TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Definição do objeto:

O objeto do presente Termo de Referência consiste na contratação de empresa especializada para o fornecimento de subscrições das soluções de segurança da informação Hillstone sBDS I2850 e Syhunt, incluindo suporte técnico remoto em regime 24 horas por dia, 7 dias por semana, com tempo de resposta de até 4 (quatro) horas, pelo período de 24 (vinte e quatro) meses. A contratação visa assegurar a continuidade e a evolução da estratégia de proteção cibernética da Administração Pública Municipal, mantendo a infraestrutura tecnológica atualizada e protegida contra ameaças emergentes, com alto grau de confiabilidade e disponibilidade. O fornecimento da subscrição da solução Hillstone compreende a disponibilização de atualizações contínuas de assinaturas de ameaças, acesso às funcionalidades de detecção e prevenção avançada de intrusões, análise comportamental, sandbox em nuvem, inteligência de ameaças e correlação de eventos, integradas ao equipamento Hillstone sBDS I2850 de propriedade da Administração, devidamente configurado e em operação. No que se refere à solução Syhunt, o fornecimento de subscrição contempla a plataforma de análise de vulnerabilidades em aplicações web e móveis, com suporte às metodologias DAST, SAST, FAST, OAST e HAST, integrando a varredura dinâmica, estática e híbrida de segurança de aplicações, com atualizações de motores de detecção e suporte técnico especializado. As subscrições fornecidas deverão garantir plena integração às soluções atualmente em operação, sem prejuízo à continuidade dos serviços e às políticas de segurança já estabelecidas. O período de vigência do fornecimento será de 24 (vinte e quatro) meses, contados a partir da assinatura do contrato, sendo o objeto essencial para assegurar a manutenção da resiliência digital da rede corporativa municipal, a conformidade com normas de segurança da informação e a proteção de dados sensíveis sob a guarda do Município.

1.2. Justificativa para a contratação

a) Descrição da situação atual:

A contratação justifica-se pela necessidade de assegurar a continuidade das ações de proteção cibernética e segurança da informação no ambiente institucional da Administração Pública Municipal, por meio do fornecimento de subscrições e serviços de suporte técnico especializado das soluções Hillstone sBDS I2850 e Syhunt, já implantadas na estrutura tecnológica da Prefeitura. Atualmente, o Município utiliza o equipamento Hillstone sBDS I2850 para a inspeção avançada de tráfego de rede, correlação de eventos e detecção de ameaças comportamentais, além da plataforma Syhunt, voltada à análise de vulnerabilidades em aplicações web e móveis. Ambas as soluções encontram-se plenamente operacionais, integradas aos sistemas institucionais, sendo indispensáveis à proteção de ativos digitais, integridade de dados, prevenção contra ataques cibernéticos e conformidade com as políticas internas de segurança da informação.

b) Justificativa para a quantidade a ser contratada:

A quantidade a ser contratada foi definida com base no inventário técnico atual e na política de licenciamento adotada pelos respectivos fabricantes, sendo necessária a contratação de uma unidade de subscrição da solução Hillstone, vinculada diretamente ao equipamento modelo sBDS I2850, e uma unidade de subscrição da solução Syhunt, compatível com o ambiente de desenvolvimento e aplicações da Administração. Ambas as subscrições deverão ter vigência de 24 (vinte e quatro) meses, período estabelecido com base no ciclo contratual padrão do mercado e na conveniência administrativa de evitar renovações frequentes, garantindo previsibilidade e economicidade à gestão pública.

c) Resultados esperados com a contratação:

Com a contratação, espera-se garantir a continuidade dos serviços essenciais de monitoramento e detecção de ameaças em tempo real, assegurar a atualização contínua dos sistemas de defesa digital, evitar vulnerabilidades decorrentes de desatualização ou interrupção de suporte técnico, e reforçar a conformidade da Administração com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), bem como com os princípios constitucionais da eficiência, segurança e continuidade do serviço público.

d) Número de contrato ou ajuste vigente ou vencido para o mesmo objeto:

Não há contrato ou ajuste vigente com o mesmo objeto. A contratação anterior encontra-se encerrada.

2. FORMA DA CONTRATAÇÃO

2.1. Tipo de contratação: A contratação será realizada por meio de licitação, na modalidade pregão eletrônico, conforme previsto no art. 28, inciso I da Lei nº 14.133/2021.

2.2. Modalidade de licitação: A modalidade a ser adotada será o pregão eletrônico, tendo em vista que o objeto consiste na aquisição de bens e serviços comuns de tecnologia da informação, com especificações padronizadas, conforme art. 6º, inciso XIII e art. 28, inciso I, da Lei nº 14.133/2021.

2.3. Indicação justificada da adoção ou não do Sistema de Registro de Preços (SRP): Não se justifica a adoção do Sistema de Registro de Preços (SRP), uma vez que a necessidade é pontual e específica para o atendimento da demanda do Núcleo de Segurança da Informação da Administração, não se tratando de contratação que demande aquisições frequentes ou futuras adesões por outros órgãos. Trata-se de fornecimento com prazo e quantidade determinados, vinculado diretamente à continuidade das operações de segurança atualmente implementadas.

2.4. Indicação justificada do critério de julgamento da contratação: O critério de julgamento a ser adotado será o de menor preço global, conforme art. 33, inciso I, da Lei nº 14.133/2021. A escolha do critério decorre da necessidade de contratação de soluções integradas e complementares de segurança da informação (Hillstone sBDS I2850 e Syhunt), cuja efetividade depende da prestação contínua e articulada dos serviços. O julgamento por menor preço global assegura que o conjunto das soluções seja contratado de maneira unificada, evitando fragmentação da execução, conflitos de responsabilidade e garantindo maior eficiência na gestão e fiscalização do contrato.

2.5. Indicação justificada do critério de adjudicação da contratação: A adjudicação será realizada de forma global, abrangendo o conjunto das soluções Hillstone sBDS I2850 e Syhunt, considerando que ambos os produtos integram, de forma sinérgica e indivisível, a política de segurança da informação da Administração Pública Municipal.

A separação dos itens, com adjudicação por lote, acarretaria risco técnico de fragmentação dos serviços, eventuais conflitos de responsabilidade na execução do suporte e impactos negativos na continuidade e na eficácia da proteção cibernética institucional. A adjudicação global assegura a uniformidade da execução, a simplificação da fiscalização contratual e a plena integração das ferramentas de segurança, em conformidade com o disposto no art. 33, §1º da Lei nº 14.133/2021.

2.6. Indicação justificada da possibilidade de participação ou não de consórcios de empresas:

Não há óbice para a participação de consórcios de empresas.

2.7. Previsão de subcontratação parcial do objeto: Não será permitida a subcontratação parcial do objeto, uma vez que a execução dos serviços de fornecimento de subscrição, suporte técnico e atualizações de segurança requer a atuação direta da empresa contratada, devidamente autorizada e certificada pelos fabricantes das soluções Hillstone e Syhunt, de modo a garantir a integridade técnica, a segurança operacional e a rastreabilidade dos serviços prestados.

2.8. indicação quanto a óbice para aplicação de adoção do tratamento diferenciado para microempresas, empresas de pequeno porte ou sociedades cooperativas, conforme disposto no art. 49 da Lei Complementar federal nº 123, de 2006, acompanhado da respectiva justificativa, quando for o caso: Será assegurado o tratamento diferenciado previsto nos arts. 47 e 48 da Lei Complementar nº 123/2006 às microempresas, empresas de pequeno porte e sociedades cooperativas que participarem do certame, não havendo óbice técnico ou operacional que inviabilize sua participação, mesmo diante da especialização do objeto. A observância dos requisitos técnicos mínimos exigidos no edital será condição para a habilitação, independentemente do porte da empresa.

2.9. indicação quanto à possibilidade de aplicação de direito de preferência, previsto em Lei, quando o objeto assim permitir: Não será aplicado direito de preferência para produtos manufaturados nacionais ou serviços nacionais em relação a similares importados, considerando que as soluções tecnológicas Hillstone e Syhunt são

de origem estrangeira, sem substitutos nacionais equivalentes disponíveis no mercado, e que a adoção de soluções diversas comprometeria a compatibilidade e a continuidade operacional da infraestrutura de segurança da informação da Administração.

2.10. Condições específicas de participação para utilização de recursos PNAFM3

Só poderão participar da presente licitação, empresas originárias dos países membros do Banco Interamericano de Desenvolvimento – BID (países elegíveis – conforme anexo do edital) que ofereçam bens cuja origem seja de um país também membro do BID, e que atendam às seguintes normas:

a) Critérios para determinar a nacionalidade:

I. Um indivíduo tem a nacionalidade de um país membro do Banco se satisfaz um dos seguintes requisitos:

a. é cidadão de um país membro; ou

b. estabeleceu seu domicílio em um país membro como residente de boa fé e está legalmente autorizado para trabalhar nesse país.

II. Uma empresa tem a nacionalidade de um país membro se satisfaz os dois seguintes requisitos:

a. está legalmente constituída ou incorporada conforme as leis de um país membro do Banco; e,

b. mais de 50 % (cinquenta por cento) do capital da empresa é de propriedade de indivíduos ou firmas de países membros do Banco.

b) Critério para determinar a origem dos bens:

I. Os bens se originam em um país membro do Banco se foram extraídos, cultivados, colhidos ou produzidos em um país membro do Banco.

II. Considera-se um bem produzido quando, mediante manufatura, processamento ou montagem, o resultado é um item comercialmente reconhecido cujas características básicas, sua função ou propósito de uso são substancialmente diferentes de suas partes ou componentes.

III. No caso de um bem que consiste de vários componentes individuais que devem ser interconectados (pelo fornecedor, comprador ou um terceiro) para que o bem possa ser utilizado, e sem importar a complexidade da interconexão, o Banco considera que este bem é elegível para financiamento se a montagem dos componentes for feita em um país membro, independente da origem dos componentes.

IV. Quando o bem é uma combinação de vários bens individuais que normalmente são empacotados e vendidos comercialmente como uma só unidade, o bem é considerado proveniente do país onde este foi empacotado e embarcado com destino ao comprador.

V. Para fins de determinação da origem dos bens identificados como "feito na União Europeia", estes serão elegíveis sem necessidade de identificar o correspondente país específico da União Europeia.

VI. A origem dos materiais, partes ou componentes dos bens ou a nacionalidade da empresa produtora, montadora, distribuidora ou vendedora dos bens não determina sua origem.

c) Critério para determinar a origem dos serviços:

I. O país de origem dos serviços é o mesmo do indivíduo ou empresa que presta os serviços conforme os critérios de nacionalidade acima estabelecidos. Estes critérios são aplicados aos serviços conexos ao fornecimento de bens (tais como transporte, seguro, instalação, montagem etc.), aos serviços de construção e aos serviços de consultoria.

3. REQUISITOS DO FORNECEDOR

3.1. indicação justificada de necessidade de vistoria, ainda que facultativa

As licitantes deverão observar os mais altos padrões éticos durante o processo licitatório e a execução do contrato, estando sujeitas às sanções previstas na legislação brasileira e nas normas do Banco Interamericano de Desenvolvimento – BID.

Considerando que o objeto da contratação se refere ao fornecimento de subscrições de softwares com suporte técnico remoto especializado, cujo escopo não demanda o acesso físico a instalações da Administração, não será exigida a realização de vistoria técnica, nem mesmo em caráter facultativo, para participação no certame.

As soluções contratadas serão operadas em equipamentos e estruturas já existentes no ambiente interno da Administração Pública Municipal, com as quais os fornecedores deverão manter compatibilidade técnica, conforme as especificações detalhadas no presente Termo de Referência. Tendo em vista que a execução contratual não envolve obras, instalações físicas, deslocamentos ou intervenções presenciais, não há peculiaridades técnicas no local de prestação do serviço que justifiquem a realização de vistoria prévia.

Ainda assim, para fins de plena ciência das condições contratuais, os licitantes deverão apresentar, juntamente com sua proposta, declaração formal assinada por representante legal da empresa, sob as penas da lei, atestando que têm pleno conhecimento do objeto, das especificações técnicas e das peculiaridades inerentes à sua execução, comprometendo-se a não alegar desconhecimento de quaisquer aspectos técnicos ou operacionais para fins de questionamento futuro, sem prejuízo à ampla competitividade do certame.

3.2. indicação justificada da capacidade técnica a ser exigida do fornecedor

Em razão da natureza crítica do objeto a ser contratado, será exigida a comprovação de capacidade técnica do fornecedor, nos termos do art. 67 da Lei nº 14.133/2021, especialmente em seu §3º, que determina que a exigência de experiência anterior deve restringir-se às parcelas de maior relevância técnica ou de valor significativo. A exigência se justifica em virtude da complexidade envolvida na execução do contrato, que abrange o fornecimento de subscrições especializadas em segurança da informação e a prestação contínua de serviços de suporte técnico remoto, com tempo de resposta reduzido e elevado grau de responsabilidade técnica.

A parcela de maior relevância técnica da contratação refere-se à prestação de serviços de suporte técnico especializado em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), com tempo de resposta de até 4 (quatro) horas, voltados às soluções Hillstone sBDS I2850 e Syhunt. Esses sistemas são estratégicos para a proteção da infraestrutura de rede e das aplicações web da Administração Municipal, e sua operação ininterrupta é essencial para garantir a continuidade e segurança dos serviços públicos. A interrupção ou falha na execução desses serviços comprometeria a integridade dos dados institucionais e a disponibilidade de sistemas internos.

Para fins de habilitação, a comprovação da capacidade técnica deverá ocorrer por meio de apresentação de atestado(s) de capacidade técnica operacional emitido(s) por pessoa jurídica de direito público ou privado, que comprovem a execução de objeto com escopo, complexidade e finalidade similares ao deste certame. Os atestados deverão conter a descrição dos serviços executados, os sistemas envolvidos e as condições técnicas da prestação, bem como ser assinados por representante legal da contratante.

A Administração poderá exigir que o fornecedor demonstre ser revenda autorizada e certificada pelos fabricantes Hillstone e Syhunt, mediante apresentação de documentação oficial emitida pelos respectivos detentores da tecnologia, como forma de assegurar que

o suporte técnico prestado tenha legitimidade, acesso aos canais oficiais de atualização e escalonamento técnico conforme exigências contratuais.

A exigência de capacidade técnica está limitada exclusivamente às parcelas de maior relevância técnica do objeto, conforme exigência legal, e não poderá ser estendida a etapas acessórias ou genéricas da contratação. Será vedada a exigência de comprovação de tempo mínimo de experiência profissional, bem como de apresentação de currículos ou documentos pessoais da equipe técnica, sendo suficiente a declaração formal de disponibilidade da equipe, nos termos da legislação vigente.

3.3. Indicação justificada de necessidade de apresentação de amostras

Não será exigida a apresentação de amostras, considerando que o objeto da contratação refere-se à subscrição de soluções tecnológicas específicas (Hillstone sBDS I2850 e Syhunt) e à prestação de suporte técnico especializado remoto, cujas características técnicas, funcionalidades e requisitos de desempenho podem ser plenamente verificadas por meio de documentação técnica, certificados de conformidade, atestados de capacidade técnica e demais comprovações formais exigidas no certame.

3.4. HABILITAÇÃO JURÍDICA

a) Ato Constitutivo, Estatuto ou Contrato Social em vigor, todos devidamente registrados, em se tratando de sociedades empresariais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

b) Inscrição do Ato Constitutivo, no caso de sociedades simples, acompanhada de prova da diretoria em exercício, devidamente registrado no órgão competente;

c) Decreto de Autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País;

3.5. QUALIFICAÇÃO TÉCNICA

a) Atestado(s), expedido(s) por Pessoa Jurídica de Direito Público ou Privado, em nome da licitante, que demonstre(m) capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior por meio da comprovação de execução dos serviços abaixo relacionados restrito às parcelas de maior relevância ou valor significativo do objeto desta licitação:

- prestação de serviços de suporte técnico especializado relacionado às subscrições objeto desta contratação, em regime 24x7, com tempo de resposta de até 4 (quatro) horas.

b) A comprovação de fornecimento mencionado neste item poderá ser feita mediante apresentação de 01 (um) ou mais atestados referentes a um único ou a diversos contratos.

c) O(s) Atestado(s) de Capacidade Técnica (Técnico Operacional), deverão ser elaborado(s) contemplando as informações detalhadas do(s) fornecimento(s) ou serviço(s) prestado(s), sendo assinado(s) e com identificação do nome, cargo ou função do(s) emitente(s), estando sujeito(s) à faculdade prevista no artigo 64 da Lei Federal nº 14.133/2021 com suas alterações.

3.6. DA AMOSTRA E/ OU CATÁLOGO

Não se aplica.

3.7. DA PROVA DE CONCEITO

Não será exigida prova de conceito.

3.8. HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA

a) Prova de Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

b) Certidão Negativa ou positiva com efeito de negativa de Tributos Municipais Mobiliários, expedida no local do domicílio ou sede do interessado, relativa as taxas de poder de polícia e ISS;

c) Certidão Negativa ou positiva com efeito de negativa de Tributos Estaduais, expedida no local do domicílio ou sede da licitante, relativo aos tributos incidentes sobre o objeto desta licitação.

d) Certidão Negativa ou positiva com efeito de negativa de Débitos relativos aos Tributos Federais e a Dívida Ativa da União, expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN);

e) Certificado de Regularidade perante o Fundo de Garantia por Tempo de Serviço (FGTS), expedido pela Caixa Econômica Federal.

f) Certidão Negativa ou Positiva com efeito de Negativa de Débitos Trabalhistas (CNDT), conforme estabelecido na Lei Federal n.º 12.440 de 08 de julho de 2011.

3.9. HABILITAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica;

4. FORMALIZAÇÃO, PRAZO DE VIGÊNCIA DO CONTRATO E POSSIBILIDADE DE PRORROGAÇÃO (SE HOUVER)

4.1. Instrumento formalizador:

A contratação será formalizada por meio de instrumento contratual específico, nos termos do art. 95 da Lei Federal nº 14.133/2021 e do art. 71 do Decreto Municipal nº 22.260/2023, uma vez que o objeto compreende obrigações futuras vinculadas à prestação contínua de suporte técnico, atualização de soluções e vigência determinada de subscrições, não sendo viável a formalização por nota de empenho isolada ou outro instrumento simplificado.

4.2. Prazo de vigência:

O prazo de vigência do contrato será de 24 (vinte e quatro) meses, contados a partir da assinatura do ajuste, abrangendo todas as etapas necessárias à plena execução do objeto, incluindo a disponibilização e ativação das subscrições contratadas, bem como a prestação ininterrupta do suporte técnico remoto especializado, conforme exigido neste Termo de Referência.

4.3. Possibilidade de prorrogação:

A contratação poderá ser prorrogada, desde que observadas as hipóteses legais previstas no art. 107, da Lei Federal nº 14.133/2021, que admite a prorrogação de contratos cujo objeto envolva prestação de serviços contínuos, mediante justificativa técnica da unidade requisitante e manifestação favorável da assessoria jurídica competente, vedada a prorrogação automática.

4.4. Motivos que fundamentam a escolha por prazo contratual superior a 12 (doze) meses:

A escolha por um prazo contratual de 24 (vinte e quatro) meses fundamenta-se na estratégia administrativa de garantir a continuidade e estabilidade na prestação dos serviços de segurança da informação, considerando a natureza do objeto, que envolve subscrições de soluções tecnológicas especializadas e suporte técnico contínuo.

Trata-se de uma contratação com características de execução duradoura, cujo ciclo operacional exige planejamento de médio prazo, em razão da necessidade de atualização permanente das ferramentas, manutenção ininterrupta do suporte e integração com os sistemas institucionais da Administração.

A vigência bienal também contribui para a racionalização de processos internos, redução de custos operacionais relacionados à frequência de novas licitações e melhor

aproveitamento dos recursos públicos, conferindo maior previsibilidade à gestão contratual e evitando descontinuidade na proteção cibernética do Município.

5. MODELO DE GESTÃO

Nos termos do art. 117 da Lei Federal nº 14.133/2021 e do art. 54 do Decreto Municipal nº 22.260/2023, a gestão e fiscalização do contrato serão realizadas por servidores formalmente designados pela autoridade competente, mediante portaria específica, assegurada a segregação de funções entre as áreas demandante, gestora e fiscalizadora.

O contrato oriundo desta contratação será acompanhado por meio do seguinte modelo de gestão:

Gestor do Contrato: Paulo Henrique Correia de Souza

E-mail: paulohenrique@saobernardo.sp.gov.br

Telefone:2630-5004

Fiscal do Contrato: Claudio Ettruri Fernandez

E-mail:claudio.ettruri@saobernado.sp.gov.br

Telefone:2630-5066

6. PRAZO PARA INÍCIO DA EXECUÇÃO OU ENTREGA DO OBJETO

A execução contratual terá início após a assinatura do instrumento contratual e emissão da respectiva ordem de fornecimento pela Administração, respeitados os prazos e condições estabelecidos neste Termo de Referência e no contrato.

O objeto será executado de forma contínua durante a vigência do contrato, compreendendo o fornecimento das subscrições das soluções Hillstone sBDS I2850 e Syhunt, a ativação técnica das licenças, a manutenção do acesso às atualizações periódicas e o suporte técnico remoto em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), com tempo de resposta de até 4 horas.

A contratada deverá realizar todas as etapas previstas no objeto com observância às boas práticas de governança em tecnologia da informação e em conformidade com os requisitos técnicos estabelecidos neste Termo de Referência.

7. OBRIGAÇÕES DA CONTRATADA

Sem prejuízo das demais obrigações legais, contratuais e previstas no edital, caberá à contratada, durante toda a vigência contratual, o cumprimento integral das seguintes obrigações, sob pena de aplicação das sanções cabíveis:

7.1. Fornecer as subscrições das soluções Hillstone sBDS I2850 e Syhunt, pelo prazo contratual estabelecido, com todas as funcionalidades previstas neste Termo de Referência, devidamente ativadas e operacionais;

7.2. Garantir a plena compatibilidade das subscrições fornecidas com os ambientes e equipamentos tecnológicos atualmente existentes na Administração, em especial com o equipamento Hillstone sBDS I2850 já instalado;

7.3. Disponibilizar suporte técnico remoto em regime 24x7 (vinte e quatro horas por dia, sete dias por semana), com início de atendimento em até 4 (quatro) horas após a abertura do chamado, conforme prazos e níveis de serviço definidos na proposta comercial;

7.4. Manter atualizados, durante toda a vigência do contrato, os componentes das soluções contratadas, incluindo motores de análise, bibliotecas de detecção, assinaturas de ameaças e quaisquer recursos complementares de segurança;

7.5. Garantir que o suporte técnico seja prestado por equipe devidamente capacitada, com domínio das soluções contratadas, observando padrões técnicos e procedimentos de segurança da informação, inclusive sigilo sobre dados sensíveis eventualmente acessados;

7.6. Realizar, sempre que necessário e sem ônus adicional, a revalidação de chaves de licença, reconfiguração de parâmetros ou ajustes técnicos para garantir a continuidade da operação das soluções contratadas;

7.7. Comunicar formalmente à Administração, de forma imediata, qualquer anormalidade, incidente de segurança, indisponibilidade sistêmica ou risco operacional que possa afetar a execução do objeto;

7.8. Responsabilizar-se por todos os encargos trabalhistas, previdenciários, fiscais, comerciais, securitários e tributários decorrentes da execução do contrato, não cabendo qualquer responsabilidade à Administração;

7.9. Reparar, corrigir, remover, substituir, sem qualquer ônus para a Administração, no prazo determinado pela fiscalização, quaisquer falhas, erros, interrupções ou defeitos técnicos detectados nas soluções contratadas, ainda que identificados após o recebimento provisório;

7.10. Responder por danos causados à Administração ou a terceiros, decorrentes de ação ou omissão culposa ou dolosa na execução do objeto contratual;

7.11. Manter, durante toda a vigência contratual, as condições de habilitação exigidas no processo licitatório;

7.12. Fornecer, sempre que solicitado, documentação técnica, manuais, relatórios de conformidade e qualquer outro material necessário à fiscalização contratual;

7.13. Atender às requisições da fiscalização e do gestor do contrato no prazo por estes fixado, sob pena de aplicação das penalidades previstas em contrato.

7.14. Manter sigilo absoluto sobre quaisquer dados, documentos, informações técnicas ou operacionais, códigos de acesso, relatórios, estatísticas ou quaisquer outros elementos sensíveis ou estratégicos a que venha a ter acesso em razão da execução contratual, sendo vedada sua divulgação, cópia ou uso para fins alheios ao contrato, sob pena de responsabilização civil, administrativa e penal.

7.15. Executar diretamente o objeto contratado, sendo vedada a subcontratação, total ou parcial, sem a prévia e expressa autorização da Administração, sob pena de rescisão contratual e aplicação das sanções previstas.

7.16. Garantir a continuidade dos serviços, inclusive no caso de afastamento, substituição ou desligamento de qualquer membro da equipe técnica designada, devendo providenciar substituição equivalente em prazo compatível com a manutenção da qualidade e regularidade da execução contratual.

8. REGIME DE EXECUÇÃO

8.1. Mecanismo de comunicação a serem estabelecidos entre a Unidade demandante e a contratada:

As comunicações entre a contratada e a Administração serão realizadas prioritariamente por e-mail institucional e telefone, devendo a contratada disponibilizar canal direto com suporte técnico em tempo integral (24x7), além de designar um ponto focal responsável pela interlocução com o fiscal do contrato, facilitando a resolução ágil de incidentes, dúvidas e atualizações.

8.2. Descrição detalhada de como deve se dar a entrega do produto ou a execução dos serviços, contendo informações sobre etapas, rotinas de execução e periodicidade do serviço:

A execução consistirá na disponibilização das licenças de subscrição dos softwares Hillstone sBDS I2850 e Syhunt, com ativação remota e validação funcional junto à infraestrutura da Prefeitura, além do fornecimento contínuo de suporte técnico

remoto 24x7, atualizações de segurança e evolução das soluções durante todo o período de vigência contratual.

8.3. Prazos de entrega ou de execução do objeto, incluindo o marco temporal para início da contagem:

O prazo para entrega das licenças e ativação das soluções será de até **10 (dez) dias úteis**, contados a partir do recebimento da Nota de Empenho e da Ordem de Início. O suporte técnico será prestado de forma contínua a partir da ativação dos produtos.

8.4. Local e horário para a entrega dos produtos ou para a execução do objeto: A entrega das licenças será feita em formato digital, com ativação remota nas instalações da Prefeitura de São Bernardo do Campo. O suporte técnico deverá estar disponível em regime ininterrupto (24x7), inclusive em finais de semana e feriados, conforme demanda.

8.5. Forma de execução do objeto:

A execução será indireta, mediante prestação remota de serviços especializados de suporte, incluindo atualização contínua, diagnóstico e resposta a incidentes, além da manutenção ativa das subscrições por meios digitais. A contratada deverá manter equipe técnica qualificada durante toda a vigência contratual.

8.6. Cronograma de realização dos serviços, incluídas todas as tarefas relevantes e seus respectivos prazos:

- Até 10 dias úteis após a Ordem de Início: entrega das licenças e ativação;
- A partir da ativação: início da prestação do suporte técnico 24x7;
- Mensalmente: relatórios de atualização e ocorrências relevantes;
- Durante toda a vigência: manutenção, atualização e suporte técnico ininterrupto.

8.7. Mecanismos para os casos em que houver a necessidade de materiais específicos, cuja previsibilidade não seja possível antes da contratação: Caso seja identificada a necessidade de recursos técnicos adicionais ou atualizações específicas não previstas inicialmente, a contratada deverá notificar formalmente a Administração, apresentando justificativa técnica e cronograma de adequação, sujeito à aprovação do fiscal do contrato.

8.8. Previsão dos recursos necessários para execução do contrato: Serão exigidos da contratada: estrutura de atendimento remoto, acesso aos portais

dos fabricantes, equipe técnica certificada, documentação técnica atualizada, e disponibilidade de profissionais com conhecimento nas soluções Hillstone e Syhunt.

8.9. Procedimentos, metodologias e tecnologias a serem empregadas: Deverão ser empregadas metodologias ágeis de atendimento técnico, com uso de tecnologias homologadas pelos fabricantes das soluções contratadas, contemplando análise de logs, detecção de ameaças, correlação de eventos e auditoria técnica.

8.10. Deveres e disciplina exigidos da contratada e de seus empregados: A contratada deverá manter postura ética, sigilo sobre as informações acessadas, cumprimento de prazos, disponibilidade técnica, e colaboração integral com o gestor e o fiscal do contrato. Toda conduta incompatível com a boa execução será objeto de advertência ou sanção, conforme previsto contratualmente.

8.11. Prazos e condições para recebimento provisório e definitivo do objeto:

- **Recebimento provisório:** ocorrerá após a ativação funcional das licenças, com emissão de termo circunstanciado pelo fiscal.
- **Recebimento definitivo:** será formalizado até **90 (noventa) dias** após o provisório, mediante verificação da conformidade funcional dos sistemas e da entrega documental de suporte e ativação.

8.12. Condições e prazo para que a contratada substitua o objeto ou refaça o serviço rejeitado pela fiscalização:

A contratada deverá substituir, corrigir ou ajustar os serviços ou subscrições rejeitados em até **5 (cinco) dias úteis** a contar da notificação formal do fiscal do contrato.

8.13. Prazo de garantia ou de validade:

a) A contratada deverá assegurar a garantia legal do produto, prevista no Código de Defesa do Consumidor, com prazo mínimo de 90 (noventa) dias para produtos duráveis (Eletrodomésticos, Equipamentos eletrônicos, mobiliários etc.) ou 30 dias para produtos não duráveis (alimentos, materiais de limpeza, etc.), contados a partir do recebimento.

b) Caso o fabricante ofereça garantia contratual adicional, que pode ser de até 12 (doze) meses, esta deverá ser plenamente assegurada à Administração, observando-se os prazos e condições estabelecidos pelo fabricante. (condição que deve estar expressa na proposta comercial)

c) A Administração não exigirá garantia contratual adicional como condição obrigatória para a contratação, mas fará jus a eventual garantia comercial normalmente praticada no mercado.

d) Eventual substituição ou reparo se dará conforme previsto no item 8.14, respeitando os prazos da garantia legal e/ou contratual aplicável.

8.14. Condições e prazos para refazimento dos serviços ou para substituição de objeto, caso apresentem defeitos durante o prazo de garantia ou de validade;

Na hipótese de falhas, defeitos ou desconformidades na execução dos serviços ou no funcionamento das soluções contratadas durante o prazo de vigência ou garantia, a contratada deverá realizar o refazimento ou substituição do objeto defeituoso no prazo máximo de 5 (cinco) dias úteis, contados a partir da notificação formal do fiscal do contrato, sem ônus para a Administração.

Quanto ao recebimento do objeto:

- Provisório: será realizado pelo responsável pela fiscalização e acompanhamento contratual, mediante termo detalhado, quando verificado o cumprimento das exigências técnicas mínimas estabelecidas.
- Definitivo: será formalizado por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o pleno atendimento das exigências contratuais.

Nos termos da legislação aplicável, o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

O recebimento provisório ou definitivo não exclui a responsabilidade civil da contratada pela solidez, desempenho e segurança do serviço, nem afasta a responsabilidade ético-profissional pela execução perfeita do contrato, nos limites estabelecidos pela legislação vigente e pelas cláusulas contratuais firmadas.

9. PREVISÃO DE PENALIDADES POR DESCUMPRIMENTO CONTRATUAL

9.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

9.2. Der causa à inexecução parcial do contrato;

9.3. Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.4. Der causa à inexecução total do contrato;

9.5. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

9.6. Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

9.7. Praticar ato fraudulento na execução do contrato;

9.8. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

9.9. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.10. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

9.11. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

9.12. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos itens 9.3, 9.4 e 9.5, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

9.13. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos itens 9. itens 9.3, 9.4 e 9.5, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

9.14. Multa:

9.15. Moratória de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias ficando o Município autorizado a extinguir o contrato após este período;

9.16. Compensatória, para as infrações descritas nos itens 9.6 a 9.9, de 15% a 30% do valor do Contrato.

9.17. Compensatória, para a inexecução total do contrato prevista no item 9.4, de 15% a 30% do valor do Contrato.

9.18. Para infração descrita no item 9.3, a multa será de 15% a 30% do valor do Contrato.

9.19. Para infrações descritas no item 9.5, a multa será de 0,5% a 15% do valor do Contrato.

9.20. Para a infração descrita no item 9.2, a multa será de 0,5% a 15% do valor do Contrato, ressalvadas as seguintes infrações:

9.21. A aplicação das sanções previstas no Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Município (art. 156, §9º, da Lei nº 14.133, de 2021)

9.22. Todas as sanções previstas no Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

9.23. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

9.24. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Município ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada, se houver, ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

9.25. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.26. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

9.27. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) A natureza e a gravidade da infração cometida;

b) As peculiaridades do caso concreto;

c) As circunstâncias agravantes ou atenuantes;

d) Os danos que dela provierem para o Município;

e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.28. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

9.29. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos no Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021)

9.30. O Município deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

9.31. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

9.32. Os débitos do contratado para com o Município, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes do contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante.

10. PREVISÃO DE ADOÇÃO DE IMR, QUANDO EXIGÍVEL

Este Termo de Referência considera a avaliação quanto à necessidade de utilização de Instrumento de Medição de Resultados – IMR, conforme previsto nas diretrizes administrativas da Administração Pública Municipal.

No caso deste objeto, não foram identificadas características que justifiquem a adoção de IMR, tendo em vista que não há previsão de metas de desempenho mensuráveis, produtividade vinculada a indicadores específicos ou entrega de serviços com variação de volume, intensidade ou qualidade que demandem controle técnico apurado por indicadores formais.

O acompanhamento e a fiscalização do contrato se darão por meio das rotinas de verificação de conformidade técnica da execução, conforme previsto neste Termo de Referência, com base na documentação fornecida, prazos, qualidade e entrega dos serviços ou produtos contratados.

11. FORMA DE PAGAMENTO

O pagamento será efetuado conforme os trâmites administrativos usuais da Administração Pública Municipal de São Bernardo do Campo, mediante apresentação da nota fiscal/fatura devidamente atestada pelo fiscal do contrato, e após a verificação da conformidade da execução do objeto.

O pagamento dar-se-á em parcela única, após a completa ativação das subscrições contratadas, comprovação da disponibilidade plena das soluções Hillstone sBDS I2850 e Syhunt, início efetivo da prestação do suporte técnico remoto em regime 24x7, e emissão do termo de recebimento provisório pelo fiscal designado, observado o prazo máximo de 30 (trinta) dias contados da data do atesto.

A contratada deverá apresentar a documentação fiscal exigida, juntamente com os relatórios ou documentos comprobatórios da execução, conforme definido neste Termo de Referência, sob pena de suspensão do pagamento até a devida regularização.

O pagamento será efetuado por meio de ordem bancária, em conta corrente de titularidade exclusiva da contratada, previamente informada à Administração, sendo vedado qualquer pagamento em nome de terceiros.

Eventuais glosas, deduções ou retenções legais serão aplicadas diretamente no momento da liquidação, de acordo com a legislação vigente. O não cumprimento das obrigações contratuais poderá acarretar a suspensão do pagamento até que as irregularidades sejam sanadas, sem prejuízo da aplicação das sanções cabíveis.

12. CONDIÇÕES DE REAJUSTE

Em conformidade com o disposto no art. 67 do Decreto Municipal nº 22.260/2023 e no art. 25, §7º da Lei Federal nº 14.133/2021, o presente Termo de Referência prevê a

possibilidade de reajuste dos preços contratados, de forma a preservar o equilíbrio econômico-financeiro do contrato, independentemente de sua duração inicial.

12.1. Ultrapassados os 12 (doze) meses da data do orçamento estimado, mediante o requerimento expresso da contratada os preços poderão ser reajustados, obedecido o seguinte critério:

12.2. Fica eleito o ICTI (Índice de Custo da Tecnologia da Informação**)**, como índice geral de preços básicos a ser utilizado, como segue:

a) Na eleição do índice (observada a variação de 12 meses):

- Um mês de retroação da data base (mês do orçamento estimado);
- Um mês de retroação da incidência.

12.3. A incidência do reajuste contratual dar-se-á no 13º (décimo terceiro) mês, contado da data do orçamento estimado e assim sucessivamente.

12.4. O índice de reajuste adotado, nos termos do art. 24 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, é obrigatório nas contratações de serviços de Tecnologia da Informação em que haja previsão de reajuste de preços por aplicação de índice de correção monetária

12.5. Fica reservado ao Município o direito de efetuar pesquisa de mercado para fins de avaliação de preços.

12.6. Em decorrência da avaliação da pesquisa de mercado, o Município poderá deferir, deferir parcialmente ou indeferir o pleiteado, mediante ato devidamente fundamento.

12.7. O pagamento do reajuste apurado, somente será devido a partir da data do pedido protocolado pela Contratada no Departamento de Licitações e Materiais, sito a Avenida Kennedy, nº 1.100, neste Município.

13. GARANTIA CONTRATUAL

Considerando a natureza do objeto contratado, que compreende o fornecimento de subscrições de software e serviços de suporte técnico remoto, sem entrega de bens permanentes, mobilização de recursos físicos relevantes ou riscos financeiros expressivos à Administração, não será exigida garantia contratual para a formalização do ajuste.

A dispensa da exigência de garantia está amparada no art. 96 da Lei Federal nº 14.133/2021, e fundamenta-se na análise técnica da complexidade, dos riscos envolvidos na execução do contrato e na habitualidade da prestação deste tipo de serviço, que não justifica a imobilização de recursos financeiros da contratada a título de caução, seguro ou fiança.

Caso, durante a execução do contrato, surjam elementos que justifiquem a exigência superveniente de garantias (ex: falhas reiteradas na execução, risco de descontinuidade ou inadimplemento), a Administração poderá, mediante justificativa técnica e autorização da autoridade competente, revisar esta condição, respeitados os limites legais e o direito ao contraditório.

14. ESPECIFICAÇÕES TÉCNICAS DOS ITENS A SEREM CONTRATADOS

ESPECIFICAÇÕES – SERVIÇOS DE SUPORTE TÉCNICO REMOTO 24X7

CARACTERÍSTICAS GERAIS

a) Os serviços de suporte técnico remoto às soluções deverão ser fornecidos por empresa autorizada pelo fabricante da solução, comprovando-se a autorização através de documento oficial do fabricante, e deverão estar disponíveis para abertura de chamados técnicos por parte da Prefeitura 24 horas por dia, sete dias por semana, inclusive feriados.

b) O início do atendimento deverá se dar em até 4 (quatro) horas após a abertura do chamado através de telefone, site ou e-mail da contratada.

c) Os serviços de suporte técnico remoto devem contemplar suporte e correção de defeitos de hardware, bugs de software, problemas relacionados à operação do dispositivo, problemas de configuração do dispositivo e ações de troubleshooting e correção.

d) Os serviços deverão ser fornecidos por empresa autorizada e certificada pelo fabricante da solução, comprovando-se a certificação e autorização através de documento oficial do fabricante.

e) Caberá à equipe de atendimento técnico da contratada o acionamento para o reparo ou substituição sem custo dos equipamentos cobertos por este contrato e que estejam danificados, exceto para os casos de defeitos causados por negligência, uso indevido, reparo ou manutenção realizados por terceiros que não a contratada, modificação não autorizada, tensão ou interferência física ou elétrica extrema, flutuações ou picos de energia elétrica, relâmpagos, eletricidade estática, incêndios, eventos de força maior ou outras causas externas

ESPECIFICAÇÕES – SOLUÇÃO DE DETECÇÃO DE BRECHAS DE SEGURANÇA E PROTEÇÃO A SERVIDORES:

CARACTERÍSTICAS GERAIS

- Deverão ser fornecidas subscrições de serviços para o equipamento Hillstone Modelo sBDS I2850 de propriedade desta Prefeitura pelo período de 24 (vinte e quatro) meses.
- Os serviços deverão ser fornecidos por empresa autorizada e certificada pelo fabricante da solução (Hillstone), comprovando-se a certificação e autorização através de documento oficial do fabricante.
- A subscrição deverá ser ativada mantendo todas as regras e políticas atualmente instaladas.
- O dispositivo objeto desta nova subscrição deverá ter seu sistema atualizado para a última versão estável disponibilizada pelo fabricante, mantendo-se todas as suas configurações e regras instaladas.
- Os serviços de garantia incluídos na subscrição deverão contemplar o reparo ou substituição sem custo dos equipamentos danificados, exceto para os casos de defeitos causados por negligência, uso indevido, reparo ou manutenção realizados por terceiros que não a contratada, modificação não autorizada, tensão ou interferência física ou elétrica extrema, flutuações ou picos de energia elétrica, relâmpagos, eletricidade estática, incêndios, eventos de força maior ou outras causas externas

SERVIÇOS DA SUBSCRIÇÃO

- SERVIÇOS DE REDE
- A solução proposta deve suportar operar em tapping mode
- Deve permitir a integração com a plataforma de firewall para bloqueio de ameaças
- Deve permitir a integração ao gerenciamento centralizado da solução de gerência

IDENTIFICAÇÃO DE APLICAÇÕES

- A solução deve suportar mais de 4.000 aplicações, incluindo IM, p2p, e-mail, transferência de arquivos, e-mail, jogos online, streaming de mídia, etc.
- A solução deve prover estatísticas multidimensionais de aplicação baseadas em zonas, interface, localização, usuário e endereço IP
- A solução deve identificar aplicações móveis Android e IOS

DETECÇÃO DE INVASÃO

- A solução deve dispor de no mínimo 8.000 assinaturas IPS

- A solução deve suportar detecção para SQL injection, injeção C&C e XSS, verificação de link externo, Referer checking e verificação de iframe
- A solução deve possuir recursos para detecção de ataques buffer overflow, SQL injection e Cross-site Scripting
- A solução deve suportar a detecção de anomalias de protocolo e rate based, com suporte a pelo menos 20 tipos de protocolos como HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS, etc.
- A solução deve dispor de opção de captura de pacotes
- A solução deve permitir assinaturas personalizadas, atualizações manuais, automáticas e push/pull, e possuir enciclopédia de ameaças integrada.
- A solução deve suportar configuração de perfis IPS pré-definidos

ANTIVÍRUS

- A solução deve suportar no mínimo 13 milhões de assinaturas de Antivírus, com atualizações manuais, automáticas e push/pull
- A solução deve suportar ação Antivírus baseado no fluxo, dispondo no mínimo dos seguintes protocolos: HTTP, SMTP, POP3, IMAP, FTP/SFTP.
- A solução deve suportar a detecção de vírus em arquivos comprimidos como:
- RAR
- ZIP
- GZIP
- BZIP2
- TAR
- A solução deve suportar detecção em arquivos comprimidos em várias camadas, suportando no mínimo 5 camadas de descompactação, e personalizar a ação para comportamentos de excesso
- A solução deve suportar arquivo comprimido criptografado

DETECÇÃO DE BOTNETS E C&C NA INTRANET

- A solução deve suportar a descoberta de bots de intranet e ser capaz prevenir novos ataques de ameaças avançadas através da comparação de informações obtidas com banco de dados próprio de endereços de C&C
- A solução deve suportar a atualização automática da biblioteca de assinaturas de defesa contra botnets C&C

- A solução deve suportar dois tipos de banco de dados de endereços C&C: banco de dados de endereços IP (excluindo endereços IPv6) e banco de dados de domínios.
- A solução deve suportar a detecção de IP e nome de domínio C&C em TCP, HTTP e tráfego DNS.

INTELIGÊNCIA CONTRA AMEAÇAS

- Dispor de atualização automática para o dispositivo, em tempo real, de informações sobre as ameaças a partir da nuvem
- Deve dispor de recurso para exibir as últimas informações de ameaças em janela popup
- Deve permitir registrar e verificar se uma ameaça correspondente à do registro em nuvem ocorreu na rede
- Deve fornecer informações detalhadas sobre ameaças e sugestões de remediação

SANDBOX

- A solução deve permitir a execução de possível aplicação maliciosa em ambiente virtual baseado em nuvem para identificar ameaças desconhecidas
- A solução deve executar o upload dos possíveis arquivos maliciosos para a sandbox em nuvem para análise
- A solução deve suportar o upload dos possíveis arquivos maliciosos a partir de protocolos, no mínimo, HTTP/HTTPS, POP3, IMAP4, SMTP e FTP
- A solução deve suportar avaliar pelo menos os seguintes tipos de arquivos:
- PE (Portable Executable)
- ZIP
- RAR
- Office
- PDF
- APK
- JAR
- SWF
- A solução deve fornecer um relatório completo de análise comportamental dos arquivos maliciosos detectados
- A solução deve pertencer a um grupo de compartilhamento global de informações sobre ameaças, para detectar novas ameaças desconhecidas

ANTISPAM

- A solução deve prover a classificação e detecção de Spam em tempo real
- A solução deve poder classificar como SPAM, BULK SPAM, SUSPECTED SPAM, VALID BULK
- A solução deve permitir a detecção independentemente do idioma, formato ou conteúdo da mensagem
- A solução deve suportar ambos os protocolos de e-mail SMTP e POP3
- A solução deve suportar White-lists para e-mails de domínios confiáveis

DETECÇÃO DE ATAQUES

- A solução deve permitir a detecção de ataques de anormalidade de protocolo (abnormal protocol)
- A solução deve permitir a detecção de ataques DoS/DDoS, incluindo pelo menos SYN Flood e DNS Query Flood.
- A solução deve permitir a defesa contra ataques ARP, incluindo a ARP bindig e ARP inspection.
- A solução deve suportar ARP Spoofing Inspection

RECURSOS INTELIGENTES DE SEGURANÇA

- A solução deve dispor de análises de correlação de ameaças, correlação entre ameaças desconhecidas, comportamento anormal e comportamento de aplicação para descobrir ameaças ou ataques potenciais
- A solução deve suportar regras analíticas de correlação de ameaças multidimensionais, com atualização diária automática a partir da nuvem
- A solução deve suportar a detecção de pelo menos 2000 famílias de malware conhecidas e desconhecidas, incluindo Vírus, Worm, Trojan, Overflow, etc.
- A solução deve prover detecção avançada de malware baseada no comportamento
- A solução deve prover a detecção dos principais malwares ransomware e criptomining
- A solução deve suportar modelagem de comportamento baseada no tráfego L3-L7 para revelar o comportamento anômalo da rede, como HTTP scanning, Spider, SPAM, senha fraca SSH/FTP para servidor e host.
- A solução deve detectar ataques DDoS incluindo:
- Flood
- Sockstress

- Zip of Death
- Reflect
- DNS query
- SSL DDos
- DDoS a aplicação
- A solução deve suportar a inspeção do tráfego em túneis criptografados para aplicações desconhecidas
- A solução deve suportar a atualização online e em tempo real do de banco de dados de comportamentos anormais
- A solução deve fornecer análise forense de ameaças, incluindo análise de ameaças, base de conhecimento, histórico e topologia de ameaças.
- A solução deve permitir ações administrativas para mudar o status de eventos de ameaça incluindo: Abertos, Falsos Positivos, Fixos, Ignorados, Confirmados.
- A solução deve suportar a limpeza com um clique das ameaças do servidor/computador e a reavaliação da segurança do host.
- A solução deve prover whitelist de eventos de ameaça, incluindo nome da ameaça, IP de origem/destino, contagem de acertos, etc.
- A solução deve suportar a captura de pacotes on-line.
- A solução deve suportar traps locais (honeypot) para traps de ataques de ameaças a rede e poder confirmar a fonte de ameaça, tipo de ameaça e incidência.
- A solução deve prover recurso local de deception com atualização regular dos modelos de deception.
- A solução deve suportar a detecção de deception comportamental para protocolos FTP, HTTP, MYSQL, SSH, TELNET, e simulação para Web, Doc ou Servidores de Banco de Dados.
- A solução deve apoiar o recurso de caça de ameaças para coletar provas abrangentes e fornecer uma análise aprofundada.
- A solução deve suportar recurso de rastreamento de ameaças (hunting) e integração ao serviço Sysmon do endpoint.
- Deve suportar a detecção de software de ransomware e mining.
- Adicionar IOCs (Indicator of Compromise) de eventos de ameaça para rastreamento de ameaças, tais como craking de força bruta da área de trabalho

remota, criação de arquivos suspeitos e processos powershell maliciosos, de modo a melhorar a capacidade de detecção da função de rastreamento de ameaças.

RESPOSTA A INCIDENTES

- A aplicação deve suportar a configuração de regras de alerta de ameaça, incluindo condições da ameaça e método de ação. Quando ocorre um evento de ameaça que atenda às condições de ameaça (como tipo de ameaça, gravidade, categoria de comportamento, nome da ameaça, etc.), o sistema deverá notificar o usuário a tempo em conformidade com o método de ação especificado na regra (como SMS ou e-mail) para que usuário possa realizar o processamento de ação subsequente ao evento de ameaça.

ADMINISTRAÇÃO

- A solução deve possuir interface de usuário Web integrada (WebUI) e Interface de Linha de Comando (CLI).
- A solução deve suportar acesso gerencial a partir de HTTP/HTTPS, SSH, telnet, console.
- A solução deve ser capaz de proteger o sistema contra ataques de força bruta a nome de usuário e senha.
- A solução deve suportar política de reforço de senha para contas administrativas.
- A solução deve suportar o monitoramento de hosts e servidores de rede interna, identificando nome, sistema operacional, navegador, tipo e registro estatístico de ameaças de rede.

MONITORAMENTO

- A solução deve permitir o monitoramento de tráfego total e de sessões.
- Deve possuir painel de controle dinâmico, com status em tempo real e widgets de monitoramento de drill-in.
- Deve prover projeção de monitoramento de risco na intranet.
- Deve oferecer uma visão geral do status de risco da rede interna, incluindo lista TOP 5 de servidores/computadores em risco, tendências de ameaças, status de risco de ativos críticos, status de risco do host, gravidade e tipo de ameaça, geolocalização de ataque externo, etc.
- Deve prover detalhes visuais do status de ameaça para ativos críticos e outros hosts em risco, incluindo nível de risco, certeza do risco, geolocalização do ataque, mapeamento da kill chain e outras informações estatísticas.

- Deve prover detalhes visuais de eventos de ameaças na rede, incluindo análise de ameaças.

ALERTAS, LOGS E RELATÓRIOS

- A solução deve prover alertas com base na largura de banda da aplicação e nova conexão.
- Deve prover pelo menos três tipos de alertas: Email, mensagem de texto e traps.
- A solução deve manter registros, incluindo registros de eventos, rede, ameaças, configuração e sessões.
- Deve suportar SYSLOG padrão e log de formato binário;
- Deve possuir suporte a armazenamento distribuído de log binário para vários servidores de log, e o algoritmo distribuído deve suportar Round Robin, SRC IP HASH.
- A solução deve suportar o registro na memória local ou nos servidores Syslog.
- Os logs podem ser exportados via Syslog ou Email.
- Deve permitir a criação de relatório definido pelo usuário.
- Deve suportar a emissão de relatório de ameaças por servidor/computador.
- Deve poder gerar arquivos de relatório em formato DOC e HTML, e deverão poder ser exportados em PDF via e-mail e FTP.
- Deve emitir pelo menos os relatórios pré-definidos:
- Tráfego de Rede e Aplicação.
- Top10 Endpoints e Servidores por rede.
- Relatório Global Rede e Risk Assessment.
- Top10 Endpoints e Servidores por Tráfego de Aplicação.
- Relatório de Ameaças de rede.
- Deve possuir funções de análise, recomendação e comparação de suporte além do tráfego, usuários, estatísticas de ameaças.

VISIBILIDADE DE RISCO E AMEAÇAS

- A solução deve prover a visibilidade de servidores em risco, hosts em risco, ameaças e exibição de mapa mundi assinalando origem de ataques externos.
- A solução deve prover a perspectiva de ameaças na Intranet para ameaças baseadas em servidores, destacar o nível de risco do servidor em diferentes cores, suportar filtragem condicional multidimensional.

- A solução deve prover a perspectiva de tráfego na Intranet para o tráfego baseado no servidor, monitorar o tráfego anormal via servidores, suportar a filtragem condicional multidimensional.
- A solução deve prover visibilidade de informações básicas dos servidores, tais como índice de risco, ameaças e tráfego.
- A solução deve apresentar o Top 5 de servidores em risco e a tendência de risco considerando o período de duas semanas.
- A solução deve apresentar o Top 10 de servidores em risco e por tráfego com interface espelho de perspectiva.
- A solução deve prover visibilidade das ameaças para os hosts em risco através de lista que inclua o host name, Sistema Operacional, browser e tipo de serviço para registrar as ameaças e o tráfego anormal do host.
- A solução deve prover visibilidade dos hosts baseada em informações sobre índice de risco, ameaças e tráfego anômalo.
- A solução deve prover visibilidade da ameaça, incluindo informações sobre o nome e tipo da ameaça, nível de risco, KB, pacote forense e suportar filtragem condicional multidimensional.
- A solução deve dar visibilidade à eventos de extração anômala de informações, comportamento anômalo e de ameaças.
- A solução deve prover estatísticas de classificação de todos IOCs de eventos de ameaça e a tendência de eventos de ameaça pelo período de duas semanas.
- Deve poder exibir o caminho do ataque.
- A solução deve suportar a Arbitragem de Ameaças por parte do administrador, contemplando as tags IGNORE,FALSE POSITIVE,CONFIRMED e FIXED para marcar o status de análise de ameaça.
- A solução deve permitir adicionar ameaça à whitelist para o processamento de assinaturas de detecção de ameaças, fornecer informações de nome, hitcount e status sobre a whitelist de ameaças.
- A solução deve permitir a conexão com solução de defesa de perímetro (NGFW) para gerar política de defesa através da mitigação de riscos.
- A solução deve suportar ação de limpeza de eventos de ameaça baseados em servidor/hospedeiro.

- Deve poder exibir tag de ameaça relacionada a servidores, endpoints e eventos de ameaça, como EternalBlue, Ransomware, Crypto Mining, Trojan, etc., facilitando aos usuários a compreensão do conteúdo profissional.

ESPECIFICAÇÕES – SOLUÇÃO DE ANÁLISES DINÂMICA E ESTÁTICA DE VULNERABILIDADES DE APLICAÇÕES WEB

CARACTERÍSTICAS GERAIS

- Deverá ser fornecida subscrição de serviço compatível com a licença Syhunt de propriedade desta Prefeitura pelo período de 24 (vinte e quatro) meses.
- Os serviços deverão ser fornecidos por empresa autorizada e certificada pelo fabricante da solução (Syhunt), comprovando-se a certificação e autorização através de documento oficial do fabricante.
- A subscrição deverá ser ativada mantendo todas configurações atualmente instaladas.
- O objeto desta nova subscrição deverá ter seus sistemas atualizados para a última versão estável disponibilizada pelo fabricante, mantendo-se todas as suas configurações e regras instaladas.

LICENCIAMENTO

- As licenças da solução de software devem ter prazo de validade de 24 (vinte e quatro) meses
- Devem incluir os direitos de atualização de versões e suporte técnico, além de prover documentação técnica em português e inglês nos formatos PDF e HTML.
- Devem permitir a adição de pacote de expansão de uso da solução, seja com base nas linguagens e plataformas alvo suportadas ou quantidade de módulos adicionais, de acordo com o modelo de negócios do fabricante.
- Devem permitir um número ilimitado de varreduras em um número ilimitado de URLs por ano, que deverão ser executadas a partir de um dispositivo.

ARQUITETURA DA SOLUÇÃO

- Deve ser composta por módulos de sistema de software, que se integrem em uma única console de gerenciamento que agregue as funções de administração das configurações da solução e de apresentação das análises.
- Deve possuir uma interface de linha de comando (CLI), monolítica ou modular, que permita a execução de varreduras dinâmicas e de código-fonte e outras tarefas.

- Deve ser capaz de realizar e combinar, no mínimo, os seguintes tipos de análise:
- SAST: Análise Estática da segurança do código-fonte de aplicações web;
- MAST: Análise Estática da segurança do código-fonte de aplicações móveis (Android e iOS);
- DAST: Análise Dinâmica da segurança de aplicações web com mapeamento profundo e injeção de dados;
- FAST: Análise Forense da segurança de aplicações a partir de arquivos de logs de servidor.
- Os módulos que realizam as análises de segurança devem ser do mesmo fabricante para garantir integração e compatibilidade entre os diferentes componentes.
- Deve ser on-premise, ou seja, a solução deve ser implantada nas dependências da CONTRATANTE, de forma que os códigos-fonte e resultados das análises não saiam de sua rede interna ou de redes sob seu controle.
- Deve possuir base de dados de vulnerabilidades interna, que deve contemplar ao menos os seguintes conjuntos de vulnerabilidades publicamente disponibilizados e regulações:
- CWE/SANS Top 25: versão 2019 ou mais atual;
- OWASP Top 10: versão 2017 ou mais atual;
- OWASP Mobile Top 10: versão 2016 ou mais atual;
- OWASP PHP Top 5;
- CWE/SANS Top 25 Most Dangerous Software Errors: versão 2019 ou mais atual;
- Common Weakness Enumeration (CWE);
- Common Vulnerabilities and Exposures (CVE);
- WASC (The Web Application Security Consortium) Threat Classification;
- WAVSEP (Web Application Vulnerability Scanner Evaluation Project);
- NIST SAMATE (Software Assurance Metrics And Tool Evaluation) Project;
- Payment Card Industry Data Security Standard (PCI DSS): versão 3.2, 3.2.1 ou mais atual.
- ISO/IEC 27001
- O banco de vulnerabilidades da ferramenta deve ser atualizado periodicamente no período contratado, garantindo que a solução esteja atualizada com as novas vulnerabilidades publicadas pelos bancos internacionais de vulnerabilidades, tais como OWASP e CWE.

- A solução deve ser capaz de analisar aplicações concebidas para as seguintes plataformas alvo:
- Android
- Apple iOS e MacOS
- BSD
- Linux
- Microsoft Windows
- Solaris
- Unix
- A solução deve ser capaz de identificar vulnerabilidades em aplicações que abranjam ao menos as seguintes linguagens, ambientes e frameworks:
- C# (ASP.Net);
- Java: JEE, JSP, Android e Spring Framework;
- JavaScript:
- No lado do cliente e lado do servidor;
- Node.js: barebone ou com frameworks tais como Express.js e Koa.js;
- Angular: versão 2 ou mais alta;
- AngularJS;
- JScript (ASP Clássico);
- ElectronJS (Desktop).
- Lua: ngx_lua, mod_lua, CGILua e Lua Pages;
- Objective-C, C e C++: iOS;
- Perl;
- PHP;
- Python: CGI, mod_python, PSP, WSGI e Django;
- Ruby: Rails, ERB e mod_ruby;
- Swift: iOS;
- TypeScript, a ser compilado para:
- JavaScript a ser executado no lado do cliente e lado do servidor;
- Node.js: barebone ou com frameworks tais como Express.js e Koa.js;
- Angular: versão 2 ou mais alta;
- AngularJS;

- VB: VB.Net (ASP.Net) e VBScript (ASP Clássico);
- HTML
- A solução deve incluir interface gráfica e linha de comandos documentada e com exemplos que possa ser instalada sobre a plataforma Microsoft Windows versão 7, 8 ou 10, ou Windows Server 2008 a 2019; e interface de linha de comandos documentada e com exemplos que possa ser instalada ao menos nas seguintes distribuições Linux:
- Ubuntu Server/Desktop 18.10 e posterior
- CentOS 7.7 e posterior
- Deve ser fornecida com todos os recursos necessários para integração com as ferramentas abaixo relacionadas:
- Sistemas de gerenciamento de tickets: possibilitar o acionamento de webservices via tecnologia REST para abertura de tickets em ferramentas de acompanhamento de casos tais como JIRA e GitHub;
- Lua APIs: Deve disponibilizar APIs Lua que possibilitem no mínimo estender o console de administração, iniciar varreduras, visualização dos resultados de varredura e geração de relatórios a partir de scripts;
- Web APIs: Deve disponibilizar APIs REST que possibilitem no mínimo iniciar varreduras e a visualização dos resultados de varredura. Admite-se o uso de servidores web open source tais como Apache ou Nginx em sua arquitetura. A solução deve prover documentação e exemplos de uso de API;
- Sistemas de gerenciamento de controle de processo de desenvolvimento: Deve possuir integração com pipeline para integração contínua via extensão ou agente com os seguintes sistemas:
- Jenkins
- GitLab: CI (Integração Contínua) e Dashboard de Segurança;
- Email: Deve permitir o envio dos resultados de varredura ou alertas de vulnerabilidade por email;
- Sistemas de controle de versão: acessar repositórios GIT públicos e privados, repositórios Azure GIT, GitHub e branches.
- Navegadores: Deve permitir realizar login manual em navegadores como Google Chrome e Mozilla Firefox através de extensão ou outro método que permita disparar uma análise que utilize a sessão em uso no navegador.

- Integração com Powershell documentada e com exemplos.
- Deve ser assíncrona, ou seja, a solução deverá trabalhar em várias análises simultaneamente, sem a necessidade de esperar a finalização de cada análise.
- Deve armazenar os resultados das varreduras realizadas ou em andamento.
- Deve ser multi-abas e multi-processo, ou seja, cada aba de navegação ou varredura é um processo diferente no sistema operacional.
- Deve ser capaz de realizar Análise Híbrida Aumentada que deve combinar as metodologias SAST, DAST e OAST:
- SAST-in-DAST: Realizar SAST de dentro do DAST para identificar vulnerabilidades no código-fonte JavaScript no lado do cliente ao longo de uma análise dinâmica.
- Hybrid Learning Mode (Modo de Aprendizagem Híbrida): Oferecer modo que permita usar detalhes assimilados durante análise de código de uma aplicação web para aprimorar sua análise dinâmica.

ANÁLISE DE CÓDIGO-FONTE

- Deve ser capaz de analisar o código fonte de aplicações em busca de vulnerabilidades de segurança, no mínimo, através das seguintes metodologias:
- SAST (Static Application Security Testing): Deve ser capaz de analisar o código fonte de aplicações web, incluindo web services;
- MAST (Mobile Application Security Testing): Deve ser capaz de analisar o código-fonte de aplicações móveis de Android e iOS
- Deve realizar a auditoria de segurança no código fonte dos projetos, e não em seus arquivos binários, podendo realizar descompilação (engenharia reversa) de arquivos APK de Android.
- Deve vir configurada com vulnerabilidades conhecidas de aplicações, no mínimo, nas seguintes linguagens de programação e ambientes:
- ASP.Net: C# e VB.Net;
- ASP Clássico: VBScript e JavaScript;
- Java: JEE, JSP, Android e Spring Framework;
- JavaScript: Client e Server-Side, Node.js, Angular, AngularJS, Express.js e Koa.js;
- Lua: ngx_lua, mod_lua, CGILua e Lua Pages;

- Perl;
- PHP;
- Python: CGI, mod_python, PSP, WSGI e Django;
- TypeScript: a ser compilado para JavaScript Client e Server-Side, Node.js, Angular, AngularJS, Express.js e Koa.js;
- Objective-C, C e C++ (iOS);
- Ruby: Rails, ERB e mod_ruby;
- Swift (iOS);
- HTML
- Deve ser capaz de identificar vulnerabilidades em aplicações desktop nas linguagens de programação e ambientes suportados pela solução, incluindo ElectronJS.
- Deve suportar códigos embutidos em HTML e formas abreviadas de print.
- Deve ser capaz de identificar vulnerabilidades no lado do cliente ou no lado do servidor (client-side e server-side).
- Deve ser capaz de identificar o uso de scripts vulneráveis desatualizados, locais ou remotos, tais como AngularJS, jQuery, fullPage, Bootstrap e momentjs.
- Deve ser capaz de realizar a análise de vulnerabilidades sobre códigos-fonte completos, trechos de código-fonte e arquivos de configuração.
- Deve suportar multi-auditoria de diversas linguagens de programação em um mesmo projeto.
- Deve ser capaz de identificar e navegar por áreas chave do código, tais como marcadores HTML específicos, JavaScript, requisições XHR, pontos de entrada e palavras-chave interessantes.
- Deve permitir a identificação de vulnerabilidades em códigos mal concebidos, ou seja, erros de programação que exponham o sistema a riscos de ataques baseados em fatos identificáveis
- Deve suportar integração com GIT para analisar códigos em repositórios versionados, incluindo Azure GIT Repos e branches.
- Deve identificar e exibir graficamente pontos no código-fonte onde é possível com apenas uma correção, resolver duas ou mais vulnerabilidades encontradas no código-fonte da aplicação.
- Deve ser capaz de realizar análise de segurança em web services.

- Deve permitir a visualização em tempo real do status das varreduras em execução, incluindo:
- Árvore de arquivos analisados e vulneráveis:
- Duração da varredura;
- Total de scripts analisados e vulneráveis;
- Total de vulnerabilidades encontradas e por nível de severidade;
- Total de linhas analisadas;
- Lista das vulnerabilidades encontradas.
- Deve ser capaz de analisar arquivos de configuração para avaliar ameaças de segurança e identificar contra-medidas apropriadas ainda no estágio da configuração do servidor, ambiente ou aplicação.
- Deve reconhecer casos de filtragem e validação de entrada de dados para aumento de precisão de análise.
- Deve ser capaz de realizar análise incremental, na qual os resultados e dados de varreduras anteriores executadas contra uma base de código específica são automaticamente armazenados e usados para acelerar varreduras futuras.
- Deve suportar TypeScript, permitindo que a ferramenta identifique vulnerabilidades no código antes de o código ser compilado para JavaScript (seja cliente ou servidor, Node.js ou Angular).
- Deve ser capaz de identificar em aplicações móveis os seguintes riscos que fazem parte do documento Mobile Top 10 elaborado pelo projeto de código aberto OWASP (Open Web Application Security Project):
- Uso Inadequado da Plataforma;
- Armazenamento Inseguro de Dados;
- Comunicação Insegura;
- Autenticação Insegura;
- Criptografia Insuficiente;
- Autorização Insegura;
- Qualidade do Código do Cliente;
- Adulteração de Código;
- Engenharia Reversa;
- Funcionalidade Estranha.

ANÁLISE DINÂMICA

- Deve detectar vulnerabilidades de segurança em aplicações web dinâmicas e servidores web, no mínimo, através das seguintes metodologias:
- DAST (Dynamic Application Security Testing) convencional;
- DAST Aumentado (Augmented Dynamic Application Security Testing): Deve combinar as metodologias DAST e OAST em uma mesma análise;
- HAST Aumentado (Augmented Hybrid Application Security Testing): Deve combinar as metodologias DAST, OAST e SAST em uma mesma análise.
- Deve vir configurada com vulnerabilidades conhecidas de aplicações web, no mínimo, nas seguintes linguagens de programação e ambientes:
- ASP.Net: C# e VB.Net;
- ASP Clássico: VBScript e JavaScript;
- Java: JEE e JSP;
- JavaScript: Client e Server-Side, Node.js, Angular, AngularJS, Express.js e Koa.js;
- Lua: ngxlua, mod_lua, CGILua e Lua Pages;
- Perl;
- PHP;
- Python;
- Ruby.
- Deve ser capaz de mapear a estrutura, incluindo todos os links e pontos de entrada de dados da aplicação alvo, no mínimo através das seguintes técnicas:
- Análise de código HTML;
- Reconhecimento e preenchimento automático de formulários;
- Seguimento de redirecionamentos;
- Análise e execução de código JavaScript e chamadas XHR;
- Análise do arquivo robots.txt de um website, se houver.
- Deve ser capaz de realizar injeções de dados e manipular parâmetros na aplicação alvo em URLs e formulários (GET e POST).
- Deve ser capaz de realizar mutações na injeção de dados em aplicações, de modo a abranger todas as linguagens de programação e plataformas alvo suportadas pela solução.
- Deve ser capaz de identificar vulnerabilidades no lado do cliente ou no lado do servidor (client-side e server-side).

- Deve ser capaz de identificar vulnerabilidades como injeção de SQL, injeção de NoSQL, injeção de comando, exposição e injeção de código, e outras vulnerabilidades, no mínimo através das seguintes técnicas:
- Dentro da banda (in-band): através de análise do tempo de resposta (inferencial), mensagem de erro e print de mensagem em todas as linguagens de programação suportadas pela solução;
- Fora da banda (out-of-band): através de metodologia OAST (Out-of-band Application Security Testing);
- Análise Passiva;
- Deve ser capaz de identificar os seguintes tipos de software desatualizado e vulnerável:
- Aplicações conhecidas vulneráveis em todas as linguagens de programação suportadas pela solução, incluindo ColdFusion, Flash, Server Side Includes (SSI)
- Uso de JavaScript desatualizados e vulneráveis
- Uso de software de servidor e outros componentes que possam estar desatualizados e vulneráveis.
- A solução deve ser capaz de imitar um navegador moderno, incluindo;
- Suporte ao HTML 5 e CSS 3;
- Análise inteligente de HTML capaz de lidar com HTML deformado;
- Emulação de JavaScript: capacidade de se comportar no mínimo como Google Chrome, Mozilla Firefox ou Microsoft Edge, com suporte para requisições XHR e arquivos JS externos;
- Simulação de interação do usuário: pressionar de teclas e cliques com mouse;
- Gerenciamento de cookies e sessões na aplicação web;
- Suporte de redirecionamento HTTP, Meta refresh e através de JavaScript;
- Preenchimento automático de formulários e login;
- Isolamento de processos e varredura multi-processo: cada aba de navegação ou varredura é um processo diferente no sistema operacional;
- Suporte aos protocolos HTTP 1.0 e 1.1;
- Suporte aos protocolos SSL 2/SSL 3/TLS 1;
- Suporte ao método Keep-Alive;
- Suporte a compressão GZIP;
- Suporte a caminhos relativos;

- Envio de Referer;
- Envio de User Agent personalizado.
- Deve ser capaz de realizar ataques de força-bruta estrutural e de autenticação: HTTP e em formulários de login de maneira automática
- Deve ser otimizado para testar aplicações rodando nos seguintes servidores HTTP:
- Apache
- Apache Tomcat
- Microsoft IIS
- Nginx
- Deve permitir a criação de perfis de varreduras para Ativos, que especifiquem:
- Tecnologias usadas pela aplicação, de modo otimizar o tempo de varredura, tais como a linguagem no servidor, o servidor web, o sistema operacional e banco de dados da aplicação alvo;
- Caminhos de Início;
- Certificados SSL;
- Credenciais para autenticação permitindo realizar a análise logado no sistema alvo, no mínimo, nos métodos Básico e formulário web;
- Exclusão de Objetos da varredura, tais como caminhos, formulários e vulnerabilidades específicas;
- Limitação de profundidade e camada.
- Assinaturas para detecção de páginas de erro 404 personalizadas;
- Configuração manual de cookies e token de sessão.
- Deve possuir capacidade de varredura invasiva e não invasiva.
- Deve permitir desligar testes de negação de serviço (DoS) que possam afetar a disponibilidade da aplicação web.
- Deve permitir configurar número de tentativas e o tempo de timeout de acesso ao servidor web,
- Deve permitir configuração de proxy nos protocolos HTTP, Socks 4 e 5.
- Deve permitir analisar URL contendo endereço IPv6.
- Deve suportar sistemas de gerenciamento de conteúdo, tais como Drupal, Joomla, WII e WordPress.
- Deve realizar análise em páginas SPAs (Single Page Applications).

- Deve identificar as tecnologias usadas na aplicação e otimizar o tempo de varredura com base nas tecnologias detectadas, sendo capaz de identificar versões ocultadas de software de servidor e componentes, como o Apache, Nginx, PHP, mod_ssl, OpenSSL e Phusion Passenger através de técnicas de reconhecimento (fingerprinting).
- Deve ser capaz de lidar de forma inteligente com websites grandes e complexos com geração de conteúdo dinâmico
- Deve incluir mecanismos para prevenir situações de loop durante o mapeamento da aplicação.
- Deve permitir limitar a profundidade de varreduras, incluindo:
- Número máximo de links por servidor
- Número máximo de links por página
- Tamanho máximo de URL em bytes
- Tamanho máximo de resposta HTTP em kilobytes
- Deve permitir a visualização em tempo real do status das varreduras em execução, incluindo:
- Árvore de caminhos encontrados e vulneráveis;
- Duração da varredura;
- Total de URLs vulneráveis;
- Total de URLs usando POST, autenticação e JavaScript;
- Total de pontos de entrada;
- Total de timeouts;
- Total de vulnerabilidades encontradas e por nível de severidade;
- Total de verificações de segurança realizadas;
- Tecnologias web detectadas;
- Tipo do sistema operacional do alvo;
- Linguagens de programação do alvo;
- Profundidade Atingida;
- Lista das vulnerabilidades encontradas.
- Deve possuir navegador moderno próprio com funcionalidades para testes manuais e apoio para testes automatizados, tais como:
- Login manual em aplicações web;
- Captura de URLs em navegação manual;

- Cabeçalhos HTTP em tempo real e capacidade de visualização para os formatos mais comuns de arquivos da web, tais como CSS, Flash, HTML, formatos comuns de imagens (bmp, gif, ico, jpg, png e svg), JavaScript, JSON, texto e XML;
- Desofuscação automática de JavaScript.
- Extensões para análise de vulnerabilidades, tais como fuzzer, executor de script, editores HTTP e XHR, carregador de requisição e capacidade de replay de requisição.
- Deve ser capaz de identificar vulnerabilidades do tipo out-of-band em aplicações web dinâmicas:
- Deve se integrar com serviço online na Internet fornecido pelo fabricante que ouve requisições forçadas provenientes de um servidor web vulnerável alvo ao longo de uma análise e sinaliza de volta para a ferramenta;
- Deve permitir que a ferramenta identifique variantes invisíveis de vulnerabilidades de alto risco conhecidas como out-of-band (OOB) dos seguintes tipos:
- Execução de Comandos
- Inclusão de Arquivo Remoto (RFI)
- Falsificação de Requisição do Lado do Servidor (SSRF)
- Injeção de SQL
- Injeção de Entidade Externa XML (XXE)
- Deve correlacionar de maneira automática os alertas recebidos com requisições de ataque previamente executadas, dispensando etapas manuais extras;
- Deve adicionar vulnerabilidades identificadas para o relatório e interface do usuário;
- Deve extrair automaticamente dados de um alvo vulnerável, adicionando tais dados para os resultados da análise;
- Deve recorrer a diferentes comandos e técnicas específicas para ambientes e sistemas operacionais diversos.
- Deve ser capaz de realizar análise incremental, na qual resultados e dados de varreduras anteriores executadas contra um URL alvo específico são automaticamente armazenados e usados para acelerar varreduras futuras.

CONSOLE DE GERENCIAMENTO

- A solução não deve requerer conhecimento prévio de segurança da informação e programação segura para uso da solução.
- Deve necessitar de pouca ou nenhuma intervenção por parte do usuário antes e durante o andamento de varreduras.
- Deve prover uma visão gráfica que indique o progresso da análise e o nível de risco da análise realizada.
- Deve exibir informações de licença do software, apresentando no mínimo o tipo de licença, a data de expiração da licença e linguagens de programação suportadas.
- Deve permitir ao usuário desabilitar Regras de análise e identificar quais Regras de detecção de vulnerabilidades foram desabilitadas.
- Deve permitir a alteração de estado, de severidade, e inserção de comentários nas vulnerabilidades encontradas.
- Deve permitir que o usuário configure para ignorar vulnerabilidades específicas ou múltiplas.
- Deve permitir o agendamento de varreduras com agendador próprio e os seguintes campos e opções:
- Horário, data ou dia da semana;
- Tipo do scan: dinâmico ou código;
- Alvo de varredura;
- Geração de relatório com escolha de modelo de relatório;
- Envio de relatório por email após o término da análise;
- Possibilidade de executar varredura de maneira oculta (sem janela);
- Possibilidade de exportar linha de comando para ser usada em agendadores de terceiros ou outras ferramentas;
- Deve permitir a pausa, retomada e cancelamento imediato de varredura.
- Deve permitir identificar, remover, exportar e importar os resultados de varreduras realizadas.
- Deve permitir cadastrar e gerir Ativos.
- Deve permitir exportar e importar listas de alvos de arquivos no formato CSV ou lista.
- Deve permitir exportar e importar a configuração atual da ferramenta de arquivos.

- Deve permitir a visualização em tempo real da lista das vulnerabilidades encontradas.
- Deve permitir a edição e visualização de um alerta de vulnerabilidade. Tais alertas devem conter as seguintes informações:
- Nome da vulnerabilidade;
- Descrição da vulnerabilidade;
- Localidade da vulnerabilidade, que pode ser um URL ou arquivo.
- Código de referência de bases de vulnerabilidades conhecidas, tais como CVE, CWE, NVD, OSVDB, se houver;
- Pontuação CVSS: versão 2 ou 3;
- Nível de severidade (Alta, Baixa, Média ou Informacional);
- Guia de remediação;
- Os parâmetros e variáveis afetadas;
- O número das linhas afetadas;
- Assinatura correspondente, quando houver;
- Trecho do código-fonte vulnerável, quando aplicável
- Exemplos de código de remediação, quando aplicável;
- Requisição, Cabeçalhos e Resposta HTTP, no caso de análise dinâmica;
- Dados extraídos, se houver;
- Anotações do usuário;
- ID único para a verificação;
- ID de rastreamento - um ID único de vulnerabilidade por varredura executada pela ferramenta.
- Deve fornecer realce de sintaxe para as linguagens de programação suportadas pela solução.
- Deve possuir um bloco de notas próprio de apoio para testes manuais, incluindo coleção de geradores de strings comuns de injeção, geradores de hash, codificadores e decodificadores, funções de HTML e manipulação de texto.
- Deve prover kit de desenvolvimento de extensões em inglês ou português, para permitir a adição de novos recursos no console.

FUNCIONALIDADES TÉCNICAS DE ANÁLISE

- Deve permitir a identificação dos seguintes tipos de vulnerabilidade e exposições em aplicações web, bem como em aplicações móveis sempre que aplicável:

- Abuso & Uso Indevido de API;
- Aleatoriedade Insegura;
- Algoritmos Criptográficos e de Hash Inseguros;
- Armazenamento Inseguro de Dados: casos de proteção de dados ausentes ou insuficientes;
- Autenticação Quebrada;
- Backdoor Baseada na Web;
- Arquivos e Pastas Comuns de Backup e Backup com Extensão Comum ou Dupla;
- Cabeçalhos de Segurança HTTP Ausentes ou Fracos;
- Comentários Suspeitos em Código-Fonte e HTML;
- Comunicação Insegura;
- Configuração Incorreta de Segurança;
- Conteúdo Inapropriado ou Malicioso;
- Conteúdo Padrão;
- Criptografia Quebrada;
- Cross-Site Scripting (XSS), incluindo XSS baseado em DOM, específico para HTML5, Filtro Fraco de XSS e Cross Frame Scripting (XFS);
- Directory Traversal;
- Estouro de Buffer;
- Execução de Comando;
- Exposição de Caminho, Código-Fonte, Banco de Dados, Senha, Endereço IP Interno, Tecnologia Web e outros;
- Falsificação de Registro (Log), Solicitação Entre Sites e Solicitação do Lado do Servidor (SSRF);
- Fraquezas Comuns em Formulários, incluindo sequestro de formulário de email, campo de preço oculto, preenchimento automático ativado e transação de cartão de crédito não criptografada;
- Hashing Fraco de Senha;
- Inclusão de Arquivo Local ou Remoto;
- Injeção de cabeçalho HTTP, Divisão de resposta HTTP;
- Injeção de Código, EL (Expression Language) e Expressão Regular;
- Injeção de JSON, XML, XPath e XXE (XML External Entity);
- Injeção de LDAP;

- Injeção de NoSQL, SQL e HQL;
- Injeção de SSI (Server-Side Includes);
- Informações Confidenciais Codificadas ou Registradas;
- Informações Sensíveis do Lado do Cliente
- Listagem de Diretório
- Login Não Criptografado
- Manipulação Arbitrária de Arquivos;
- Manipulação de Cookies;
- Más Práticas
- Métodos Perigosos;
- Negação-de-Serviço (DoS), no lado do cliente e servidor;
- Pontos de Entrada de Depuração, incluindo Parâmetros de Depuração Ocultos;
- Protocolos Fracos;
- Redirecionamentos Não Validados
- Salting Inseguro;
- String de Formato Não Controlada;
- Uso de Armazenamento Local, bem como dados confidenciais guardados no armazenamento local;
- Vazamento de Informações.
- A solução deve ser capaz de identificar vulnerabilidades de injeção de SQL e NoSQL, através de análise dinâmica e de código-fonte, que abranjam ao menos os seguintes bancos de dados:
- Firebird/InterBase
- IBM DB2
- Informix
- MariaDB / MySQL
- Microsoft Access
- Microsoft SQL Server
- MongoDB
- Oracle
- PostgreSQL
- SQLite

- Sybase
- Deve ser capaz de realizar varreduras com os seguintes métodos pré-definidos:
- Scan de Aplicação (Dinâmico): mapeia a estrutura de um website e realiza Análise Passiva e Ataques Ativos;
- Scan de Código de Aplicação: focado em todos os tipos de vulnerabilidades no código-fonte;
- Apenas Mapeamento: apenas mapeia a estrutura de um site sem realização de Análise Passiva ou ataques;
- Scan Passivo: apenas map
- eia a estrutura de um site com realização de Análise Passiva e sem ataques;
- Métodos baseados em documentos abertos:
- Top 10 OWASP: baseado no OWASP Top 10 de Riscos à Segurança de Aplicações Web
- Top 25 CWE: Baseado no CWE Top 25, os Erros Mais Perigosos de Software
- Top 5 PHP: baseado no OWASP PHP Top 5, porém não apenas limitado ao PHP;
- Injeção de Falhas: focado em falhas de injeção de dados, tais como XSS, Injeção de SQL, Inclusão de Arquivos e Execução de Comandos;
- Força-Bruta de Estrutura: focado em descobrir arquivos comuns de backup, páginas administrativas e exposições similares;
- Arquivos de Backup: focado em arquivos de backup, ocultos e obsoletos, mas não tão agressivamente quanto o método Força-Bruta de Estrutura.
- Teste Completo de Penetração: realiza todos os testes dinâmicos da maneira extensa e demorada;
- SQL Injection: focado em vulnerabilidades de Injeção de SQL e NoSQL;
- XSS: focado em vulnerabilidades de Cross-Site Scripting (XSS) e evasão de filtros anti-XSS;
- Inclusão de Arquivos: focado em vulnerabilidades de inclusão de arquivo local ou remoto;
- Conteúdo Malicioso: focado em malware, backdoors, pontos de entrada ocultos e sinais de invasão;
- Redirecionamentos Não Validados: focado em vulnerabilidades em redirecionamentos.

- Scan de Aplicação Focado no Lado Servidor: focado apenas em vulnerabilidades no lado do servidor através de análise dinâmica ou de código-fonte.
- Deve ser capaz de confirmar se ocorreu a violação da segurança de uma aplicação a partir de vestígio
- Deve permitir a comparação entre duas varreduras executadas sobre o mesmo alvo ou código-fonte, apresentando as diferenças através de relatório e do console de gerenciamento que deve indicar claramente as diferenças com tabelas: vulnerabilidades novas, inalteradas ou removidas.
- Deve apresentar o resultado das análises e emitir relatórios em português ou inglês.
- Deve permitir o envio automático dos resultados das análises para um endereço de e-mail selecionado.
- Deve ser capaz de produzir alertas para cada tipo de vulnerabilidade única que for identificada.
- Deve possuir conformidade com o padrão CVSS (Common Vulnerability Scoring System) versão 2.0 e 3.0, para comunicar a gravidade de uma vulnerabilidade e ajudar a determinar a urgência e prioridade da resposta de segurança, incluindo os seguintes cálculos:
- Pontuação Base
- Pontuação de Impacto
- Pontuação de Exploração
- Pontuação Temporal
- A solução deve ser capaz de gerar relatórios sobre as vulnerabilidades encontradas:
- Deve gerar relatórios em formatos distintos, incluindo ao menos os formatos: PDF e HTML (para leitura por usuários) e XML e CSV (para processamento por outras ferramentas).
- Deve ordenar as vulnerabilidades com base na pontuação de CVSS3 ou CVSS2 (indo de 0.0 Nenhuma a 10.0 Crítica).
- Deve oferecer a possibilidade de ordenar as vulnerabilidades com base em quatro etapas de severidade (alta, baixa, média ou informacional).
- Deve oferecer a possibilidade de geração de relatório nos seguintes modelos:
- Padrão: relatório gerencial padrão;

- Comparação: incluindo a comparação de resultados de uma análise com análises anteriores, indicando claramente as diferenças com gráficos de tendências e tabelas;
- Conformidade: relatório de aprovação / reprovação com itens do OWASP Top 10, CWE/SANS Top 25 Most Dangerous Software Errors, ISO/IEC 27001 e PCI DSS em suas versões mais atuais;
- Conformidade (Móvel): relatório de aprovação / reprovação com itens do OWASP Mobile Top 10, CWE/SANS Top 25 Most Dangerous Software Errors, ISO/IEC 27001 e PCI DSS em suas versões mais atuais;
- Completo: incluindo a comparação de resultados, conformidade e todas as informações técnicas.
- Os relatórios gerados pela solução devem apresentar as seguintes informações:
- Detalhes gerais da varredura: data de início, alvo, status da varredura, duração e método de varredura utilizado;
- Gráficos e Estatísticas: total consolidado de vulnerabilidades e por nível de severidade, incluindo gráficos;
- Detalhes das vulnerabilidades: todos os detalhes sobre cada alerta de vulnerabilidade, como exibido pelo console de gerenciamento;
- Detalhes de Cobertura: estrutura mapeada, lista de formulários, emails, arquivos JavaScript e outros recursos encontrados, bem como tecnologias e plataformas detectadas durante a análise;
- Versão e descrição breve da licença de uso da solução.
- Deve ser capaz de realizar, sob demanda, análise heurística de segurança de arquivos de log de servidores web para detectar ataques, incluindo:
- Identificação da origem (endereço IP), o país, o tipo e os métodos usados para tentar comprometer aplicações web;
- Reconstrução da sessão de ataque, diferenciando de maneira precisa tráfego legitimo de tráfego malicioso, além de diferenciar ataques automatizados de ataques manuais;
- Detecção de ocorrência de invasão, com instalação de backdoor;
- Detecção de ferramentas de invasão usadas;
- Detecção de ataques para explorar vulnerabilidades do OWASP Top 10;

- Suporte aos arquivos de log gerados, no mínimo, pelos seguintes servidores web: Apache, Microsoft IIS e Nginx, com detecção automática do formato;
- Detecção de uso de técnicas de evasão de sistemas de defesas.

15. QUANTIDADE DOS ITENS A SEREM CONTRATADOS

Item	Produto/Serviço	Qtd.
1	Subscrição da solução de detecção de brechas na intranet (Hillstone sBDS I2850)	1
2	Subscrição da solução de análise de vulnerabilidades em aplicações web (Syhunt)	1
3	Serviço de suporte técnico remoto 24x7 para ambas as soluções	1

16. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE, QUANDO COUBER

Considerando que o objeto da contratação refere-se exclusivamente à subscrição de soluções tecnológicas e à prestação de serviços remotos de suporte técnico especializado, não se aplicam, neste caso, critérios ou práticas específicas de sustentabilidade ambiental ou socioeconômica, uma vez que não há fornecimento físico de bens, insumos materiais ou geração de resíduos.

A execução contratual se dará de forma totalmente digital e remota, não envolvendo atividades que demandem mitigação de impacto ambiental ou adoção de medidas compensatórias, razão pela qual não há exigência de requisitos adicionais de sustentabilidade nesta contratação.

SA-3, 05 de maio de 2025.

Paulo Henrique Correia de Souza

Departamento de Tecnologia da Informação