ANEXO II
QUANTITATIVO E CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO

1. FINALIDADE

As informações contidas neste anexo descrevem os requisitos da Solução de Antimalware que é objeto deste Edital. Os requisitos para o fornecimento da Solução especificados neste documento têm caráter obrigatório, devendo ser rigorosamente atendidos pelos licitantes. O não atendimento a quaisquer das exigências, por completo ou em parte, desclassifica a proposta e sujeitará o licitante à aplicação de sansões contratuais.

2. TERMOS E DEFINIÇÕES

2.1. **Banco**
O termo *Banco* deverá ser compreendido como referência ao Banco do Nordeste do Brasil S/A.

2.2. **BNB**
O termo *BNB* deverá ser compreendido como referência ao Banco do Nordeste do Brasil S/A.

2.3. **Solução**
É o conjunto de todos os requisitos e componentes (*hardwares*, *softwares* e serviços) que se integram para a satisfação plena do objeto desta contratação.

2.4. **Requisitos da Solução**
Conjunto de especificações que necessariamente devem ser satisfeitas pela proposta do Licitante.

2.5. **Malware**
Qualquer tipo de *software* ou *script* malicioso destinado a prejudicar sistemas computacionais por meio da destruição, modificação, espionagem, furto, roubo, propagação, sequestro etc de dados e informações.

2.6. **EDR**
Ferramenta que monitora em tempo real e analisa os dados de dispositivos (endpoints) podendo responder continuamente para mitigar ameaças cibernética.

2.7. **Agente**
Componente da ferramenta de proteção de antimalware que é instalado nos dispositivos (endpoints).

2.8. **CAPGV**
Acrônimo de *Centro Administrativo Presidente Getúlio Vargas*. É o campus onde funciona a direção geral do Banco e onde ficam os Centros de Dados (*datacenters*) primário e secundário da corporação, localizados no município de Fortaleza - CE cujo endereço é Avenida Doutor Silas Munguba, nº 5.700, bairro Passaré, CEP 60.743-902.

2.9. **Unidades Distribuídas**
Todas as unidades do Banco, incluindo agências, superintendências e centrais.

2.10. **Dias úteis**
Os dias úteis considerados para os fins deste Edital são os que não forem sábado nem domingo e não constarem das tabelas de feriados nacionais, do estado do Ceará e do município de Fortaleza/CE.

2.11. ***End-Of-Life (EOL)***
Data em que é encerrada a produção ou comercialização de um dado produto pelo seu fabricante.

2.12. ***End-Of-Support (EOS)***
Data em que são encerrados ou limitados os serviços de garantia, suporte e manutenção corretiva de um dado produto pelo seu fabricante.

3. COMPOSIÇÃO DA SOLUÇÃO

3.1. A Solução deverá ser composta de:

3.1.1. Solução de Antimalware:

- **Ferramenta de Antimalware**: componentes de software que implementem as funcionalidades de combate e prevenção a malwares;
- **Serviço de Implantação da Solução**: implantação de todos os componentes da Solução.
- **Serviço de Suporte Técnico**: banco de horas de 300 horas (60 horas anuais);
- **Serviço de Treinamento da Solução**: 2 turmas de treinamento remoto de, no mínimo, 30 horas para 12 (doze) participantes cada turma.
- **Serviço de Assistência Técnica**: prestado pelo prazo de 60 (sessenta) meses.

4. REQUISITOS GERAIS DA SOLUÇÃO

4.1. Os REQUISITOS GERAIS DA SOLUÇÃO aplicam-se à Solução considerada em sua totalidade.

4.2. Os requisitos constantes deste documento têm caráter obrigatório devendo ser rigorosamente atendidos pelos fornecedores sob pena de desclassificação da proposta e sujeição à aplicação de sanções contratuais.

4.3. Todos os componentes da Solução deverão constar do catálogo de produtos do respectivo fabricante.

4.4. No momento da apresentação das propostas, todos os componentes constantes da Solução deverão possuir EOL (*End-of-life*) e EOS (*End-of-support*) não definidos ou anunciados para um prazo superior a 36 (trinta e seis) meses.

4.5. Todos os componentes da Solução deverão ser propostos e fornecidos com a versão mais atualizada dos *softwares* e *firmwares* considerando-se, respectivamente, a data do pregão e a data da implantação da Solução.

4.6. Todos os componentes da Solução deverão ser fornecidos para o ambiente de homologação.

4.7. Todos os componentes da Solução deverão guardar total compatibilidade entre si, não podendo o Licitante alegar eventuais incompatibilidades de qualquer ordem para deixar de cumprir os requisitos do Edital.

4.8. Todas as funcionalidades requeridas neste Edital deverão estar licenciadas e disponíveis para seu uso pleno tendo em vista a totalidade dos recursos da Solução, salvo quando o Edital dispuser especificamente de outra forma.

4.9. A proposta do Licitante deverá conter, obrigatoriamente, um relatório denominado Relação de Componentes, que deverá relacionar todos os componentes da Solução (*hardware* e *software*) discriminando, no mínimo, as seguintes informações: marca, modelo, descrição, unidade, quantidade e *part number*.

4.10. Mesmo que não estejam diretamente especificados neste documento, deverão ser fornecidos todos os componentes necessários para o cumprimento dos requisitos do Edital, tais como mídias de *software*, licenças de *software*, mão de obra especializada, transporte de recursos humanos, seguros, meios de comunicação, hardware, etc. Esses componentes serão automaticamente incorporados à Solução sempre que forem necessários ao seu pleno funcionamento sem que isso incorra em qualquer tipo de ônus para o BNB.

4.11. A composição da Solução deverá estar de acordo com as melhores práticas estabelecidas pelo fabricante dos componentes para o porte da Solução ofertada e em conformidade com os níveis de serviço exigidos pelo Edital.

4.11.1. Não serão aceitas Soluções que estejam formatadas de forma diversa das práticas preconizadas pelo fabricante dos componentes.

4.11.2. Para o estabelecimento da melhor prática considerar sempre o cenário que traga mais vantagens para o BNB, principalmente em termos de segurança.

4.11.3. As melhores práticas deverão constar da documentação técnica oficial e pública do fabricante dos componentes.

4.12. Não será permitida a oferta de *softwares livres,* ou cujas edições sejam baseadas no desenvolvimento realizado por comunidades.

4.13. Todos os componentes da Solução deverão guardar total compatibilidade entre si não podendo o Licitante alegar eventuais incompatibilidades de qualquer ordem para deixar de cumprir os requisitos do Edital.

4.14. Todos os componentes e serviços da Solução deverão possuir garantia de 60 (sessenta) meses contra defeito de fabricação e mau funcionamento contados a partir da data de assinatura do contrato.

4.15. Os Licitantes poderão valer-se do licenciamento perpétuo do *software* da Solução que o BNB possui (discriminado abaixo) para compor a proposta da Solução de Antimalware desde que o modelo de licenciamento ofertado esteja em conformidade com todos os requisitos deste documento. Essa possibilidade não afasta nenhum requisito presente neste Edital.

Part Number	Descrição	Quantidade
SES-PSE-SUB	Symantec Protection Suite Enterprise	18.000
EML-CDL-SUB	Symantec messaging gateway (4 appliances virtuais: 3 Scanner e 1 Control Center);	18.000
SMS-EXC-Premium	Symantec mail security for microsoft exchange (Agente instalado nos servidores de Exchange)	18.000
SEP-EE-SUB	Symantec Endpoint Protection (Console (2 servidores Virtuais)+ o agente em todos os desktop e servidores, inclusive Linux)	18.000

4.16. O Banco realizará a desativação do agente que compõem a Solução anterior ao contrato. Caso haja conflito com o agente da nova solução, a Contratada será responsável por realizar a desinstalação nos dispositivos clientes da ferramenta de Antimalware que compõem a Solução anterior ao contrato

4.16.1. O processo de desativação/desinstalação deverá ocorrer de forma simultânea à instalação das ferramentas da Solução contratada de forma que os dispositivos e serviços do BNB não sejam expostos aos riscos de contaminação de *malwares*.

4.16.2. O processo de desinstalação deverá contemplar a exclusão digital dos dispositivos de gravação.

4.16.3. A desinstalação poderá ocorrer de forma remota desde que seja realizada por equipe que esteja fisicamente presente no Centro Administrativo Presidente Getúlio Vargas (CAPGV) e mediante prévia autorização da equipe técnica do BNB.

4.16.4. Para fins de estimativa do esforço do processo de desinstalação, o Licitante deverá considerar o quantitativo de 3.000 (três mil) dispositivos do tipo servidores.

4.17. A Solução deverá vir acompanhada de todo o material/serviço/aparato tecnológico necessário para a sua instalação, configuração, personalização e ativação.

4.18. Os manuais necessários à instalação, configuração, manutenção e utilização da solução, deverão ser fornecidos através de uma ou mais das seguintes mídias: papel, CD/DVD, página web, estando a mídia com conteúdo obrigatoriamente em inglês ou português do Brasil, sendo essa última linguagem preferencial e obrigatória, caso a ferramenta possua material em ambos os idiomas.

4.19. É preferencial que o direito de uso das licenças dos softwares seja perpétuo, entretanto será aceita a manutenção do direito de uso, por 60 meses, por subscrição, a qual deverá manter também o direito à atualização das versões dos softwares, sendo que a contratada será responsável por fornecer/manter a solução por período de 60 meses sem que a subscrição gere qualquer tipo de ônus de caráter financeiro ou técnico para a contratante, ou seja, a aplicação da subscrição além de não gerar encargos financeiros, também não deverá consumir as horas de suporte técnico à solução.

4.20. O Idioma da instalação e de todos os componentes de softwares que compõem a solução a ser fornecida deve obrigatoriamente ser inglês ou português do Brasil, ou ambos os idiomas, nos servidores.

4.21. O Idioma da instalação e de todos os componentes de softwares que compõem a solução a ser fornecida deve obrigatoriamente ser português do Brasil nos desktops, inclusive as notificações para o usuário por e-mail.

4.21.1. Com relação às notificações, a ferramenta poderá possuir um sistema para customização das notificações no idioma Português. Nesse caso, a customização das notificações para o idioma Português deverá ser efetuada pela Contratada.

5. FERRAMENTA DE ANTIMALWARE

5.1. Todos os componentes da Ferramenta de Antimalware deverão constar do catálogo do respectivo fabricante. Não serão aceitas composições *ad hoc* elaboradas com o objetivo de atender às especificações deste certame.

5.2. A Solução deverá contemplar o fornecimento de licenças de uso do *software* de Antimalware para 22.000 (vinte e dois mil) dispositivos.

5.3. Caso a solução utilize uma plataforma em nuvem, esta deverá cumprir com os requisitos abaixo descritos:

5.3.1. A plataforma em nuvem deverá cumprir com os requisitos exigidos no item 5 da certificação PCI-DSS V3.2 (Padrão de segurança de dados do setor de cartões de pagamento para organizações que lidam com cartões de crédito de marca das principais bandeiras de cartões) que lhe competem;

5.3.2. A plataforma em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes);

5.4. Todas as licenças do *software* de antimalware deverão ser compatíveis com os seguintes Sistemas Operacionais:

- Microsoft Windows Server 2019;
- Microsoft Windows Server 2016;
- Microsoft Windows 10;
- Red Hat Enterprise Linux;
- CentOS;
- Ubuntu;
- Debian;
- MacOS 12 ou superior.

5.5. Deverá gerenciar de forma centralizada os dispositivos de todos os sistemas operacionais solicitados, oferecendo as seguintes características de detecção e proteção:

- Antimalware
- Anti-Spyware

- Endpoint Detection and Response (EDR)

5.6. Deverá disponibilizar todas as funcionalidades com 1 (um) agente de segurança no dispositivo cliente.

5.7. O gerenciamento da solução deverá ser feito através de console única.

5.8. A comunicação dos sensores com a console de gerenciamento, no caso de mudanças de política, configuração, remediação, envio de eventos e qualquer outra comunicação, devem ser seguras usando minimamente TLS 1.2 ou superior.

5.9. A proteção deverá ser mantida mesmo que o dispositivo não esteja conectado à internet ou à rede interna.

5.10. Não serão aceitas soluções que utilizem somente assinaturas para reconhecer ameaças.

5.11. Funcionalidades de Inspeção de Pacotes:

5.11.1. Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, as seguintes aplicações padrão de mercado, tais como: Adobe Acrobat, Mozilla Firefox, Microsoft EDGE, Google Chrome.

5.11.2. Possibilitar a criação de regras customizadas, de bloqueio ou liberação, para proteger aplicações desenvolvidas pelo BNB

5.11.3. A solução deverá proteger qualquer aplicação em análise de comportamento e índices de ataques.

5.11.4. Bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de um determinado navegador web ou aplicação de backup.

Deve mitigar a exploração de vulnerabilidades (Exploit Mitigation) utilizando tecnologia para redução da superfície de ataque baseado em análise comportamental do ataque.

5.12. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware:

5.12.1. A solução deve possuir mecanismos dedicados e especializados contra ameaças do tipo Ransomware.

5.12.2. A solução deve ser capaz de detectar e bloquear tentativa de ataque de Ransomware baseado em Powershell e outras linguagens de scripts.

5.12.3. A solução deve oferecer proteção em camadas para garantir que qualquer processo malicioso seja detectado e bloqueado, seja na sua pré-execução como na pós-execução.

5.13. Deve contemplar a funcionalidade Endpoint Detection and Response (EDR), tais como:

5.13.1. O sensor com EDR deve coletar minimamente informações de: processos pai, processos filhos, IP e porta de origem, IP e porta de destino, chamadas de biblioteca, operações CRUD (Create, Read, Update, Delete) em chaves de registro (regmods) e

em arquivos (filemods), linha de comando, process injection, chamadas RPC, Logs de Sistema Operacional e detalhes de protocolos (ex. User Agent, Content Type, DNS Resolution, etc).

5.13.2. As coletas de eventos de EDR devem acontecer para 100% das operações, não somente para as que forem identificadas como maliciosas.

5.13.3. A solução deve ser capaz de desofuscar scripts em Powershell que estão encodados e/ou cifrados *(Powershell deobfuscation)*.

5.13.4. Deve fornecer na console informações estatísticas do *Threat Hunting*, com o maior número de conexões de rede, principais alterações de arquivo, principais alterações de registro, principais processos-filho, principais processos pai.

5.13.5. Em caso de incidente a solução deve apresentar painel com a linha do tempo e os ativos infectados de forma visual em sua console.

5.13.6. Ainda em caso de incidente, deve ser possível verificar a linha de comando executada.

5.14. Acesso Remoto para Remediação:

5.14.1. Através do console de gerenciamento, deve ser permitida a possibilidade de acesso a sensores remotos para remediação, podendo enumerar processos, eliminá-los, modificar o registro, executar qualquer comando ou programa no primeiro ou segundo plano, upload/download de arquivo, interagir com a CLI do endpoint e execução de scripts, como por exemplo Python e PowerShell..

5.14.2. Deve ser possível enviar alarmes automaticamente através de *syslog*, e-mail e API REST, usando critérios de alerta específicos.

5.14.3. Deve ser possível colocar em quarentena de rede um dispositivo com um sensor instalado, impedindo qualquer comunicação desse dispositivo com a rede, exceto a conexão com o console de gerenciamento.

5.15. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado ou um emulador antes da execução do mesmo no ambiente de produção.

5.16. Deverá possuir no mínimo os seguintes módulos: console de gerenciamento fornecendo funcionalidades de gestão, módulos para estações físicas, laptops, servidores físicos e virtuais e modulo para VDI (Virtual Desktop Infrastructure).

5.17. Deverá registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.

5.18. Deverá possuir a interface de gerenciamento unificada e esta deve ser suficiente para a realização de todas as configurações necessárias para o adequado funcionamento dos respectivos serviços solicitados, possibilitando:

5.18.1. A console de gerenciamento deverá ter a capacidade de criar pacote de instalação de agente para 32 bits e 64 bits;

5.18.2. O uso de um fator de autenticação duplo deve ser utilizado para autenticação na console de gerenciamento da solução;

5.18.3. Deve ser possível a definição de papéis (RBAC) e atributos (ABAC) para os usuários dentro da console de administração, delimitando as permissões e/ou acesso as funcionalidades e capacidades disponíveis dentro da plataforma;

5.18.4. Deve ser possível a remoção do software de antivírus de forma remota pela console de gerenciamento ou por GPO, Script de Instalação ou Remoção ou MDM.

5.18.5. Deve possibilitar atualização remota de agentes e versões.

5.18.6. Deve implementar proteção de desinstalação do agente para todos os dispositivos gerenciados pela solução, seja através de senha específica ou controlada diretamente pela plataforma de gerenciamento.

5.18.7. Deve detectar tentativas de manipulação indevida dos componentes do agente.

5.18.8. Deve permitir busca em tempo real pelo menos com os seguintes filtros: nome, sistema operacional e IP.

5.18.9. Deve contemplar, no mínimo, as seguintes visualizações ou equivalentes:
- 5.18.9.1. Agentes ativos (se for baseado em agente);
- 5.18.9.2. Agentes por sistema operacional (se for baseado em agente);
- 5.18.9.3. Detecções por objetivo do ataque;
- 5.18.9.4. Detecções por tática do ataque;
- 5.18.9.5. Detecções por severidade do ataque.

5.18.10. Deve prover painéis que exibam, em tempo real, lista priorizada de ações e alertas que requerem atenção da equipe de administração de operações e segurança, bem como, uma visão gráfica das anomalias que requerem investigação;

5.18.11. Deve ser centralizada para gerenciar todos os dispositivos, independentemente da localização geográfica;

5.18.12. Deve ser acessível em qualquer ponto da rede da contratante e na Internet;

5.18.13. Deve ter autenticação integrada com AD (Azure AD) ou possuir Single Sign ON (SSO) com compatibilidade com o Active Directory Federation Services (AD FS) ou SAML 2.0;

5.18.14. Deve suportar duplo fator de autenticação (2FA ou MFA) para acesso à console de administração da solução.

5.18.15. A console de gerenciamento deve ser acessada somente via protocolo HTTPS;

5.18.16. Deve ter capacidade de separar os dispositivos gerenciados através de grupo via seleção manual ou por critérios;

5.18.17. Deve permitir aplicação de políticas para grupos de máquinas ou máquinas individuais;

5.19. Relatórios:

5.19.1. Relatório para serviços de segurança ou eventos de segurança.

5.19.2. Exportar o relatório nos formatos .pdf e/ou .csv.

5.19.3. Possibilidade de criar relatórios de maneira dinâmica no dashboard da solução.

5.19.4. Deverá ser possível ter um relatório com as estações instaladas e as pendentes da instalação, ou integrar-se com o System Center.

5.20. Usuários:

5.20.1. Deverá possuir Administração baseada em regras.

5.20.2. Tipos de usuários pré-definidos como no mínimo:

- Administrador – Administrador dos componentes da solução;
- Administrador Limitado – Permitir a segregação de funções de forma customizada;
- Operador – Realiza alterações operacionais nos componentes da solução;
- Monitoramento – Acesso em modo leitura, permitindo apenas visualização das configurações;

5.20.3. Possibilitar a aplicação de políticas customizadas em função de atributos, no mínimo: endereço IP, domínio e hostname parcial ou completo, do cliente.

5.20.4. Deverá possibilitar criar grupos de máquinas e políticas baseadas em informações de OU (Unidade Organizacional) do Active Directory e subnet.

5.21. Logs:

5.21.1. Registrar as ações do usuário na console de gerenciamento.

5.21.2. Detalhar cada ação do usuário.

5.21.3. Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

5.21.4. Para cada infecção detectada deverá ser possível visualizar qual foi a origem (computador e arquivo/link/dispositivo).

5.21.5. A console de gerenciamento deverá incluir sessão de log com pelo menos as seguintes informações:

- Login;
- Edição;

- Criação;
- Logout.

5.22. Certificado de Segurança:

5.22.1. Deverá prover o acesso via HTTPS.

5.23. Gerenciamento e Instalação Remota:

5.23.1. Capacidade de fazer a instalação pela console ou por meios de criação de GPO, script de instalação ou MDM.

5.24. Componentes e Funcionalidades:

5.24.1. Deverá fazer o monitoramento automático em tempo real;

5.24.2. Deverá apontar na console alerta de indícios de atividades maliciosas baseado na análise da telemetria e comportamento;

5.24.3. Deverá armazenar informações gerais de telemetria, no mínimo por 30 dias, mesmo que estas não estejam associadas a uma detecção, e para os identificados como maliciosos, guardar por pelo menos 180 dias;

5.24.4. Deverá agrupar detecções relacionadas em um incidente, atribuindo um índice de risco específico;

5.24.5. Para dispositivos de armazenamento em massa, deve permitir acesso granular com, no mínimo, as seguintes permissões:

5.24.5.1. Leitura somente;

5.24.5.2. Escrita e leitura;

5.24.5.3. Escrita leitura e execução;

5.24.5.4. Bloqueio total;

5.24.6. Deve permitir a criação de regras de exceção para um grupo de usuários do Active Directory;

5.24.7. Deve permitir que proteção de dispositivos seja habilitada em modos de detecção somente, ou bloqueio efetivo;

5.24.8. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;

5.24.9. Deve permitir bloqueio de scripts e comandos em Powershell considerados suspeitos;

5.24.10. Deve permitir bloqueio automático de processos suspeitos;

5.24.11. Deve permitir bloqueio baseado em análise do centro de inteligência do fabricante;

5.24.12. Deve permitir bloqueio de operações em registros suspeitos;

5.24.13. Deve permitir que arquivos maliciosos possam ser movidos para uma área de quarentena, ou possuir tecnologia de quarentena in-place, onde os arquivos ficam inutilizados no próprio local de origem;;

5.24.14. Para melhor proteção, o antivírus deverá ter os tipos de detecção e prevenção:

5.24.14.1. Baseada em monitoramento contínuo de processos.

5.24.14.2. Baseada em aprendizado de máquina (Machine Learning);

5.24.14.3. Baseada em análise comportamental;

5.24.14.4. Baseada em análise de memória RAM, capaz de proteger contra ataques de injeção de código em processos legítimos e outros tipos de ataques que exploram a execução de processos em memória RAM;

5.24.14.5. Deve construir um baseline comportamental para identificar anomalias que podem indicar ataques ou tentativas de acessos não autorizados;

5.24.14.6. Deve permitir configurar políticas de remediação em caso de surto de vírus;

5.24.14.7. Deve atribuir índice ou score de risco associado a cada alerta de segurança e a cada usuário;

5.24.14.8. Deve ser capaz de enviar notificações por e-mail;

5.24.15. Deve ser capaz de agregar eventos em um incidente para facilitar a investigação, além de atribuir um nível de risco a cada incidente para auxiliar na priorização das tratativas;

5.24.16. Deve ser capaz de impedir ataques que utilizem a técnica de Heap Spray Preallocation;

5.24.17. Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling);

5.24.18. Deve ser capaz de impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos;

5.24.19. Deve ser capaz de detectar malwares do tipo *ransomware* com base em, no mínimo, os comportamentos abaixo:

5.24.19.1. Deletar backups;

5.24.19.2. Operações em excesso ao sistema de arquivos;

5.24.19.3. Criptografia de arquivos;

5.24.19.4. Processos associados a malwares de ransomware, no mínimo, Cryptowall, Wannacry, Locky;

5.24.20. Deve ser capaz de detectar exploração baseado em, no mínimo, os seguintes comportamentos:

5.24.20.1. Criação de processos suspeitos originados de navegadores;

5.24.20.2. Detecção de comprometimento de servidores Web através de webshell;

5.24.20.3. Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;

5.24.20.4. Injeção de código não esperada de um processo a outro;

5.24.20.5. Execução de JavaScript através do executável Rundll32.

5.24.21. Deve ser capaz de detectar movimentação lateral através de circunvenção do processo de logon do Windows;

5.24.22. Deve ser capaz de detectar de processos que tentam obter credenciais de login;

5.24.23. A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas dentro da avaliação do MITRE ATT&CK:

5.24.23.1. T1003, T1012, T1018, T1021, T1026, T1027, T1036, T1047, T1048, T1049, T1053, T1055, T1059, T1061, T1070, T1087, T1095, T1102, T1110, T1112, T1132, T1136, T1204, T1218, T1219, T1222, T1543, T1547, T1548, T1550, T1559, T1560, T1562, T1564, T1567, T1570, T1574.

5.24.24. O agente para estações Windows deve suportar a RFC 5246;

5.24.25. A plataforma deverá prevenir e remediar ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código (polimorfismo, criptografia, e outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais.

5.24.26. Quarentena:

5.24.26.1. Deverá possuir serviço de Sandbox ou Centro de Inteligência contra Ameaças, na nuvem do fabricante para a realizar análise comportamental automatizada, de malware ou mesmo arquivos suspeitos ou sem reputação.

5.24.26.2. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador.

5.24.26.3. Caso a solução utilize mecanismo de quarentena no Endpoint, deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir.

5.24.26.4. Quarentena deverá possibilitar a restauração remota, ou possibilitar coleta desde a console do binário para backup, restore e possíveis futuras análises.

5.24.27. Atualização:

5.24.27.1. Deve permitir suprimir a reinicialização no processo automático de atualização do agente.

5.25. **Compatibilidade com Microcomputadores Servidores**

5.25.1. Tendo em vista a proteção de dispositivos Microcomputadores Servidores, todas as licenças deverão guardar compatibilidade com os requisitos a seguir.

5.25.2. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:

5.25.2.1. Windows Server 2016;

5.25.2.2. Windows Server 2019;

5.25.2.3. Red Hat Enterprise Linux, CentOS e Ubuntu.

5.25.3. Deve inspecionar o tráfego de entrada e saída local para detectar e bloquear atividades suspeitas.

5.25.4. Detectar alterações em aplicações e permitir ao administrador da solução bloquear o software e, opcionalmente, bloquear o computador.

5.25.5. Possuir lista de permissões de aplicativos.

5.25.6. Deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", protegendo o sistema operacional e as aplicações de vulnerabilidades recém-descobertas.

5.25.7. Prover segurança para servidores físicos e Virtuais.

5.25.8. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, adwares, ransomwares e rootkits em:

5.25.8.1. Armazenamento local.

5.25.8.2. Memória RAM.

5.25.8.3. Processos em execução em memória principal e cache, sem a necessidade de escrita de arquivo.

5.25.8.4. Arquivos lidos, escritos, executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando.

5.25.8.5. Arquivos compactados automaticamente, em pelo menos os seguintes formatos: zip, rar, 7z, exe, arj, mime/uu, Microsoft cab.

5.25.8.6. Scripts escritos em linguagens como javascript e Activex que executam nos navegadores Chrome, Edge, Mozila, Edge e Internet Explorer.

5.25.9. Deve ser capaz de prevenir intrusão em navegadores de internet.

5.25.10. Deve ser capaz de realizar rastreamento de ameaças de forma manual, agendada e também em tempo real na memória ram.

5.26. **Compatibilidade com Estações de Trabalho**

5.26.1. Tendo em vista a proteção de dispositivos Microcomputadores Estações de Trabalho (Desktops e Notebooks), todas as licenças deverão guardar compatibilidade com os requisitos a seguir.

5.26.2. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

- Windows 10 64Bits;
- Windows 7 64Bits e 32Bits.

5.26.3. Prover segurança para estações de trabalho sejam físicas ou em ambiente virtualizado (VDI).

5.26.4. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria, e guardar esses eventos de auditoria por no mínimo 30 dias.

5.26.5. Deve possuir console de gerenciamento centralizada juntamente com os demais itens solicitados deste edital.

5.26.6. Deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", protegendo o sistema operacional e as aplicações de vulnerabilidades recém-descobertas.

5.26.7. Deve mitigar a exploração de vulnerabilidades (Exploit Mitigation).

5.26.8. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, adwares, Ransomware e rootkits em:

5.26.8.1. Armazenamento local.

5.26.8.2. Memória RAM.

5.26.8.3. Processos em execução em memória principal e cache, sem a necessidade de escrita de arquivo.

5.26.8.4. Arquivos lidos, escritos, executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando.

5.26.9. Deve ser capaz de prevenir intrusão em navegadores de internet.

5.26.10. Deve ser capaz de realizar rastreamento de ameaças de forma manual, agenda e também em tempo real na memória RAM.