DOCUMENTO de OFICIALIZAÇÃO da DEMANDA

1 IDENTIFICAÇÃO DA DEMANDA

1.1 Título:

Aquisição de ferramenta de detecção de vulnerabilidades.

1.2 Unidade Demandante:

SENIC/COINF/STIC

1.3 Responsável pela Unidade Demandante:

Nome:	MARIA DAS GRAÇAS OLIVEIRA MAGALHÃES HENRIQUES
Matrícula:	308
Telefone:	(81) 3194-9414
E-mail:	graca.magalhaes@tre-pe.jus.br

2 CONTEXTO DE NEGÓCIO

2.1 Situação Atual:

Visando atender às solicitações contidas no plano de ação referente à resolução n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, bem como o contido no plano de segurança cibernética encaminhado pelo TSE aos regionais, quanto a detecção de vulnerabilidades e tratamento de vulnerabilidades, torna-se necessária a aquisição de ferramenta de detecção para que a equipe técnica possa realizar varreduras na rede local em busca de ativos desatualizados ou vulneráveis para que sejam tratadas as descobertas.

A ferramenta deve ser capaz de realizar a avaliação do ambiente, a priorização preditiva - que é a priorização das vulnerabilidades a serem tratadas, o monitoramento dos ativos da organização quanto às vulnerabilidades divulgadas por seus fabricantes, bem como a descoberta constantes de novos ativos existentes na rede de dados. Com a ferramenta poderemos realizar uma detecção mais rápida de vulnerabilidades que possam ser exploradas bem como apontar esforços para a sua correção.

Inicialmente, utilizaremos para a contratação o valor referencial de 1.500 dispositivos existentes no órgão, além de serviços de implantação e suporte.

2.2 Descrição da Oportunidade ou do Problema:

a) Detecção e priorização de vulnerabilidades encontradas nos ativos de rede;

b) Detecção de ativos estranhos à organização por meio de varreduras automáticas.

2.3 Motivação da Demanda:

1. Atender aos novos requisitos da ENSEC-JUD quais sejam:

"3.1 Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior para identificar todas as vulnerabilidades potenciais nos sistemas da organização.
3.3 Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos."

2. Atender às solicitações contidas no plano de ação referente à resolução n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, quanto a detecção de vulnerabilidades e tratamento de vulnerabilidades.

3. Atender ao contido no plano de segurança cibernética criado pelo TSE e encaminhado aos Regionais.

4. Atender ao contido na IN 61/2021 - gestão de vulnerabilidades de ativos do TRE-PE.

2.4 Resultados Pretendidos:

1. Atendimento aos requisitos de segurança contidos da ENSEC-JUD, aos demais planos de ação para protocolo de investigação para ilícitos cibernéticos e segurança cibernética quanto à detecção e tratamento de vulnerabilidades;

2. Atendimento ao contido na IN 61/2021 - gestão de vulnerabilidades de ativos do TRE-PE.

2.5 Alinhamento Estratégico:

Esta aquisição está alinhada com:

Objetivo Estratégico 11 do PEI 2021-2026 (Aperfeiçoar, ampliar e consolidar a utilização de práticas de governança e gestão de tecnologia da informação e comunicação, com vistas a otimizar o suporte tecnológico aos diversos processos finalísticos e de apoio do TRE-PE);

Objetivo Estratégico 08 do PDTIC 2021-2022 (Promover Serviços de Infraestrutura e Soluções Corporativas);

Foi solicitada a sua inclusão no Plano de Contratações 2022, por meio do SEI nº 0025048-05.2021.6.17.8000.

3 CONTEXTO DA DEMANDA

3.1 Ciclo de Vida da Demanda

3.1.1 Qual a expectativa de tempo de utilização ou validade da solução objeto da demanda?

[ ] Menos de 1 ano [X] De 1 a 3 anos [ ] Mais de 3 anos

3.1.2 Trata-se de uma demanda com caráter definitivo ou temporário? Há algum fato já conhecido que poderá implicar a descontinuidade da demanda ou a sua substituição?

Definitivo, dentro do tempo de utilização da demanda.

3.2 Clientes que farão uso da solução (objeto da demanda) ou serão beneficiados.

SENIC/COINF/STIC

3.2.1 Demanda de âmbito Interno ao TRE:

[x] Até 1 Unidade [ ] 2 ou 3 Unidades [ ] 4 ou mais Unidades do TRE

3.2.2 Demanda de âmbito Externo ao TRE:

[ ] Até 1 órgão [ ] 2 ou 3 órgãos [ ] 4 ou mais órgãos [x] não se aplica

3.3 Expectativa de entrega da solução.

Expectativa de entrega até julho/2022.

3.4 Integrante Demandante:

Nome:	MARIA DAS GRAÇAS OLIVEIRA MAGALHÃES HENRIQUES
Matrícula:	308
Telefone:	(81) 3194-9414
E-mail:	graca.magalhaes@tre-pe.jus.br

Indico como **Integrante Técnico**:

Nome:	Alexandre Luiz Azevedo de Oliveira
Matrícula:	1224
Telefone:	(81)3194-9415
E-mail:	alexandre.oliveira@tre-pe.jus.br

4 ANEXOS

5 AUTORIZAÇÃO

De acordo, encaminhe-se à Diretoria Geral.

Em: 04/01/2022.

Devem assinar este documento o responsável pela área demandante, sua chefia imediata e o titular da unidade.

Documento assinado eletronicamente por **ALEXANDRE LUIZ AZEVEDO DE OLIVEIRA**, **Chefe de Seção em Exercício**, em 27/01/2022, às 13:03, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANDRÉ RICARDO NEVES DE MORAES**, **Coordenador(a) em Exercício**, em 27/01/2022, às 13:24, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MLEXENER BEZERRA ROMEIRO**, **Secretário(a) em Exercício**, em 27/01/2022, às 16:22, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

ESTUDOS PRELIMINARES

DESCRIÇÃO DO OBJETO CONTRATADO:

Aquisição de ferramenta de detecção e gerenciamento de vulnerabilidades.

1 ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (Res. TRE/PE nº 249/2016, Art.14)

Contextualização

O monitoramento das vulnerabilidades de segurança num ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações. Neste contexto, buscamos implementar uma solução de software capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento deste trabalho de identificação e mitigação de riscos.

Outro item que torna necessária a contratação é o atendimento às solicitações contidas no plano de ação referente à Resolução n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, bem como o contido no plano de segurança cibernética encaminhado pelo TSE aos regionais, quanto à detecção e tratamento de vulnerabilidades.

A ferramenta deve ser capaz de realizar a avaliação do ambiente, a priorização preditiva - que é a priorização das vulnerabilidades a serem tratadas, o monitoramento dos ativos da organização quanto às vulnerabilidades divulgadas por seus fabricantes, bem como a descoberta constante de novos ativos existentes na rede de dados. Com a ferramenta, poderemos realizar uma detecção mais rápida de vulnerabilidades que possam ser exploradas bem como apontar esforços para a sua correção.

Em 2021, alguns TRE's e o TSE fizeram a contratação da ferramenta, porém não foi possível a nossa participação por conta do orçamento envolvido não estar indicado no Plano de Contratações Anual. Dessa forma, em 2022, incluímos o item em orçamento para aquisição.

Equipe de Planejamento da Contratação:

Integrante Demandante: Maria das Graças Oliveira Magalhães Henriques

Telefone: 3194-9414 / E-mail: graca.magalhaes@tre-pe.jus.br

Integrante Técnico: Alexandre Luiz Azevedo de Olivieira

Telefone: 3194-9415 / E-mail: alexandre.oliveira@tre-pe.jus.br

Integrante Administrativo: Renata Fernanda P. E. de Abreu

Telefone: 3194-9337 / E-mail: renata.espindula@tre-pe.jus.br

1.1 Definição e Especificação dos Requisitos da Demanda (Art. 14, I)

ITEM 1 - FERRAMENTA DE DETECÇÃO E GERENCIAMENTO DE VULNERABILIDADES

1. REQUISITOS DE NEGÓCIO

A ferramenta deve atender às seguintes necessidades de negócio:

1.1. Gerenciamento de Vulnerabilidades em Sistemas Operacionais;

Funcionalidade associada: Testar os hosts (físicos e virtuais), comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software;

1.2. Gerenciamento de Vulnerabilidades em Sistemas e páginas Web;

Funcionalidade associada: Testar as aplicações e páginas web, internas e externas, comparando a bases de dados de vulnerabilidades mantidas por organizações especializadas em segurança da informação e por grandes fabricantes de software.

1.3. Emissões de Relatórios;

Funcionalidade associada: Emitir relatórios de acompanhamento dos testes e das vulnerabilidades encontradas, apontando quando forem solucionadas.

2. REQUISITOS TECNOLÓGICOS

2.1. A solução deve estar licenciada e também possuir inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware) para, no mínimo, 500 IPs;

2.2. A solução deve ser fornecida na modalidade *on premise* com a instalação do servidor no próprio ambiente do TRE-PE;

2.3. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

2.4. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

2.5. A solução deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);

2.6. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas;

2.7. A solução deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score (Common Vulnerability Scoring System);

2.8. A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;

2.9. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;

2.10. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

2.11. A solução deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

2.11.1. Por sistema operacional;

2.11.2. Por um determinado software instalado;

2.11.3. Por ativos impactados por uma determinada vulnerabilidade.

2.12. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability and Assessment Language);

2.13. A solução deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;

2.14. A solução deve possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

2.15. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;

2.16. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;

2.17. O sistema de pontuação e priorização de vulnerabilidades deve avaliar, no mínimo, as seguintes características:

2.17.1. CVSSv3 Impact Score;

2.17.2. Idade da Vulnerabilidade;

2.17.3. Se existe ameaça ou *exploit* que explore a vulnerabilidade;

2.17.4. Número de produtos afetados pela vulnerabilidade;

2.18. A solução deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo;

2.19. A solução deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no SIEM;

2.20. A solução deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;

2.21. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

2.22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV ou HTML;

2.23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

2.24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

2.25. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

a. Execução de verificação completa do sistema (rede), adequada para qualquer host;

b. Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;

c. Autenticação de hosts e enumeração de atualizações ausentes;

d. Execução de varredura simples para descobrir hosts ativos e portas abertas;

e. Utilização de um scanner para verificar aplicativos da web;

f. Avaliação de dispositivos móveis;

g. Auditoria de configuração de serviços em nuvem de terceiros;

h. Auditoria de configuração dos gerenciadores de dispositivos móveis;

i. Auditoria de configuração dos dispositivos de rede;

j. Auditoria de configurações do sistema em relação a uma linha de base conhecida;

k. Detecção de desvio de segurança Intel AMT;

l. Verificação de malware nos sistemas Windows e Unix;

2.26. Deve ser possível determinar, em tempo real, quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;

2.27. A solução deve ser capaz de realizar, em tempo real, a descoberta de novos ativos para, no mínimo:

a) Bancos de dados;

b) *Hypervisors* (no mímino VMWare ESX/ESXi);

c) Dispositivos móveis;

d) Dispositivos de rede;

e) *Endpoints*;

f) Aplicações;

2.28. A solução deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

2.29. A solução deve permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;

2.30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

2.31. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas nestes estudos.

2.32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

2.33. Configuração de segurança e acesso à gerência da solução:

a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) Os dados em trânsito devem usar, ao menos, o algoritmo TLS 1.2 de chave 2048 bits;

c) Os dados em trânsito devem ser criptografados, ao menos, com o algoritimo AES-128 bits;

d) Os algoritimos de hash devem usar, ao menos, o algoritimo SHA-256;

e) Será aceito como comprovação dos critérios de criptografia a publicação em site do fabricante ou a declaração do próprio fabricante;

f) Os dados armazenados devem ser criptografados, ao menos, com o algoritmo AES-256 bits;

g) Somente servidores da contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

h) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

i) A empresa contratada não deverá ter acesso à rede interna da contratante e todo tráfego de dados deverá ser de saída e iniciado pelos scanners (on-premises).

2.34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

2.35. Dos Relatórios:

2.35.1. A solução deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;

2.35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo, inclusive, a seleção de todos os ativos existentes;

2.35.3. A solução deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;

2.35.4. A solução deve suportar o envio automático de relatórios para destinatários específicos;

2.35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

2.35.6. A solução deve permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

2.35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;

2.35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;

2.36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;

2.37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

2.37.1. Hosts verificados sem credenciais;

2.37.2. Top 100 Vulnerabilidades mais criticas;

2.37.3. Top 10 Hosts infectados por Malwares;

2.37.4. Hosts exploráveis por Malwares;

2.37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

2.37.6. Vulnerabilidades criticas e exploráveis;

2.37.7. Máquinas com vulnerabilidades que podem ser exploradas;

2.38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;

2.39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

2.40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 500 IPs;

2.41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);

2.42. Deve permitir a configuração de vários painéis e widgets;

2.43. Deve ser capaz de medir e reportar ameaças;

2.44. Deve ser capaz de visualizar ameaças criticas ao ambiente monitorado;

2.45. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;

2.46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

2.47. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades;

2.48. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

2.49. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

2.50. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como, por exemplo, em determinados dias do mês ou determinados horários do dia;

2.51. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, a mesma deve ser capaz de ser reiniciada de onde parou;

2.52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;

2.53. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

2.54. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

2.55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;

2.56. A solução deve possuir módulo para realizar análise dinâmica em aplicações Web;

2.56.1 A solução deve possuir módulo para realizar varreduras de vulnerabilidades para, no mínimo, 5 aplicações Web, cobrindo, no mínimo, mas não limitando-se, à base de ameaças apontadas pelo OWASP Top 10, CWE e WASC:

2.56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;

2.56.3. A solução de análise deve ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);

2.56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;

2.56.5. Para varreduras do tipo extensas e detalhadas, a solução deve varrer e auditar, no mínimo, os seguintes elementos:

a) Cookies, Headers, Formulários e Links;

b) Nomes e valores de parâmetros da aplicação;

c) Elementos JSON e XML;

d) Elementos DOM;

2.56.6. A solução deve também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

2.56.7. A solução de análise deve suportar a integração com o software de automação de testes para permitir sequências de autenticação complexas;

2.56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;

2.56.9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade específica que foi detectada anteriormente no aplicativo Web;

2.56.10. A solução deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário;

2.56.11. A solução deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

2.56.12. A solução deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

2.56.13. A solução deve ser capaz de instituir, no mínimo, os seguintes limites:

a) Número máximo de URLs para *crawling* e navegação;

b) Número máximo de diretórios para varreduras;

c) Número máximo de elementos DOM;

d) Tamanho máximo de respostas;

e) Tempo máximo para a varredura;

f) Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web;

g) Número máximo de requisições HTTP(S) por segundo;

2.56.14. A solução deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

2.56.15. A solução deve suportar o envio de notificações por e-mail;

2.56.16. A solução deve ser compatível com avaliação de web services REST e SOAP;

2.56.17. A solução de análise deve suportar os seguintes esquemas de autenticação:

a) Autenticação Básica (Digest);

b) NTLM;

c) Autenticação de Cookies;

2.56.18. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;

2.56.19. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

2.56.20. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

2.56.21. Para cada vulnerabilidade encontrada, devem ser exibidos detalhes e evidências;

2.56.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;

2.56.23. Serviço de Detecção de Malware:

a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;

b) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware;

c) A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação especifica, que serão exportados para os formatos XML, HTML ou PDF.

2.56.24. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:

a. WordPress;

b. IIS 6.x e IIS 10.x;

c. ASP 6;

d. NET 2;

e. Apache HTTPD 2.2.x e 2.4.x;

f. Tomcat 6.x, 7.x, 8.x e superiores;

g. Jetty 8 e superiores;

h. Nginx;

i. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;

j. Java 1.5, 1.6, 1.7 e 1.8 e superiores;

k. Jboss 4.x e 7.x e superiores;

l. WildFly 8 e 10 e superiores;

m. Plone 2.5.x e 5.2.1.41.x e superiores;

n. Zope;

o. Python 2.4.4 e superiores;

p. J2EE;

q. Ansible;

r. Joomla;

s. Moodle;

t. Docker Conteiner;

u. Elk;

v. GIT;

w. Grafana; e

x. Redmine.

2.57. A solução não deve ser baseada em java script nem utilizar agentes baseados em java script;

2.58. O suporte técnico remoto é uma obrigação acessória do licenciamento das ferramentas e deverá estar disponível ao Contratante;

2.59. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia, mesmo que desatualizadas, e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

ITEM 2. INSTALAÇÃO E TREINAMENTO HANDS ON

1
Contratante, para uso da solução proposta, incluindo criação de scans, relatórios, filtros, permissões de usuários e demais funcionalidades da solução;

2. A instalação e configuração da solução deverá ocorrer de acordo com as melhores práticas, com a inclusão mínima dos seguintes entregáveis:

2.1. Planejamento e desenho da instalação e configuração;

2.2. Criação de políticas de scan;

2.3. Configuração de dashboards, queries e alertas iniciais;

2.4. Entrega de documentação com as principais informações do ambiente e futuras recomendações;

2.5. Instalação de scanners e agentes on-premises, quando aplicável;

2.6. Todas as licenças de uso de software devem ser registradas, na data de entrega, em nome da CONTRATANTE no site do fabricante;

2.7. Se houver necessidade, deverá ser fornecido o licenciamento do banco de dados corporativo para a instalação e monitoração da solução;

2.8. O fornecedor assinará, no ato de entrega das licenças e do serviço, Termo de Compromisso, em que se comprometerá a não acessar sem autorização, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

3. O repasse tecnológico deve ser realizado com, no mínimo, 20 (vinte) horas de capacitação para, no mínimo, 2 (dois) servidores da STIC a operacionalizar a ferramenta com as configurações efetuadas.

1.1.1 Soluções Disponíveis no Mercado (Art. 14, I, a)

1. Utilização de softwares livres:

Nome da Solução: Softwares livres OpenVas e Nmap

Fornecedor: Comunidades Open Source e páginas específicas dos projetos.

Descrição: Utilizar ferramentas livres ou gratuitas, como os softwares OpenVas e Nmap.

2. Solução paga com gerenciamento e armazenamento na nuvem (On Cloud)

Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On Cloud

Fornecedores: Qualys, Tenable e Rapid7

Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em nuvem, com modelo de subscrição por 60 meses.

3. Solução paga com gerenciamento e armazenamento na rede local do Tribunal (On premise)

Nome da Solução: Ferramenta de Gestão de Vulnerabilidades On premises

Fornecedores: Tenable e Rapid7

Descrição: Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de subscrição por 60 meses ou de licença perpetua com suporte de 60 meses.

1.1.2 Contratações Públicas Similares (Art. 14, I, b)

As contratações similares estão descritas no Quadro B destes estudos preliminares.

1.1.3 Outras Soluções Disponíveis (Art. 14, II, a)

Não há alternativas de software de gerenciamento de vulnerabilidades em outras entidades da APF.

1.1.4 Portal do Software Público Brasileiro (Art. 14, II, b)

Não há software de gerenciamento de vulnerabilidades disponível no Portal do Software Público Brasileiro.

1.1.5 Alternativa no Mercado (Art. 14, II, c)

O mercado oferece algumas soluções de software livre neste segmento, porém, como descrito no item 1.1.10 destes estudos, não solucionam a demanda existente no TRE-PE.

1.1.6 Modelo Nacional de Interoperabilidade - MNI (Art. 14, II, d)

Não aplicável, pois a solução não requer observância às regulamentações estabelecidas no MNI.

1.1.7 Infraestrutura de Chaves Públicas Brasileira - ICP Brasil (Art. 14, II, e)

Não é aplicável, pois a solução não requer o uso de certificado digital e observância às regulamentações estabelecidas na ICP-Brasil.

1.1.8 Modelo de Requisitos Moreq-Jus (Art. 14, II, f)

Não é aplicável, pois a solução não requer observância às regulamentações estabelecidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário.

1.1.9 Análise dos Custos Totais da Demanda (Art. 14, III)

Para o item 1, iniciamos a pesquisa consultando o Painel de Preços e obtivemos 5 (cinco) resultados de pregões cujo objeto envolvia softwares de detecção e gerenciamento de vulnerabilidades (PESQUISA DE MERCADO - VANTAJOSIDADE RESUMO - PAINEL DE PREÇOS (1795714)). A consulta foi realizada com os parâmetros: Ano de compra (2021 ou 2022), Esfera (Federal, Municipal e Estadual) e Descrição complementar (Software Vulnerabilidade). A análise dos resultados encontrados está discriminada a seguir:

1) PREGÃO 14/2021 COMANDO DO EXÉRCITO - BASE ADMINISTRATIVA DO CCOMGEX - ITEM 01: Software vencedor não atende recomendações de nossa demanda identificadas no item 1, tais como não utiliza clientes java script.

VENCEDOR: DUOWARE SOFTWARES LTDA

CNPJ: 19885972000139

MICRO EMPRESA

2) PREGÃO 17/2021 TRIBUNAL DE CONTAS DO ESTADO DE RORAIMA - ITEM 01 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão 172021 TCE RR (1795678)): A quantidade de IP's a ser gerenciada é de um quarto da que estamos exigindo e o tempo de vigência também é de 36 meses, dessa forma, para efeitos de comparação, podemos estimar qual seria o valor anual por licença que seria de R$ 61.000,00 / 128 (IPs) / 3 (anos) = R$ 158,85;

VENCEDOR: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI

CNPJ: 233789230001-87

PEQUENA EMPRESA

3) PREGÃO 26/2021 COMANDO DO EXÉRCITO - BASE ADMINISTRATIVA DO CCOMGEX - ITEM 01 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão 262021 Exército Base Administrativa (1795692)): O software não atende às recomendações de nossa demanda por ser uma versão mais básica do software de vulnerabilidades pretendido, que não possui análise de criticidade nem os relatórios exigidos.

VENCEDOR: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI

CNPJ: 233789230001-87

PEQUENA EMPRESA

4) PREGÃO 14/2021 COMANDO DO EXÉRCITO - COORDENAÇÃO GERAL DE LOGÍSTICA/DF - ITEM 01 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão 142021 MJ-CGS-DF (1795680) e PESQUISA DE MERCADO - VANTAJOSIDADE pregão eletrônico 142021 MJ-CGS-DF (1795698)): A quantidade de IP's a ser gerenciada é o dobro da que estamos exigindo e o tempo de vigência é de 24 meses, dessa forma, para efeitos de comparação, podemos estimar qual seria o valor anual por licença que seria de R$ 514.157,00 / 1000 (IPs) / 2 (anos) = R$ 257,07;

VENCEDOR: TELTEC SOLUTIONS LTDA

CNPJ: 048929910001-15

5) PREGÃO 116/2021 DEFENSORIA PÚBLICA DA UNIÃO - ITEM 02 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão eletrônico 1162021 Defensoria Publica (1795709)): A contratação utiliza como parâmetro de dimensão 40 FQDNs e 400 ativos, logo não há como mensurar apenas por um dos dois itens (requisito - 2.56.3 do tópico 1.1). Dessa forma o preço é inválido para nossa pesquisa.

VENCEDOR: EVERY TI TECNOLOGIA & INOVACAO EIRELI

CNPJ: 089250280001-41

Em paralelo, enviamos mensagem solicitando cotação para várias empresas (E-mail SOLICITAÇÃO COTAÇÃO 01 (1795747), E-mail SOLICITAÇÃO COTAÇÃO 02 (1795752) e E-mail SOLICITAÇÃO COTAÇÃO 03 (1795756)). Por enquanto, só obtivemos cotação das empresas 7 SECURE (Cotação SEVEN SECURE (1795781)) e APPROACH TECNOLOGIA (Cotação APPROACH (1796510)). Também em pesquisa, em sítios na internet, conseguimos obter o preço em dólar da licença do software RAPID 7 INSIGHT VM (Cotação INTERNET RAPID 7 INSIGHTVM (1795824)) junto com a cotação do dólar PTAX na data da pesquisa (Cotação VALOR DOLAR PTAX 29032021 (1795828)).

Também entramos em contato com outros Regionais para a busca por aquisições recentes e conseguimos a ARP N.º 13/2022 TRE-BA (Ata de Registro de Preços 132022 TRE-BA (1795719)) que acabou de adquirir uma licença similar à solicitada para o TRE-PE, tendo como vencedora a 7 SECURE, porém, não permitiu em sua contratação a participação de outros regionais.

Elaboramos uma planilha com os preços obtidos na pesquisa, considerando excessivos os valores acima de 30% da média das demais cotações e obtivemos o custo unitário estimado para

o item 1 de R$ 128,03 (cento e vinte e oito reais e três centavos) por licença por ano, o que gera o custo total, para 500 licenças com suporte por 5 anos, de R$ 320.072,92 (trezentos e vinte mil, setenta e dois reais e noventa e dois centavos) para o item 1. Para o item 2, recebemos apenas duas propostas e pelo serviço ser muito específico, não encontramos valores comparativos na internet, desta forma, utilizamos as duas cotações recebidas, obtendo o valor médio de R$ 55.659,95 (cinquenta e cinco mil, seiscentos e cinquenta e nove reais e noventa e cinco centavos).

Item 1 – ferramenta de detecção e gerenciamento de vulnerabilidades com suporte por 60 meses									
PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS									
Empresa/Fonte	**Tipo de Fonte***	**CNPJ**	**ME OU EPP**	**Preço****	**Média dos demais preços**	**Percentual em relação à média dos demais preços**	**Avaliação**	**Preço médio válido**	**Custo Total**
IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI	I	233789230001/87	NÃO	R$ 158,85	R$ 170,00	93,45%	Válido	R$ 128,03	**R$ 320.072,92**
TELTEC SOLUTIONS LTDA	I	048929910001/15	-	R$ 257,08	R$ 150,35	170,99%	Excessivamente		
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 140,80	R$ 173,61	81,10%	Válido		
RAPID 7	III	-	-	R$ 105,07	R$ 180,75	58,13%	Válido		
ARP 13-2022 TRE-BA (SEVEN SECURE TEC. DA INFORMAÇÃO LTDA)	II	308964510001/10	NÃO	R$ 107,39	R$ 180,29	59,56%	Válido		
APPROACH TECNOLOGIA	IV	243765420001/21	NÃO	R$ 239,63	R$ 153,84	155,77%	Excessivamente		

Obs.: O preço é excessivo quando o percentual é superior a 130%.

Excluindo os preços excessivos, ficamos com todos os preços válidos e exequíveis, com valores acima de 70% da média dos demais.

Item 1 – ferramenta de detecção e gerenciamento de vulnerabilidades com suporte por 60 meses									
PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS									
Empresa/Fonte	**Tipo de Fonte***	**CNPJ**	**ME OU EPP**	**Preço****	**Média dos demais preços**	**Percentual em relação à média dos demais preços**	**Avaliação**	**Preço médio válido**	**Custo Total**
IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI	I	233789230001/87	NÃO	R$ 158,85	R$ 70,65	224,84%	Válido	R$ 128,03	**R$ 320.072,92**
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 140,80	R$ 74,26	189,60%	Válido		
RAPID 7	III	-	-	R$ 105,07	R$ 81,41	129,07%	Válido		
ARP 13-2022 TRE-BA (SEVEN SECURE TEC. DA INFORMAÇÃO LTDA)	II	308964510001/10	NÃO	R$ 107,39	R$ 80,95	132,67%	Válido		

Obs.: O preço é válido quando o percentual é superior a 70%.

Item 2 – Implantação e repasse de conhecimento hands on da ferramenta									
PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS									
Empresa/Fonte	**Tipo de Fonte***	**CNPJ**	**ME OU EPP**	**Preço****	**Média dos demais preços**	**Percentual em relação à média dos demais preços**	**Avaliação**	**Preço médio válido**	**Custo Total**
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 40.000,00	R$ 71.319,89	56,09%	Válido	R$ 55.659,95	**R$ 55.659,95**
APPROACH TECNOLOGIA	IV	243765420001/21	NÃO	R$ 71.319,89	R$ 40.000,00	178,30%	Válido		

Obs.: O preço é excessivo quando o percentual é superior a 130%. Porém, como só tivemos duas cotações mantivemos os preços das duas para tirar a média.

Dessa forma, o custo total da aquisição será de R$ 375.732,87 (trezentos e setenta e cinco mil, setecentos e trinta e dois reais e oitenta e sete centavos), sendo R$ 320.072,92 (trezentos e vinte mil, setenta e dois reais e noventa e dois centavos) para o item 1 e R$ 55.659,95 (cinquenta e cinco mil, seiscentos e cinquenta e nove reais e noventa e cinco centavos) para o item 2.

1.1.10 Escolha e Justificativa da Solução (Art. 14, IV)

Conforme tópico 1.1.1, temos conhecimento de 3 (três) tipos de solução existentes no mercado para a demanda.

A solução 1, baseada em Software Livre, atende apenas parte da necessidade, pois a utilização desse cenário implica em não contar com suporte técnico especializado, além disso a atualização da base de vulnerabilidades e falhas não possui a mesma frequência de cenários com softwares pagos. Outro ponto desfavorável ao uso do Software Livre é que os relatórios fornecidos pelas ferramentas não apresentam rastreabilidade das atividades já realizadas nos ativos e sistemas.

A solução 2, baseada em nuvem (cloud computing), apresenta facilidade de gerenciamento e facilidade nas atualizações da solução que serão todas feitas pelo fabricante. Todas os requisitos de funcionalidades do projeto são atendidos por esse cenário. As soluções analisadas Qualys (VM e módulo WAS), Tenable (Tenable.io e módulo WAS) e Rapid7 (IVM e módulo IAS) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Porém, como os dados armazenados pela ferramenta (vulnerabilidades dos ativos de TIC) são muito sensíveis, não é recomendável estarem armazenados em nuvem pública. Por este motivo, descartamos esta opção.

A solução 3, baseada em gerenciamento em rede local do tribunal (On premise), apesar de trazer o trabalho de atualização para a equipe de infraestrutura de rede, possui um menor risco de vazamento de dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal pois os mesmos serão armazenados na rede local do Tribunal e não em nuvem pública. Todas os requisitos de funcionalidades do projeto também são atendidos por esse cenário. As soluções analisadas Tenable (Tenable.sc) e Rapid7 (Nexpose e módulo AppSpider) conseguem fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web. Outro ponto favorável à solução 3, fornecida pela Tenable, é o fato de que, após o término do suporte, a STIC continuará a ter acesso a ferramenta embora sem o direito de recebimento de atualizações de versão e de novas vulnerabilidades. Sendo assim, não resta outra alternativa para o TRE no momento, senão a solução 3, baseada no gerenciamento em rede local do tribunal, tendo em vista o fato de fazer o gerenciamento de vulnerabilidades em ativos de tecnologia da informação além de testes em aplicações Web, sem armazenar em nuvem pública os dados sensíveis que são as vulnerabilidades dos ativos de TIC do tribunal.

1.1.11 Descrição da Solução (Art. 14, IV, a)

A solução será composta de lote único com dois itens visto que, como há possibilidade de mais de uma ferramenta vencer a licitação, os serviços associados de instalação e repasse de conhecimento hands on previstos no item 2 tem de obrigatoriamente ser atribuídos à mesma licitante vencedora do item 1.

LOTE ÚNICO - ITEM	ITEM	QUANTIDADE
01	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de licença perpétua com suporte de 60 meses.	500
02	Instalação da ferramenta e repasse de conhecimento hands on	01

1.1.12 Alinhamento da Solução (Art. 14, IV, b)

Esta aquisição está alinhada com:

> Objetivo Estratégico 11 do PEI 2021-2026 (Aprimorar a estratégia de tecnologia da informação e comunicação e proteção de dados);
>
> Objetivo Estratégico 08 do PDTIC 2021-2022 (Promover Serviços de Infraestrutura e Soluções Corporativas);

Foi solicitada a sua inclusão no Plano de Contratações 2022, por meio do SEI nº 0025048-05.2021.6.17.8000, recebendo o sequencial n.º 318.

1.1.13 Benefícios Esperados (Art. 14, IV, c)

1. Atendimento aos requisitos de segurança contidos da ENSEC-JUD, aos demais planos de ação para protocolo de investigação para ilícitos cibernéticos e segurança cibernética quanto à detecção e tratamento de vulnerabilidades;

2. Atendimento ao contido na IN 61/2021 - gestão de vulnerabilidades de ativos do TRE-PE;

3.Gerenciamento de vulnerabilidades, mitigando riscos de ataques cibernéticos e protegendo os sistemas de tecnologia da informação da Justiça Eleitoral;

4. Conformidade às normas de gestão de segurança da informação.

1.1.14 Relação entre a Demanda Prevista e a Contratada (Art. 14, IV, d)

Como a ferramenta é dimensionada pelo número de dispositivos e máquinas a serem monitorados, estamos solicitando a aquisição de 500 licenças, levando em consideração a existência atual de um parque de 200 dispositivos internos ao Centro de Processamento de Dados, envolvendo máquinas virtuais, máquinas físicas, switches, firewalls, e a existência de cerca de mais 150 switches em cartórios eleitorais, além de cerca de 100 firewalls e 24 access points. As licenças restantes (26) são para possíveis expansões de monitoramento de vulnerabilidades. O suporte das licenças será pelo período de 60 meses.

1.1.15 Adequação de Ambiente (Art. 14, V, a, b, c, d, e, f)

Há necessidade de preparação de ambiente virtual para que a ferramenta passe a funcionar. Porém tal preparação não implicará em custos adicionais na contratação, e será realizada pela equipe da SENIC.

1.1.16 Orçamento Estimado (Art. 14, II, g)

Conforme demonstrado no item 1.1.9, o custo total da aquisição será de R$ 375.732,87 (trezentos e setenta e cinco mil, setecentos e trinta e dois reais e oitenta e sete centavos), sendo R$ 320.072,92 (trezentos e vinte mil, setenta e dois reais e noventa e dois centavos) para o item 1 e R$ 55.659,95 (cinquenta e cinco mil, seiscentos e cinquenta e nove reais e noventa e cinco centavos) para o item 2.

2 SUSTENTAÇÃO DO CONTRATADO (Art. 15)

2.1 Recursos Materiais e Humanos (Art. 15, I)

Não há necessidade de disponibilização de materiais ou recursos humanos para a aquisição.

2.2 Descontinuidade do Fornecimento (Art. 15, II)

Visando minimizar os efeitos em caso de eventual interrupção do fornecimento parcial ou total do objeto, solicitamos a aquisição da licença perpétua com os serviços de suporte associados, evitando a perda de funcionamento da ferramenta até que a interrupção seja resolvida com a renovação ou nova aquisição.

2.3 Transição Contratual (Art. 15, III, a, b, c, d, e)

A licença perpétua garante o funcionamento da ferramenta em tempo suficiente para uma transição contratual, embora desatualizada.

2.4 Estratégia de Independência Tecnológica (Art. 15, IV, a, b)

Para a independência tecnológica, estamos solicitando como item adicional o repasse de conhecimento para a nossa equipe sobre o funcionamento da ferramenta, trazendo o conhecimento para o próprio órgão e independência em relação à estratégia de segurança a ser adotada.

3 ESTRATÉGIA PARA A CONTRATAÇÃO(Art. 16).

3.1 Natureza do Objeto (Art. 16, I)

O objeto é de natureza comum no mercado.

3.2 Parcelamento do Objeto (Art. 16, II)

A solução será composta de lote único com dois itens, visto que, como há possibilidade de mais de uma ferramenta vencer a licitação, os serviços associados de instalação e repasse de conhecimento hands on previstos no item 2 tem de obrigatoriamente ser atribuídos à mesma licitante vencedora do item 1.

LOTE ÚNICO - ITEM	ITEM	QUANTIDADE
01	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de licença perpétua com suporte de 60 meses.	500
02	Instalação da ferramenta e repasse de conhecimento hands on	01

3.3 Adjudicação do Objeto (Art. 16, III)

A adjudicação do objeto pode ser feito por lote único, a um único fornecedor, tendo em vista que os itens do lote compõem uma solução global, interdependente e indivisível.

3.4 Modalidade e Tipo de Licitação (Art. 16, IV)

A licitação deve ocorrer por meio de pregão eletrônico, porém, por pertencer à estratégia nacional de segurança e também por meio das recomendações recentes do CNJ para compras compartilhadas, em que nos comprometemos nacionalmente a realizar o pregão eletrônico aberto a outras entidades, entendemos ser adequado que façamos a abertura de Intenção de Registro de Preços para os itens indicados para que os outros Regionais do Brasil que ainda não adquiriram a ferramenta possam participar do processo licitatório.

3.5 Classificação e Indicação Orçamentária (Art. 16, V)

Foram previstos o valor total de R$ 306.000,00 (trezentos e seis mil reais) para 500 unidades do software e R$ 50.000,00 para o serviço de implantação e repasse de conhecimento no PCI 2022, porém, como o valor médio para o item 1 ficou em R$ 320.072,92 e o valor médio para o item 2 ficou em R$ 55.659,95, caso não haja a chegada de novas cotações até a finalização do Termo de Referência, realizaremos um pedido de acréscimo de R$ 19.732,87 (dezenove mil, setecentos e trinta e dois reais e oitenta e sete centavos) no PCI.

3.6 Vigência da Prestação de Serviço (Art.16, VI)

A garantia de atualização do software deve ser de, no mínimo, 60 (sessenta) meses, contados a partir da publicação do extrato do contrato.

3.7 Equipe de Apoio à Contratação (Art. 16, VII)

Prestarão apoio à contratação os servidores integrantes da Equipe de Planejamento da Contratação referenciados no tópico 1 deste documento;

Maria das Graças Oliveira Magalhães Henriques

Telefone: 3194-9414 / E-mail: graca.magalhaes@tre-pe.jus.br

Alexandre Luiz Azevedo de Olivieira

Telefone: 3194-9415 / E-mail: alexandre.oliveira@tre-pe.jus.br

Renata Fernanda P. E. de Abreu

Telefone: 3194-9337 / E-mail: renata.espindula@tre-pe.jus.br

3.8 Equipe de Gestão da Contratação (Art. 16, VIII)

Equipe de Planejamento da Contratação:

Gestora do contrato: Maria das Graças Oliveira Magalhães Henriques

Telefone: 3194-9414 / E-mail: graca.magalhaes@tre-pe.jus.br

Gestor Substituto: Alexandre Luiz Azevedo de Olivieira

Telefone: 3194-9415 / E-mail: alexandre.oliveira@tre-pe.jus.br

Fiscal Administrativo: a ser indicado pela COMAP/SECOM

4. ANÁLISE DE RISCOS (Art. 17, I, II, III, IV e V)

Risco 1	**Risco:**	Contratação frustrada		
	Probabilidade:	**Id**	**Dano**	**Impacto**
	Média	**1**	Não cumprimento de normas de segurança da informação	Alto
	Id	**Ação de Mitigação e Contingência**		**Responsável**
	1	• Aceitação de riscos e notificação quanto à possibilidade de existência de vulnerabilidades e possíveis facilidades para ataques hackers.		STIC
	2	• Realização de nova contratação		COINF/STIC

Risco 1	**Risco:**	Atraso no fornecimento das licenças		
	Probabilidade:	**Id**	**Dano**	**Impacto**
	Baixa	**1**	Atraso na implantação do gerenciamento de vulnerabilidades	Alto
	Id	**Ação de Mitigação e Contingência**		**Responsável**
	1	• Solicitação de patrocínio da Gestão para apoio quanto à contratação.		COINF/STIC

Risco 1	**Risco:**	Empresa contratada não entregar o produto ou serviço		
	Probabilidade:	**Id**	**Dano**	**Impacto**
	Baixa	**1**	Possibilidade de comprometimento no funcionamento da detecção e correção de vulnerabilidades em ativos.	Alto
	Id	**Ação de Mitigação e Contingência**		**Responsável**
	1	• Realização de nova contratação.		COINF/STIC

5. ANEXOS

QUADRO A

Lista de Potenciais Fornecedores	
1	**Nome:** 7 SECURE **Sítio:** http://sevensecure.com.br **Telefone:** (61) 998710900 **E-mail:** douglas@sevensecure.com.br **Contato:** Douglas Araújo
2	**Nome:** SERVIX **Sítio:** http://www.servix.com **Telefone:** (085) 98838-1966 **E-mail:** diego.zupo@servix.com **Contato:** Diego Zupo
3	**Nome:** APPROACH **Sítio:** http://www.approach.com **Telefone:** (48) 998226849 **E-mail:** rafael.campos@approach.com **Contato:** Rafael Campos

QUADRO B

Contratações Públicas Similares	
1	PREGÃO ELETRÔNICO 37/2020 - TRE-PB
2	ARP N.º 13/2022 TRE-BA
3	PREGÃO 14/2021 - COMANDO DO EXÉRCITO - COORDENAÇÃO GERAL DE LOGÍSTICA/DF

QUADRO C

Memórias de Cálculos
Os cálculos estão apresentados no tópico 1.1.9 Análise dos Custos Totais da Demanda deste documento.

Declaração de Ciência - Res. CNJ 182

Declaro estar ciente das regras e diretrizes estabelecidas pela Resolução nº 182, de 17 de Outubro de 2013, do Conselho Nacional de Justiça - CNJ.

Técnico(a) Judiciário(a), em 01/04/2022, às 13:45, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARIA DAS GRAÇAS OLIVEIRA MAGALHÃES HENRIQUES**, **Chefe de Seção**, em 01/04/2022, às 13:49, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ALEXANDRE LUIZ AZEVEDO DE OLIVEIRA**, **Analista Judiciário(a)**, em 01/04/2022, às 13:50, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1791294** e o código CRC **ACF0F5DB**.

TERMO DE REFERÊNCIA

DEFINIÇÃO DO OBJETO CONTRATADO (Art.18, § 3º, I):

Aquisição de ferramenta de detecção e gerenciamento de vulnerabilidades.

1 FUNDAMENTAÇÃO DA CONTRATAÇÃO (Art. 18, § 3º, II)

1.1 Motivações da Contratação (Art. 18, § 3º, II, a)

O monitoramento das vulnerabilidades de segurança num ambiente computacional é absolutamente necessário para se manter a confidencialidade, a disponibilidade e a integridade das informações. Neste contexto, buscamos implementar uma solução de software capaz de testar os ativos de TI e as aplicações web periodicamente em busca de quaisquer vulnerabilidades, sejam elas relativas a atualização de sistemas operacionais e servidores de aplicação, configurações de serviços ou outras falhas técnicas. Além disso, é preciso que a solução forneça relatórios para que seja possível o acompanhamento deste trabalho de identificação e mitigação de riscos.

Outro item que torna necessária a contratação é o atendimento às solicitações contidas no plano de ação referente à Resolução n.º 362/2020, relativa ao protocolo de investigação para ilícitos cibernéticos, bem como o contido no plano de segurança cibernética encaminhado pelo TSE aos regionais, quanto à detecção e tratamento de vulnerabilidades.

A ferramenta deve ser capaz de realizar a avaliação do ambiente, a priorização preditiva - que é a priorização das vulnerabilidades a serem tratadas, o monitoramento dos ativos da organização quanto às vulnerabilidades divulgadas por seus fabricantes, bem como a descoberta constante de novos ativos existentes na rede de dados. Com a ferramenta, poderemos realizar uma detecção mais rápida de vulnerabilidades que possam ser exploradas bem como apontar esforços para a sua correção.

Em 2021, alguns TRE's e o TSE fizeram a contratação da ferramenta, porém não foi possível a nossa participação por conta do orçamento envolvido não estar indicado no Plano de Contratações Anual. Dessa forma, em 2022, incluímos o item em orçamento para aquisição.

1.2 Objetivos da Contratação (Art. 18, § 3º, II, b)

1. Atender aos novos requisitos da ENSEC-PJ estabelecidos no Anexo IV da Portaria n.º 162/2021 CNJ (Manual de Referência – Proteção de Infraestruturas Críticas de TIC) quais sejam:

"3.1 Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior para identificar todas as vulnerabilidades potenciais nos sistemas da organização.
3.3 Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos."

2. Atender às solicitações contidas no plano de ação referente à Resolução CNJ n.º 362/2020 (atual nº 396/2021), relativa ao protocolo de investigação para ilícitos cibernéticos, quanto a detecção de vulnerabilidades e tratamento de vulnerabilidades.

3. Atender ao contido no plano de segurança cibernética criado pelo TSE e encaminhado aos Regionais.

4. Atender ao contido na IN 61/2021 - gestão de vulnerabilidades de ativos do TRE-PE.

5. Detecção e priorização de vulnerabilidades encontradas nos ativos de rede.

6. Detecção de ativos estranhos à organização por meio de varreduras automáticas.

1.3 Benefícios da Contratação (Art. 18, § 3º, II, c)

1. Atendimento aos requisitos de segurança contidos da ENSEC-PJ estabelecidos no Anexo IV da Portaria n.º 162/2021 CNJ (Manual de Referência – Proteção de Infraestruturas Críticas de TIC) e aos planos de ação encaminhados ao CNJ referentes ao protocolo de investigação contra ilícitos cibernéticos, segurança cibernética e detecção e tratamento de vulnerabilidades;

2. Atendimento ao contido na IN 61/2021 - gestão de vulnerabilidades de ativos do TRE-PE.

1.4 Alinhamento Estratégico (Art. 18, § 3º, II, d)

Esta aquisição está alinhada com:

- Objetivo Estratégico 11 do PEI 2021-2026 (Aprimorar a estratégia de tecnologia da informação e comunicação e proteção de dados);
- Objetivo Estratégico 08 do PDTIC 2021-2022 (Promover Serviços de Infraestrutura e Soluções Corporativas);
- Plano de Contratações 2022, sob sequencial n.º 318 (SEI nº 0000044-29.2022.6.17.8000).

1.5 Referência aos Estudos Preliminares (Art. 18, § 3º, II, e)

Os estudos preliminares estão no documento SEI 'Estudos Preliminares SENIC (1791294)'.

1.6 Relação entre a demanda prevista e a quantidade de bens e/ou serviços contratados (Art. 18, § 3º, II, f)

Como a ferramenta é dimensionada pelo número de dispositivos e máquinas a serem monitorados, estamos solicitando a aquisição de 500 (quinhentas) licenças, levando em consideração a existência atual de um parque de 200 dispositivos internos ao Centro de Processamento de Dados, envolvendo máquinas virtuais, máquinas físicas, switches, firewalls, e a existência de cerca de mais 150 switches em cartórios eleitorais, além de cerca de 100 firewalls e 24 access points. As licenças restantes (26) são para possíveis expansões de monitoramento de vulnerabilidades. O suporte das licenças será pelo período de 60 (sessenta) meses.

Para efeitos de expansão futura para todo o parque de TIC do TRE-PE, estamos solicitando mais 1.000 licenças, levando em conta o quantitativo aproximado de 1.500 computadores existentes atualmente no TRE-PE. Além das licenças, há necessidade de contratação do serviço de implantação e treinamento *hands on* da ferramenta a ser adquirida.

Também, como se trata de uma compra que pode servir a outros Tribunais da Justiça Eleitoral, solicitaremos manter a permissão para carona (adesão por órgão não participante) na ata de registro de preços a ser gerada, se possível, apenas para os demais órgãos da Justiça Eleitoral.

1.7 Análise de Mercado (Art. 18, § 3º, II, g)

A pesquisa de preços foi realizada pela Coordenadoria de Infraestrutura, através do coordenador José Ferreira de Lima Júnior.

A demanda será dividida em dois itens:

1 - aquisição das licenças da ferramenta; e

2 - implantação e treinamento *hands on* da ferramenta.

Para o item 1, iniciamos a pesquisa consultando o Painel de Preços e obtivemos 5 (cinco) resultados de pregões cujo objeto envolvia softwares de detecção e gerenciamento de vulnerabilidades (vide documento 'PESQUISA DE MERCADO - VANTAJOSIDADE RESUMO - PAINEL DE PREÇOS (1795714)'). A consulta foi realizada com os parâmetros: Ano de compra (2021 ou 2022), Esfera (Federal, Municipal e Estadual) e Descrição complementar (Software Vulnerabilidade). A análise dos resultados encontrados está discriminada a seguir:

1) PREGÃO 14/2021 COMANDO DO EXÉRCITO - BASE ADMINISTRATIVA DO CCOMGEX - ITEM 01

VENCEDOR: DUOWARE SOFTWARES LTDA

CNPJ: 19885972000139

MICRO EMPRESA

Análise: Descartado, pois o software vencedor não atende recomendações de nossa demanda especificadas para o item 1, tais como: não utiliza clientes java script.

2) PREGÃO 17/2021 TRIBUNAL DE CONTAS DO ESTADO DE RORAIMA - ITEM 01 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão 172021 TCE RR (1795678))

VENCEDOR: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI

CNPJ: 233789230001-87

PEQUENA EMPRESA

Análise: A quantidade de IP's a ser gerenciada é de um quarto da que estamos exigindo e o tempo de vigência é de 36 meses (3 anos), dessa forma, para efeitos de comparação, podemos estimar qual seria o valor anual por licença que seria de R$ 61.000,00 / 128 (IPs) / 3 (anos) = R$ 158,85.

3) PREGÃO 26/2021 COMANDO DO EXÉRCITO - BASE ADMINISTRATIVA DO CCOMGEX - ITEM 01 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão 262021 Exército Base Administrativa (1795692))

VENCEDOR: IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI

CNPJ: 233789230001-87

PEQUENA EMPRESA

Análise: Descartado, pois o software não atende às recomendações de nossa demanda por ser uma versão mais básica do software de vulnerabilidades pretendido, que não possui análise de criticidade nem os relatórios exigidos.

4) PREGÃO 14/2021 COMANDO DO EXÉRCITO - COORDENAÇÃO GERAL DE LOGÍSTICA/DF - ITEM 01 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão 142021 MJ-CGS-DF (1795680) e PESQUISA DE MERCADO - VANTAJOSIDADE pregão eletrônico 142021 MJ-CGS-DF (1795698))

VENCEDOR: TELTEC SOLUTIONS LTDA

CNPJ: 048929910001-15

Análise: A quantidade de IP's a ser gerenciada é o dobro da que estamos exigindo e o tempo de vigência é de 24 meses (2 anos), dessa forma, para efeitos de comparação, podemos estimar qual seria o valor anual por licença que seria de R$ 514.157,00 / 1000 (IPs) / 2 (anos) = R$ 257,08.

5) PREGÃO 116/2021 DEFENSORIA PÚBLICA DA UNIÃO - ITEM 02 (PESQUISA DE MERCADO - VANTAJOSIDADE pregão eletrônico 1162021 Defensoria Publica (1795709))

VENCEDOR: EVERY TI TECNOLOGIA & INOVACAO EIRELI

CNPJ: 089250280001-41

Análise: A contratação utiliza como parâmetro de dimensão 40 FQDNs (Fully Qualified Domain Names - Nomes de Domínio completamente qualificados) e 400 ativos, logo não há como mensurar apenas por um dos dois itens (requisito - 1.56.3 do tópico 3). Dessa forma o preço foi descartado para nossos cálculos, visto que nossa contratação baseia-se apenas no número de ativos e não na utilização de nomes de domínio, o que encarece bastante a contratação.

Em paralelo, enviamos mensagem solicitando cotação para várias empresas (E-mail SOLICITAÇÃO COTAÇÃO 01 (1795747), E-mail SOLICITAÇÃO COTAÇÃO 02 (1795752) e E-mail SOLICITAÇÃO COTAÇÃO 03 (1795756)). Obtivemos cotação das empresas 7 SECURE (Cotação SEVEN SECURE (1795781)), APPROACH TECNOLOGIA (Cotação APPROACH (1796510)) e, por último, as cotações das empresas BLUEEYE (E-mail cotação blueeye (1807689), Cotação blueeye (1807690)), FASTHELP (E-mail cotação fasthelp (1807688) e Cotação FASTHELP (1807686)). Também em pesquisa, em sítios na internet, conseguimos obter o preço em dólar da licença do software RAPID 7 INSIGHT VM (Cotação INTERNET RAPID 7 INSIGHTVM (1795824)) junto com a cotação do dólar PTAX na data da pesquisa (Cotação VALOR DOLAR PTAX 29032021 (1795828)).

Também entramos em contato com outros Regionais para a busca por aquisições recentes e conseguimos a ARP N.º 13/2022 TRE-BA (Ata de Registro de Preços 132022 TRE-BA (1795719)), que acabou de adquirir uma licença similar à solicitada para o TRE-PE, tendo como vencedora a 7 SECURE, porém, não permitiu em sua contratação a participação de outros regionais.

Elaboramos uma planilha para cada item com os preços obtidos na pesquisa, considerando excessivos os valores acima de 30% da média das demais cotações e obtivemos, após desconsiderar os valores excessivos, o custo unitário estimado para o item 1 de R$ 131,35 (cento e trinta e um reais e trinta e cinco centavos) por licença por ano, o que gera o custo total, para 500 licenças com suporte por 5 anos, de R$ 328.375,00 (trezentos e vinte e oito mil, trezentos e setenta e cinco reais) para o item 1.

ITEM 1 - FERRAMENTA DE DETECÇÃO E GERENCIAMENTO DE VULNERABILIDADES COM SUPORTE POR 60 MESES

Item 1 – ferramenta de detecção e gerenciamento de vulnerabilidades com suporte por 60 meses

PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS

Empresa/Fonte	Tipo de Fonte*	CNPJ	ME OU EPP	Preço**	Média dos demais preços	Percentual em relação à média dos demais preços	Avaliação	Preço médio válido	Custo Total
IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI	I	233789230001/87	NÃO	R$ 158,85	R$ 160,85	98,76%	Válido	R$ 131,35	**R$ 328.375,00**
TELTEC SOLUTIONS LTDA	I	048929910001/15	-	R$ 257,08	R$ 146,82	175,10%	Excessivamente		
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 140,80	R$ 163,43	86,15%	Válido		
RAPID 7	III	-	-	R$ 105,07	R$ 168,54	62,35%	Válido		
ARP 13-2022 TRE-BA (SEVEN SECURE TEC. DA INFORMAÇÃO LTDA)	II	308964510001/10	NÃO	R$ 107,39	R$ 168,21	63,84%	Válido		
FAST HELP INFORMÁTICA LTDA	IV	05.889.039/0001-25	NÃO	R$ 132,00	R$ 164,69	80,15%	Válido		
Blueye Soluções em Tecnologia Ltda	IV	26.025.401/0001-90	NÃO	R$ 144,00	R$ 162,98	88,36%	Válido		
APPROACH TECNOLOGIA	IV	243765420001/21	NÃO	R$ 239,63	R$ 149,31	160,49%	Excessivamente		

Obs.: O preço é excessivo quando o percentual é superior a 130%.

*Tipo de fonte:
I - Painel de preços/Comprasnet
II – Contratação similar
III - Internet
IV - Fornecedor

**** Composição dos preços explicados no item 5 – Quadro C (Memória de Cálculo)**

Excluindo os preços excessivos, ficamos com todos os preços válidos e exequíveis, com valores acima de 70% da média dos demais, conforme tabela abaixo:

Item 1 – ferramenta de detecção e gerenciamento de vulnerabilidades com suporte por 60 meses									
PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS									
Empresa/Fonte	**Tipo de Fonte***	**CNPJ**	**ME OU EPP**	**Preço****	**Média dos demais preços**	**Percentual em relação à média dos demais preços**	**Avaliação**	**Preço médio válido**	**Custo Total**
IT PROTECT SERVICOS DE CONSULTORIA EM INFORMÁTICA EIRELI	I	233789230001/87	NÃO	R$ 158,85	R$ 125,85	126,22%	Válido	R$ 131,35	**R$ 328.375,00**
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 140,80	R$ 129,46	108,76%	Válido		
RAPID 7	III	-	-	R$ 105,07	R$ 136,61	76,92%	Válido		
ARP 13-2022 TRE-BA (SEVEN SECURE TEC. DA INFORMAÇÃO LTDA)	II	308964510001/10	NÃO	R$ 107,39	R$ 136,15	78,88%	Válido		
FAST HELP INFORMÁTICA LTDA	IV	05.889.039/0001-25	NÃO	R$ 132,00	R$ 131,22	100,59%	Válido		
Blueye Soluções em Tecnologia Ltda	IV	26.025.401/0001-90	NÃO	R$ 144,00	R$ 128,82	111,78%	Válido		

Para o item 2, não conseguimos propostas na internet, nem contratações similares, nem no painel de preços, visto ser um item muito específico para a instalação que será realizada no TRE, sem parâmetros para comparação com outras porventura realizadas em outros órgãos. Dessa forma, utilizamos propostas obtidas com fornecedores (Cotação SEVEN SECURE (1795781), Cotação Blueeye (1807690) e Cotação FASTHELP (1807686)), sendo excluída a proposta da APPROACH (Cotação APPROACH (1796510)) por estar com valor excessivamente superior.

ITEM 2 - IMPLANTAÇÃO E REPASSE DE CONHECIMENTO *HANDS ON* DA FERRAMENTA

Item 2 – Implantação e repasse de conhecimento hands on da ferramenta									
PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS									
Empresa/Fonte	**Tipo de Fonte***	**CNPJ**	**ME OU EPP**	**Preço****	**Média dos demais preços**	**Percentual em relação à média dos demais preços**	**Avaliação**	**Preço médio válido**	**Custo Total**
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 40.000,00	R$ 55.439,96	72,15%	Válido	R$ 45.000,00	**R$ 45.000,00**
APPROACH TECNOLOGIA	IV	243765420001/21	NÃO	R$ 71.319,89	R$ 45.000,00	158,49%	Excessivamente		
FAST HELP INFORMÁTICA LTDA	IV	05.889.039/0001-25	NÃO	R$ 50.000,00	R$ 52.106,63	95,96%	Válido		
Blueye Soluções em Tecnologia Ltda	IV	26.025.401/0001-90	NÃO	R$ 45.000,00	R$ 53.773,30	83,68%	Válido		

Obs.: O preço é excessivo quando o percentual é superior a 120%. Porém, como só tivemos duas cotações mantivemos os preços das duas para tirar a média.

*Tipo de fonte:
I - Painel de preços/Comprasnet
II – Contratação similar
III - Internet
IV - Fornecedor

** Composição dos preços explicados no item 5 – Quadro C (Memória de Cálculo)

Excluindo os preços excessivos, ficamos com todos os preços válidos e exequíveis, com valores acima de 70% da média dos demais. Ao fim, obtivemos o valor médio de R$ 45.000,00 (quarenta e cinco mil reais) para o serviço de implantação e repasse de conhecimento.

Item 2 – Implantação e repasse de conhecimento hands on da ferramenta									
PREÇO DE MERCADO EXCLUINDO OS EXCESSIVAMENTE ELEVADOS OU OS INEXEQUÍVEIS									
Empresa/Fonte	**Tipo de Fonte***	**CNPJ**	**ME OU EPP**	**Preço****	**Média dos demais preços**	**Percentual em relação à média dos demais preços**	**Avaliação**	**Preço médio válido**	**Custo Total**
SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA	IV	308964510001/10	NÃO	R$ 40.000,00	R$ 47.500,00	84,21%	Válido	R$ 45.000,00	**R$ 45.000,00**
FAST HELP INFORMÁTICA LTDA	IV	05.889.039/0001-25	NÃO	R$ 50.000,00	R$ 42.500,00	117,65%	Válido		
Blueye Soluções em Tecnologia Ltda	IV	26.025.401/0001-90	NÃO	R$ 45.000,00	R$ 45.000,00	100,00%	Válido		

Obs.: O preço é excessivo quando o percentual é superior a 120%. Porém, como só tivemos duas cotações mantivemos os preços das duas para tirar a média.

*Tipo de fonte:
I - Painel de preços/Comprasnet
II – Contratação similar
III - Internet
IV - Fornecedor

** Composição dos preços explicados no item 5 – Quadro C (Memória de Cálculo)

Ao fim, o custo total da aquisição para o ano de 2022 será de R$ 373.375,00 (trezentos e setenta e três mil, trezentos e setenta e cinco reais), sendo R$ 328.375,00 (trezentos e vinte e oito mil, trezentos e setenta e cinco reais) para o item 1 e R$ 45.000,00 (quarenta e cinco mil reais) para o item 2.

1.8 Natureza do Objeto (Art. 18, § 3º, II, h)

A contratação possui características comuns e usuais encontradas no mercado.

1.9 Parcelamento ou não dos itens (Art. 18, § 3º, II, i)

A solução será composta de lote único com dois itens, visto que, como há possibilidade de mais de uma ferramenta vencer a licitação, os serviços associados de instalação e repasse de conhecimento *hands on* previstos no item 2 têm de obrigatoriamente ser atribuídos à mesma licitante vencedora do item 1. Visto tratar-se de ata de registro de preços, foram estabelecidas quantidades mínima e máxima para adesão. A quantidade mínima de adesão para o item 1 ficou em 250, para possibilitar que o TRE-PE possa escalonar melhor a implantação do uso da ferramenta em sua rede.

LOTE ÚNICO - ITEM	ITEM	QUANTIDADE MÍNIMA PARA O PEDIDO	QUANTIDADE MÁXIMA
01	Aquisição de software de gerenciamento de vulnerabilidades e análise dinâmica de aplicações web baseado em gerenciamento e armazenamento na rede local do tribunal, com modelo de licença perpétua com suporte de 60 meses.	250	1.500
02	Instalação da ferramenta e repasse de conhecimento na modalidade *hands on*	01	02

1.10 Seleção do Fornecedor (Art. 18, § 3º, II, j)

A sugestão da equipe de planejamento é pela contratação por licitação via pregão.

Tendo em vista que há possibilidade de expansão de licenças no ano de 2023, após a primeira fase de implantação, sugerimos que a licitação seja realizada na forma de **Registro de Preços,** segundo disposto no inc. II do art. 3º do Decreto 7892/2013:

"II - quando for conveniente a aquisição de bens com **previsão de entregas parceladas** ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;"

Seguem os códigos BR correspondentes na tabela abaixo:

ITEM	CÓDIGO	DESCRIÇÃO
01	27464	Licenciamento de Direitos Permanentes de Uso de Software para Servidor
02	26972	Serviços de instalação, transição e configuração / parametrização de software

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União não deve ser aplicado nesta aquisição por se tratar de bem de informática lote único com itens de natureza diversa, um deles envolvendo serviços de TIC, ao qual não se aplicaria o referido decreto.
Ver https://tcu.jusbrasil.com.br/jurisprudencia/590381921/representacao-repr-rp-82320171/voto-revisor-590382021?ref=juris-tabs

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

Considerando tratar-se de solução que pode servir para outros entes da justiça eleitoral, sugerimos que seja permitida a opção de carona (adesão de órgão não participante) à ARP gerada, possibilitando que outros tribunais eleitorais possam utilizar a ata para sua contratação. A sugestão pela possibilidade de aceitação de órgãos exclusivamente da Justiça Eleitoral como carona advém do fato da necessidade de expansão do uso de ferramenta de detecção e gerenciamento de vulnerabilidades em toda a justiça eleitoral, como meio de aumentar a segurança no próprio TRE-PE, visto que nossa rede é integrada com o TSE e os demais Regionais.

Instrumento Contratual

Para o item demandado, há necessidade de contrato.

Critério de Julgamento, Adjudicação e Homologação

O critério de julgamento será pelo menor preço para o lote e a adjudicação e a homologação deverão ser efetuadas para um único fornecedor.

Apresentação de Amostra

Não será necessária indicação de catálogo ou site.

Tratamento Diferenciado - Microempresas e Empresas de Pequeno Porte

Como não encontramos, em nossa pesquisa de mercado, um mínimo de 03 (três) fornecedores competitivos enquadrados como Microempresas ou Empresas de Pequeno Porte, sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório, sugerimos que a participação no presente certame não deve ser exclusivamente destinada a Microempresas – ME e Empresas de Pequeno Porte – EPP. Ressaltamos que a pesquisa foi realizada por meio das fontes Painel de Preços, contratações similares, sites e fornecedores, conforme demonstrado no tópico 1.7 Análise de Mercado.

1.11 Vigência

A garantia de atualização do software deve ser de, no mínimo, 60 (sessenta) meses, contados a partir da publicação do extrato do contrato.

1.12 Impacto Ambiental (Art. 18, § 3º, II, k)

Não há impacto, visto se tratar de ferramenta de software.

1.13 Conformidade (Art. 18, § 3º, II, l)

A contratação deve obedecer à Resolução CNJ n.º 182/2013 e à Resolução TRE n.º 249/2016.

1.14 Obrigações Contratuais (Art. 18, § 3º, II, m)

Do TRE-PE:

1. Efetuar o pagamento nas condições e preços ora pactuados, desde que não haja qualquer óbice legal nem fato impeditivo provocado pela CONTRATADA;

2. Prover todas as condições necessárias para o desenvolvimento das atividades contratadas;

3. Comunicar à CONTRATADA as alterações que entender necessárias à realização do objeto da contratação, nos termos da proposta comercial;

4. Notificar a CONTRATADA, via e-mail, salvo a abertura de chamados técnicos, sobre a ocorrência de eventuais falhas no curso da execução dos serviços por meio de seus Fiscais ou Gestores;

5. Acompanhar e fiscalizar a execução do contrato por meio de servidores da Coordenadoria de Infraestrutura especialmente designados pela administração, nos termos do art. 67 da Lei 8.666/93, exigindo seu fiel e total cumprimento;

6. Responsabilizar-se pela comunicação, em tempo hábil, dos serviços a serem executados;

7. Arcar com as despesas com a publicação do extrato do contrato no Diário Oficial da União, que será providenciada pela administração até o 5º (quinto) dia útil do mês subsequente ao de sua assinatura, para ocorrer no prazo máximo de 20 (vinte) dias daquela data, nos termos do parágrafo único do art. 61 da Lei 8.666/93;

8. Efetuar toda a comunicação originada pelo contratante através de mensagem de correio eletrônico, salvo a abertura de chamados técnicos, endereçada ao representante da CONTRATADA;

9. Realizar, através da gestão contratual, todo o acompanhamento referente à ativação e utilização dos serviços contratados.

Da empresa contratada:

1. Cumprir fielmente as obrigações assumidas, conforme as especificações constantes neste Termo de Referência, utilizando-se de todos os recursos materiais e humanos necessários para entregar os produtos licitados no prazo.

2. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, sem qualquer ônus ao TRE-PE;

3. Prestar todos os esclarecimentos que forem solicitados pelo TRE-PE, credenciando um representante para prestar os devidos esclarecimentos e atender às reclamações que porventura surgirem durante a execução do objeto;

4. Quando, por problemas técnicos, os prazos pactuados não puderem ser cumpridos, a CONTRATADA deverá comunicar por escrito ao TRE-PE até 2 (dois) dias úteis anteriores ao término do prazo, cabendo ao gestor do contrato aceitar ou rejeitar as justificativas;

5. A CONTRATADA é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;

6. Não transferir a outrem, no todo ou em parte, o objeto da presente contratação, sem prévia e expressa anuência do TRE-PE;

7. Informar qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereços, razão social, telefone, fax, dissolução da sociedade, falência e outros;

8. Comunicar imediatamente ao gestor do contrato, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia;

9. Responder, para cada um dos itens do contrato, por todas e quaisquer obrigações relativas a direitos de marcas e patentes, ficando esclarecido que o CONTRATANTE não aceitará qualquer imputação nesse sentido; além de atender a todos os encargos, inclusive os de natureza tributária, incidentes sobre o funcionamento do objeto (ISS, PIS e COFINS), cabendo-lhe, também, a responsabilidade total e exclusiva, pela reparação de quaisquer danos diretos causados a pessoas e a bens ou serviços do CONTRATANTE ou de terceiros), ou em virtude de manuseio ou utilização dos produtos por ela fornecidos;

10. Garantir, na atualização dos softwares, enquanto vigente a contratação, o fornecimento de upgrades para versões mais recentes, bem como releases e patches das licenças de uso dos softwares, não implicando em custos adicionais para a contratação;

11. Garantir acesso aos canais de suporte técnico no regime de 24x7 - 24 horas, 7 dias na semana - através de número de telefone de discagem gratuita (0800) e/ou internet, para abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto ao funcionamento dos softwares, bem como permitir a utilização de estrutura de pesquisa em base de conhecimento de solução de problemas e documentos técnicos, todos de propriedade da CONTRATADA;

12. Manter confidencialidade e, em nenhum momento, divulgar a terceiros, sem a ciência e o consentimento do CONTRATANTE, documentos, imagens/fotos, dados ou outra informação que tiver sido direta ou indiretamente proporcionada pelo CONTRATANTE, antes, durante ou depois de encerrada a vigência do contrato, nos termos da política de suporte técnico da CONTRATADA.

1.15 Proposta de Preços

Conforme item 1.7, o custo total da aquisição para o ano de 2022 será de R$ 373.375,00 (trezentos e setenta e três mil, trezentos e setenta e cinco reais), sendo R$ 328.375,00 (trezentos e vinte e oito mil, trezentos e setenta e cinco reais) para o item 1 e R$ 45.000,00 (quarenta e cinco mil reais) para o item 2.

1.16 Valor e Recursos Orçamentários

Conforme demonstrado no item 1.7, o custo total da aquisição para o ano de 2022 será de R$ 373.375,00 (trezentos e setenta e três mil, trezentos e setenta e cinco reais), sendo R$ 328.375,00 (trezentos e vinte e oito mil, trezentos e setenta e cinco reais) para o item 1 e R$ 45.000,00 (quarenta e cinco mil reais) para o item 2. A despesa encontra-se prevista no PCI 2022.

1.17 Reajuste

Como o pagamento será realizado em uma única vez não há necessidade de reajuste.

2 ESPECIFICAÇÃO TÉCNICA (Art. 18, § 3º, III)

2.1 Modelo de Execução e Gestão Contratual (Art. 18, § 3º, III, a)

O modelo de execução e gestão da contratação seguirá o descrito nos tópicos 2.1.1 a 2.1.11 deste termo de referência.

2.1.1 Papéis (Art. 18, § 3º, III, a, 1)

Equipe de Gestão da Contratação:

Gestora do contrato: Maria das Graças Oliveira Magalhães Henriques

Telefone: 3194-9414 / E-mail: graca.magalhaes@tre-pe.jus.br

Gestor Substituto e Fiscal Técnico: Alexandre Luiz Azevedo de Olivieira

Telefone: 3194-9415 / E-mail: alexandre.oliveira@tre-pe.jus.br

Fiscal Administrativo: Renata Fernanda P. E. de Abreu

Telefone: 3194-9337 / E-mail: renata.espindula@tre-pe.jus.br

Não será necessária a indicação de fiscal demandante, posto que o fiscal técnico também exercerá a fiscalização demandante, visto que é servidor da unidade demandante e conhece os aspectos técnicos e funcionais da demanda.

Caberá ao Gestor da Contratação:

a) Cumprir e fazer cumprir nesta contratação as determinações insertas na Resolução TSE 23.234/2010;

b) Reportar-se à Administração Superior e à Contratada quanto à execução da contratação;

c) Comunicar à Diretoria Geral o descumprimento de cláusula contratual e instaurar procedimento administrativo para apuração de irregularidade quando devidamente autorizado;

d) Efetuar o acompanhamento, solicitação e aceite definitivo do objeto da contratação.

Caberá ao Fiscal Técnico/Demandante:

a) fiscalizar o contrato quanto aos aspectos técnicos e funcionais da solução;

Caberá à Contratada:

a) Manter durante todo o período de vigência contratual as condições de sua habilitação;

b) Responder aos questionamentos ou esclarecimentos efetuados pelo gestor da contratação no tempo indicado na referida solicitação;

c) Cumprir suas obrigações descritas neste Termo de Referência, bem como os requisitos técnicos indicados no item 3 deste documento.

2.1.2 Dinâmica (Art. 18, § 3º, III, a, 2)

A contratação será formalizada através de instrumento contratual entre as partes.

Após a assinatura e publicação do extrato do contrato, o TRE-PE encaminhará os referidos empenhos à contratada.

Após o recebimento das licenças do software, o gestor da contratação solicitará a implantação e o repasse *hands on*, efetuando o pagamento do primeiro item após a implantação da ferramenta e do segundo item após o término do repasse de conhecimento solicitado.

Durante a vigência contratual, a equipe da SENIC/COINF do TRE-PE fará uso dos serviços disponíveis conforme discriminado no tópico 3 deste termo de referência.

2.1.3 Instrumentos Formais (Art. 18, § 3º, III, a, 3)

A solicitação do objeto deve ser formalizada pelo Gestor da Contratação à Contratada através de mensagem eletrônica.

2.1.4 Acompanhamento (Art. 18, § 3º, III, a, 4)

A gestão do contrato verificará, durante o período de vigência contratual, o cumprimento dos requisitos técnicos descritos no tópico 3 deste termo de referência, podendo solicitar a aplicação de sanção em caso de descumprimento.

2.1.5 Comunicação (Art. 18, § 3º, III, a, 5)

A comunicação ocorrerá sempre através de mensagem de correio eletrônico endereçada ao representante da Contratada.

2.1.6 Recebimento (Art. 18, § 3º, III, a, 6)

a) Entrega do Objeto

A SENIC/COINF/STIC acompanhará o recebimento das licenças referentes ao item 1 que deverá ocorrer em até 30 (trinta) dias corridos contados a partir da publicação do extrato do contrato e emitirá a ordem de serviço, por e-mail, para a implantação e repasse de conhecimento previstos no item 2 da solução que deverá ser concluído em até 15 dias corridos contados da emissão da ordem de serviço.

b) Aceite do Objeto

O fiscal técnico verificará se foi finalizada a implantação da ferramenta no ambiente do TRE-PE com a execução de testes de funcionamento básicos, quando liberará o item 1 para aceite definitivo do gestor. Após a verificação de repasse do treinamento *hands-on* para a equipe, o fiscal liberará o item 2 para aceite definitivo do gestor.

Quando não houver o item de implantação, casos de expansão simples da solução já existente sem o repasse hands on previsto no item 2, o fiscal liberará o item 1 para aceite definitivo após o recebimento e verificação das licenças no sistema.

Após a verificação, pelo fiscal técnico, do item, o Gestor da Contratação emitirá, em até 5 (cinco) dias corridos, o aceite definitivo, que, por sua vez, será necessário para a liberação da nota fiscal para pagamento.

Após o aceite definitivo, o gestor encaminhará a nota fiscal atestada para pagamento.

Se houver algum problema no recebimento dos serviços, a empresa licitante será notificada por meio de mensagem eletrônica do gestor da contratação e terá, após confirmação de recebimento, 10 (dez) dias corridos para solução do(s) problema(s) apontado(s).

2.1.7 Pagamento (Art. 18, § 3º, III, a, 7)

Após o aceite definitivo, o gestor da contratação encaminhará a nota fiscal, com o devido atesto, para a Secretaria de Orçamento, Finanças e Contabilidade, para que sejam realizados os trâmites necessários para pagamento.

2.1.8 Transferência de Conhecimento (Art. 18, § 3º, III, a, 8)

A transferência de conhecimento se dará no modo *hands-on* (Item 2 da contratação), conforme previsto no tópico 3. Requisitos Técnicos deste documento, após a implementação da ferramenta no TRE.

2.1.9 Propriedade Intelectual (Art. 18, § 3º, III, a, 9)

As licenças de *software* serão de propriedade do TRE-PE.

2.1.10 Qualificação Técnica (Art. 18, § 3º, III, a, 10)

As licitantes deverão apresentar a seguinte documentação complementar para fins de qualificação técnico-operacional:

- Declaração da licitante, informando ser representante do fabricante dos *softwares* ofertados ou empresa autorizada a comercializar seus produtos;
- Atestado de capacidade técnica, emitido por entidade de direito público ou privado, certificando que a empresa já forneceu *softwares* equivalentes ao do objeto do pregão eletrônico;
- Tantos atestados quanto forem necessários para comprovar o item acima.

JUSTIFICATIVAS

A exigência referente ao primeiro tópico tem o intuito de evitar que a garantia do produto, geralmente atribuída ao fornecedor e não ao licitante, não seja válida no Brasil. Ademais, a referida declaração é de autoria da própria empresa licitante e não do fornecedor, não restringindo a competição, já que não há dependência de indicação ou escolha por parte do fornecedor, sendo passível de verificação por meio de diligência, caso seja necessária, durante o pregão eletrônico.

Quanto aos demais documentos, visam preservar a integridade do Centro de Processamento de Dados (CPD) e a continuidade de seus serviços, visto que os *softwares* a serem adquiridos são críticos e podem, em caso de manuseio inadequado, causar paralisação de serviços em produção.

2.1.11 Descumprimento Contratual (Art. 18, § 3º, III, a, 11)

a) A hipótese de descumprimento de acesso ao suporte previstos no tópico 1.14 deste Termo de Referência sem apresentação de justificativa, ensejará caso de inexecução parcial do objeto.

a.1) As justificativas serão analisadas pelo gestor da contratação, que opinará sobre a aceitação ou não dos motivos alegados. A aceitação será dada caso a justificativa seja baseada em problemas decorrentes de terceiros, alheios a decisões e responsabilidades da própria empresa, tais como: desastres naturais, acidentes, condições climáticas ou similares.

b) A licitante contratada ficará sujeita às sanções administrativas previstas nos arts. 86 e 87 da Lei nº 8.666/93, a serem aplicadas pela autoridade competente do TRE-PE, conforme a gravidade do caso, assegurado o direito à ampla defesa e ao contraditório, sem prejuízo do ressarcimento dos danos porventura causados à Administração e das cabíveis cominações legais.

c) No caso de inexecução total ou parcial, as seguintes sanções poderão ser aplicadas, nos termos do art. 87 da Lei nº 8.666/1993, sendo que as previstas nos incisos I, III e IV poderão ser aplicadas cumulativamente com a prevista no inciso II:

I Advertência;

II Multa prevista na forma da lei;

III Suspensão temporária de participar de licitação e/ou contratação promovida pelo TRE-PE, por prazo não superior a dois anos;

IV Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação perante a autoridade que aplicou a penalidade, que será concedida sempre que a licitante contratada ressarcir a Administração pelos prejuízos resultantes, e depois de decorrido o prazo da sanção aplicada com base no inciso anterior.

d) A inexecução total do objeto se caracterizará pela não entrega do objeto findos os prazos e condições definidos nos itens 1.14 e 2.1.6;

e) A inexecução parcial do objeto se caracterizará pela não entrega de parte do objeto findos os prazos e condições definidos no item 2.1.6, bem como pelo disposto no item 2.1.11, alínea "a".

2.1.12 Sustentabilidade

Visando à efetiva aplicação de critérios, ações ambientais e socioambientais que contribuam para a promoção do desenvolvimento nacional sustentável, e em atendimento ao disposto no art. 3º da Lei n.º 8.666/93, bem como no Acórdão nº 1056/2017 – Plenário do TCU; na Resolução n.º 201/2015 do CNJ e na Resolução nº 23.474/2016 do TSE, serão exigidos os seguintes requisitos de sustentabilidade:

a) Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH nº 4, de 11 de maio de 2016;

b) Não ter sido condenada, a licitante vencedora ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta à previsão aos artigos 1° e 170 da Constituição Federal de 1988; do artigo 149 do Código Penal Brasileiro; do Decreto n° 5.017, de 12 de março de 2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nºs 29 e 105;

c) Obedecer às normas técnicas, de saúde, de higiene e de segurança do trabalho, de acordo com as normas do Ministério do Trabalho e Emprego e normas ambientais vigentes.

É obrigação da contratada a manutenção dessas condições, o que poderá ser verificado constantemente durante toda a vigência do contrato, sob pena de rescisão contratual.

Em igualdade de condições, como critério de desempate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação. (Lei nº 8.666, de 1993, Art.3º, §2º, Inciso V e §5º, Inciso II; incluído pela Lei nº 13.146, de 2015, Art. 104º).

As comprovações do disposto **nas alíneas "a"** e **"b"** deverão ser feitas mediante apresentação de declaração(ões) pela licitante vencedora, para fins de análise pelo setor demandante, no prazo de 24 (vinte e quatro) horas, contado a partir da confirmação do recebimento da nota de empenho.

3 REQUISITOS TÉCNICOS (Art.18, § 3º, IV):

ITEM 1 - FERRAMENTA DE DETECÇÃO E GERENCIAMENTO DE VULNERABILIDADES

1.1. A solução deve estar licenciada e também possuir inclusas todas as funcionalidades para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance), indícios e padrões de códigos maliciosos conhecidos (malware) para, no mínimo, 500 IPs;

1.2. A solução deve ser fornecida na modalidade *on premise* com a instalação do servidor no próprio ambiente do TRE-PE;

1.3. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

1.4. A solução de gestão de vulnerabilidades deve suportar varreduras de dispositivos de IoT;

1.5. A solução deve ser capaz de identificar no mínimo 50.000 CVEs (Common Vulnerabilities and Exposures);

1.6. A solução deve ter a capacidade de adicionar etiquetas (tags) aos ativos de maneira automática, manual e possibilitar o uso de regras com parâmetros específicos para aplicação das mesmas;

1.7. A solução deve atribuir a todas as vulnerabilidades uma severidade baseada no CVSSv3 score (Common Vulnerability Scoring System);

1.8. A solução deve calcular a criticidade com base nos dados agregados e consolidados do ativo, dados de segurança, sistema e conformidade, bem como hierarquias e prioridades;

1.9. A solução deve fornecer criptografia de ponta a ponta dos dados de vulnerabilidades;

1.10. A solução deve possuir a capacidade de armazenar informações dos ativos descobertos no ambiente;

1.11. A solução deve possuir um sistema de busca de informações de um determinado ativo com, no mínimo, as seguintes características:

1.11.1. Por sistema operacional;

1.11.2. Por um determinado software instalado;

1.11.3. Por ativos impactados por uma determinada vulnerabilidade.

1.12. A solução deve possuir suporte para a adição de detecções personalizadas usando o OVAL (Open Vulnerability and Assessment Language);

1.13. A solução deve permitir aceitar o risco de uma determinada vulnerabilidade encontrada no ambiente;

1.14. A solução deve possibilitar alterar a criticidade de determinada vulnerabilidade de forma manual;

1.15. A solução deve possuir um sistema de pontuação e priorização das vulnerabilidades;

1.16. A solução deve ser capaz de aplicar algoritmos de aprendizagem de máquina (machine learning) para analisar as características relacionadas a vulnerabilidades;

1.17. O sistema de pontuação e priorização de vulnerabilidades deve avaliar, no mínimo, as seguintes características:

1.17.1. CVSSv3 Impact Score;

1.17.2. Idade da Vulnerabilidade;

1.17.3. Se existe ameaça ou *exploit* que explore a vulnerabilidade;

1.17.4. Número de produtos afetados pela vulnerabilidade;

1.18. A solução deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra vulnerabilidades encontradas, incluindo *feeds* de inteligência de ameaças ao vivo;

1.19. A solução deve possuir uma API para automação de processos e integração com aplicações terceiras permitindo, no mínimo, a extração de dados para carga no SIEM;

1.20. A solução deve possuir uma API para automação de processos e integração com aplicações ITSM do órgão para as vulnerabilidades encontradas, permitindo o agrupamento no chamado por ações corretivas;

1.21. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

1.22. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV ou HTML;

1.23. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

1.24. A solução deve ser licenciada para o uso ilimitado de sensores passivos de rede para realizar o monitoramento em tempo real;

1.25. A solução deve possuir sensores, no mínimo, com as seguintes funcionalidades:

a. Execução de verificação completa do sistema (rede), adequada para qualquer host;

b. Verificação sem recomendações da rede, para que se possa personalizar totalmente as configurações da verificação;

c. Autenticação de hosts e enumeração de atualizações ausentes;

d. Execução de varredura simples para descobrir hosts ativos e portas abertas;

e. Utilização de um scanner para verificar aplicativos da web;

f. Avaliação de dispositivos móveis;

g. Auditoria de configuração de serviços em nuvem de terceiros;

h. Auditoria de configuração dos gerenciadores de dispositivos móveis;

i. Auditoria de configuração dos dispositivos de rede;

j. Auditoria de configurações do sistema em relação a uma linha de base conhecida;

k. Detecção de desvio de segurança Intel AMT;

l. Verificação de malware nos sistemas Windows e Unix;

1.26. Deve ser possível determinar, em tempo real, quais portas de serviços (UDP/TCP) estão abertas em determinado ativo;

1.27. A solução deve ser capaz de realizar, em tempo real, a descoberta de novos ativos para, no mínimo:

a) Bancos de dados;

b) *Hypervisors* (no mímino VMWare ESX/ESXi);

c) Dispositivos móveis;

d) Dispositivos de rede;

e) *Endpoints*;

f) Aplicações;

1.28. A solução deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede;

1.29. A solução deve permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede;

1.30. A solução deve possuir interface para integração com as principais soluções de SIEM de mercado, tais como IBM QRadar, Microfocus ArcSight e Splunk.

1.31. A solução deve possibilitar a realização de cópias de segurança, funcionamento em alta disponibilidade e criptografia de todos os dados armazenados, além de incluir todo o software e licenciamento necessários para o funcionamento completo de acordo com as funcionalidades previstas nestes estudos.

1.32. A atualização das ameaças deve ocorrer diariamente e sem interrupção dos serviços.

1.33. Configuração de segurança e acesso à gerência da solução:

a) Todos os dados armazenados nos servidores da solução devem ser criptografados e possuir logs de acesso;

b) Os dados em trânsito devem usar, ao menos, o algoritmo TLS 1.2 de chave 2048 bits;

c) Os dados em trânsito devem ser criptografados, ao menos, com o algoritimo AES-128 bits;

d) Os algoritimos de hash devem usar, ao menos, o algoritimo SHA-256;

e) Será aceito como comprovação dos critérios de criptografia a publicação em site do fabricante ou a declaração do próprio fabricante;

f) Os dados armazenados devem ser criptografados, ao menos, com o algoritmo AES-256 bits;

g) Somente servidores da contratante ou pessoa por ela autorizada poderão ter acesso aos dados da solução;

h) A solução deve permitir a criação de, no mínimo, 20 contas para gerência e acesso aos relatórios, sem custo adicional;

i) A empresa contratada não deverá ter acesso à rede interna da contratante e todo tráfego de dados deverá ser de saída e iniciado pelos scanners (on-premises).

1.34. Todas as licenças de uso de software devem ser registradas, na data da entrega, em nome da Contratante no site do fabricante.

1.35. Dos Relatórios:

1.35.1. A solução deve ser capaz de executar relatórios periódicos de acordo com a frequência estabelecida pelo administrador, bem como a geração de relatórios sob demanda;

1.35.2. A solução deve possibilitar a criação de relatórios baseados na seleção de ativos, permitindo, inclusive, a seleção de todos os ativos existentes;

1.35.3. A solução deve suportar a criação de relatórios criptografados (protegidos por senha configurável) ;

1.35.4. A solução deve suportar o envio automático de relatórios para destinatários especificos;

1.35.5. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

1.35.6. A solução deve permitir especificar níveis de permissão nos relatórios para usuários e grupos especificos;

1.35.7. A solução deve fornecer relatórios do tipo “scorecard” para as partes interessadas da empresa;

1.35.8. A solução deve fornecer relatórios de correções aplicadas, classificados pelos seguintes critérios: grupo de ativos, usuários e vulnerabilidades;

1.36. A solução deve permitir mecanismo de varredura baseado em inferência com técnicas de varredura não intrusivas;

1.37. A solução deve possuir ou permitir a criação de relatórios com as seguintes informações:

1.37.1. Hosts verificados sem credenciais;

1.37.2. Top 100 Vulnerabilidades mais críticas;

1.37.3. Top 10 Hosts infectados por Malwares;

1.37.4. Hosts exploráveis por Malwares;

1.37.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

1.37.6. Vulnerabilidades críticas e exploráveis;

1.37.7. Máquinas com vulnerabilidades que podem ser exploradas;

1.38. A solução deve possuir dashboards customizáveis onde o administrador pode criar, editar ou remover painéis de acordo com a necessidade;

1.39. A solução deve ser capaz de inventariar todos os ativos da rede local e publicados na Internet, sem limites de endereços IPs.

1.40. A plataforma de software deve ser capaz de realizar varreduras (scans) de vulnerabilidades para no mínimo 500 IPs;

1.41. A plataforma de software deve ser licenciada para um número ilimitado de scanners (prevendo redundância);

1.42. Deve permitir a configuração de vários painéis e widgets;

1.43. Deve ser capaz de medir e reportar ameaças;

1.44. Deve ser capaz de visualizar ameaças críticas ao ambiente monitorado;

1.45. A plataforma de software deve realizar varreduras em uma variedade de sistemas operacionais, suportando pelo menos hosts baseados em Windows, Linux e Mac OS, bem como appliances virtuais;

1.46. A plataforma de software deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

1.47. A plataforma de software deve fornecer agentes instaláveis em sistemas operacionais, pelo menos Windows, Linux e Mac OS, para o monitoramento contínuo de configurações e vulnerabilidades;

1.48. A plataforma de software deve permitir o monitoramento através de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

1.49. A plataforma de software deve permitir o monitoramento sem a necessidade de agentes instalados, até o limite de licenças adquiridas, para varredura diretamente no sistema operacional.

1.50. A plataforma de software deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como, por exemplo, em determinados dias do mês ou determinados horários do dia;

1.51. No caso onde uma atividade de varredura seja interrompida por invadir o período não permitido, a mesma deve ser capaz de ser reiniciada de onde parou;

1.52. A plataforma de software deve ser configurável para permitir a otimização das parametrizações de varredura;

1.53. A plataforma de software deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

1.54. A plataforma de software deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

1.55. A plataforma de software deve ser capaz de realizar pesquisas de dados confidenciais;

1.56. A solução deve possuir módulo para realizar análise dinâmica em aplicações Web;

1.56.1 A solução deve possuir módulo para realizar varreduras de vulnerabilidades para, no mínimo, 5 aplicações Web, cobrindo, no mínimo, mas não limitando-se, à base de ameaças apontadas pelo OWASP Top 10, CWE e WASC:

1.56.2. A solução de análise deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web;

1.56.3. A solução de análise deve ser capaz de executar varreduras em sistemas Web através de seus endereços IP ou FQDN (DNS);

1.56.4. A solução de análise deve ser capaz de identificar vulnerabilidades de divulgação de dados, como vazamento de informações de identificação pessoal;

1.56.5. Para varreduras do tipo extensas e detalhadas, a solução deve varrer e auditar, no mínimo, os seguintes elementos:

a) Cookies, Headers, Formulários e Links;

b) Nomes e valores de parâmetros da aplicação;

c) Elementos JSON e XML;

d) Elementos DOM;

1.56.6. A solução deve também permitir a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

1.56.7. A solução de análise deve suportar a integração com o software de automação de testes para permitir sequências de autenticação complexas;

1.56.8. A solução de análise deve ser capaz de realizar testes/varreduras em aplicações separadas, simultaneamente limitadas ao número de licenças;

1.56.9. A solução de análise deve oferecer suporte à capacidade de testar novamente a vulnerabilidade especifica que foi detectada anteriormente no aplicativo Web;

1.56.10. A solução deve ser capaz de utilizar scripts customizados de *crawling* com parâmetros definidos pelo usuário;

1.56.11. A solução deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

1.56.12. A solução deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

1.56.13. A solução deve ser capaz de instituir, no mínimo, os seguintes limites:

a) Número máximo de URLs para *crawling* e navegação;

b) Número máximo de diretórios para varreduras;

c) Número máximo de elementos DOM;

d) Tamanho máximo de respostas;

e) Tempo máximo para a varredura;

f) Número máximo de conexões HTTP(S) ao servidor hospedando a aplicação Web;

g) Número máximo de requisições HTTP(S) por segundo;

1.56.14. A solução deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

1.56.15. A solução deve suportar o envio de notificações por e-mail;

1.56.16. A solução deve ser compatível com avaliação de web services REST e SOAP;

1.56.17. A solução de análise deve suportar os seguintes esquemas de autenticação:

a) Autenticação Básica (Digest);

b) NTLM;

c) Autenticação de Cookies;

1.56.18. Deve ser capaz de importar scripts de autenticação previamente configurados pelo usuário;

1.56.19. A solução de análise deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

1.56.20. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

1.56.21. Para cada vulnerabilidade encontrada, devem ser exibidos detalhes e evidências;

1.56.22. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;

1.56.23. Serviço de Detecção de Malware:

a) A solução de análise deve utilizar a plataforma de gerenciamento de vulnerabilidades existente;

b) A solução de análise deve permitir visualizar o acompanhamento das atividades de verificação, páginas infectadas e tendências de infecção por malware;

c) A solução de análise deve fornecer relatórios de resumo geral de todas as aplicações web e resumo de uma aplicação específica, que serão exportados para os formatos XML, HTML ou PDF.

1.56.24. A solução deve ser capaz de realizar varreduras nos seguintes componentes/aplicações:

a. WordPress;

b. IIS 6.x e IIS 10.x;

c. ASP 6;

d. NET 2;

e. Apache HTTPD 2.2.x e 2.4.x;

f. Tomcat 6.x, 7.x, 8.x e superiores;

g. Jetty 8 e superiores;

h. Nginx;

i. PHP 5.3.x, 5.4.x, 5.6.x, 7.0.x e 7.1.x e superiores;

j. Java 1.5, 1.6, 1.7 e 1.8 e superiores;

k. Jboss 4.x e 7.x e superiores;

l. WildFly 8 e 10 e superiores;

m. Plone 2.5.x e 5.2.1.41.x e superiores;

n. Zope;

o. Python 2.4.4 e superiores;

p. J2EE;

q. Ansible;

r. Joomla;

s. Moodle;

t. Docker Conteiner;

u. Elk;

v. GIT;

w. Grafana; e

x. Redmine.

1.57. O suporte técnico remoto é uma obrigação acessória do licenciamento das ferramentas e deverá estar disponível ao Contratante;

1.58. A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia, mesmo que desatualizadas, e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;

ITEM 2: IMPLANTAÇÃO E TREINAMENTO *HANDS ON*

IMPLANTAÇÃO

1
Contratante, para uso da solução proposta, incluindo criação de scans, relatórios, filtros, permissões de usuários e demais funcionalidades da solução;

2. A instalação e configuração da solução deverá ocorrer de acordo com as melhores práticas, com a inclusão mínima dos seguintes entregáveis:

2.1. Planejamento e desenho da instalação e configuração;

2.2. Criação de políticas de scan;

2.3. Configuração de dashboards, queries e alertas iniciais;

2.4. Entrega de documentação com as principais informações do ambiente e futuras recomendações;

2.5. Instalação de scanners e agentes on-premises, quando aplicável;

2.6. Todas as licenças de uso de software devem ser registradas, na data de entrega, em nome da CONTRATANTE no site do fabricante;

2.7. Se houver necessidade, deverá ser fornecido o licenciamento do banco de dados corporativo para a instalação e monitoração da solução;

2.8. O fornecedor assinará, no ato de entrega das licenças e do serviço, Termo de Compromisso, em que se comprometerá a não acessar sem autorização, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

2.9 A implantação deve ser realizada por equipe treinada e certificada na solução adquirida;

2.10 A implantação deve ser realizada em até 15 dias após a emissão da ordem de serviço pelo Gestor da Contratação em data a ser agendada pelo TRE-PE junto à contratada;

2.11 A implantação deve ser realizada no ambiente do TRE-PE na forma presencial ou remota;

2.12 Caso haja alguma restrição de acesso à rede do TRE-PE que impeça a instalação de forma remota, a empresa deverá providenciar a vinda de técnico na forma presencial para proceder à instalação da ferramenta;

2.13 A ferramenta deverá ser configurada inicialmente com as detecções básicas e configurações personalizadas indicadas pela equipe técnica do TRE-PE que acompanhará a instalação;

2.14 A implantação deverá ser realizada em horário e dias indicados pela Gestão da contratação, podendo ocorrer inclusive em fins de semana ou feriados;

TREINAMENTO *HANDS ON*

3.1 O repasse tecnológico deve ser realizado com, no mínimo, 20 (vinte) horas de capacitação para, até 04 (quatro) servidores da STIC a operacionalizar a ferramenta com as configurações efetuadas.

3.2 O treinamento *hands on* será realizado após a implantação em data e horário agendados com a Gestão da Contratação, podendo ser realizado à distância (desde que não haja nenhuma restrição ao acesso externo) ou presencial;

3.3 Deverá ser repassada toda a configuração realizada e as operações básicas para utilização da ferramenta;

3.4 Deverá ser fornecida toda a documentação de instalação e atualização de versão incluindo local de download e procedimentos necessários para a execução destas tarefas;

3.5 Deverá ser fornecida senha e usuário de acesso à plataforma na web, caso necessário, para o download de novas versões e atendimento de suporte;

3.6 Deverá ser fornecido telefone e/ou e-mail e/ou site para esclarecimentos e dúvidas técnicas;

3.7 Deverá ser indicado sítio eletrônico para informações técnicas.

4 MODELOS (Art.18, § 3º, V):

Apresentar a proposta de modelos (templates) a serem utilizados na contratação.

Declaração de Ciência - Res. CNJ 182

Declaro estar ciente das regras e diretrizes estabelecidas pela Resolução nº 182, de 17 de Outubro de 2013, do Conselho Nacional de Justiça - CNJ.

Documento assinado eletronicamente por **RENATA FERNANDA PEREIRA ESPINDULA DE ABREU**, **Técnico(a) Judiciário(a)**, em 01/07/2022, às 12:27, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARIA DAS GRAÇAS OLIVEIRA MAGALHÃES HENRIQUES**, **Chefe de Seção**, em 01/07/2022, às 12:30, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1899701** e o código CRC **04BD9A9E**.