BANCO DE DESENVOLVIMENTO DE MINAS GERAIS S.A. – BDMG
PREGÃO ELETRÔNICO BDMG-27/2021
Nº DO PROCESSO DE COMPRAS NO PORTAL COMPRAS MG: 5201006 000008/2021
ESCLARECIMENTOS

RESPOSTAS A QUESTIONAMENTOS

QUESTIONAMENTO 5: "Em relação ao APÊNDICE I – AMBIENTE COMPUTACIONAL E DE SEGURANÇA DO BDMG, entendemos que para precificação adequada devemos considerar apenas os ativos de segurança conforme informado abaixo:

Descrição da solução	Fabricante/Produto	Quantidade total
Next Generaton Firewall IDS/IPS/VPN/Web Filter	Checkpoint	2 (dois) em HA
Next Generton Firewall IDS/IPS/VPN/Web Filter	Fortnet Fortgate	2 (dois) em HA
Web Applicaton Firewall (WAF)	Web Application Firewall (WAF)	
VPN site-site	Checkpoint Azure VPN Gateway	3 (três)
Controladores de domínio	Actve Directory	6 (seis)
Azure Actve Directory		
Servidores de bancos de dados	Microsoft SQL Server 2008 R2, 2012, 2017 e 2019	12
Servidores web	Servidores web	
Proteção de e-mail (antspam, antphishing e antmalware)	Microsoft Defender for Office 365	520 usuários
Prevenção de vazamento de dados (DLP)	Microsoft Defender for Office 365	520 usuários
Proteção de Endpoint (EPP)	Symantec Endpoint Security versão 14	1 (um) servidor de gerência 800 agentes

Considerando os ativos de segurança acima, é possível, através das métricas de mercado disponíveis a todos os concorrentes, que a utilização seja próxima do estimado, ou seja, 68 GB/dia, não alterando a estimativa de preços realizada pelo CONTRATANTE.

Caso seja necessário contabilizarmos todos os ativos informados na tabela apresentada no APÊNDICE I – AMBIENTE COMPUTACIONAL E DE SEGURANÇA DO BDMG, através das métricas de mercado disponíveis a todos os concorrentes, teremos que considerar aproximadamente 200 GB/dia. Este valor equivale a uma quantidade aproximadamente 3 vezes superior ao informado, número este que não foi considerado para estimativa deste certame. A adição de todos ativos neste momento agregará pouco tecnicamente ao serviço solicitado pelo BDMG, objeto deste edital.

Levando em consideração o exposto acima, entendemos que a forma de cálculo utilizada para métrica e precificação deva ser realizada com os ativos de segurança acima informados.

Está correto nosso entendimento"?

RESPOSTA: sim, está correto o entendimento.

QUESTINAMENTO 6: "Relativo ao ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL - LOTE 1 na sua CLÁUSULA QUINTA - SERVIÇO DE MONITORAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA, item: '5.3.2. Efetuar a resposta, investigação e encerramento dos incidentes de segurança da informação, incluindo o acionamento dos seus especialistas de nível sênior (nível 3) nos casos de incidentes críticos ou de severidade alta'.

Em um processo de resposta a incidentes, o conhecimento do ambiente é de extrema importância para correta investigação, contenção e erradicação deste. Considerando que a CONTRATANTE continuará responsável pela administração do ambiente, entendemos que toda a resposta, onde for necessária a atuação da CONTRATADA, esta ficará de apoio e definição das ações a serem tomadas, porém, sempre acompanhada de pessoas com conhecimento do ambiente e devidos acessos para execução das atividades.

Está correto nosso entendimento"?

RESPOSTA: sim, está correto o entendimento.

QUESTINAMENTO 7: "Relativo ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL - LOTE 1 na sua CLÁUSULA QUINTA - SERVIÇO DE MONITORAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA, item '5.4.2. Todos os componentes da solução serão fornecidos por um único fabricante' e na sua CLÁUSULA SÉTIMA - SERVIÇO DE GESTÃO DE VULNERABILIDADES item '7.5.2. Os componentes da solução poderão ser fornecidos por fabricantes distintos, desde que funcionem de forma integrada e os relatórios e painéis (dashboards) de gestão sejam apresentados em uma interface unificada;'

Entendemos que assim como no item 5.4.2, referente ferramenta de SIEM, no item 7.5.2, referente a gestão de vulnerabilidades, o software utilizado em todo o processo deva ser do mesmo fabricante visando aumentar a interoperabilidade, diminuir as possíveis incompatibilidades no ambiente, reduzir as interações na resolução de problemas e reduzir os tempos de atendimentos, além de aumentar a qualificação dos softwares participantes e consequentemente a qualidade da entrega e resultados dos serviços.

Está correto nosso entendimento"?

RESPOSTA: não está correto o entendimento. A solução de Gestão de Vulnerabilidades poderá utilizar componentes de fabricantes distintos, desde que observados todos os termos do item 7.5.2.

QUESTINAMENTO 8: "Relativo ao ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL - LOTE 1 na sua CLÁUSULA SÉTIMA - SERVIÇO DE GESTÃO DE VULNERABILIDADES item: '7.3.3.

Descobrir, classificar e atualizar continuamente o inventário de ativos de TI monitorados pelo serviço, tais como switches, access points, roteadores, firewalls, servidores, desktops, notebooks, sistemas operacionais, aplicações web, bancos de dados, contêineres, etc.;'

A precificação do processo de Gestão de Vulnerabilidades varia conforme a quantidade de itens monitorados. Entendemos que, na hipótese de mudanças que, comprovadamente, afetem o dimensionamento inicial dos serviços especificados no objeto do Lote 1 deste edital, poderá ser feito aditamento contratual nos termos legais.

Está correto nosso entendimento"?

RESPOSTA: sim, está correto o entendimento.

QUESTINAMENTO 9: "Relativo ao ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL - LOTE 1 na sua CLÁUSULA SÉTIMA - SERVIÇO DE GESTÃO DE VULNERABILIDADES item '7.5.5. Possuir tecnologia de priorização dinâmica de vulnerabilidades (Vulnerability Priorization Technology) baseada em riscos (risk-based priorizaton) e não apenas em ameaças e padrões como CVSS, CVE ou CWE;'

Diante do cenário cada vez maior de incidentes de segurança e aumento exponencial de vulnerabilidades, entendemos a importância da priorização dentro do processo de gestão de vulnerabilidade como essencial. Existem ainda outros métodos para avaliar como a empresa está posicionada em relação ao seu mercado e assim auxiliar no correto desprendimento de esforços e investimentos para correções. Podemos citar, por exemplo, uma pontuação global de exposição cibernética da organização baseada na pontuação de cada ativo. Entendemos desta maneira que a solução de Gestão de Vulnerabilidades deva ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor.

Está correto nosso entendimento"?

RESPOSTA: não está correto o entendimento. A capacidade de a solução de Gestão de Vulnerabilidades realizar benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor não é requisito do edital.

QUESTINAMENTO 10: "Relativo ao ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL - LOTE 1 na sua CLÁUSULA OITAVA - TESTES DE INVASÃO (PENTESTS) item '8.4. Os Testes de Invasão serão originados interna e externamente ao ambiente computacional do BDMG e serão executados em etapas de acordo com as modalidades descritas a seguir:

I. Caixa-preta (Black-Box): os especialistas da CONTRATADA (pentesters) buscarão informações relevantes sobre o escopo do teste disponíveis em fontes públicas;

II. Caixa-cinza (Gray-Box): os especialistas da CONTRATADA (pentesters) receberão do BDMG informações limitadas sobre o escopo do teste.

III. Caixa-branca (White-Box): os especialistas da CONTRATADA (pentesters) receberão do BDMG informações completas sobre o escopo do teste.'

Os esforços empregados na realização de um teste de invasão podem variar consideravelmente a depender do tipo e escopo, principalmente nas modalidades Gray-Box e White-Box.

BANCO DE DESENVOLVIMENTO DE MINAS GERAIS S.A. – BDMG
PREGÃO ELETRÔNICO BDMG-27/2021
Nº DO PROCESSO DE COMPRAS NO PORTAL COMPRAS MG: 5201006 000008/2021
ESCLARECIMENTOS

Para uma correta mensuração de esforço quais serão os limites de cada teste de invasão? Ou estes serão sempre acordados entre as partes para a emissão da ordem de serviços"?

RESPOSTA: não está correto o entendimento. Cada teste de invasão contemplará integralmente as modalidades e o escopo descritos nos itens 8.4 e 8.5.

QUESTINAMENTO 11: "Relativo ANEXO IV – MINUTA DO INSTRUMENTO CONTRATUAL - LOTE 1 na sua CLÁUSULA QUINTA - SERVIÇO DE MONITORAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA, item '5.4.2. Todos os componentes da solução serão fornecidos por um único fabricante;'

Entendemos a importância deste item, posto que, esta exigência auxilia na redução de problemas oriundos de situações que envolvam compatibilidade e interoperabilidade entre componentes da solução, dentre outros. Contudo, alguns dos principais fabricantes, líderes de mercado no segmento de SIEM, não possuem hardware próprio e fazem parceria com outros fabricantes para construção dos seus softwares com compatibilidade completa.

Entendemos que a solicitação de que todos os componentes da solução sejam do mesmo fabricante refere-se ao Software e será aceito hardware de fabricantes diferentes, desde que seja comprovado a compatibilidade entre eles.

Está correto nosso entendimento"?

RESPOSTA: o entendimento está parcialmente correto. Caso a arquitetura da solução SIEM seja fornecida como hardware, este será provisionado e customizado pelo fabricante da referida solução (appliance).

QUESTINAMENTO 12: "Entendemos que como uma forma de garantir os SLAs e a qualidade do atendimento dos serviços de Monitoramento e Resposta a Incidentes de Segurança, Proteção de Endpoint contra Ameaças Avançadas e Gestão de Vulnerabilidades, os softwares ofertados deveram ser, obrigatoriamente, de propriedade ou estarem licenciados para CONTRATADA e não poderão ser do tipo open source (software livre).

Está correto nosso entendimento"?

RESPOSTA: sim, está correto o entendimento, conforme o edital, Anexo IV, item 2.4.

Belo Horizonte, 22 de novembro de 2021.

Sérgio Vieira de Souza Júnior
Pregoeiro do BDMG