá ser executada pelo corpo técnico do FABRICANTE da solução de SIEM ofertada pela CONTRATADA, devidamente certificado nos moldes do edital, que atuará sob gestão da CONTRATADA, de forma a acompanhar fim a fim o processo de instalação e configuração.

Nosso entendimento está correto?

Resposta 08:

Não, o entendimento está errado. Conforme item 6.2.41 a CONTRATADA tem como dever e responsabilidade: "6.2.41. Não subcontratar, ceder ou transferir, total ou parcial o objeto desta contratação.". A responsabilidade da instalação, implantação, configuração e outras etapas que necessárias para o correto funcionamento do SIEM é do corpo técnico da CONTRATADA e deve ser executada pela CONTRATADA. Todavia, não há impedimento da CONTRATADA contar com o suporte técnico do FABRICANTE.

Pergunta 09:

DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O edital e seus ANEXOS definem que:

"10.1.1.9. Objetivando facilitar e agilizar o processo de validação das especificações técnicas da Solução e como forma de comprovação, a licitante deverá anexar todas as documentações técnicas comprobatórias das características e especificações para cada item do Serviços a serem adquiridos.

10.1.1.10. Deverá ser anexado junto a sua proposta, documento contendo o item do Edital e sua referência comprobatória, informando/indicando/referenciando as referidas documentações técnicas comprobatórias."

Estamos entendendo que para atendimento deste item, será suficiente a apresentação de documentação técnica (datasheet, folheto, folder, manual) do FABRICANTE da solução a ser ofertada. Nosso entendimento está correto?

Resposta 09:

O entendimento esta errado. É obrigatório a apresentação da documentação tecnica (item 10.1.1.9) e documento informado no item 10.1.1.10.

Pergunta 10:

Com relação aos documentos que precisarão ser assinados, entendemos que as assinaturas poderão ser feitas de forma digital, por meio do sistema Docusign, já que este é capaz de garantir a confiabilidade do processo, por meio da criptografia utilizada. Está correto nosso entendimento?

Resposta 10:

O entendimento esta errado. O TJCE não usa e não conhece a plataforma Docusign. Desta forma, a apresentação dos documentos assinados digitalmente desta licitação e da futura assinatura da Ata de Registro de Preço / Contrato deverá ocorrer em arquivo do tipo PDF, utilizando certificado valido da plataforma ICP-Brasil.

Pergunta 11:

1.1 ITEM DE REFERÊNCIA: ANEXO I - ITEM 1.6: "A CONTRATADA deverá realizar todas suas atividades com o suporte de ferramenta de Gerenciamento de Serviços de TI (ITSM) do TJCE..."

QUESTIONAMENTO: Para fins de uma possível conectividade via API entre a ferramenta de ITSM da CONTRATADA e o da CONTRATANTE, qual a ferramenta de ITSM utilizada pelo TJCE?

Resposta 11:

Atualmente a ferramenta de Gerenciamento de Serviços de TI (ITSM) do TJCE é o Assyst 10 SP7.5.

Pergunta 12:

2.1 ITEM DE REFERÊNCIA: 2.2. Monitoramento de segurança:

QUESTIONAMENTO: Entendemos que para inclusões de ativos monitorados a CONTRATADA será responsável pela parametrização no SIEM. Já a configuração de APIs e outras devidas configurações dentro das ferramentas de segurança a serem monitoradas será de responsabilidade da CONTRATANTE ou da empresa terceirizada responsável pelo suporte desta respectiva ferramenta. Está correto este entendimento?

Resposta 12:

Sim, o entendimento está correto.

Pergunta 13:

3.1 ITEM DE REFERÊNCIA: 2.3.2. Análise de ameaças:

QUESTIONAMENTO: A gestão da ferramenta Tenable citada neste termo é de responsabilidade do time de segurança do TJCE?

Resposta 13:

Sim, o entendimento está correto.

Pergunta 14:

4.1 ITEM DE REFERÊNCIA: "2.3.3. Gerenciamento de vulnerabilidades: Será responsabilidade do Blue Team realizar avaliações regulares de vulnerabilidades nos sistemas do TJCE e recomendar as medidas necessárias para mitigar essas vulnerabilidades. Eles também devem acompanhar as atualizações de segurança, patches e correções fornecidas pelos fornecedores de software e hardware, assim como demandar e supervisionar que essas atualizações sejam implementadas."

Questionamento: Entendemos que o Blue Team será responsável por avaliações regulares de vulnerabilidades nos sistemas do TJCE, através dos logs correlacionados no SOC e recomendando as medidas necessárias para correção destas vulnerabilidades. O time de especialistas do TJCE será responsável pela execução destas correções de vulnerabilidades, tais como Atualizações de S.O, instalação de patches e etc. Está correto este entendimento?

Resposta 14:

Sim, o entendimento está correto.

LUIS LIMA VERDE SOBRINHO:00033309310

Assinado de forma digital por LUIS LIMA VERDE SOBRINHO:00033309310
Dados: 2023.12.01 15:28:23 -03'00'

Luis Lima Verde Sobrinho
Presidente da Comissão Permanente de Contratação do TJCE

À empresa interessada em participar do Pregão Eletrônico 19/2023.