ANEXO II – ESPECIFICAÇÕES TÉCNICAS

1. FINALIDADE

As informações contidas neste Anexo descrevem os requisitos gerais, quantitativos e características técnicas para aquisição de solução de Gestão de Vulnerabilidades, contemplando a contratação de licenças de uso, serviços de instalação, configuração e integração da solução, serviço de assistência suporte à solução, incluindo serviços de manutenção e atualização de versões dos componentes de software para o período de 48 (quarenta e oito) meses e repasse de conhecimento para a equipe da CONTRATANTE.

2. REQUISITOS TÉCNICOS

2.1. Descritivo da solução

ITEM	SUBITEM/ MÓDULOS	DESCRIÇÃO	PREVISÃO DE UTILIZAÇÃO DE LICENÇAS
1	1	**Solução de Gestão de Vulnerabilidades para Endpoints**, baseada e com análise contínua e adaptável de riscos e confiança.	**4875**
	2	**Solução de Gestão de Vulnerabilidades para FQDNs** Internos e Externos dos ativos de tecnologia da informação, baseada e com análise contínua e adaptável de riscos e confiança.	**105**
	3	**Solução de Gestão de Vulnerabilidades e Visibilidade de Ataques em tempo real para Estrutura de Diretório de Usuários** baseada e com análise contínua e adaptável de riscos e confiança.	**23.500**
2		Implantação **(ANEXO III – PLANO DE IMPLANTAÇÃO)**	1
3		Suporte e Assistência Técnica **(ANEXO IV – Suporte e Assistência Técnica)**	48 meses
4		Serviço de Treinamento	1

Tabela 1 - Itens da Solução

Dado o regime de contratação Empreitada por preço unitário, o quantitativo de licenças dos subitens/módulos é meramente referencial que deverão ser aferidos e pagos de acordo com as medições.

2.2. Requisitos da Ferramenta de Gestão de Vulnerabilidade (Item 1)

2.2.1. **Licenciamento e arquitetura**

2.2.1.1. A solução deverá ser capaz de descobrir, avaliar, priorizar e gerenciar vulnerabilidades em estações de trabalho e servidores, ativos de rede, dispositivos de segurança, *hypervisors*, máquinas virtuais, orquestradores de contêineres, contêineres, ativos de nuvem (Microsoft Azure, Google Cloud Plataform e Amazon Web Services) e aplicações Web e API, proporcionando, através de única interface, o gerenciamento centralizado de todos os ativos, sem a necessidade de incorrer em consoles ou componentes adicionais fora dele para a administração dos serviços oferecidos;

2.2.1.2. A solução deve ser entregue como serviço SaaS (Software-as-a-Service) em uma nuvem própria do fabricante para todos os seus serviços e módulos exigidos neste documento (e seus anexos). Serviços fornecidos por nuvens de terceiros não serão aceitos;

2.2.1.3. Todos os dados e metadados gerados na solução devem ser armazenados obrigatoriamente em território brasileiro, em conformidade com a Instrução Normativa Nº 5, de 30 de agosto de 2021;

2.2.1.4. A Contratada deve entregar todas as licenças de software necessárias, atendendo as especificações recomendadas pelo fabricante durante toda a vigência do contrato, considerando o cenário de utilização de todo o volume de licenças previsto no edital;

2.2.1.5. O licenciamento da plataforma deverá ser por ativo, englobando: estações de trabalho e servidores, ativos de rede, dispositivos de segurança, hypervisors, máquinas virtuais, contêineres, ativos de nuvem e aplicações Web e API;

2.2.1.6. O licenciamento poderá ser flexível, ou seja, não limitado por módulo;

2.2.1.7. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados;

2.2.1.8. A garantia da solução ofertada deve permitir a atualização de versões de software pelo período de 48 (quarenta e oito) meses, contados a partir da emissão do Termo de Aceitação Definitivo (TAD).

2.2.1.9. A solução deverá suportar a instalação em Ambiente virtualizado. A infraestrutura tecnológica do Banco do Nordeste (VMWare ESXi) poderá ser utilizada para suportar a instalação da solução. Licenças dos sistemas operacionais Windows Server e Red Hat Enterprise Linux não precisam ser ofertadas nesse cenário;

2.2.1.10. A solução deverá ser ofertada de maneira redundante, isto é, devem estar instaladas em ambos os datacenters;

2.2.1.11. Todos os componentes de software requeridos para atender às funcionalidades exigidas neste Edital devem ser fornecidos, inclusive licenças de Bancos de Dados, caso sejam necessárias;

2.2.1.12. A solução deve suportar API (Application Programming Interface) para automação de processos e integração com aplicações terceiras (que estão em ambiente on-Premise e soluções de segurança de mercado adotadas pelo Banco);

2.2.1.13. A solução deve ser capaz de se integrar e disponibilizar insumos para soluções de correlação de eventos externa (SIEM);

2.2.1.14. A solução deve possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados, conforme estabelecido na Instrução Normativa Nº 5, de 30 de agosto de 2021.

2.2.2. **Console de gerenciamento**

2.2.2.1. A solução deve ser licenciada para realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e identificar falhas de conformidade (baseline e compliance) e indícios de padrões de códigos maliciosos conhecidos (malware);

2.2.2.2. Deve ter administração centralizada por console único de gerenciamento;

2.2.2.3. As configurações de todos os módulos e criação de relatórios deverão ser realizadas através da mesma console;

2.2.2.4. O gerenciamento da solução deve ser baseado em plataforma WEB, com acesso via navegadores de mercado (Google Chrome, Microsoft Edge e Firefox), utilizando comunicação criptografada (HTTPS/TLS, versão 1.2 ou superior);

2.2.2.5. Deve ter a capacidade para criação das contas de usuário no console de gerenciamento com diferentes níveis de acesso;

2.2.2.6. Deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional;

2.2.2.7. Deve permitir configurar quais usuários ou grupos de usuários tem permissão de visualizar determinados ativos da organização e suas vulnerabilidades, e quais tem permissão de executar scans de vulnerabilidades nesses ativos;

2.2.2.8. Deve suportar autenticação de dois fatores para login;

2.2.2.9. Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados;

2.2.2.10. Deve possuir as senhas do sistema com hash e criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados;

2.2.2.11. Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas.

2.2.3. **Implementação e gerenciamento do agente**

2.2.3.1. A solução deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede;

2.2.3.2. A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede corporativa e na nuvem;

2.2.3.3. O agente deve ser suportado, no mínimo, nos seguintes Sistemas Operacionais:

- Microsoft: Windows 7 SP1, Windows 8 ou 8.1, Windows 10 ou superior, Windows Server 2008 R2 e versões superiores;
- Apple: MAC OS X 10.15.0 e versões superiores;
- Linux: Red Hat Enterprise 6 ou superior, CentOS 6.5+ ou posterior, Debian 9 ou superior, Ubuntu 14 ou superior, Oracle Solaris 10 ou superior, FreeBSD.

2.2.3.4. O agente deve suportar plataformas de nuvem Microsoft Azure, AWS (Amazon Web Services) e GCP (Google Cloud Platform), e possuir conectores compatíveis para atendê-las;

2.2.3.5. A solução deve fornecer agentes prontos para instalação compatível com os principais sistemas operacionais do mercado, para monitoramento de configurações e vulnerabilidades;

2.2.3.6. A gerência da solução deverá ser responsável pela distribuição (deploy), instalação, gerenciamento e desinstalação do agente nas estações, ou suportar o uso do Microsoft System Center Configuration Manager para este fim;

2.2.3.7. Deve ser capaz de coletar informações sobre o inventário dos ativos;

2.2.3.8. As funcionalidades de gestão de ativos, gestão de vulnerabilidade e detecção de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes;

2.2.3.9. Deve prover nativamente um dispositivo (conector) capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma;

2.2.3.10. Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento;

2.2.3.11. Deve permitir a definição de um período global de inatividade dos agentes;

2.2.3.12. O acesso a console de gerenciamento deve ser fornecida para pelo menos 10 usuários simultâneos;

2.2.4. **Requisitos gerais – comum a todos os subitens/módulos**

2.2.4.1. A solução deve possuir canais de comunicação autenticados e criptografados de ponta a ponta entre os componentes do sistema, bem como a transferência de dados e a sincronização da solução, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256;

2.2.4.2. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com todos os ativos gerenciados, propiciando um panorama completo sobre as vulnerabilidades existentes e de forma a permitir direcionar esforços para mitigação,

com fins de atingir melhores níveis de segurança cibernética para o ambiente de TI da organização;

2.2.4.3. A solução deve ser capaz de orquestrar scanners ilimitados dentro da infraestrutura;

2.2.4.4. A solução deve permitir agrupamento de scanners para facilitar o gerenciamento e aplicação de políticas;

2.2.4.5. A solução deve possibilitar, por meio da console, no mínimo 4 (quatro) métodos de escaneamento: scan ativo (autenticado ou não), scan com uso de agentes, scan passivo e scan em nuvem;

2.2.4.6. A solução deve incluir possibilidade de gerenciamento de scans: execução, agendamento, exceções, frequências, horários e periodicidade;

2.2.4.7. A solução deve possuir modelos (templates) prontos de scans e também deve ser possível a criação de modelos personalizados;

2.2.4.8. A solução deve permitir scans sob demanda para um ou mais ativos, de forma manual ou automatizada, sem limite de execuções;

2.2.4.9. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para, no mínimo, banco de dados, hypervisors, dispositivos de rede, endpoints e aplicações;

2.2.4.10. A solução deve ser capaz de realizar escaneamento de descoberta de rede utilizando os seguintes critérios como alvo: IP, CIRD e Range;

2.2.4.11. A solução deve ser capaz de realizar a descoberta de serviços utilizando os seguintes critérios: sondagem de todas as portas para encontrar serviços e procura por serviços baseados em SSL/TLS;

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

2.2.4.13. A solução deve capaz de classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante;

2.2.4.14. A solução deve permitir a avaliação de certificados digitais e configurações de TLS em busca de problemas e vulnerabilidades de certificados, resultando em diferentes graus de conformidade de acordo com os resultados da avaliação de seu emissor, prazo de validade, tipo de certificado, robustez de algoritmo e conjunto de criptografia usados;

2.2.4.15. A solução deve permitir a utilização de operadores lógicos na busca de informações de um determinado ativo para que seja possível encontrar, no mínimo, características como: sistema operacional, tipo de vulnerabilidade, criticidade do ativo, determinado software instalado;

2.2.4.16. A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, características como: que tenham associação com ransonware e patches disponíveis, em um determinado segmento de rede, em serviços específicos, em hardware específico;

2.2.4.17. A solução deve possuir a habilidade de etiquetagem (tags) de ativos para facilitar a identificação, permitindo a geração de tags de, no mínimo, os seguintes parâmetros: palavras-chave, segmento de rede, portas abertas, sistema operacional e softwares instalados;

2.2.4.18. A solução pode possibilitar a configuração de quais usuários ou grupos de usuários podem editar as Tags;

2.2.4.19. A solução deve possibilitar o uso das Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada Tag;

2.2.4.20. A solução deve fornecer informações detalhadas sobre a natureza das vulnerabilidades encontradas, bem como evidências de sua existência e recomendações para mitigá-las;

2.2.4.21. A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL);

2.2.4.22. A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade CVSS (Common Vulnerability Scoring System), sendo que deve possuir uma base de dados capaz de identificar no mínimo 50.000 CVEs, devendo ser atualizada periodicamente;

2.2.4.23. A solução deve atribuir a todas as vulnerabilidades uma severidade baseada no score do CVSSv3;

2.2.4.24. A solução deve calcular a criticidade e priorização de vulnerabilidades com base nos dados dos ativos, de preferência utilizando algoritmos de inteligência artificial (IA);

2.2.4.25. A solução deve atribuir uma pontuação para cada um dos ativos, onde devem ser levadas em conta as vulnerabilidades presentes naquele ativo, assim como sua classificação (peso do ativo);

2.2.4.26. A solução deve fornecer fontes de inteligência de ameaças em tempo real, além de técnicas de aprendizado de máquina para fornecer dados agregados e relacionados a vulnerabilidades encontradas nos ativos da organização, com capacidade de apontar o risco, a criticidade e priorizações, identificando quais corrigir primeiro;

2.2.4.27. A solução deve possuir mecanismo de priorização sujeito a modificações e atualizações diárias com base em inteligência de ameaças e observação de tendências na Internet;

2.2.4.28. A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS e CVE;

2.2.4.29. A solução deve ser capaz de indicar exploits e códigos disponíveis para uma determinada vulnerabilidade, quando aplicável;

2.2.4.30. A solução deve entregar serviços como “maturidade de avaliação”, orientação para remediação (*playbooks*) e ser capaz de efetuar cálculos e exibição de índices de exposição a vulnerabilidades;

2.2.4.31. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

2.2.4.32. A solução pode permitir a segregação lógica entre áreas distintas da organização a fim de obter a pontuação referente à exposição cibernética por área;

2.2.4.33. A solução pode permitir a segregação lógica entre aplicações ou grupo de aplicações distintas da organização a fim de obter a pontuação referente à exposição cibernética por aplicação;

2.2.4.34. A solução deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

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

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

2.2.4.37. A solução deve possibilitar alterar a classificação do ativo (atribuição de pesos diferentes) de forma manual, podendo sobrescrever a classificação atribuída automaticamente pelo sistema;

2.2.4.38. A solução deve permitir a exclusão de vulnerabilidades encontradas em uma porta ou serviço que não está em execução;

2.2.4.39. A solução deve permitir a exclusão de vulnerabilidades que não são exploráveis devido à configuração do sistema/plataforma onde foi detectada;

2.2.4.40. A solução deve apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

2.2.4.41. Quanto à análise de ataques exploráveis, a solução deve disponibilizar visibilidade nas técnicas de ataque baseado no framework MITRE ATT&CK, identificando sua criticidade, em no mínimo: alto, médio e baixo;

2.2.4.42. A solução deve prover a evidência relacionada a descoberta do ataque, apresentando informações do objeto relacionado a este, além de disponibilizar detalhamento de mitigação para o ataque em análise;

2.2.4.43. A solução deve permitir upgrade e aplicação de patches sem parada ou comprometimento de disponibilidade dos sistemas envolvidos;

2.2.4.44. As atualizações de serviço deverão ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados;

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

2.2.4.46. A solução deve garantir a inviolabilidade no armazenamento, tráfego, e eventual manuseio dos dados durante qualquer intervenção técnica a ser realizada;

2.2.4.47. Quanto à criptografia de tráfego em trânsito, a solução deve garantir conectividade privada e segura entre as partes envolvidas;

2.2.4.48. Quanto ao armazenamento dos dados em repouso, a solução deve criptografar todos os resultados provenientes de varreduras;

2.2.5. **Requisitos específicos – Endpoints (subitem/módulo 1)**

2.2.5.1. A solução deve permitir scans de vulnerabilidades baseadas em: IP ou ranges de IP, sistemas operacionais, serviços Web, portas TCP e UDP, serviços, aplicações, banco de dados e tipos de dispositivos de rede, incluindo switches, roteadores e balanceadores de carga;

2.2.5.2. A solução deve ser capaz de detectar e analisar vulnerabilidades, no mínimo, nos seguintes sistemas operacionais: Microsoft Windows, Linux e MacOS;

2.2.5.3. A solução deve ser capaz de detectar e analisar vulnerabilidades, no mínimo, nos seguintes bancos de dados: Microsoft SQL Server, MySQL, PostgreSQL, IBM DB2, Oracle Database;

2.2.5.4. A solução deverá ser capaz de detectar e analisar vulnerabilidades em aplicativos desktop em geral;

2.2.5.5. A solução deve ser capaz de detectar e analisar vulnerabilidades em aplicativos comerciais diversos e proprietários, incluindo, mas não limitando-se a: Java, Adobe, Oracle, Apple, Microsoft, Check Point, Palo Alto Networks, Cisco, Fortinet, Fireeye, McAfee etc;

2.2.5.6. A solução deve suportar o uso de SMB e WMI para verificação de sistemas Microsoft Windows;

2.2.5.7. A solução deve ser capaz de iniciar e parar automaticamente serviços de registro remoto em sistemas Windows ao executar um scan credenciada;

2.2.5.8. O scanner deve oferecer suporte a shell seguro (SSH) com a capacidade de escalar privilégios para varredura de vulnerabilidades e auditorias de configuração em sistemas Unix;

2.2.5.9. A solução deve suportar o uso do netstat (Linux) e WMI (Windows) para uma enumeração rápida e precisa de portas em um sistema quando as credenciais são fornecidas;

2.2.5.10. A solução deve possibilitar a verificação remota de portas, além da enumeração local de portas, para ajudar a determinar se algum mecanismo de controle de acesso está sendo utilizado;

2.2.5.11. A solução deve fornecer auditoria de patch (MS Bulletins) para as principais versões de Windows e para todos os principais sistemas operacionais Unix incluindo Mac OS, Linux, Solaris e IBM AIX;

2.2.5.12. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

2.2.5.13. A solução deve permitir o envio de alertas em tempo real sobre irregularidades na rede, identificando ameaças e monitorando mudanças inesperadas;

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

2.2.5.15. A solução deve permitir visibilidade a respeito de hosts que executam contêineres e contêineres em execução.

2.2.5.16. A solução deve correlacionar vulnerabilidades e patches automaticamente para os hosts da organização;

2.2.5.17. A solução deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente;

2.2.5.18. A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas.

2.2.6. **Requisitos específicos – FQDNs/APLICAÇÕES WEB (SUBITEM/MÓDULO 2)**

2.2.6.1. A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

2.2.6.2. A solução deve ser capaz de executar scans em sistemas web através de seus endereços FQDN/URL;

2.2.6.3. A solução deve habilitar scans profundos e dinâmicos para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa interna, externa e instâncias de nuvem;

2.2.6.4. A solução deve ter capacidade de encontrar aplicações web aprovadas e não aprovadas na rede, gerando um processo contínuo de catalogação e descoberta de aplicações web;

2.2.6.5. A solução deve ser capaz de detectar e analisar vulnerabilidades, no mínimo, nas seguintes plataformas de aplicações web: Microsoft IIS, Apache, Apache Tomcat, NGINX, IBM WebSphere, IBM HTTP Server IHS, JBoss, Flask, DJango;

2.2.6.6. Deve ser capaz de identificar e classificar vulnerabilidades de máquinas virtuais em nuvem pública em infraestruturas como serviço nas plataformas AWS, Microsoft Azure e Google Cloud;

2.2.6.7. A solução deve permitir scans autenticados, complexos e progressivos;

2.2.6.8. Cada licença deve possibilitar a análise de vulnerabilidades de todas as URIs (Uniform Resource Identifier) dentro de uma mesma URL (FQDN);

2.2.6.9. A solução deve avaliar sistemas web utilizando protocolos HTTP e HTTPS;

2.2.6.10. A solução deve suportar scans programados de serviços SOAP e REST API;

2.2.6.11. A solução deve realizar scan e auditar, no mínimo, os seguintes elementos: cookies, headers, formulários e links, nomes e valores de parâmetros da aplicação, elementos JSON e XML, elementos DOM;

2.2.6.12. A solução deve exibir os resultados agregados de acordo com as categorias do OWASP Top 10 e PCI (Payment Card Industry Data Security Standard) para detectar, identificar, avaliar e rastrear os 10 principais riscos, como também ameaças de WASC e fragilidades CWE/CVEs associados em aplicações web;

2.2.6.13. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF etc), a solução deve evidenciar nos detalhes do evento encontrado: Payload injetado, evidência em forma de resposta da aplicação, detalhes da requisição HTTP e detalhes da resposta HTTP;

2.2.6.14. A solução deve fornecer detalhes das vulnerabilidades que contenham descrição da falha e referências didáticas, como também soluções propostas para mitigação ou remediação destas vulnerabilidades;

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

2.2.6.16. A solução deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

2.2.6.17. A solução deve contar com uma API e integração com Jenkins para automação em um ambiente de CI/CD;

2.2.6.18. A solução deve possuir importação de arquivos .YARA;

2.2.6.19. A solução deve consolidar os dados de scans automatizados da solução com dados de ferramentas que permitem a avaliação manual de vulnerabilidades, para uma visão unificada de vulnerabilidades de aplicações web detectadas automática e manualmente;

2.2.6.20. A solução deve permitir integração nativa com as principais ferramentas de WAF do mercado, dentre estas: F5, Checkpoint, Fortinet, Forcepoint, Cisco etc.

2.2.6.21. A solução deve fornecer informações acerca da disponibilidade de códigos de exploração das vulnerabilidades encontradas em frameworks de exploração para as plataformas mais populares: Core, Metasploit e Canvas;

2.2.7. **Requisitos específicos – ESTRUTURA DE DIRETÓRIOS (SUBITEM/MÓDULO 3)**

2.2.7.1. A solução deve identificar fraquezas ocultas em configurações dedicadas ao Microsoft Active Directory (AD);

2.2.7.2. A solução deve possuir ações preventivas de hardening para o AD;

2.2.7.3. A solução deve identificar ataques específicos para a estrutura do AD;

2.2.7.4. A solução deve possuir funcionalidade para analisar em detalhes cada configuração incorreta do AD que acarreta riscos de segurança e fornecer recomendações para sua correção;

2.2.7.5. A solução deve permitir a correlação de mudanças no Active Directory e desvios de segurança;

2.2.7.6. A solução deve possuir dashboard com os principais ataques e vulnerabilidades por domínio;

2.2.7.7. A solução não deve armazenar ou sincronizar nenhuma credencial de objetos do AD;

2.2.7.8. A solução deve descobrir e mapear a superfície de ataque do Active Directory e seus domínios monitorados sem depender de agentes ou sensores para coleta de informações do AD;

2.2.7.9. A solução deve seguir as boas práticas de menor privilégio, a conta de serviço utilizada para conexão com o AD, sendo o menor nível de acesso esperado para a conta de serviço como parte do grupo Domain User;

2.2.7.10. A solução deve analisar continuamente a postura de segurança do AD, validando no mínimo:

- Contas desativadas em grupos privilegiados,
- Contas com senhas que nunca expiram,
- Uso de senhas reversíveis em contas de usuário,
- Utilização de protocolo criptográfico fraco (ex.: DES) em contas de usuário,
- Uso do LAPS (solução de senha de administrador local) para gerenciar senhas de contas locais com privilégios,
- Contas de usuário utilizando senha antiga,
- Se o atributo AdminCount está definido em usuários padrão,
- Uso recente da conta de administrador padrão,
- Usuários com permissão para ingressar computadores no domínio,
- Contas dormentes,
- Contas que possuem um atributo perigoso de histórico SID (SID History),
- Última alteração de senha do KDC,
- Última alteração da senha da conta SSO do Azure AD,
- Contas que podem ter senha em branco/vazia,
- Utilização do grupo nativo Protected Users,
- Possível uso de senha em clear-text,
- Uso de algoritmos de criptografia fracos na PKI do AD,
- Contas de serviço com SPN (Service Principal Name) que fazem parte de grupos privilegiados,
- Contas anormais nos grupos administrativos padrão do AD,
- Delegação Kerberos perigosa,
- Políticas de senhas fracas aplicadas aos usuários,
- Permissões relacionadas às contas do Azure AD Connect,
- Controladores de domínio gerenciados por usuários ilegítimos,
- Validação de certificado mapeado através de atributo altSecurityIdentities em contas privilegiadas,
- Uso de protocolo Netlogon inseguro (Zerologon/CVE-2020-1472),
- Domínio sem GPOs de proteção de computador, desativando protocolos vulneráveis antigos, como NTLMv1,
- Uso de senhas reversíveis em GPOs;
- Sanidade das GPOs e componentes CSEs (Client-Side Extension),
- Permissões em GPOs sensíveis associadas aos Containers Configuration, Sites, Root Partition e OUs sensíveis como Domain Controllers;

2.2.7.11. A solução deve monitorar continuamente os indicadores de possíveis ataques como: DCSync, DCShadow, Password Spraying, Password Guessing/Brute Force, Lsaas Injecton nos controladores de domínio, Golden Ticket, NTLM Relay, entre outros

2.2.7.12. A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;

2.2.7.13. A solução deve permitir a criação de listas de exclusões, suportando minimamente exclusão por domínios do AD monitorados e por itens analisados.

2.2.8. **Relatórios, Dashboards e Auditoria**

2.2.8.1. A solução deve apresentar um painel de controle para visualização dos relatórios;

2.2.8.2. A solução deve permitir agrupar, filtrar e classificar relatórios;

2.2.8.3. A solução deve permitir exportar relatórios, no mínimo, para formato PDF, HTML, DOC, XML ou CSV;

2.2.8.4. A solução deve ter capacidade de enviar relatórios por e-mail via agendamento (datas específicas e periodicamente);

2.2.8.5. A solução deve ter a capacidade para configurar, salvar relatórios e painéis de controle personalizados por usuário;

2.2.8.6. A solução deve ter opção de publicar relatórios salvos para todos os usuários ou mantê-los como relatórios pessoais;

2.2.8.7. A solução deve suportar reter os eventos coletados por no mínimo um ano;

2.2.8.8. A solução deve permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos;

2.2.8.9. A solução deve gerar relatórios por IPs, Grupo e Tags;

2.2.8.10. A solução deve possuir relatórios pré-configurados com as seguintes informações: ativos verificados sem credencias; Top "n" vulnerabilidades mais críticas; Top "n" ativos exploráveis por malwares; vulnerabilidades críticas e exploráveis; ativos com vulnerabilidades que podem ser exploradas;

2.2.8.11. A solução deve permitir gerar relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório;

2.2.8.12. A solução deve permitir gerar relatórios que possibilitem o cálculo de risco do negócio, utilizando para o cálculo o risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório;

2.2.8.13. A solução deve permitir a geração de relatórios que possibilite avaliar a configuração segura de sistemas e aplicações, e a conformidade com as melhores práticas de segurança, com base nos padrões da indústria, no mínimo para: CIS Benchmarks, NIST, ISO/IEC 27001, HIPAA (Health Insurance Portability and Accountability Act) e PCI DSS (Payment Card Industry Data Security Standards);

2.2.8.14. A solução deve permitir a customização de dashboards fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades;

2.2.8.15. A solução deve fornecer dashboards executivos personalizáveis com uma visão unificada de todos os componentes do sistema;

2.2.8.16. A solução deve fornecer dashboards que contenham quantidades de vulnerabilidades associadas a ransonware, que contém exploits públicos e que permitem exploração sem autenticação;

2.2.8.17. Deve possuir logs detalhados de auditoria de atividade de transações do banco de dados;

2.2.8.18. Deve possuir logs detalhados de auditoria de criação/alteração/exclusão de scans;

2.2.8.19. A solução deve permitir que os registros em trilha de auditoria tenham proteção contra violação de confidencialidade e integridade, ou seja, somente deve ser possível sua consulta a usuários autorizados e não deve ser possível operações de alteração e exclusão.

3. O **Plano de implantação (ITEM 2)** da solução contratada está descrito no **ANEXO III – Plano de Implantação**

4. O **Serviço de Suporte e Assistência técnica (ITEM 3)** da solução contratada estão descritos no **ANEXO IV– Suporte e Assistência técnica**

5. SERVIÇO DE TREINAMENTO (ITEM 4)

5.1. O Contratado deve fornecer treinamento em formato virtual e online (ao vivo) para duas turmas de até 15 colaboradores indicados pelo Banco, contemplando, no mínimo:

5.1.1. Guia passo a passo para a instalação correta da ferramenta, incluindo configuração inicial e requisitos de sistema.

5.1.2. Configuração Personalizada: Ajustes e configurações específicas para atender às necessidades do ambiente do Banco.

5.1.3. Gerenciamento de Usuários: Criação, modificação e remoção de usuários, além de gerenciamento de permissões e papéis

5.1.4. Execução de Scans: Procedimentos para executar varreduras de vulnerabilidades em diferentes cenários;

5.1.5. Resolução de Problemas Comuns: Soluções para problemas recorrentes que os operadores possam encontrar no dia a dia, erros de configuração e interpretação de resultados.

5.1.6. Geração de Relatórios: Criação e personalização de relatórios de vulnerabilidade, com foco em diferentes públicos-alvo, tais como equipes técnicas, gerenciais e executivas.

5.1.7. Monitoramento Contínuo: Implementação de processos de monitoramento contínuo para identificar e mitigar vulnerabilidades em tempo real.

5.1.8. Atualização da Ferramenta: Procedimentos para manter a ferramenta atualizada com as últimas versões e patches de segurança.

5.1.9. Boas Práticas de Segurança: Orientações sobre as melhores práticas para garantir a eficácia da ferramenta e a segurança do ambiente do Banco.

5.2. A carga horária mínima de cada turma deve ser de 40 (quarenta) horas, respeitando o limite de 4 (quatro) horas por dia;

5.3. O treinamento de cada turma deverá ser iniciado em até 30 (trinta) dias corridos, após a solicitação do Banco do Nordeste;

5.4. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático) serão de exclusiva responsabilidade do Contratado.

5.5. O material didático deve ser fornecido em mídia eletrônica, em formatos padrão de mercado (PDF, DOC, HTML ou PPT).