ANEXO I
ESPECIFICAÇÕES TÉCNICAS

ADITAMENTO 2

Sumário

SERVIÇO ESPECIALIZADO DE SEGURANÇA DA INFORMAÇÃO 3
1. Escopo 3
1.1. Objeto 3
1.2. Condições Gerais 3
1.3. Planejamento 4
2. Serviço de Tratamento de Incidentes de Segurança e *Blue Team* 5
3. Serviço de Red Team e Testes de Invasão 6
4. Serviço de Gestão Contínua Vulnerabilidades 9
5. Software de Análise e Gestão de Vulnerabilidades 10
6. Serviço Gerenciado de Inteligência de Ameaças 15
7. Serviço de Integração de ferramentas de segurança 21
8. Suporte Técnico Local e Remoto 21
9. Requisitos Técnicos dos Profissionais 23
10. Forma de Contratação 25
11. Ambiente Tecnológico 26
Anexo A - Informações Técnicas 27

Índice de Tabelas

Tabela 1: Tipos de Serviços e Critério de Equivalência: 22
Tabela 2: Tabela de Severidade 23
Tabela 3: Formas e Periodicidade de Contratação 25
Tabela 4: Ambiente Tecnológico 26

SERVIÇO ESPECIALIZADO DE SEGURANÇA DA INFORMAÇÃO

1. ESCOPO

1.1. OBJETO

Contratação de empresa especializada na área de Segurança da Informação para manter, melhorar e prover suporte técnico especializado para ITAIPU BINACIONAL, lado brasileiro, com os respectivos serviços:

I. Planejamento do Contrato;
II. Serviço de Tratamento de Incidentes de Segurança e *Blue Team*;
III. Serviço de *Red Team* e Testes de Invasão;
IV. Serviço de Gestão Contínua de Vulnerabilidades
V. Software de Análise de Contínua de Vulnerabilidades;
VI. Serviços de monitoramento constante da *Internet* com o objetivo de prevenir e antecipar ameaças identificadas – *Threat Intel* (item com possibilidade de subcontratação);
VII. Serviço de Integração de ferramentas de segurança;
VIII. Banco de Horas – Atividades relacionadas aos serviços.

1.2. CONDIÇÕES GERAIS

1.2.1 Os trabalhos a serem executados devem estar baseados nos seguintes padrões e melhores práticas:

I. Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal;
II. ISO/IEC 27000:2018 – Sistema de Gestão de Segurança da Informação – Visão Geral e Vocabulário;
III. ISO/IEC 27001:2022 – Sistema de Gestão de Segurança da Informação – Requisitos;
IV. Toda família da ISO/IEC 27XXX aplicáveis;
V. COBIT;
VI. ITIL;
VII. *Framework CIS Controls* (*Critical Security Controls* – Versão 8.1 ou superior);
VIII. *Framework Cybersecurity NIST – National Institute of Standards and Technology*
IX. FIRST CSIRT *Services Framework* v2.1 e PSIRT *Services Framework* v1.1;
Os trabalhos deverão ser realizados na Central Hidroelétrica de Itaipu, em horário comercial da mesma, exceto aqueles que de comum acordo entre a CONTRATADA e ITAIPU considerem relevantes realizá-los em outro local e horário;

1.2.2. Todos os documentos e informes gerados pelo CONTRATADA, deverão ser padronizados e normalizados de acordo as definições de ITAIPU. A CONTRATADA deverá entregar os documentos, também em formato digital;

1.2.1. Todos os dados e informações recolhidos durante a execução dos serviços contratados são confidenciais e de uso exclusivo de ITAIPU, portanto, o padrão de sigilo

da documentação deve ser TLP:RED/CONFIDENCIAL, somente alterado por pedido expresso da ITAIPU. Não poderão ser publicados, compartilhados e copiados sem o consentimento expresso e escrito da ITAIPU;

1.2.2. As reuniões deverão ser documentadas em Atas de Reunião sob responsabilidade da CONTRATADA, enumeradas unicamente e aprovadas pela CONTRATADA e a CONTRATANTE;

1.2.3. A CONTRATADA deve disponibilizar um ou mais contatos para vulnerabilidades de segurança (podendo ser através de um CSIRT/CERT);

1.2.4. Todas as FABRICANTES eventualmente envolvidas deverão disponibilizar um ou mais contatos para vulnerabilidades de segurança (podendo ser através de um CSIRT/PSIRT ou CERT);

1.2.5. Depois da recepção das entregas previstas para cada etapa e satisfeitas todas as condições de análise referentes aos serviços prestados, a ITAIPU terá um prazo máximo de 10 (dez) dias corridos para que se posicione formalmente acerca dos resultados apresentados, indicando ações necessárias para a adequação e/ou aceitação dos resultados;

1.2.6. A ITAIPU se reserva o direito de não aceitar atendimento dos serviços por profissionais não qualificados, devendo a CONTRATADA substituir imediatamente o profissional de forma a não comprometer o atendimento final;

1.2.7. A CONTRATADA deverá comprovar a qualificação técnica dos analistas envolvidos através de documentação, apresentando em até 10 (dez) dias úteis, a partir da data estabelecida na OIS, os certificados de especialização dos profissionais envolvidos nas atividades desta contratação;

1.3. PLANEJAMENTO DO CONTRATO

1.3.1. A CONTRATADA, em conjunto com a ITAIPU, deverá elaborar o Plano de Trabalho detalhado, incluindo Cronograma, que reflita: as atividades, datas, metodologia de trabalho, desenho do esquema de controle de avanço do projeto e instancias de reporte dos avanços;

1.3.2. As principais atividades e entregáveis desta etapa:

I. Reunião Presencial de Início de Projeto;
II. Definição da equipe de trabalho do CONTRATADA e ITAIPU;
III. Elaboração do Plano de Trabalho detalhado, incluindo cronograma, esquema de controle do avanço, pontos de controle e instancias de reporte;
IV. Revisar o processo de resposta a incidentes corrente, indicando ajustes ou melhorias e a inclusão da equipe da CONTRATADA no referido processo;
V. Revisar os normativos que tratam os serviços alcançados no objeto desse contrato. Propor ajustes e melhorias, caso necessário;
VI. Definição dos padrões de documentação para as distintas instancias do projeto;
VII. Revisar o plano de contingência em TI da ITAIPU;
VIII. Apresentação e lançamento do projeto.

2. SERVIÇO DE TRATAMENTO À INCIDENTES DE SEGURANÇA E *BLUE TEAM*

2.1 Tem por objetivo a realização de atividades especializadas de Gestão de Incidentes de Segurança da Informação e implementação de melhores práticas e controles, de acordo com as demandas solicitadas pela ITAIPU, as atividades prestadas por esta equipe:

2.1.1 **Detecção e resposta a incidentes:** Monitorar e responder incidentes de segurança em tempo real e supervisão do SNOC (o qual já é operativo);

2.1.2 **Caça de ameaças (*Threat Hunting*):** Buscar proativamente ameaças e indicadores de comprometimento (IoC) dentro do ambiente de TI;

2.1.3 Supervisionar o monitoramento de segurança (realizado pelo SNOC): monitoramento continuado do tráfego de rede, logs de sistemas e atividades de usuários para detecção de anomalias e potenciais brechas de segurança;

2.2 A ITAIPU possui um processo de Gestão de Incidentes de Segurança da Informação, que estabelece os fluxos de tratamento e resposta a incidentes e propicia uma gestão capaz de supervisionar e operacionalizar as ações necessárias à apuração dos eventos e os meios de respostas adequadas a cada situação. A CONTRATADA será acionada pela ITAIPU, sob demanda, para realizar atividades específicas dentro deste processo;

2.3 O processo de gestão de incidentes da ITAIPU é cíclico, contendo um conjunto de medidas que são repetidamente aplicadas até que o incidente seja totalmente resolvido, e todas as partes envolvidas tenham as informações necessárias relacionadas ao incidente. O processo inicia-se com a etapa de recebimento de notificações externas e internas, passando pelas etapas de registro, análise, classificação, tratamento e realização de melhorias, conforme detalhado a seguir:

2.3.1 **Receber**: os incidentes são recebidos mediante as notificações externas e internas;

2.3.2 **Registrar**: o incidente reportado é registrado na ferramenta específica da ITAIPU. Após o registro, é realizada a triagem e classificação do incidente. A CONTRATADA pode ser acionada para o devido suporte técnico nesta fase do processo;

2.3.3 **Analisar**: a equipe de triagem realiza uma ação para verificar se realmente é um incidente e qual a área especializada que deverá ser acionada. A CONTRATADA pode ser acionada para o devido suporte técnico nesta fase do processo;

2.3.4 **Classificar**: após a triagem, o incidente deve ser classificado de acordo com o seu tipo e suas consequências. Com base na classificação é definido o tipo adequado de tratamento a ser adotado. A CONTRATADA pode ser acionada para o devido suporte técnico nesta fase do processo;

2.3.5 **Tratar**: a ITAIPU investigará o incidente para identificação da causa raiz e possíveis meios para reduzir os impactos. O tratamento é estruturado nas fases de contenção, erradicação e restauração. A CONTRATADA poderá ser acionada para o

devido suporte técnico nesta fase do processo, podendo inclusive ser demandada para a preservação de evidências e análise forense do ataque cibernético;

2.3.6 **Melhorias**: um relatório detalhado do incidente (chamado de *post mortem*), com as recomendações de melhoria, dever ser gerado ao término desta fase. Caso a CONTRATADA atue em qualquer etapa do processo ela dever fazer um relatório minucioso de todas as atividades elaboradas. A CONTRATADA deverá realizar, sob supervisão da ITAIPU, a geração de *post mortems* e a respectiva base de conhecimento interna da ITAIPU, visando a melhoria contínua do processo e ferramentas e controles de detecção;

2.4 Para a adequada prestação deste serviço, a CONTRATADA deverá:

2.4.1 Utilizar as boas práticas de mercado, listadas no item 1.2;

2.4.2 O regime de disponibilidade e execução deste serviço deverá ser 12x5 (doze horas por dia, cinco dias por semana, em horário da ITAIPU), devendo ser demandado conforme o acionamento da ITAIPU;

2.4.3 Possuir acesso total às ferramentas utilizadas pelo SNOC da ITAIPU, de forma a verificar, proativamente, possíveis incidentes que estejam ocorrendo, bem como sua dinâmica e materialidade;

2.4.4 Interagir com a ITAIPU e equipe de ataque (RED TEAM) para que o serviço de resposta a incidentes ocorra de forma integrada;

2.4.5 Produzir conhecimentos das táticas e técnicas de ataque que são utilizados e compartilhá-los com os membros da ITAIPU e SOC, para que ocorra o aumento da efetividade de proteção do ambiente;

2.4.6 A ITAIPU deve ser notificada de todas as ações de resposta a incidentes realizada pela CONTRATADA, de acordo com o processo estabelecido pelo ITAIPU;

2.4.7 A CONTRATADA deve fornecer, no mínimo, as seguintes bases de conhecimento para alimentar o SNOC:

I. Relatórios de ameaças e segurança;
II. Relatórios de *botnets* e centros de comando e controle;
III. Indicadores de ataques *zeroday*;
IV. Indicadores de comprometimento, suspeitas e avisos informativos;
V. Inteligência de tendências;
VI. Proxies anônimos;
VII. Endereços de rede TOR.

3. SERVIÇO DE TESTES DE INVASÃO (*RED TEAM*)

3.1 Tem como objetivo principal identificar, mapear e documentar possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica da

ITAIPU. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas específicas para tentar obter acesso não autorizado e privilegiado aos ativos de informações, bem como a indicação de soluções para a correção das vulnerabilidades encontradas. As atividades prestadas por esta equipe, consistem:

3.1.1 **Testes de invasão:** conduzir ataques simulados em redes, sistemas e aplicações para identificar vulnerabilidades e avaliação das defesas de segurança, prover relatórios nas descobertas, entregar respectivas recomendações (mitigações temporárias e investigação de causa raiz);

3.1.2 **Emulação de ameaças:** simular técnicas, táticas e procedimentos (TTPs) usados por adversários do mundo real para avaliação da capacidade de detecção e tempo de resposta;

3.2 Para a adequada prestação deste serviço a CONTRATADA deverá:

3.2.1 Observar as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATANTE;

3.2.2 Realizar testes de vulnerabilidades e invasão em endereços IP's, URL´s, aplicações ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança e outros equipamentos relacionados ao teste de invasão;

3.2.3 Realizar os Testes de Invasão (TDI) conforme a quantidade definida em Ordem de Serviço (OS);

3.2.4 Os testes solicitados em Ordem de Serviço poderão ser do tipo White Box, Black Box ou Grey Box;

3.2.5 Os testes poderão ser realizados a partir da rede interna da CONTRATANTE ou a partir da *Internet*, conforme solicitação da CONTRATANTE;

3.2.6 Obedecer às premissas e condições das atividades de testes nos alvos definidos, de acordo com o estabelecido na respectiva Ordem de Serviço (OS);

3.2.7 Reportar imediatamente quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo do ITAIPU, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

3.2.8 Suspender imediatamente os testes sempre que uma indisponibilidade for causada em virtude da sua execução;

3.2.9 O teste de invasão deverá obedecer às seguintes fases:

a) **Planejamento**: todas as premissas, processos, atividades descritas e aprovadas na OS, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento. Conterá informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):

I. *Técnica Black Box* (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista) ;

II. *Técnica White Box* (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste) ;

III. *Técnica Grey Box* (conhecimento limitado sobre o alvo).

b) **Descoberta**: deverão ser utilizadas, pelo menos, as ferramentas de análise de vulnerabilidades, descritas no lote 02, gestão de vulnerabilidades, além de técnicas manuais de análise de vulnerabilidades. As ferramentas deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades. As técnicas de descoberta, estão listadas no **Anexo A**;

c) **Exploração**: deverão ser utilizadas, pelo menos, as técnicas de ataques listadas no Anexo A, se houverem novas técnicas, é encorajado o seu uso. As técnicas deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise da efetividade e riscos envolvidos, bem como limitação de exploração – conforme planejamento aprovado pela CONTRATANTE;

d) **Relatório prévio de Teste de Invasão**: ao final de cada TDI, deverá ser elaborado um relatório pela CONTRATADA. Cada relatório, deve contemplar, no mínimo, as seguintes informações:

I. Objetivos, premissas e escopo do teste;
II. Datas e horas dos testes;
III. Metodologia de análise de vulnerabilidades;
IV. Descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis;
V. Recomendações e controles de segurança necessários para correção das vulnerabilidades;
VI. Apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências do sucesso da invasão;
VII. Detalhes da infraestrutura descoberta, alvo dos testes de invasão;
VIII. Equipamentos e recursos demandados para este teste;
IX. Tipos de ataque;
X. Prazos (janelas de tempo para execução dos testes) ;
XI. Pontos de contato da contratada (responsáveis para tratamento de questões abordadas nos testes) ;
XII. Tipos de testes realizados pelos especialistas em segurança da informação;
XIII. Confirmação ou refutação da existência de vulnerabilidades;
XIV. Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;
XV. Obtenção de acesso e possível escalada de privilégios;
XVI. Detalhamento da metodologia do ataque;
XVII. Recomendações para sanar riscos e vulnerabilidades;

XVIII. Deverá ser realizada reunião para apresentação do relatório e descrição das atividades executadas durante o teste.

e) **Relatório de Teste de Invasão**: após a entrega do relatório do item anterior (4.2.9.4), a ITAIPU analisará o documento para aplicar as recomendações, remediar os riscos ou mesmo assumi-los;

I. Após essa análise e aplicadas medidas de remediação, a ITAIPU poderá solicitar que o teste de invasão seja refeito para aferição dos resultados com emissão de novo relatório;

II. O prazo para conclusão de cada Ordem de Serviço (OS), incluindo, diagnósticos, análises, avaliações e testes com fornecimento de todos os relatórios específicos de avaliação de vulnerabilidades, dos ambientes relacionados nesta especificação técnica, será definido de acordo com cada atividade, sendo divididas em:

1) Atividades do Teste de Invasão (TDI) ;
2) Entrega do relatório "Teste de Invasão" ;
3) Ações corretivas das vulnerabilidades apontadas pela Contratada e aplicadas pela ITAIPU;
4) Reavaliação do TDI, caso necessário;
5) Entrega do relatório "Relatório Final do Teste de Invasão";
6) Aprovação por parte da ITAIPU do referido relatório final.

3.3 A ITAIPU deverá aplicar, no que couber, correções ou soluções de contorno que minimizem/corrijam as vulnerabilidades apontadas pelo Relatório "Teste de Invasão", a partir do final da reunião para apresentação do relatório de recomendações e descrição das atividades executadas durante o TDI.

4. SERVIÇO DE GESTÃO CONTÍNUA VULNERABILIDADES

4.1 A CONTRATADA deverá fornecer, instalar e configurar um software de gerência de vulnerabilidades capaz de detectar, inventariar e avaliar vulnerabilidades dos sistemas e recursos de TI, seus impactos no ambiente computacional e os riscos inerentes à segurança das informações;

4.2 Avaliar os controles de segurança implementados dos frameworks de segurança adotados pela ITAIPU e listados no item 1.2.1;

4.3 Alinhar as necessidades e expectativas das partes interessadas levantando os requisitos relevantes para uma Gestão de Vulnerabilidades no Ambiente Corporativo de TI da Itaipu.

4.4 Revisar e propor ajustes em Instruções de Procedimento (IP) relativas à Gestão de Vulnerabilidades;

4.5 Revisar e propor ajustes em metodologias de coleta de indicadores, cálculo de métricas e índices de priorização dos ativos críticos de TI;

4.6 Levantar, avaliar e propor correções de vulnerabilidades do ambiente corporativo;

4.7 Prover, manter disponível e atualizado o software de análise e gestão de vulnerabilidades;

4.8 Capacitar os técnicos da Itaipu em padrões, melhores práticas e processos de Gestão Contínua de Vulnerabilidades;

4.9 Avaliar o desempenho e a eficácia dos processos de Gestão Contínua de Vulnerabilidades;

4.10 Manter um inventário de ativos críticos real e completo conforme Anexo A;

4.11 Emitir recomendações para um processo de melhoria e correção de vulnerabilidades, *hardening* de configurações, sugerir implementações de mecanismos de detecção de vulnerabilidades e proteção da informação.

5. SOFTWARE DE ANÁLISE E GESTÃO DE VULNERABILIDADES

5.1 Disposições Gerais sobre o serviço:

5.1.1 A Solução ofertada deve suportar a quantidade de 6.000 ativos, sendo servidores físicos, virtuais, dispositivos de rede, estações de trabalhos, notebooks e dispositivos móveis (celulares e *tablets*);

5.1.2 A solução deve estar licenciada para todos as funcionalidades que envolvem a gestão contínua de vulnerabilidades e funções complementares para atingir a maior segurança no funcionamento da solução;

5.1.3 O FABRICANTE da solução deve possuir equipe de pesquisa de vulnerabilidades;

5.1.4 Substituição do hardware ou de um ou mais componentes, caso a solução contemple hardware e este apresente algum problema;

5.1.5 Possuir módulos de varredura diferenciados para análise intrusiva e não intrusiva;

5.1.6 Oferecer varredura “segura” de sistemas SCADA – Supervisory Control and Data Acquisition;

5.1.7 A solução deve possuir integração nativa com *Atlassian Bamboo, Gitlab e Jenkins;*

5.1.8 A solução deve possuir a capacidade de reprodução do ataque a partir de qualquer ponto do ciclo de desenvolvimento, validando assim se a vulnerabilidade foi ou não corrigida;

5.1.9 A solução deve suportar descoberta de containers e hosts utilizando containers;

5.1.10 A solução deve suportar integração com *ServiceNow* para abertura de tickets;

5.1.11 A Solução deve verificar a aderência e conformidade com as principais normas e regulamentações do mercado, como por exemplo COBIT, PCI-DSS, SOX, CIS Controls e ISO 27001 e com as melhores práticas do mercado. Além de ser listada pela Forrester ou Gartner na parte de gestão contínua de vulnerabilidades;

5.1.12 O software deve constar no quadrante magico do Gartner de gestão de vulnerabilidades, ano 2024 ou superior, classificada como Líder, ou no Forrester Wave, em gestão de riscos de vulnerabilidades, ano 2024 ou superior, classificada como Líder;

5.1.13 Caso a solução fornecida necessite de outros softwares para seu funcionamento, como Sistema Gerenciador de Banco de Dados, Geradores de Relatórios, entre outros, as licenças desses softwares deverão ser fornecidas em conjunto com a solução, sem ônus adicional para a ITAIPU;

5.1.14 Os softwares não deverão constar nas listas dos respectivos fabricantes como que não serão mais desenvolvidos, atualizados, suportados ou comercializados durante a vigência do contrato;

5.1.15 Os colaboradores da ITAIPU deverão ter acesso à base de conhecimento e a fóruns da solução no site do fabricante;

5.1.16 Deverá prover a atualização dos softwares, direito estendido de atualização de versão por todo o contrato, incluindo versões maiores (*major release*), versões menores (*minor release*), versões de manutenção (*maintenance release*) e atualizações de qualquer natureza (updates e patches) que forem disponibilizadas para todos os softwares especificados acima, tradicionalmente disponibilizadas através de download a partir da página *Web* do Fabricante, sem ônus adicionais;

5.1.17 Atualização dos softwares fornecidos, se houver lançamento de novos softwares em substituição aos fornecidos ou pela descontinuidade dos softwares;

5.1.18 Ao identificar uma vulnerabilidade de segurança do software, a FABRICANTE, através da CONTRATADA, deve prover uma correção de segurança em 5 (cinco) dias úteis. Até a entrega da correção, a CONTRATADA e a FABRICANTE devem disponibilizar uma forma de mitigação de risco em até 4 (quatro) horas corridas;

5.1.19 O Fabricante da solução deve possuir equipe de pesquisa de vulnerabilidades;

5.2 Requisitos da solução de análise de vulnerabilidades:

5.2.1 Utilizar listas de vulnerabilidades da SANS/FBI e IAVA *(Information Assurance Vulnerability Alert);*

5.2.2 Integrar-se com base de dados de vulnerabilidades CVE;

5.2.3 Deve contemplar realizar scan de hardening, baseados em *benchmarks* de mercado como CIS Controls;

5.2.4 Possibilitar o filtro da varredura por: destino, serviço ou vulnerabilidade;

5.2.5 A solução deve suportar a configuração de exceção de um device;

5.2.6 A solução deve ser capaz de trazer informação sobre mudança no nível de risco por vulnerabilidade, seja por uma nova classificação ou por novas máquinas que possuem esta vulnerabilidade, essa variação deverá ser apresentada em dashboard;

5.2.7 A solução deve possuir forma de entender o risco não somente baseado em CVSS, mas também trazer informações de vulnerabilidades que possuem e quais malwares e exploits associados conhecidos para esta vulnerabilidade;

5.2.8 A solução deve suportar nativamente forma de trabalhar com remediação das vulnerabilidades, criando projetos de remediação, assinalando usuários específicos para trabalharem nos projetos e trazer soluções conhecidas para as vulnerabilidades;

5.2.9 A solução deve realizar a validação de patches e hotfix de segurança;

5.2.10 A solução deve suportar análise de risco quantitativa e qualitativa;

5.2.11 A solução deve possuir uma forma de priorizar a remediação de vulnerabilidades baseada em redução de risco;

5.2.12 Efetuar descoberta de topologia dos ativos da rede;

5.3 Requisitos da Console de Administração da solução de análise de vulnerabilidades:

5.3.1 A console de administração e gerência da solução deve ser Web, com HTTPS/TLS 1.3, e o acesso a ela deve ser autenticado com usuário e senha de forma integrada ao Microsoft Active Directory da ITAIPU.

5.3.2 A solução deve possuir dashboard com o resultado das últimas verificações realizadas;

5.3.3 A solução deve contar com recursos analíticos como: evolução, tendências, tempos médios de resolução, campos personalizáveis (TAGs);

5.3.4 A solução deve suportar autenticação dos usuários através de AD ou SAML;

5.3.5 A solução deve suportar RBAC (role based access control) com no mínimo 5 tipos de usuários pré-definidos;

5.3.6 A solução deve fornecer auditoria da segurança para registrar ações de alterações de usuários, roles, configurações na ferramenta, execução de tarefas entre outros;

5.3.7 A solução deve suportar tags customizadas para identificar ativos, donos dos ativos e entre outras tags customizadas;

5.3.8 A solução deve ser capaz de agrupar assets por características específicas;

5.3.9 A solução deve suportar gerenciamento centralizado para todos os scanners, agentes, emissão de relatórios, configurações de scan e administração web based;

5.3.10 A solução deve suportar o balanceamento de carga entre scan engines, para assim utilizar scanners que estiverem com menos utilização quando necessário;

5.3.11 A solução deve suportar: *Multi-factor authentication: TOTP e U2F/FIDO2*;

5.4 Requisitos de varreduras da solução de análise de vulnerabilidades:

5.4.1 A solução deve possuir as seguintes opções de configuração de *scans:*

I. Proxy;
II. Authentication;
III. Crawler Restrictions;
IV. Attack Restrictions;
V. HTTP Headers;
VI. Performance;
VII. Reporting;
VIII. Web Service;
IX. Recorded Traffic;
X. Browser Macro;
XI. Selenium Recordings;
XII. Custom URLs.

5.4.2 A solução deve possuir, como mínimo, as seguintes opções de scans

I. Seleção de destino: IPs, lista de IPs, sub-redes;
II. Seleção de porta de serviços;
III. Por vulnerabilidade ou conjunto de vulnerabilidades;
IV. Grupos de rótulos ou sistemas/hosts.

5.4.3 A solução deve detectar e analisar vulnerabilidades conforme listadas no **Anexo A**;

5.4.4 A solução deve realizar a varredura em APIs (REST, SOAP, entre outras);

5.4.5 A solução deve suportar configurações de envio de comandos via API (REST, SOAP, entre outras);

5.4.6 A solução deve ter mecanismos para checar uma vulnerabilidade com diferentes variações do ataque, não aceitando apenas uma variância.

5.4.7 A solução deve suportar Discovery utilizando NMAP com ICMP, TCP e UDP, Além de suportar integração com VMWare vSphere e DHCP.

5.4.8 A solução deve suportar scan customizado buscando uma vulnerabilidade específica.

5.4.9 A solução deve ser capaz de criar baselines e fazer comparativos de scans passados com scans recentes e trazer uma visão de risco e a causa dessa variação de risco.

5.4.10 A solução deve suportar armazenamento das credenciais para scan autenticados de forma segura.

5.4.11 A solução deve possuir forma de criar projeto baseado no Patch Tuesday da Microsoft, trabalhando de maneira dinâmica, onde o projeto é atualizado depois dos scans realizados.

5.4.12 A solução deve possuir forma de em um mesmo scan identificar vulnerabilidades e realizar checagem de compliance de configuração de máquinas.

5.4.13 Verificar vulnerabilidades em ambiente Windows para, no mínimo: detecção de hot fixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviço habilitadas e antivírus.

5.4.14 Apresentar o nível de criticidade de cada ativo, indicando seu grau de exposição a worms, exploits e malwares em geral.

5.4.15 Possuir capacidade de configurar a velocidade da varredura de forma a não impactar a desempenho da rede.

5.5 Requisitos da análise de ameaças da solução de análise de vulnerabilidades:

5.5.1 A solução deve possuir plataforma de threat feeds integrada trazendo informações sobre vulnerabilidades que atacantes estejam utilizando para exploração.

5.5.2 A solução deve possuir integração para feeds do MISP (malware information sharing platform), correlacionando os riscos, exploits e usos já registrados.

5.5.3 A solução deve permitir a realização dos seguintes testes de ameaças, conforme listados no Anexo A.

5.6 Requisitos de suporte a relatórios da solução de análise de vulnerabilidades:

5.6.1 A solução deve possuir a capacidade de exportar relatórios em PDF, HTML, CSV, SCAP XML e XML;

5.6.2 A Solução deve suportar, no mínimo, as seguintes classes de relatórios:

I. Relatório executivo com o resumo gerencial das vulnerabilidades e riscos associados;

II. Relatório técnico com informações detalhadas;

III. Relatório de tendências que mostre a evolução do nível de conformidade.

5.6.3 A Solução deve permitir o gerenciamento de baselines de configuração dos ativos, que podem ser comparados com as novas avaliações para a determinação de desvios e envia alertas por e-mail;

5.6.4 A solução deve possuir a capacidade de criar e / ou exportar relatórios com as informações descritas no Anexo A.

5.7 Licenciamento mínimo, mas não limitado, à:

5.7.1. Correção de vulnerabilidades: *TruRisk Eliminate* com previsão de 6.000 ativos;

5.7.2 Avaliação de vulnerabilidades / Descoberta de ativos / Análise de risco do ambiente: VMDR com previsão de 6000 ativos;

5.7.3. Solução para análise dinâmica de aplicações web: *Qualys TotalAppSec* com previsão de 400 APIs.

6. SERVIÇO GERENCIADO DE INTELIGÊNCIA SITUACIONAL DE AMEAÇAS

6.1 Monitorar e coletar, de forma automatizada, potenciais ameaças à ITAIPU BINACIONAL, promovendo a antecipação de medidas defensivas e preventivas;

6.2 Deve possuir interface de gerenciamento no idioma português do Brasil, inglês e espanhol;

6.3 A solução deve ser disponibilizada em plataforma web, acessível via Internet, e possibilitar o acesso, sem falhas, ao menos pelos navegadores listados: *Mozilla Firefox (versão 127.0 ou superior), Google Chrome (versão 127 ou superior), Microsoft Edge (versão 127 ou superior), Apple Safari (versão 17 ou superior)*, de forma a também possibilitar à equipe da ITAIPU BINACIONAL as consultas aos resultados obtidos;

6.4 O monitoramento deverá ser realizado por equipe contratada em regime 24x7, durante toda a vigência do contrato, mediante parâmetros de pesquisa indicados pela ITAIPU BINACIONAL;

6.5 O monitoramento deverá ser realizado por solução baseada em aplicação ou conjunto de aplicações apropriadas para esta finalidade, instaladas sobre ambiente da CONTRATADA, que possuam mecanismo de captura automatizado de informações em sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais e arquivos de logs;

6.6 Deve possuir fontes que abranjam pelo menos os seguintes assuntos: Hacktivismo, ataques cibernéticos, fraudes, *ransomware, CVE´s, vulnerabilidades, malwares, phishing,* vazamentos de credencias, vazamentos de informação, ameaças cibernéticas, resposta a incidentes, prevenção de perda de dados, proteção de marca, risco de terceiros, fraude, golpes, ameaças internas;

6.7 Realizar o monitoramento na internet (fontes abertas, redes sociais, aplicativos de mensagens instantâneas, *fóruns, blogs, deep web e dark web*), e deve ser capaz de realizar pesquisas automatizadas previamente cadastradas, periódicas, manuais, avulsas e conforme estabelecido pela ITAIPU BINACIONAL; conforme listado no Anexo A, mas não limitado ao mesmo;

6.8 Exibir os endereços ou IP nos resultados das pesquisas realizadas sobre qualquer site, inclusive os existentes na *Deep Web e Dark Web;*

6.9 Deve realizar buscas em redes sociais com o intuito de identificar perfis falsos de autoridades, perfis corporativos falsos relacionados à ITAIPU BINACIONAL, pesquisas em grupos abertos para assuntos de interesse dela;

6.10 Deve ser capaz de realizar a pesquisa e monitoramento em grupos de aplicativos de mensagens instantâneas para busca de ameaças relacionadas à ITAIPU, no mínimo: 15.000 (quinze mil) grupos de *Telegram, Whatsapp;*

6.11 Capaz de realizar a transcrição de áudios, fotos e vídeos capturados em aplicativos de mensagens instantâneas;

6.12 Capacidade de criação de avatares por tipo de rede social, para, no mínimo: *Twitter, Facebook, Instagram, Snapchat e Linkedin*, bem como fóruns e blogs previamente definidos pela ITAIPU BINACIONAL, para a realização de pesquisas e coletas de dados;

6.13 Capacidade de realização de pesquisa de informações nos seguintes contextos:

6.13.1 Ameaças cibernéticas;
6.13.2 Resposta a Incidentes;
6.13.3 Prevenção de perdas de dados;
6.13.4 Proteção de Marca;
6.13.5 Fraudes;
6.13.6 Domínios Web;
6.13.7 Ameaças Internas.

6.14 Não deve limitar quantidade de recursos pesquisados;

6.15 Uma vez que os eventos forem coletados pela ferramenta, estes devem permanecer disponíveis por tempo indeterminado, mesmo que haja remoção original do conteúdo;

6.16 Sobre o monitoramento de domínios de internet:

6.16.1 Realizar a detecção de domínios recentemente registrados que possam oferecer, no mínimo: riscos de serem utilizados de forma maliciosa, variações comuns de nomes, permutações de caracteres, desvio de URL (typosquatting);

6.16.2 Informar anomalias nos registros “Whois” dos domínios monitorados;

6.16.3 Detectar as páginas internas (intranet) dos recursos pesquisados que estejam expostas na internet;

6.16.4 Identificar as vulnerabilidades dos domínios monitorados que tenham sido tornadas públicas.

6.17 Sobre a interface de consulta:

6.17.1 Os resultados das pesquisas devem conter, no mínimo, os seguintes campos: contexto pesquisado, data, idioma, endereço web, conteúdo original completo;

6.17.2 Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo, no mínimo, ordenáveis por data e hora, da ocorrência mais recente para a mais antiga;

6.17.3 Permitir a atualização do resultado das pesquisas realizadas anteriormente com a sinalização das atualizações;

6.17.4 Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;

6.17.5 Possuir interface de fácil visualização para demonstrar os resultados das buscas por cada tipo de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web);

6.17.6 Permitir que o usuário veja o conteúdo em seu local original, por meio de um link atrelado ao resultado da pesquisa;

6.17.7 Exibir os relacionamentos de pessoas pesquisadas por um determinado contexto ou seleção feita;

6.17.8 Disponibilizar um ambiente para visualização das pesquisas realizadas e alertas cadastrados;

6.17.9 Permitir exportar qualquer pesquisa realizada de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha eletrônica e DOCX, sem limitação da quantidade de registros.

6.18 Relatórios e Gráficos:

6.18.1 Permitir a emissão de relatórios e gráficos;

6.18.2 Possuir a capacidade de analisar dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades: visualização de perfis relacionados a palavras-chave, realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes, vínculos com outros indivíduos;

6.18.3 Exibir todos os relatórios e gráficos em painel de bordo (dashboard);

6.18.4 Permitir exportar todos os relatórios e gráficos de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha eletrônica e DOCX, sem limitação da quantidade de registros.

6.19 Do Controle de Acesso ao Sistema:

6.19.1 A CONTRATADA deverá fornecer a ITAIPU BINACIONAL direitos de acesso para a realização de consultas e geração de relatórios para no mínimo 18 (dezoito) colaboradores;

6.19.2 A CONTRATADA deverá fornecer um acesso adicional por API (Application Programming Interface) ou REST (Representational State Transfer) para 04 (quatro) usuários para integração com sistemas da ITAIPU – com suporte a seleção de papéis e granularidade de acesso a informações;

6.19.3 A autenticação para acesso ao sistema deverá contar com duplo fator de autenticação (2FA), oferecendo, no mínimo, as opções de SMS, *Email e One Time Password (OTP);*

6.19.4 A opção de duplo fator de autenticação por meio de SMS deverá ser completamente implementada pela CONTRATADA, e o efetivo envio de mensagens deve ocorrer sem qualquer custo adicional;

6.19.5 Caso a opção de OTP não seja implementada por meio de uso de aplicação para smartphones ou computadores pessoais, a contratada deverá fornecer aos colaboradores da ITAIPU os equipamentos necessários para utilização dessa funcionalidade;

6.19.6 Suporte a FIDO2 (*Fast IDentity Online 2*).

6.20 A plataforma deve ter mecanismo de armazenamento de logs de acesso dos usuários por um período mínimo de 1 (um) ano;

6.21 Os logs de acesso devem ser armazenados com no mínimo as seguintes informações:

6.21.1 Usuário;
6.21.2 Atividade executada;
6.21.3 IP de acesso;
6.21.4 Data e hora de acesso;
6.21.5 User Agent.

6.22 Todos os serviços serão solicitados *sob demanda*, mediante emissão de Ordem de Início de Serviço, e poderão ser suspensos no futuro, caso os servidores da CONTRATANTE estejam qualificados e em número suficiente para a sustentação das soluções de segurança;

6.23 Para serviços solicitados *sob demanda* não há garantia de consumo mínimo de meses. Além disso, esta contratação prevê, em alguns casos, o fornecimento de serviços na modalidade *"Software as a Service – SaaS"*, onde o software necessário para a proteção do ambiente é fornecido e operado pela CONTRATADA, que garantirá a aplicação contínua das melhores práticas.

6.24 Da Confidencialidade, Integridade e Disponibilidade dos dados do referido serviço:

6.25 A CONTRATADA deverá implementar os controles necessários para que apenas os seus profissionais vinculados à prestação do serviço, e os usuários e grupos criados

pela ITAIPU BINACIONAL, tenham acesso às pesquisas realizadas e aos dados armazenados;

6.26 A CONTRATADA deverá guardar as informações coletadas por períodos, de no mínimo, 6 (seis) meses;

6.27 A CONTRATADA realizará cópia de segurança dos dados coletados de forma a permitir ao menos a restauração do ambiente na situação equivalente à véspera da data de eventual solicitação formalizada pela ITAIPU BINACIONAL;

6.28 A CONTRATADA deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos as contas de usuários envolvidos nesta contratação. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada;

6.29 A solução deve possuir funcionalidade de busca de vazamento de credenciais por domínios e *e-mail*;

6.30 A solução deve possuir funcionalidade de abertura e gerenciamento de chamados;

6.31 A solução deve possuir funcionalidade de criação de variáveis para facilitar pesquisas avançadas;

6.32 A solução deve possuir funcionalidade de salvar buscar avançadas adicionando pesquisas com *regex*;

6.33 A CONTRATADA deverá complementar os relatórios gerados pela própria solução, elaborando o documento mensal contendo os principais achados do monitoramento, indicando os principais riscos identificados e formas de mitigação de tais riscos;

6.34 A solução deve possuir profissional destacado do quadro próprio para realização das seguintes atividades:

6.34.1 Realização de *Threat Hunting* por meio da plataforma contratada em busca dos assuntos de interesse dentro do contexto de inteligência cibernética e de potenciais ameaças direcionadas a CONTRATANTE;

6.34.2 Configuração e parametrização da plataforma para coleta dos assuntos de interesse da CONTRATANTE dentro do contexto de inteligência cibernética de forma a direcionar as informações coletadas na plataforma;

6.34.3 Criação de buscas pré-configuradas na plataforma direcionadas para contextos distintos em busca de potenciais ameaças à CONTRATANTE;

6.34.4 Criação de robôs pela plataforma para coleta de informações de interesse da CONTRATANTE;

6.34.5 Criação de alertas automáticos da plataforma nos assuntos de interesse da CONTRATANTE no contexto de inteligência cibernética;

6.34.6 Elaboração de relatórios de inteligência sobre ameaças de interesse da CONTRATANTE;

6.34.7 Interação com Threat Actors no intuito de adquirir informações pertinentes às ameaças em estudo;

6.34.8 Interação com o time da CONTRATANTE;

6.34.9 Interação com o time interno do fabricante para configuração de monitoramento de fontes de interesse para a CONTRATANTE;

6.34.10 Realização de serviços de suporte técnico pelo fabricante;

6.34.11 Realização de *takedown* de perfis falsos e sites maliciosos (limitados à 40 mensais);

6.34.12 Elaboração de relatório mensal consolidado com todos os tickets abertos no mês e informações importantes sobre a CONTRATANTE e setor elétrico.

6.35 Sobre o Acompanhamento de Takedown:

6.35.1 Deve possuir uma tela para solicitação de *takedowns*, com no mínimo as seguintes opções: URL para *takedown*, Empresa, Prioridade, Categoria;

6.35.2 Deve ser possível adicionar um feedback às ocorrências fechadas, colocando o nível de relevância.

6.35.3 Deve possuir uma tela para visualização dos *takedowns* solicitados;

6.35.4 No painel de gerenciamento, deve ser possível visualizar a quantidade total de takedowns e ordenar por data e prioridade.

6.35.5 Possuir filtros para a busca de takedowns solicitados com no mínimo as seguintes opções de filtro: Empresa, Status, Categoria, Período, Responsável pela criação, Número da ocorrência, Responsável pelo takedown;

6.35.6 Quanto ao Takedown, a plataforma deve disponibilizar dashboard com pelo menos: Quantidade de Takedowns solicitados no período, Status dos takedowns solicitados, Tempo médio de mudança de status do takedown, Lista de takedowns solicitados, Aba de pesquisa de takedowns com filtro por ao menos: Status, Categoria, Período;

6.36 Gerar alertas cibernéticos em tempo real, de acordo com as condições estabelecidas:

6.36.1 A CONTRATADA deverá configurar na solução o envio de alertas relacionados aos monitoramentos realizados;
6.36.2 Os alertas deverão ser configurados, no mínimo, nos seguintes contextos:

6.37 A solução deve ser capaz de emitir alertas e relatórios de inteligência sobre ameaças iminentes e tendências nos seguintes períodos pré-definidos: online, diário, semanal, mensal, anual e determinado;

6.38 Formas de envio dos Alertas:

6.38.1 Os alertas devem ser emitidos por periodicidade ou por expressão de busca;

6.38.2 Os alertas devem ser enviados à equipe da ITAIPU BINACIONAL por e-mail, SMS ou aplicativos de mensageria, tais como: *Whatsapp, Telegram ou Signal*;

6.38.3 Os alertas devem incluir, no mínimo: tipo da fonte, contexto procurado, e o *Timestamp* do momento da geração do alerta;

6.38.4 A solução deve permitir a customização dos textos dos alertas;

6.38.5 A solução deve possibilitar o envio de e-mails criptografados, de acordo com os padrões de segurança a serem validados pela ITAIPU BINACIONAL.

7. SERVIÇO DE INTEGRAÇÃO DE FERRAMENTAS DE SEGURANÇA

7.1 A CONTRATADA deverá possuir instância que compartilhe as informações de inteligência através do MISP (*Malware Information Sharing Platform*), executando também a gestão através da equipe local, bem gerindo a integração entre o MISP da CONTRATANTE com o da CONTRATADA;

7.2 A CONTRATADA deverá ter capacidade de identificar vulnerabilidades em no máximo um dia após o surgimento desta, executar o correlacionamento com o inventário (integrado com a ferramenta de CMDB) e informar via evento no MISP sobre os sistemas vulneráveis;

7.3 A CONTRATADA deverá possuir plataforma de inteligência que informe IoCs (Indicadores de comprometimento) contendo, no mínimo, hashes de binários maliciosos nos formatos MD5, SHA1, SHA256, filename, domínios maliciosos, URLs maliciosas, bem como IPs maliciosos com geolocalização e pontuação de risco, reduzindo a possibilidade de falso positivo;

7.4 Permitir integração com API REST com suporte no retorno de informações no padrão JSON;

7.5 Permitir a integração a ferramentas externas por meio de API REST e/ou SDK;

7.6 Deve possuir API com controle de acesso baseado em usuário e times para consumo de informações via outras ferramentas;

8. SUPORTE TÉCNICO LOCAL E REMOTO (BANCO DE HORAS)

A CONTRATADA, a pedido de ITAIPU, poderá realizar avaliações eventuais e específicas relacionadas ao objeto do contrato. Estas atividades serão realizadas por chamado, utilizando o Banco de Horas previsto;

Esta contratação prevê um banco de horas de 2.900 (dois mil e novecentas) horas para suporte técnico local ou remoto (ver *tabela 1* do subitem 8.2 para equivalências).

Obs.: Não existe garantia de faturamento sobre estas horas, que serão consumidas de acordo com a necessidade de ITAIPU.

8.1 As principais atividades consistem:

8.1.1 **Análise forense:** realizar análise forense digital para preservação de evidências em incidentes de segurança;

8.1.2 **Gestão e Controles:** apoiar no refinamento de políticas e processos de segurança. Gerar relatórios, tendências de ameaças, priorização de riscos e métricas para apoio à tomada de decisão e gestão de segurança;

8.1.3 **Engenharia social:** conduzir avaliações através de técnicas de engenharia social para avaliar o elemento humano e respectivas medidas de defesa;

8.1.4 Relatórios de análise de inteligência cibernética sobre os monitoramentos realizados e assuntos de análise de ameaças e pontenciais APTs/Atores maliciosos;

8.1.5 Prover apoio técnico relativo ao objeto do contrato, em forma local e/ou remota, em atividades de segurança referentes a mudanças de infraestrutura e serviços de TI (*hardware, software*, dispositivos de comunicação, entre outros) e mudanças nas aplicações de negócio;

8.1.6 Responder dúvidas, indicar melhorias em relação as tecnologias e processos internos da ITAIPU;

8.1.7 Avaliar e revisar controles conforme itens listados na seção 1.2.1;

8.2 As horas previstas para suporte técnicos locais podem ser utilizadas em qualquer quantidade e período, com previsão mínima de 20hrs em caso de deslocamento para ITAIPU (CHI), devendo ser previamente solicitadas, agendadas e aprovadas pela ITAIPU, devendo obedecer ao seguinte critério de equivalência para o consumo em horas:

Tabela 1: Tipos de Serviços e Critério de Equivalência:

Tipos de Serviço	Unidade	Quantidade	Equivalência
Suporte off-site *(independente de horário)*	Horas	1	0,5
Suporte on-site *(horário comercial)*	Horas	1	1
Suporte on-site *(noturno)*	Horas	1	1,5
Suporte on-site *(finais de semana e feriados)*	Horas	1	2

8.3 Somente poderá ser parte deste cômputo as horas consumidas nas atividades aprovadas pela ITAIPU. Não deverá ser parte deste cálculo as horas consumidas desde o deslocamento do técnico até sua apresentação na ITAIPU ou qualquer outra atividade não aprovada expressamente pela ITAIPU.

8.4 Enquanto dure o serviço de suporte técnico local, os consultores não poderão atender a chamados de suporte técnico oriundos de fontes distintas as explicitamente especificadas pela ITAIPU.

8.5 O serviço de suporte técnico remoto será realizado através de contato telefônico ou meios eletrônicos, devendo a CONTRATADA disponibilizar ferramentas para registro e acompanhamento de chamados.

8.6 A CONTRATADA deverá garantir a disponibilidade técnica e o atendimento dos serviços de suporte técnico remoto em regime de 24x7, para todo o conjunto de serviços que faz parte do Contrato, em *português ou espanhol*, sem limites de acionamentos e devendo responder aos requisitos dos niveis de serviço especificados na seguinte *tabela*:

Tabela 2: Tabela de Severidade

Severidade	Descrição	Início de Atendimento	Encerramento do Chamado
1	CRÍTICA	Imediato	4 horas corridas
2	ALTA	2 horas corridas	8 horas corridas
3	MÉDIA	4 horas úteis	12 horas úteis
4	BAIXA	8 horas úteis	48 horas úteis

8.7 O início da prestação do Suporte Técnico Remoto, poderá ser realizado mediante solução de acesso remoto (definida pela CONTRATANTE) ou solução da própria CONTRATADA, não poderá ultrapassar o tempo máximo (em horas úteis) estabelecido na coluna INICIO DO ATENDIMENTO, a partir da abertura do chamado pela ITAIPU, tendo a CONTRATADA até o tempo máximo (em horas úteis) estabelecido na coluna ENCERRAMENTO DO CHAMADO para concluir as atividades de suporte, informando a efetiva solução do problema ou solução de contorno;

8.8 O encerramento do atendimento e encerramento do chamado somente pode ser realizado depois de validado e certificado pela ITAIPU;

8.9 O pagamento do Suporte Técnico "Remoto" será *sob demanda*, quando houver(em) chamado(s) realizados, consultas ou apoio remotos.

9. REQUISITOS TÉCNICOS MÍNIMOS DOS PROFISSIONAIS

9.1 A CONTRATADA deverá comprovar a qualificação técnica dos profissionais (analistas) envolvidos através de documentação, apresentando em até 10 (dez) dias úteis, a partir da data estabelecida na OIS, os certificados de especialização dos profissionais envolvidos nas atividades desta contratação;

9.2 Todos profissionais envolvidos deve ser da categoria PLENO, e cada time deve conter, ao mínimo, um profissional SENIOR. Devem ter experiências comprovadas e conforme:

9.2.1 **PLENO**: no mínimo 3 anos de experiencia comprovada na função, com sólido conhecimento entre em segurança de redes, sistemas operacionas e incidentes de segurança. E, conforme a equipe, o seguintes conhecimentos:

I. ***Blue Team:*** Detecção de ameaças, processos de resposta a incidentes. Deve ser apto na análise de incidentes de segurança, conduzir investigações forenses e implementação de controles de segurança;
II. ***Red Team:*** Metodologias de ataque, técnicas de exploração, ferramentas (como metasploit, burp suite, entre outros). Deve ser apto na execução independente de partes do *engage* de um *red team* e desenvolvimento de exploits customizados;

9.2.2 **SENIOR**: no mínimo 6 (seis) anos de experiencia comprovada na função, sólido conhecimento técnico e de processos correlatos. E, conforme a equipe, o seguintes conhecimentos:

I. ***Blue Team:*** Habilidades avançadas na detecção de ameaças (*threat hunting*), gerenciamento de incidentes e arquitetura segura. Responsabilidade no desenvolvimento e refinamento de políticas de segurança, liderança em resposta a incidentes e colaboração com o red team para melhorar a postura de segurança como um todo. Conhecimento consolidado em estratégias de operações de cibersegurança e com habilidade de projetar mecanimos de defesa robustos;

II. ***Red Team***: Habilidades avançadas em testes de invazão, engenharia social e simulação de adversários (APTs). Responsabilidade na liderança de engajamento do *red team* e desenvolver estratégias sofisticadas de ataques. Conhecimento profundo na superfície de ameaças e com habilidade de mimetizar adversários conforme cenários do mundo real;

9.3 Os profissionais envolvidos com o projeto deverão pertencer ao quadro próprio da CONTRATADA, **exceto os profissionais envolvidos nos serviços do item 6 (Serviço Gerenciado de Inteligência situacional de Ameaças) e item 7 (Serviços de Integração de Ferramentas de Segurança).**

9.3.1 A comprovação do vínculo dos profissionais com a CONTRATADA poderá ser efetuada por meio de **Carteira de Trabalho e Previdência Social - CTPS assinada ou vínculo societário**, no caso dos profissionais que deverão pertencer ao quadro próprio da CONTRATADA, e sendo o caso, por **contrato de prestação de serviços** regido pela legislação civil comum para aqueles profissionais alocados nos serviços que admitem subcontratação, conforme previsto nos itens 6 (Serviço Gerenciado de Inteligência Situacional de Ameaças) e 7 (Serviços de Integração de Ferramentas de Segurança).

9.4 Os profissionais devem comprovar, através de documentação apropriada, com prazo máximo de 90 (noventa) dias contados da OIS, possuírem as seguintes certificações:

9.4.1 Os técnicos envolvidos no item 3 (*blue team*) devem possuir, duas ou mais certificações listadas a seguir:

I. GIAC Certified Intrusion Analyst Certification (GCIA);
II. GIAC Certified Incident Handler Certification (GCIH);
III. GIAC Cyber Incident Leader (GCIL).

9.4.2 Os técnicos envolvidos no item 4 (Red Team) e item 5 (Gerenciamento De Vulnerabilidades), devem possuir duas ou mais certificações listadas, a seguir:

I. GIAC Penetration Tester (GPEN);
II. GIAC Red Team Professional (GRTP);
III. GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);
IV. Offensive Security Certified Professional – OSCP;
V. Offensive Security Certified Experienced Penetration Tester – OSEP.

9.4.3 Os técnicos envolvidos no item 6 (Inteligência de Ameaças) e item 7 (Integração de Ferramentas de Segurança), devem possuir 2(duas) ou mais certificações listadas a seguir:

I. CompTIA Cibersecurity Analyst (CySA+);
II. Certified Ethical Hacker – CEH ou Certified Expert Penetration Tester – CEPT/GIAC;
III. Certified Hacking Forensic Investigator – CHFI.

9.5 A ITAIPU se reserva o direito de não aceitar atendimento por profissionais não qualificados, devendo a CONTRATADA substituir imediatamente o profissional de forma a não comprometer o atendimento final;

9.6 Todos profissionais da CONTRATADA, envolvidos na prestação do serviços, deverão assinar um termo de conduta ético e de proteção de informações fornecido pela ITAIPU.

10. FORMA DE CONTRATAÇÃO

Tabela 3: Formas e Periodicidade de Contratação

Item	Descrição dos Serviços	Periodicidade dos Serviços	Prazo máximo de execução (dias corridos)
1	Planejamento do Contrato	1 vez ao início do Contrato	60 dias, a partir da (*) OIS
2	Serviço de Tratamento de Incidentes de Segurança e *Blue Team*	1 vez ao mês	30 dias, a partir da OIS
3	Serviço de Testes de Invasão e *Red Team*	1 vez ao mês	30 dias, a partir da OIS
4	Serviço de Gestão Contínua de Vulnerabilidades	1 vez ao mês	30 dias, a partir da OIS
5	Software de Gerenciamento de Vulnerabilidades	Sob-demanda	30 dias, a partir da OIS
6	Serviço Gerenciado de Inteligencia Situacional (*Threat Intel*)	1 vez ao mês	30 dias, a partir da OIS
7	Serviço de Integração com ferramentas de segurança	1 vez	90 dias, a partir da OIS
8	Banco de Horas de Suporte Local e Remoto: Atividades relacionadas aos serviços listados no Item 1 (Objeto)	Banco de Horas	Conforme a criticidade do pedido ou Plano de Trabalho aprovado.

(*) OIS – Ordem de Inicio de Serviços, documento formalizado a ser emitido pela ITAIPU à CONTRATADA, para início oficial dos serviços deste Contrato.

11. AMBIENTE TECNOLÓGICO (ATUAL)

Tabela 4: Ambiente Tecnológico

Item	Mínimo	Máximo	Observações
Estações Windows	1500	2000	
Servidores Windows	100	200	
Servidores Linux	200	400	
Ativos de Rede	500	700	Metade consiste em antenas Wifi
DNS externos	50	100	
Sistemas suportados	100	400	
Contas de domínio	1500	2500	
Banco de Dados	100	150	

Anexo A - Informações Técnicas

Abaixo, a complementação de informações técnicas para atendimento do Contrato.

1. Técnicas de descoberta

1.1. Coleta passiva, onde deverá ser utilizada:
- 1.1.1. *Whois* e *nslookup* (consultas DNS) ;
- 1.1.2. Sites de busca;
- 1.1.3. Listas de discussão;
- 1.1.4. Blogs de colaboradores;
- 1.1.5. *Dumpster diving* ou *trashing* ;
- 1.1.6. Informações livres;
- 1.1.7. *Packet sniffing "passive eavesdropping"* ;
- 1.1.8. Captura de *banner*.

1.2. Coleta ativa, onde deverá ser utilizada:
- 1.2.1. *Port scanning* (Mapeamento de rede);
- 1.2.2. Varredura de vulnerabilidade

1.3. A varredura de vulnerabilidade deverá verificar/identificar, entre outros:
- 1.3.1. *Hosts* ativos na rede;
- 1.3.2. Portas e serviços em execução;
- 1.3.3. Serviços ativos e vulneráveis nos *hosts*;
- 1.3.4. Sistemas operacionais;
- 1.3.5. Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas;
- 1.3.6. Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
- 1.3.7. Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;
- 1.3.8. Identificação de vetores de ataque e cenários para exploração;
- 1.3.9. Vulnerabilidades detectadas (CVE);
- 1.3.10. Vulnerabilidades de alto risco;
- 1.3.11. Vulnerabilidades de médio risco;
- 1.3.12. Vulnerabilidades de baixo risco;
- 1.3.13. Informações a serem aplicadas na fase de ataques.

1.4. Serviços e aplicações web:
- 1.4.1. Uso indevido de sistema de arquivos e arquivos temporários;
- 1.4.2. Evasão de informação por configurações default de tratamento de erros;
- 1.4.3. Tratamento indevido de entrada;
- 1.4.4. Problemas relacionados à má configuração dos serviços;
- 1.4.5. Gerenciamento inseguro de sessões web.

2. Técnicas de exploração

2.1. Os seguintes tipos de ataques:
- 2.1.1. Violações do protocolo HTTP;

2.1.2. SQL injection ;
2.1.3. LDAP injection ;
2.1.4. Cookie tampering ;
2.1.5. Cross-site scripting (XSS);
2.1.6. XML eXternal Entity (XXE)
2.1.7. Directory transversal;
2.1.8. Buffer overflow;
2.1.9. OS command execution;
2.1.10. Command injection;
2.1.11. Remote code inclusion;
2.1.12. Expression Language Injection;
2.1.13. Server Side Request Forgery (SSRF)
2.1.14. Server side includes injection (SSI);
2.1.15. Server Side Template Injection (SSTI) (incluindo em APIs)
2.1.16. Prototype Pollution;
2.1.17. Desserialização em Java, PHP, DotNET, Python, NodeJS, entre outras linguagens;
2.1.18. HTTP Request Smuggling;
2.1.19. Exploração de GraphQL;
2.1.20. File disclosure ;
2.1.21. Information Leak;
2.1.22. Zero day attacks;
2.1.23. Contra protocolo TCP;
2.1.24. Ataques contra a aplicação.

2.2. Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas:
2.2.1. Bugs em serviços, aplicativos e sistemas operacionais;
2.2.2. SYN flooding ;
2.2.3. Fragmentação de pacotes de IP;
2.2.4. Smurf e fraggle ;
2.2.5. Teardrop, nuke e land;

2.3. Para ataques contra o protocolo TCP:
2.3.1. Sequestro de conexões;
2.3.2. Prognóstico de número de sequência do protocolo TCP;
2.3.3. Ataque de mitnick ;
2.3.4. Source routing.

2.4. Para ataques em nível da aplicação:
2.4.1. Buffer overflow ;
2.4.2. Problemas com o SNMP;
2.4.3. Vírus, worms e cavalos de Tróia.

2.5. Injeção de Código:
2.5.1. Ataques XSS (cross-site script);
2.5.2. Comprometimento do acesso remoto;
2.5.3. Manutenção de acesso;
2.5.4. Encobrimento de rastros da invasão.

3. Tipos de vulnerabilidades

3.1. Buffer overflow, Brute Force (HTTP Auth), Brute Force (Form Auth), Miscofiguration, Default Password usage;
3.2. Queries SQL de aplicações WEB, suscetíveis a SQL injection - tais como: Blind SQL, SQL Information Leakage, SQL Injection, SQL injection Auth Bypass, SQL Parameter Check;
3.3. Cross-Site-Scripting (XSS) - incluindo a detecção de vulnerabilidades em AJAX e WEB 2.0; Cross-site tracing (XST), DOM Cross-site scripting (XSS), Persistent Cross-site scripting (XSS) e Reflected Cross-site scripting (XSS), Cross Origin Resources Sharing (CORS) e Cross-Site Request Forgery (CSRF);
3.4. HTTP Strict Transport Security, HTTP Authentication over insecure channel, HTTPS Downgrade, HTTP Headers, HTTP Response Splitting, HTTP Verb Tampering e SSL Strength;
3.5. Cookie attributes, Credentials stored in clear text in a cookie, Credentials over an insecure channel, Directory Indexing, Forced Browsing e Sensitive data over an insecure channel;
3.6. Collecting Sensitive Personal Information , Information Disclosure in comments, Expression Language Injection, Secure and non-secure content mix, Autocomplete attribute, Sensitive Data Exposure, Form Session Strength, Email Disclosure e Business logic abuse attacks;
3.7. Server Configuration, Server Side Include (SSI) Injection, Nginx NULL code, OS Commanding, Parameter Fuzzing, ASP.NET Misconfiguration, ASP.NET ViewState security;
3.8. X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, XML External Entity Attack, XPath Injection e X-Powered-By;
3.9. Browser Cache directive (web application performance) e Browser Cache directive (leaking sensitive information), Local Storage Usage, File Inclusion;
3.10. Reverse Clickjacking, Reverse Proxy, Unvalidated Redirect, URL rewriting, Web Beacon, Information Disclosure in response, Information Leakage in responses, Arbitrary File Upload e Clients Cross-Domain Policy Files;
3.11. FrontPage Checks, Heartbleed Check, Java Grinder e PHP Code Execution, LDAP Injection;
3.12. Privacy Disclosure, Privilege Escalation e Information Disclosure in scripts;
3.13. Profanity, Reflection, Predictable Resource Location, Session Fixation, Session Strength, Source Code Disclosure.

4. Testes de ameaças

4.1. Protocol analyser: Enriquecidas com informações de vulnerabilidades conhecidas dos protocoles nas suas versões descobertas;
4.2. Port scanner: Enriquecidas com informações das aplicações similiar a nmap;
4.3. Wireless scanner: Contendo informações com SSID, criptografia e senhas default do fabricante, entre outros similares a Cain / Abel;
4.4. Network mapping: Com capacidade de plotar a topologia das relações da infraestructura resultante do descubrimento;
4.5. Banner grabbing: Com capacidade de determinar sistemas operacionais, suas aplicações e versões. Opcionalmente enriquecidas com informações adicionais de vulnerabilidades nas versões detectadas;

4.6. Network enumeration: Com capacidade de fazer descobrimentos em um range de ip de dispositivos com informações de suas características. Opcionalmente enriquecidas com informações do fabricante;
4.7. Vulnerability scanner: Enriquecido com informações scap das vulnerabilidades detectadas;
4.8. Compliance scanner: De forma agendada e com capacidade de configurações fora de conformidade acordados no planejamento e com possibilidade de aplicar restauração ou alternativas como isolamento ou bloqueio de portas, ou qualquer outro acionamento automático;
4.9. Password cracker: A ferramenta deve contar com dicionário de senhas ou realizar testes de forca bruta, ou qualquer outra técnica do estado da arte, para deteccao de senha fracas nos ativos inventariados na ferramenta;
4.10. Exploitation framework: A solução deve contar com diversas alternativas de estado da arte para realizar exploitation das vulnerabilidades detectadas de forma segura, similar a metasploit.

5. Tipos de Relatórios

5.1. Localização da vulnerabilidade (página e parâmetro);
5.2. Descrição detalhada, recomendações e várias referências e links;
5.3. Tráfego de solicitação e resposta no tráfego original e no ataque;
5.4. Vulnerabilidade destacada, tipo de ataque, valor original, valor do ataque e erro;
5.5. Capacidade de interagir com o aplicativo ativo e enviar e comparar new request / response traffic;
5.6. Baseline Comparison;
5.7. Highest Risk Vulnerabilities;
5.8. Risk Scorecard;
5.9. Remediation Plan;
5.10. Vulnerability Trends;
5.11. Nível de risco por plataforma e por vulnerabilidade;
5.12. Executivo (resumo gerencial para C-Levels);
5.13. Tendências que mostre a evolução das remediações nos ativos/sistemas varridos.

6. Fontes Mínimas de Pesquisa

O sistema deverá possuir mecanismo de captura automatizado de informações em diversas fontes da internet incluindo, no mínimo:

6.1. Mídias sociais:

6.1.1. Facebook;
6.1.2. Facebook ADS
6.1.3. Twitter;
6.1.4. LinkedIn;
6.1.5. Instagram;
6.1.6. TikTok;
6.1.7. Snapchat;
6.1.8. YoutTube;
6.1.9. Koo App;

6.1.10. Mastodon;
6.1.11. Pinterest;
6.1.12. Volo;
6.1.13. Bluesky;

6.2. Aplicações de mensageria instantâneas:
6.2.1. WhatsApp;
6.2.2. Telegram;
6.2.3. IRC;
6.2.4. Discord;
6.2.5. Slack;

6.3. Motores de busca:
6.3.1. Google;
6.3.2. Yahoo;
6.3.3. Bing;
6.3.4. DuckDuckGo;

6.4. Sites de e-commerce:
6.4.1. OLX;
6.4.2. Mercado Livre;

6.5. Lojas de aplicativos oficiais e não-oficiais:
6.5.1. Aptoide;
6.5.2. Google play/apkpure;

6.6. Fóruns de discussão:
6.6.1. Altenen;
6.6.2. Bestcarding Forum;
6.6.3. BHF;
6.6.4. Blackbones;
6.6.5. Bleepin computer
6.6.6. Breached;
6.6.7. CarderUK
6.6.8. Card Shops;
6.6.9. Caveiratech;
6.6.10. Chan;
6.6.11. Club2crd;
6.6.12. Cyber Carders
6.6.13. Eleaks;
6.6.14. Exploitin;
6.6.15. GodOne
6.6.16. Hackforums;
6.6.17. Leak Forums;
6.6.18. LeakedDataCC;
6.6.19. Patched;
6.6.20. Perfect Hackers;
6.6.21. Ramp;
6.6.22. Raid Forums;
6.6.23. Reddit;
6.6.24. RussianCarder
6.6.25. Russian Market

6.6.26. Shield
6.6.27. Sinister
6.6.28. VerifiedCarder
6.6.29. Xssls
6.6.30. 1877

6.7. Repositório de códigos:
6.7.1. GitHub;
6.7.2. Bitbucket;
6.7.3. GitLab;
6.7.4. SourceForge;

6.8. Indexadores de malware:
6.8.1. Anyrun;
6.8.2. Hybrid Analysis;
6.8.3. Malware Bazaar;
6.8.4. Ransomware;
6.8.5. Virus Total;
6.8.6. Vx-underground;

6.9. Serviços de paste:
6.9.1. Pastebin;
6.9.2. Ghostbin;
6.9.3. Dontpad;

6.10. Feed de Domínios:
6.10.1. CertStream;
6.10.2. Open Phish;
6.10.3. Phishtank;
6.10.4. Whoxy;
6.10.5. Zone Files IO;
6.10.6. Fuzzydns;
6.10.7. URL Scan;
6.10.8. URL haus;

6.11. Vulnerabilidades:
6.11.1. CVE;
6.11.2. Circl.lu;
6.11.3. Open Bug Bounty;
6.11.4. ExploitDB;

6.12. Serviços/Dispositivos de Rede:
6.12.1. Binary Edge;
6.12.2. Censys;
6.12.3. Shodan;
6.12.4. Zoom Eye;
6.12.5. LeakIX;
6.12.6. Zoom Eye;

6.13. Defacement:
6.13.1. MirrorH;
6.13.2. Zone-H;

6.14. Blogs de grupos de ransomware:
6.14.1. Arvin

6.14.2. Atomsilo
6.14.3. Against the West
6.14.4. Babuk
6.14.5. BianLian
6.14.6. Black Basta
6.14.7. Black Byte
6.14.8. Blackbyte Auction
6.14.9. BLACKCAT (ALPHVM)
6.14.10. Blackshadow
6.14.11. Bl@ckt0r
6.14.12. 54BB47H Blog
6.14.13. Cheers
6.14.14. Cl0p
6.14.15. Continews
6.14.16. CRYP70N1C0D3
6.14.17. Cuba
6.14.18. Daixin
6.14.19. Dark Leak
6.14.20. DataLeak
6.14.21. Donut
6.14.22. Entropy
6.14.23. Everest
6.14.24. Free Civilian
6.14.25. Grief
6.14.26. Hive
6.14.27. Industrial Spy
6.14.28. Karakurt
6.14.29. Kelvin Security
6.14.30. LapSus
6.14.31. LockBit
6.14.32. Lock Data
6.14.33. Lorenz
6.14.34. LV Blog
6.14.35. Mallox
6.14.36. Marketo
6.14.37. Medusa
6.14.38. Midas
6.14.39. Mindware
6.14.40. Moses
6.14.41. Night Sky
6.14.42. 0mega
6.14.43. Onyx
6.14.44. Pandora
6.14.45. Pay2Key
6.14.46. Payload.bin
6.14.47. Project Relic
6.14.48. Pysa

6.14.49. Qilin
6.14.50. Quantum
6.14.51. Ragnar Locker
6.14.52. Ransomexx
6.14.53. Ransom House
6.14.54. Red Alert
6.14.55. Revil
6.14.56. Rook
6.14.57. Royal Landing
6.14.58. Scattered Spider
6.14.59. ShinyHunters
6.14.60. Snatch
6.14.61. Suncrypt
6.14.62. Vendetta
6.14.63. Vice Society
6.14.64. Xing Locker
6.14.65. Yanluowang

6.15. Outros:

6.15.1. External Threats;
6.15.2. GrayhatWarfare;
6.15.3. ONION;
6.15.4. RSS;
6.15.5. The Pirate Bay;