12. APÊNDICE I - ESPECIFICAÇÕES TÉCNICAS

12.1.1 Suporte Técnico Especializado

12.1.1.1 A contratação deste Suporte Técnico Especializado do fabricante tem por objetivo garantir a proteção, monitoramento, disponibilidade e segurança da infraestrutura de cibersegurança, composta pelas ferramentas de ANTIMALWARE com XDR, NDR e ANTISPAM, por meio de times especialistas do próprio fabricante provido pelos fabricantes das soluções.

12.1.1.2 **Escopo do Suporte Técnico Especializado**

12.1.1.2.1 Não estão incluídas neste item de suporte técnico a instalação e configuração iniciais das ferramentas de segurança cibernética e os serviços básicos e especializados e transferência de conhecimento referente aos itens do grupo 1 e grupo 2 já que fazem parte da contratação principal;

12.1.1.2.2 O suporte técnico do fabricante a ser fornecido deve abranger, mas não se limitar, a seguinte lista de serviços:

- Monitoramento contínuo das soluções de segurança cibernética para identificar e mitigar proativamente ameaças avançadas, vulnerabilidades e incidentes antes que comprometam a operação normal, incluindo a aplicação de atualizações e patches de segurança;
- Fornecimento de suporte técnico remoto e diagnóstico de falhas nas ferramentas de segurança, com envio de suporte presencial para incidentes que não possam ser resolvidos remotamente;
- Resposta rápida a incidentes de cibersegurança e problemas reportados, com prazos de atendimento definidos de acordo com a criticidade e o impacto das ameaças detectadas, definidos no SLA descrito neste termo de referência;
- Repasse de conhecimento da equipe interna para operação básica das ferramentas de segurança e solução de problemas simples, bem como capacitação para realizar tarefas de monitoramento e manutenção preventiva das soluções implantadas;
- Procedimentos em conjunto com fornecedores, para situações em que o ambiente do Contratante necessite de adaptações ou customizações nas ferramentas, assegurando a correta configuração e solução de problemas técnicos complexos;
- Reuniões técnicas periódicas, mensais ou a critério do Contratante, para planejamento e execução de melhorias no ambiente de segurança cibernética; e
- Reuniões gerenciais mensais ou a critério do Contratante, para avaliação e acompanhamento dos serviços oferecidos e indicadores de segurança.

12.1.1.2.3 Sempre que necessário, a equipe especializada do fabricante da solução deverá efetuar análise técnica nas dependências do Contratante de modo a realizar análise e implementar as adaptações ou melhorias necessárias para garantir a eficiência e segurança das soluções de cibersegurança;

12.1.1.2.4 O fabricante deve prover o serviço de suporte com atendimento prioritário através do suporte de telefone, e-mail e/ou portal do fabricante ou ferramenta instituída pela Contratante;

12.1.1.2.5 O fabricante deverá participar da reunião inicial, introdução da solução, orientação de implantação e melhores práticas;

12.1.1.2.6 O fabricante deverá prover um Gerente de Serviço ou Engenheiro para reuniões mensais de status do ambiente, revisões trimestrais de negócios e correções aceleradas de defeitos ou implementação de melhorias; atualizações de produtos e atualizações de inteligência de ameaças;

12.1.1.2.7 Acesso a treinamento sob demanda, base de conhecimento, práticas recomendadas, guias administrativos e operacionais;

12.1.1.2.8 Verificação e apresentação das melhores práticas no uso dos produtos;

12.1.1.2.9 Acesso a especialistas em cibersegurança e CISO (Chief Information Security Officer);

12.1.1.2.10 Detecção de ataques direcionados: previsão proativa de ameaças com monitoramento 24 horas por dia, 7 dias por semana de qualquer ataque direcionado, orientação de resposta a incidentes, acesso a um especialista em ameaças;

12.1.1.2.11 Entregar relatórios mensais acerca da saúde e riscos do ambiente;

12.1.1.2.12 Previsão proativa de ameaças com monitoramento 24 horas por dia, 7 dias por semana de alertas XDR, investigação e resposta com alcance proativo, incluindo varredura/análise de IoCs, busca de IoA, análise de causa raiz, análise de impacto, priorização de incidentes, orientação de resposta e acesso a times especializados do fabricante;

12.1.1.2.13 Acompanhamento nas atualizações que devem ser do tipo “minor release” e “major release”, permitindo manter todos os componentes atualizados em sua última versão de software/firmware;;

12.1.1.2.14 O serviço deve ser fornecido pelo mesmo fabricante da plataforma ofertada, não sendo aceito nenhum tipo de integração (nem mesmo com a contratada) externa ou automatização de detecção e investigação;

12.1.1.2.15 Caso as condições de licenciamento dos softwares fornecidos sejam alteradas pelo fabricante durante o período de vigência do contrato, as funcionalidades e os quantitativos definidos não deverão ser prejudicados. Nas situações em que a alteração na forma de licenciamento implique em perdas qualitativas e/ou quantitativas, licenças complementares deverão ser fornecidas à Contratante, sem custo adicional;

12.1.1.2.16 O Contratante oficializará a solicitação dos serviços por meio da emissão de Ordem de Serviço (OS) específica;

12.1.1.2.17 O controle da execução dos serviços se dará em 03 (três) momentos, a saber:

- No início da execução, quando a OS é emitida pelo Contratante;
- Durante a execução, com o acompanhamento de responsáveis do Contratante; e
- Ao término da execução, com a entrega de um “Relatório de Atividades Realizadas” pela Contratada e seu ateste pelo Contratante.

12.1.1.2.18 O “Relatório de Atividades Realizadas” deverá conter:

- Identificação do Relatório de Atividades

- Data da emissão;;
- Número do contrato;
- Descrição detalhada das atividades realizadas, incluindo a solução proposta para os problemas identificados; e
- Horas gastas nas atividades realizadas.

12.1.1.2.19 A partir da emissão da Ordem de Serviço, a Contratada deverá iniciar as tratativas com o Contratante para execução dos serviços, salvo em casos que requeiram agendamento prévio;

12.1.1.2.20 Este serviço deverá estar disponível para acionamento 24 horas por dia, 7 dias por semana;

12.1.1.2.21 Os serviços indicados nesta seção poderão ser solicitados por qualquer dos órgãos solicitantes constantes neste TR;

12.1.2 Os serviços objeto desta contratação são caracterizados como comuns, uma vez que apresentam padrões de desempenho e de qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, nos termos do art. 6º, XIII, da Lei nº 14.133/2021.

12.2. DETALHAMENTO DA ESPECIFICAÇÃO DOS SERVIÇOS/PRODUTOS

12.2.1 Licenciamento de ferramenta de antispam de forma continuada.

12.2.1.1 Características Gerais

12.2.1.1.1 A solução deve ser compatível com Microsoft Exchange Server e Microsoft O365, configurado de acordo com o ambiente a ser protegido, com conexão segura de forma criptografada.

12.2.1.1.2 A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente ou evento.

12.2.1.1.3 A solução deve suportar a função de Relay SMTP (Simple Mail Transfer Protocol), com recurso de antispam.

12.2.1.1.4 Capacidade de atendimento ao tráfego de e-mail gerado pelo Ministério, conforme abaixo:

12.2.1.2 Deverá suportar tráfego de entrada e saída de mensagens externas de acordo com tabela disponível neste Termo de Referência.

12.2.1.2.1 Deverá suportar tráfego de entrada e saída de mensagens internas de acordo com tabela disponível neste Termo de Referência relativo a mensagens por mês.

12.2.1.3 A solução deve ser dimensionada para atender a tabela disponível neste Termo de Referência no que tange as caixas postais de usuários e corporativas.

12.2.1.3.1 A solução deve possuir controle de sessões SMTP por meio de limite de tráfego de mensagens baseado em endereços IP, sub-redes IP, domínio e reputação do emissor.

12.2.1.3.2 A solução deve inspecionar e bloquear mensagens com base no tamanho da mensagem, volume de mensagens por período, número de destinatários por mensagem, número de

destinatários por hora, destinatários inválidos, número de mensagens por conexão e número de conexões simultâneas por endereço IP.

12.2.1.3.3 A solução deve possibilitar a implementação da tecnologia SPF (Sender Policy Framework), de modo a evitar que outros domínios enviem e-mails não autorizados em nome de um domínio.

12.2.1.3.4 A solução deve possibilitar a implementação da tecnologia DKIM (Domain Keys Identified Mail), de modo a prover mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas.

12.2.1.3.5 A solução deve possibilitar a implementação da tecnologia DMARC, de modo a prevenir o recebimento de phishing e spam.

12.2.1.3.6 A solução deve apresentar as origens de e-mails da organização, a fim de demonstrar as localidades emissoras de e-mails em nome da organização.

12.2.1.3.7 A solução deve possibilitar a implementação da tecnologia Forwarded-Confirmed-Reverse DNS (FCRDNS) de modo a verificar a relação entre o IP do servidor e o nome.

12.2.1.3.8 A solução deve possibilitar a implementação de recursos de verificação de DNS reverso para validação de domínio.

12.2.1.3.9 A solução deve possibilitar a filtragem de conteúdo de e-mails por meio de assinaturas e análise para corpo e anexos de mensagens, cabeçalho da mensagem, heurística, remetente, filtro de reputação, URLs e filtros anti-phishing e antispam.

12.2.1.3.10 A solução deve possibilitar a filtragem de e-mails baseada em lista negada (deny list) e lista permitida (allow list), globais e por usuário.

12.2.1.3.11 A solução deve categorizar mensagens de entrada e saída a partir de políticas preestabelecidas.

12.2.1.3.12 A solução deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em sandbox com a gerência centralizada do fabricante.

12.2.1.3.13 A solução deve implementar recurso de antivírus.

12.2.1.3.14 A solução deve tratar mensagens com anexos contendo malware, possibilitando o encaminhamento da mensagem, sem o anexo infectado (anexo limpo), bloqueando a mensagem e alertando o destinatário do ocorrido.

12.2.1.3.15 A solução deve detectar anexos compactados e criptografados, permitindo definir a ação a ser executada.

12.2.1.3.16 A solução deve identificar a reputação de links que estejam dentro do corpo de mensagens.

12.2.1.3.17 A solução deve possuir quarentena por usuário, integrado e autenticado na base de diretório de usuários (Active Directory, LDAP ou EntraID do O365), possibilitando ao mesmo administrar sua própria quarentena, lista negada (deny list) e lista permitida (allow list), removendo mensagens ou liberando as que não considera SPAM. A Quarentena deve ser implementada

com integração direta em aplicações de correio eletrônico, ou via interface Web (HTTPS), permitindo a liberação diretamente no cliente de e-mail.

12.2.1.3.18 A solução deve implementar o recurso de envio de notificação periódica para usuários acerca de mensagens de spam e em quarentena.

12.2.1.3.19 A solução deve implementar recurso que permita ao usuário administrar a sua própria quarentena, dando a opção de visualizar, liberar e liberar e confiar.

12.2.1.3.20 A solução, ao encontrar um objeto potencialmente malicioso, deve, no mínimo:

12.2.1.3.21 Bloquear acesso ao objeto.

12.2.1.3.22 Tentar limpar o objeto e restaurá-lo para uso.

12.2.1.3.23 Caso não seja possível limpá-lo deverá mover para quarentena.

12.2.1.3.24 Após o encerramento do tempo de quarentena, apagar o objeto.

12.2.1.3.25 A solução deve permitir ao administrador da solução executar pesquisa nas áreas de quarentena de todos os usuários através de interface web segura.

12.2.1.3.26 A solução deve possibilitar a gestão de quarentena pelos administradores de forma que eles possam visualizar a razão de um determinado bloqueio, remetente, destinatário, data, assunto, IP do host, destinatário, a mensagem original, tamanho da mensagem original e permitindo, no mínimo, as ações liberar ou excluir.

12.2.1.3.27 A solução deve possibilitar gravar o arquivo infectado na área de segurança (quarentena) e não o entregar para o(s) destinatário(s).

12.2.1.3.28 A solução deve implementar a inserção de carimbo no assunto de mensagens e de texto no corpo de mensagens.

12.2.1.3.29 A solução de gerência pode ser em appliance, fornecidos pela CONTRATADA, ou solução em nuvem do fabricante. Na modalidade appliance, a solução de gerência deve considerar instalação em alta disponibilidade no modo ativo/passivo, ou seja, permitir a configuração de funcionalidade em redundância em um cluster de pelo menos 2 (dois) servidores de gerência, capaz de operar em redes distintas e separadas geograficamente. No caso de falha em um dos servidores do cluster, o outro deve ser capaz de assumir todas as operações e funcionalidades sem interrupção dos serviços.

12.2.1.3.30 A solução deve permitir bloqueios de mensagens utilizando, no mínimo, os seguintes critérios:

12.2.1.3.31 Tipo de arquivo.

12.2.1.3.32 Nome do arquivo.

12.2.1.3.33 Tamanho do arquivo.

12.2.1.3.34 A solução deve ser capaz de verificar pastas públicas, e-mails enviados, recebidos e armazenados, evitando a incidência de vírus, spywares, adwares, worms, trojans, malware

empacotado (packed malware) de forma heurística, riskwares e outros tipos de códigos maliciosos e ataques, e-mail de marketing e conteúdo indesejado(impróprio).

12.2.1.3.35 A solução deve ser capaz de detectar disseminação em massa de e-mails infectados, informando o administrador e registrando tais eventos nos logs do sistema e da aplicação.

12.2.1.3.36 A solução deve ser capaz de arquivar qualquer mensagem que viole as políticas corporativas.

12.2.1.3.37 A solução deve ser capaz de rejeitar conexões que tentem ser abertas pelos comandos “HELO” e “EHLO”, sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS.

12.2.1.3.38 A solução deve possuir e utilizar filtros de reputação.

12.2.1.3.39 A solução deve ter a capacidade de implementar pesquisas de reputação, informando seu histórico, assim como, sua reputação atual.

12.2.1.3.40 A solução deve ser capaz de filtrar por remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas.

12.2.1.3.40.1 A solução deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego.

12.2.1.3.41 A solução deve ser capaz de atualizar automaticamente os filtros sem interrupção dos serviços e/ou perda das regras pré-estabelecidas pelo administrador.

12.2.1.3.42 A solução deve bloquear servidores classificados como emissões de lixo eletrônicos por meio da metodologia conhecida por Domain Keys Identified Mail (DKIM).

12.2.1.3.43 A solução deverá possuir um sistema que permita estabelecer uma reputação (pontuação) dos endereços IP de servidores que iniciarão conexões TCP. Após estabelecida essa reputação, a solução deverá permitir ações diferenciadas de acordo com a pontuação obtida.

12.2.1.3.44 A solução deve permitir ao administrador aplicar políticas e ações por meio de pontuação.

12.2.1.3.45 A solução deve ser capaz de apresentar informações relacionadas à matriz do MITRE para cada um dos eventos detectados no ambiente, caso possuam.

12.2.1.3.46 O fabricante deve possuir uma rede de inteligência (threat inteligence) própria da solução para atualização constante de feeds de ameaças (threat feed).

12.2.1.3.47 A solução deve utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente.

12.2.1.3.48 A solução deverá possuir integração nativa com a plataforma de XDR via API, não sendo aceito integrações que necessitem agentes adicionais ou plug-ins.

12.2.1.3.49 As CONTRATADAS vencedoras dos lotes I e II deverão compartilhar, via API ou outra tecnologia, toda informação necessária para a integração dos sistemas Antispam e XDR.

12.2.1.3.50 O sistema de verificação de reputação não deverá basear-se somente em RBL´s públicas.

12.2.1.3.51 A solução deve verificar o hash das mensagens para proteção contra malware.

12.2.1.3.52 A solução deverá possuir proteção contra-ataques, no mínimo, dos tipos:

12.2.1.3.53 Negação de Serviço (DDoS).

12.2.1.3.54 Coleta de usuário/senha.

12.2.1.3.55 Spoofing.

12.2.1.3.56 Spear Phishing.

12.2.1.3.57 BEC (Business Email Compromise)

12.2.1.3.58 Whaling.

12.2.1.3.59 Vishing.

12.2.1.3.60 Phishing de e-mail.

12.2.1.3.61 Phishing HTTPS.

12.2.1.3.62 Clone Phishing.

12.2.1.3.63 Dentre outros.

12.2.1.3.64 A solução deve possuir no mínimo as seguintes tecnologias para prevenção e bloqueio de spam:

12.2.1.3.65 Recurso de Grey List;

12.2.1.4 Recurso de checagem por SPF (Sender Policy Framework) permitindo a criação de regras individuais e customizadas para usuários ou grupos, permitindo criar ações específicas para “fail” e “soft fail”, conforme descrito pelo Comitê Gestor da Internet no Brasil em seu website oficial (HTTP://www.antispam.br/admin/spf);

12.2.1.4.1 Recurso de checagem por assinatura DKIM;

12.2.1.4.2 Recurso de checagem de DNS Reverso;

12.2.1.4.3 Checagem de validade de domínio através de verificação da configuração da zona do DNS do remetente;

12.2.1.4.4 Análise de reputação de IP;

12.2.1.4.5 Filtros de URL;

12.2.1.4.6 Filtro de anti-phishing;

12.2.1.5 Consulta de RBL´s (real-time blackhole list);

12.2.1.5.1 Filtro bayesiano utilizando tecnologia Bayes Databases ou ML (Machine Learning)

12.2.1.5.2 A solução deve ser capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como SPAM, em um determinado espaço de tempo, ambos configuráveis pelo administrador, deve também ser capaz de realizar o controle da fonte emissora de SPAM baseado no Known Spam Source List (KSSL) ou seja, a lista de remetentes conhecidos por envio frequente de SPAM.

12.2.1.5.3 A solução deverá ser integrada ao LDAP, Active Directory, e EntraID do O365.

12.2.1.5.4 A solução deverá suportar dicionários de palavras e expressões regulares.

12.2.1.5.5 A solução deverá scanear os anexos compactados em várias camadas, e anexo do tipo MIME dentre outros, com a capacidade de apagá-los automaticamente.

12.2.1.5.6 A solução deve ser capaz de tomar decisões baseadas no tamanho de mensagem (corpo ou anexos).

12.2.1.5.7 A solução, após a análise, deverá incluir, no mínimo, as seguintes ações:

12.2.1.5.8 Entrega da mensagem.

12.2.1.5.9 Retorno da mensagem (bounce).

12.2.1.5.10 Descarte da mensagem.

12.2.1.5.11 Manipulação de cabeçalhos da mensagem.

12.2.1.5.12 Envio de mensagem de notificação para um outro endereço, inclusive o destinatário.

12.2.1.5.13 Envio de mensagem para quarentena.

12.2.1.5.14 A solução deve permitir a verificação do tipo real do arquivo, mesmo que o arquivo tenha sido renomeado.

12.2.1.5.15 A solução deverá possibilitar a configuração do período em que as mensagens ficarão em quarentena e após esse período as mensagens serão apagadas automaticamente.

12.2.1.5.16 A solução deverá suportar vários domínios (registros MX), e suportar roteamento de mensagens baseado em cada um desses domínios.

12.2.1.5.17 A solução deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena.

12.2.1.1.100.1. Especificações Técnicas da Console de Gerenciamento - Solução de Antispam

12.2.1.5.18 A console deve possuir integração com LDAPs e com o serviço de diretório Microsoft Active Directory ou EntraID do O365, para importação da estrutura organizacional e autenticação dos Administradores.

12.2.1.5.19 A solução deve possibilitar a visualização completa de rastreabilidade de uma mensagem permitindo analisar no mínimo: sua origem, identificar as ameaças relacionadas, os ativos de informação relacionados, e-mails e anexos e informações adicionais que gere a proteção efetiva do ambiente e subsidie uma análise sólida das ações.

12.2.1.5.20 A solução deve registrar os logs e esses devem ser acessíveis por SSH, SCP ou HTTPS por meio de API, sempre com controle de acesso.

12.2.1.5.21 A solução deverá ser acessível através de tecnologia Web HTTPS e permitir configuração de TLS para autenticação, com recurso de múltiplo fator de autenticação (MFA).

12.2.1.5.22 A solução deve possuir gerenciamento centralizado responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços.

12.2.1.5.23 A solução deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros (ferramentas para BI, por exemplo).

12.2.1.5.24 A solução deve gerenciar com perfis de acessos distintos para administração de funcionalidades, acesso, visualização de status de serviços, logs e emissão de relatórios.

12.2.1.5.25 A solução deve gerenciar com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de mensagens, throughput e desempenho dos serviços.

12.2.1.5.26 A solução deve permitir auditar as alterações de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas.

12.2.1.5.27 A solução deve informar quaisquer atualizações a serem feitas no software e deverá também aguardar validação de data e hora, permitindo agendamento dessa atualização juntamente com o cliente.

12.2.1.5.28 A solução deve permitir monitorar logs e debugging.

12.2.1.5.29 A solução deve possuir recurso de backup e importação de arquivos de configuração.

12.2.1.5.30 A solução deve possibilitar a criação de dashboards personalizados que apresente componentes gráficos para monitoração e visualização de informações de agentes (ativos), versões de agentes, linha do tempo de eventos, status de proteção, eventos listados por: endpoint, nome do processo/ameaça, regras, usuários e grupos e informações atualizadas diariamente sobre principais riscos de Cibersegurança e permitir a exportação para, no mínimo, os formatos PDF, HTML, CSV ou TXT.

12.2.1.5.31 A solução deve possuir recurso de emissão de relatórios, incluindo informações de quantidade de e-mails enviados e recebidos, quantidade de spams, quantidade de malwares, volume de tráfego, performance e estatísticas gerais.

12.2.1.5.32 A solução deve possibilitar a monitoração e geração de relatórios a partir da console de administração nos formatos PDF, HTML, CSV ou TXT, com a possibilidade de envio por e-mail e exportação.

12.2.1.5.33 A solução deve possibilitar a emissão de relatórios customizados contendo, no mínimo, as informações do tipo:

12.2.1.5.34 Principais remetentes de SPAM, por domínio e por endereço de email.

12.2.1.5.35 Principais destinatários de SPAM, por domínio e por endereço de email.

12.2.1.5.36 Estatísticas sobre a quarentena.

12.2.1.5.37 Principais fontes de ataques de diretório.

12.2.1.5.38 Principais fontes de ataques de spam.

12.2.1.5.39 Principais fontes de ataques de malwares.

12.2.1.5.40 A solução deverá fornecer acesso gráfico aos eventos e alertas detectados, com opção de salvaguardar os logs ou direcioná-los para um servidor syslog, além de oferecer mecanismos de emissão de alarmes via correio eletrônico, syslog e traps SNMP.

12.2.1.5.41 A solução deve possibilitar o envio de notificações de eventos maliciosos.

12.2.1.5.42 A solução deve possibilitar fazer uma lista de domínios aprovados que utilizam o Domain Keys Identified Mail (DKIM).

12.2.1.5.43 A solução deve possuir a detecção de spam utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta, inclusive para links com má reputação.

12.2.1.5.44 A solução deve permitir a criação de lista negada (deny list) e lista permitida (allow list) para um melhor ajuste na detecção de spam.

12.2.1.5.45 A solução deve possibilitar que as políticas possam ser aplicadas usando as diretivas de grupo.

12.2.1.5.46 Os filtros de conteúdo deverão possuir capacidade de ser configurados para mensagens de e-mail na entrada e na saída.

12.2.1.5.47 A solução deverá fornecer atualizações e permitir o agendamento para realização dessas atualizações.

12.2.1.5.48 A solução deve notificar os administradores por e-mail caso a solução não receba atualizações por um determinado período.

12.2.1.5.49 A solução deve apresentar alertas caso os dados analisados tenham relação com algum tipo de campanha de ameaças globais.

12.2.1.5.50 A solução deve possuir logs com um alto nível de detalhes (endereços IP e e-mail de origem e destino, reputação da origem, data, hora e políticas aplicadas).

12.2.1.5.51 A solução deverá permitir a parametrização pelo administrador de, no mínimo, os seguintes itens:

12.2.1.5.52 Permitir configuração de fuso horário.

12.2.1.5.53 Sincronizar via Network Time Protocol (NTP).

12.2.1.5.54 Possuir logs com um alto nível de detalhes (endereços IP e e-mail de origem e destino, reputação da origem, cabeçalho da mensagem, data, hora e políticas aplicadas).

12.2.1.5.55 Disponibilizar acesso externo de forma segura.

12.2.1.5.56 As atualizações do produto (filtros e outros componentes) não devem causar interrupção do serviço e devem ser feitas de forma automática ou manual e incremental.

12.2.1.5.57 A solução deverá permitir o gerenciamento das filas de mensagens (queues), visualizando-as e com as opções de parar e iniciar as filas e de excluir mensagens.

12.2.1.5.58 A solução deve ser capaz de fazer integrações por meio de API REST via serviço Web utilizando o protocolo HTTPS com autenticação.

12.2.1.5.59 A solução deverá suportar integração com os principais sistemas de monitoramento, tais como: Zabbix, Nagios ou outros, para análise de disponibilidade.

12.2.1.5.60 A solução deve possuir módulo de pesquisa de ameaças, possibilitando, no mínimo, as ações:

12.2.1.5.60.1 Coleta de logs e evidências.

12.2.1.5.60.2 Isolar um ativo de informação.

12.2.1.5.60.3 Terminar um processo.

12.2.1.5.60.4 Realizar dump de memória.

12.2.1.5.60.5 Listar as portas abertas dos ativos de informação.

12.2.1.5.60.6 Listar configurações de rede.

12.2.1.5.60.7 Listar e deletar arquivos ou diretórios.

12.2.1.5.61 A solução deve com base na telemetria do sensor de inspeção de rede, indicar as vulnerabilidades existentes e replicar a sequência de requisições ocorridas. A partir dessas identificações a solução deverá ser capaz de automática ou manualmente, disponibilizar e aplicar as regras de proteção.

12.2.1.5.62 A solução deve apresentar os alertas consolidados e correlacionados de ameaças para melhor análise e resposta.

12.2.1.5.63 A solução deve suportar monitoramento em múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches

12.2.1.5.64 A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise de impacto e análise de causa-raiz.

12.2.1.5.65 A solução deve elencar o nível de risco dos usuários, identificando, no mínimo:

12.2.1.5.65.1 Comprometimento de credencial.

12.2.1.5.65.2 Ataque de força bruta.

12.2.1.5.65.3 Login atípico ou impossível.

12.2.1.5.65.4 Login via IPs suspeitos.

12.2.1.5.65.5 Múltiplas tentativas de login com sucesso e insucesso.

12.2.1.5.66 A solução deve possibilitar enviar ações de mitigação a partir dos alertas de risco.

12.2.1.5.67 A solução deverá centralizar as ações e a visibilidade sobre:

12.2.1.5.67.1 Inspeção de rede contra ameaças avançadas com detecção e resposta.

12.2.1.5.67.2 Detecção e resposta para ativos de informação e cargas de trabalho.

12.2.1.5.67.3 Controle de acesso a aplicações internas, externas e na nuvem.

12.2.1.5.67.4 Prevenção de Intrusão de Rede.

12.2.1.5.68 A solução deverá apresentar relatórios customizados contendo, no mínimo:

12.2.1.5.68.1 Ativos de informação infectados.

12.2.1.5.68.2 Origem de infecções.

12.2.1.5.68.3 Tipos de ameaças.

12.2.1.5.68.4 Riscos potenciais de segurança.

12.2.1.5.68.5 Riscos de perda de informações.

12.2.1.5.68.6 Riscos de sistema comprometido.

12.2.1.5.68.7 Riscos de disseminação de ameaças.

12.2.1.5.68.8 Eventos suspeitos.

12.2.1.5.68.9

12.2.2 LICENCIAMENTO DE FERRAMENTA DE ANTIMALWARE COM XDR E NDR DE FORMA CONTINUADA

12.2.2.1 Características Gerais da Solução de Antimalware com XDR

12.2.2.2 A solução e seus componentes deverão ser do mesmo fabricante.

12.2.2.3 A solução deve se auto proteger contra-ataques aos seus serviços e processos e deve ter a capacidade de implementar a funcionalidade de "Machine Learning" (aprendizado de máquina).

12.2.2.4 A solução deve conter proteção contra execução de aplicações maliciosas (Application control) ou similares.

12.2.2.5 Os agentes da solução, caso necessário, deverão ser instalados e ativados por pacotes ou de forma automatizada por meio de scripts (shell/bash).

12.2.2.6 A solução deve permitir a instalação e atualização automática do agente sem a intervenção do usuário.

12.2.2.7 A solução deve permitir a remoção automática de agentes inativos por um período configurável.

12.2.2.8 Os agentes devem possuir, no mínimo, as seguintes funcionalidades de combate a malwares: Detectar e bloquear ameaças utilizando técnicas comportamentais e estatísticas (heurísticas, comportamental ou preditiva).

12.2.2.9 O fabricante deve possuir rede de inteligência (threat inteligence) própria da solução para atualização constante de feeds de ameaças (threat feed), bem como permitir a integração com bases de inteligência de terceiros.

12.2.2.10 A solução deve contemplar proteção contra-ataques: direcionados e suas variantes, 0Day (dia zero), ransomware, malwares, backdoors, vulnerabilidades desconhecidas ou novas, tais como as que possam causar estouro de buffer (overflow), ataques iniciados a partir de mídias removíveis, proteção contra BOTs e variantes, e ainda ter tecnologia de análise de comportamentos suspeitos para detecção e eliminação de ameaças desconhecidas, entre outras formas de ataque.

12.2.2.11 A solução deve possuir mecanismo para impedir disseminação lateral de malwares ao identificar ativos de informação infectados.

12.2.2.12 A solução deverá ser capaz de identificar ativos infectados e bloquear a comunicação entre eles, isolando o ativo infectado da rede, e possibilitando o retorno seguro e imediato do ativo isolado após a desinfecção.

12.2.2.13 A solução deve possuir mecanismo de proteção às aplicações, serviços e sistemas operacionais vulneráveis.

12.2.2.14 A solução deve possuir capacidade de executar detecção em tempo real (real-time) contra-ataques direcionados e às vulnerabilidades do navegador de internet (browser).

12.2.2.15 A solução deve possuir, no mínimo, detecção e prevenção de casos de infecção por navegação na internet em sites com código de exploração de navegadores e seus plug-ins, ataques de “drive-by download”, na abertura de documentos em formato PDF, Microsoft Office, ataques de “spear phishing” e explorações em outros vetores de ataque como Java e ActiveX.

12.2.2.16 A solução deve possuir funcionalidade de resposta automatizada e configurável aos incidentes de segurança. As funcionalidades referentes a resposta a incidentes de segurança e contenção de ameaças devem ser passíveis de automatização.

12.2.2.17 A solução deve ser capaz de executar rastreamento nos ativos de informação onde estão instalados e, após isso, deverá fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas, bem como do sistema operacional.

12.2.2.18 A solução deve possuir capacidade de implementar varreduras otimizadas em ativos de informação sejam eles físicos ou virtuais.

12.2.2.19 A solução deverá se integrar com virtualizadores e hiperconvergente, ou diretmanete com as maquinas virtuais, permitindo a sincronização das máquinas conectadas a ele, e prover a análise e proteção das camadas que compõem esse serviço.

12.2.2.20 A solução deve manter suas funcionalidades de proteção de endpoint ativas, independente de conexão com o Gerenciador, garantindo proteção contínua mesmo em caso de falha na conexão com o servidor de gerenciamento.

12.2.2.21 A solução deve possuir análise Comportamental (Behavioral Analysis) ou similar, detectando ameaças baseadas em comportamento anômalo, mesmo que sejam desconhecidas pelas assinaturas de malwares.

12.2.2.22 A solução deve monitorar atividades de criptografia de arquivos e sistemas operacionais para evitar ataques de *ransomware ou similar.*

12.2.2.23 A solução deve ser capaz de restaurar arquivos e sistemas comprometidos por ransomware, através, por exemplo, de backups e funções de recuperação de dados.

12.2.2.24 A solução deve mitigar e conter ataques de exploração de Memória (Memory Exploit Mitigation) ou similar, permitindo realizar dump de memória para subsidiar o processo de análise de incidentes.

12.2.2.25 A solução deve mitigar e conter ataques de exploração da infraestrutura interna e ambiente de nuvem.

12.2.2.26 A solução deve ser capaz de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e demais aplicações.

12.2.2.27 As vulnerabilidades descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso.

12.2.2.28 A funcionalidade de emulação para malware ou similar, deve ter suporte para as plataformas Windows (32 e 64 bits), Linux (32 e 64 bits) e Mac (32 e 64 bits), ou possuir tecnologia para análise de ameaças desconhecidas em ambiente controlado em nuvem própria do fabricante.

12.2.2.29 A solução deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de 0Day (dia zero), mitigando, no mínimo, os conhecidos comportamentos de exploração de vulnerabilidades a seguir:

12.2.2.29.1 SEHOP - Structured Exception Handler Overwrite Protection ou similar.

12.2.2.29.2 Heap Spray (Exploits que iniciam através do HEAP) ou similar.

12.2.2.29.3 Java Exploit Protection.

12.2.2.29.4 ForceDEP ou similar

12.2.2.29.5 Falha em aplicação causada por exploit.

12.2.2.29.6 Ataque ROP ou similar.

12.2.2.29.7 Drive-by download de programas.

12.2.2.29.8 Exploração de macro em arquivos do Microsoft Office.

12.2.2.29.9 Escalação de privilégios.

12.2.2.30 A CONTRATADA deverá comprovar a capacidade da solução de prove o item 12.2.2.29 e seus subitens mediante documentação técnica ou carta do fabricante.

12.2.2.31 A solução deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code" e suas variantes, assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem das aplicações, dos sistemas e dos sistemas operacionais contra exploração de vulnerabilidades conhecidas de dia zero (0day).

12.2.2.31.1 As fontes de dados para avaliação do risco não devem se limitar àquelas desenvolvidas pela própria solução, sendo aceitas soluções de terceiros.

12.2.2.32 A solução deve permitir acessar, no mínimo, às funções de:

12.2.2.33 Gerenciar o status de uma tarefa através da gerência.

12.2.2.34 Gerar logs das detecções, infecções, bloqueios e outras ações que as demais funcionalidades tenham tido alguma ação.

12.2.2.35 Permitir ao usuário realizar uma análise em pastas, arquivos, aplicações e demais arquivos a qualquer tempo.

12.2.2.36 A solução deve ter a capacidade de receber instruções de comando contra-ataques de APT (Ameaça Persistente Avançada) ou similar, sem a necessidade de interpretação pelo gerenciador do endpoint, possibilitando ações mais rápidas, assertivas e minimizando falsos positivos.

12.2.2.37 A solução deve ser do mesmo fabricante, e possibilitar a visualização de toda a cadeia de ataque ou da tentativa de exploração de uma vulnerabilidade permitindo analisar no mínimo: sua origem, identificar as ameaças relacionadas, linha de tempo dos logs, os ativos de informação

relacionados e comprometidos, os metadados relevantes à análise dos incidentes, e que gere informação para proteção efetiva do ambiente e para análise sólida das ações.

12.2.2.38 A partir dos alertas gerados, a solução deve correlacionar os ativos de informação, contendo, no mínimo: IPs, hashs envolvidos, nome do ativo, data e hora, apontando possíveis indicadores de comprometimento (IOCs) nos ambientes.

12.2.2.39 A solução deve possuir um mapa que permita a identificação visual sobre a origem das ameaças de modo a facilitar a visualização de eventos para que ações imediatas sejam providenciadas.

12.2.2.40 A solução deve possuir resposta imediata, preferencialmente de forma automática, para remediar as detecções\intrusões, agindo de forma proativa diante de suspeita de incidentes, permitindo encerrar processos, isolar e restaurar ativos de informação, fazer varreduras ou análise e aplicar atualizações de forma automatizada e restaurar qualquer configuração realizada a fim de conter um incidente ou problema, seja ele de segurança ou não.

12.2.2.41 Em caso de erro ou interrupção, durante uma varredura, a solução deve gerar logs para troubleshotting (solução de problemas).

12.2.2.42 A solução deve ser capaz de identificar ameaças em tempo real e permitir análise profunda com inteligência para identificar e prevenir ataques.

12.2.2.43 O sensor deverá gerar telemetria para correlação de eventos a fim de subsidiar o processo de gestão de incidente do Ministério.

12.2.2.44 A solução deve inspecionar os domínios e subdomínios (públicos) trazendo informações sobre possíveis comprometimentos que possam subsidiar as ações de contenções.

12.2.2.45 A solução deve possuir a capacidade de identificar artefatos com comportamento malicioso e permitir análise em Sandbox a fim de analisar comportamento de, no mínimo: execução de aplicativos, utilização de SDKs de terceiros, vulnerabilidades e categoria de aplicativos.

12.2.2.46 A solução deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em sandbox com a gerência centralizada do fabricante.

12.2.2.47 A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas.

12.2.2.48 A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente.

12.2.2.49 A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso.

12.2.2.50 A solução deve ser capaz de verificação de tráfego HTTP/HTTPS. E analisar\bloquear qualquer script do Windows Script Host (Java Script, Visual Basic Scripte e etc.) usando heurísticas.

12.2.2.51 A solução deve ter suporte total ao protocolo IPv6.

12.2.2.52 A proteção anti-spyware e adware deverá ser nativa da solução, ou seja, não dependente de plugin ou módulo adicional.

12.2.2.53 A solução deve permitir verificar arquivos por conteúdo, ou seja, verificará o arquivo se for passível de infecção. A solução deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar somente a partir da extensão do arquivo.

12.2.2.54 A solução deve ser capaz de verificar objetos usando heurística ou equivalente.

12.2.2.55 A solução deve permitir configurar quais tipos de arquivos serão verificados (ex: arquivos comprimidos, arquivos auto descompactáveis, .PST, arquivos compactados por compactadores binários, executáveis, cab, msi e outros), ou trabalhar de forma de exclusões.

12.2.2.56 A solução deve ser capaz de impedir a execução ou instalação de aplicativos e softwares que constam na lista negada (deny list).

12.2.2.57 A solução deve permitir a criação de listas de exclusões ou exceções na qual as pastas, processos, diretórios, arquivos de sistemas, arquivos e aplicações não serão verificados pela solução.

12.2.2.58 A instalação dos agentes é de responsabilidade da Contratada e deve ser feita de forma autônoma e oculta, sem a necessidade de interação com o usuário.

12.2.2.59 A solução deve utilizar comunicação segura (criptografada) entre o servidor de gerenciamento e o cliente gerenciado.

12.2.2.60 A solução deve ser capaz de procurar códigos maliciosos pelo tipo real de arquivo.

12.2.2.61 A solução não deve restringir o uso e instalação em desktops e servidores hospedados na nuvem.

12.2.2.62 A solução deve ter proteção contra desinstalação e desativação não autorizada protegendo contra mudança do seu estado, ou seja, não possibilitar que um administrador do ativo de informação possa parar o serviço da solução, bem como mecanismo para restaurar seu estado normal.

12.2.2.63 A solução deve possibilitar criar uma cópia backup do arquivo suspeito antes de qualquer ação.

12.2.2.64 A solução deve possibilitar criar uma imagem para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional.

12.2.2.65 A solução deve ser capaz de limitar o acesso dos sistemas e aplicativos a recursos do sistema operacional, como chaves do registro e pastas e arquivos, em casos de falha, permitir a limpeza de chaves e pastas.

12.2.2.66 A solução deve detectar de forma proativa de reconhecimento de novas ameaças.

12.2.2.67 A solução deve possibilitar recuperar instalação, preferencialmente de forma automática, nos ativos de informação em caso de falha.

12.2.2.68 A solução deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones.

12.2.2.69 A solução deve possuir a funcionalidade de Firewall e de Detecção e Proteção de Intrusão.

12.2.2.70 Para a funcionalidade de firewall a solução deve ser capaz de permitir ativar em modo ativo ou passivo (modo de escuta), independente da quantidade de placas de rede que o ativo tenha configuradas.

12.2.2.71 A solução deverá prover proteção, identificação e gestão de segurança aos ativos de informação do Ministério.

12.2.2.72 A solução deve proteger em tempo real ou varredura de portas lógicas do sistema operacional para identificar portas que estejam abertas possibilitando tráfego de entrada ou saída.

12.2.2.73 A solução deve proteger em tempo real contra vírus, trojans, ransomware, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos, tanto para o tráfego de entrada quanto de saída.

12.2.2.74 A solução deverá conter regras pré-definidas para detecções de ransonware e suas principais famílias.

12.2.2.75 A solução deve possibilitar o retorno da versão (rollback) anterior das vacinas, das regras, das configurações e dos agentes e seus componentes, preferencialmente de forma automatizada.

12.2.2.76 A instalação, remoção, reinstalação e configuração da solução deve possibilitar o agendamento ou adiamento da reinicialização do ativo de informação, caso necessário.

12.2.2.77 A solução deverá fornecer em tempo real o status atualizado da solução com, no mínimo, as seguintes informações: versão dos arquivos de vírus (update), dos mecanismos de verificação/correção (engine) e dos programas que compõem a solução.

12.2.2.78 A solução deverá possuir rotinas bem definidas de atualizações e de logs.

12.2.2.79 A solução deverá utilizar análise comportamental podendo utilizar como fonte de aprendizado redes de inteligências de detecção correlacionando técnicas de proteção e vetores de ataque preventivamente.

12.2.2.80 A solução deve ter a capacidade de monitorar o status de serviços e processos do sistema operacional.

12.2.2.81 A solução deve implementar a proteção contra acesso a websites ou URLs consideradas maliciosas, de baixa reputação ou não categorizadas.

12.2.2.82 A solução deve permitir a criação de listas de exclusão, possibilitando aos usuários acessar determinadas URLs especificadas pelo administrador do sistema.

12.2.2.83 As atualizações do produto (vacinas, assinaturas e outros componentes) não devem causar interrupção do serviço e devem ser feitas de forma automática, manual ou permitir o agendamento, sendo realizada por ativo, grupo de ativos, range de IP ou tags de identificação.

12.2.2.84 A solução deve ser capaz de detectar tentativas de mascaramento, evasão de detecção através do uso de portas comuns, tentativas de scan de rede, ataque de força bruta, tunelamento de protocolos, entre outras.

12.2.2.85 A solução deve analisar dinamicamente códigos, bibliotecas dinâmicas (DLL), arquivos do Adobe Flash (SWF), rootkits, daemons e outros.

12.2.2.86 A solução deve ser capaz de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e demais aplicações.

12.2.2.87 A solução deve ser capaz de analisar o ativo de informação, recomendando e permitindo aplicar

regras que protejam contra explorações de vulnerabilidades existentes

12.2.2.88 A solução deve ser capaz de armazenar o pacote capturado ou as informações de todos os artefatos quando detectar um ataque.

12.2.2.89 A solução deverá prover detecção e proteção em múltiplas camadas para verificação de malware e/ou códigos maliciosos.

12.2.2.90 A solução deve possuir funcionalidades, inclusive recursivo em vários níveis, que permitam a detecção e limpeza de arquivos contaminados por códigos maliciosos mesmo que sejam compactados. Essa limpeza deve ocorrer sem a descompactação do arquivo.

12.2.2.91 A solução deve permitir customização avançada e criação de novas regras de proteção de aplicações (blindagem), protegendo contra vulnerabilidades específicas de sistemas.

12.2.2.92 A solução deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede.

12.2.2.93 Características da Solução de Antimalware com XDR e Atualização Continuada para Desktops

12.2.2.94 A solução deve possuir proteção avançada de antimalware para estações de trabalho e notebooks.

12.2.2.95 A solução deve possuir proteção Web para verificação de sites, inclusive tráfego HTTPS, e downloads a fim de impedir o acesso e mitigar o risco de infecção por pragas virtuais.

12.2.2.96 A solução deve possuir a funcionalidade de controle de dispositivos e aplicações. O Controle de Aplicações, ou similar, deve ser capaz de identificar as aplicações por, no mínimo, dos seguintes métodos:

12.2.2.96.1 Hash do executável ou similar.

12.2.2.96.2 Atributos do certificado utilizado para assinatura digital do executável ou similar.

12.2.2.96.3 Caminho lógico do executável.

12.2.2.96.4 Base de assinaturas de certificados digitais válidos e seguros ou com base na assinatura da aplicação.

12.2.2.96.5 O Controle de Dispositivos, ou similar, deve ter a capacidade para bloqueio ou limitar a escrita e leitura de dispositivos USB e discos de armazenamento locais.

12.2.2.96.6 O Controle de Dispositivo deve possibilitar que habilite ou não, no mínimo, os dispositivos:

12.2.2.96.6.1.1 Disco de armazenamento local

12.2.2.96.6.2 Impressoras

12.2.2.96.6.3 Dispositivos de Entrada (Adaptadores de rede sem fio, Cameras, Teclado, Mouse)

12.2.2.96.7 A solução deve possibilitar limitar ou bloquear a execução de aplicativos por, no mínimo, hash, nome do arquivo, nome do aplicativo, versão do aplicativo, ainda que em armazenamento externo e removível.

12.2.2.96.8 A solução deve possuir proteção para o cliente de e-mail a fim de verificar e-mails e seus anexos.

12.2.2.96.9 A solução deve ter capacidade de implementar técnicas de XDR (Detecção e Resposta Estendidas) ou similar, possibilitando detecção e investigação nos ativos de informação, a fim de visualizar toda a cadeia de ataque ou da tentativa de exploração de uma vulnerabilidade permitindo analisar no mínimo: sua origem, identificar as ameaças relacionadas, linha de tempo dos logs, os ativos de informação relacionados e comprometidos, os metadados relevantes à análise dos incidentes, e que gere informação para proteção efetiva do ambiente e para análise sólida das ações.

12.2.2.96.10 A solução deve ser capaz de resumir automaticamente tarefas de verificação ou análise que tenham sido paradas por anormalidades (queda de energia, erros, intervenção do usuário, etc).

12.2.2.96.11 A solução deve ser capaz de identificar e bloquear a origem da infecção informando, no mínimo: nome, IP da origem, tipo de infecção, dentre outras, a fim de evitar a propagação pela rede.

12.2.2.96.12 A solução deve permitir a criação de grupos, incluindo grupo de testes, a fim de validar escaneamentos, envio de atualizações, blindagens, regras, políticas, comando de isolamentos, automações e outras para validações antes de aplicar no ambiente de produção.

12.2.2.96.13 A solução deve possibilitar a instalação e remoção de forma remota e automatizada, preferencialmente via console de gerenciamento, com opção de remoção de soluções previamente instaladas.

12.2.2.96.14 A solução deve possibilitar emulação de malwares (Emulation for Malware) ou similar.

12.2.2.96.15 A solução deve possuir a funcionalidade de mitigação e controle de exploração de vulnerabilidades (Exploit Mitigation), ou similar, em aplicações e sistemas operacionais.

12.2.2.96.16 A solução deverá ser compatível com sistemas operacionais: Windows (32 e 64 bits), MacOS nas versões (32 e 64 bits) e Linux (32 e 64 bits), incluindo Ubuntu.

12.2.2.96.17 A solução deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória ou similar, impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:

12.2.2.96.18 Adobe.

12.2.2.96.19 Flash.

12.2.2.96.20 Java.

12.2.2.96.21 Navegadores (Internet Explorer, Microsoft Edge, Chrome, Safari e Mozilla Firefox).

12.2.2.96.22 A solução deve permitir verificação de malwares, através da console de gerenciamento, em recursos mapeados da rede.

12.2.2.96.23 A solução deve ser capaz de detectar e remover vírus de macro.

12.2.2.96.24 A solução deve possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede.

12.2.2.96.25 A solução deve possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações.

12.2.2.96.26 A solução deve ser capaz de identificar e bloquear informações independente do meio de transmissão.

12.2.2.97 Características da Solução de Antimalware com XDR e Atualização Continuada para Servidores

12.2.2.4.1 A solução deve possuir a funcionalidade de controle de dispositivos e aplicações.

12.2.2.4.2 A solução deve possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações.

12.2.2.97.1 A solução deve possuir a capacidade de detectar tráfego malicioso nas portas dos sistemas operacionais, inclusive quando houver mudança no estado das portas.

12.2.2.97.2 A solução deve possuir a capacidade de criação de regras avançadas para proteção em chaves de registro, diretórios e subdiretórios.

12.2.2.97.3 A solução e suas funcionalidades deverão funcionar em servidores físicos, virtuais, em nuvem e conteinerizado, com configurações e regras específicas que possibilitem diminuir o impacto aos sistemas operacionais e aplicações.

12.2.2.97.4 A solução deve possuir funcionalidades de otimização de recursos para os sistemas operacionais em servidores físicos e virtuais, a fim de atender demandas específicas do Ministério.

12.2.2.97.5 A solução deve fornecer o escaneamento ou análise e envio de atualizações, de vacinas ou blindagens, de regras, de políticas, de anti-exploits e outras blindagens para todos os tipos de servidores.

12.2.2.97.6 A solução deve possuir a capacidade de isolamento, em caso de tráfego malicioso, de placa de rede de forma que apenas uma fique funcionando, permitindo aplicar políticas diferentes para cada placa de redes.

12.2.2.97.7 A solução deve ter capacidade de implementar técnicas de XDR (Detecção e Resposta Estendidas) ou similar, possibilitando detecção e investigação nos ativos de informação, a fim de visualizar toda a cadeia de ataque ou da tentativa de exploração de uma vulnerabilidade permitindo analisar no mínimo: sua origem, identificar as ameaças relacionadas, linha de tempo dos logs, os ativos de informação relacionados e comprometidos, os metadados relevantes à análise dos incidentes, e que gere informação para proteção efetiva do ambiente e para análise sólida das ações.

12.2.2.97.8 A solução deve possuir a capacidade de analisar o sistema operacional e aplicações, recomendando regras de monitoramento, regra de IPS e configurações que aumentem o nível de segurança de acordo com o resultado dessa análise.

12.2.2.97.9 A solução deve ser compatível com, no mínimo, os seguintes sistemas operacionais: Windows Server (32 e 64 bits). Linux e suas variantes (32 e 64 bits).

12.2.2.97.10 A solução deve permitir ao administrador do sistema não aplicar automaticamente a proteção para as vulnerabilidades, podendo escolher por host, range de IP, tags personalizadas ou outro tipo de identificação.

12.2.2.97.11 A solução deve possibilitar proteger de forma automática e transparente contra falhas de segurança descobertas, interrompendo somente o tráfego malicioso.

12.2.2.97.12 A solução deve ter a capacidade de bloquear exploits que trabalham em nível de "shell code", assim como, implementar qualquer técnica para blindagem de sistemas operacionais e aplicações contra exploração de vulnerabilidades conhecidas.

12.2.2.97.13 O firewall de host da solução deve operar em modo ativo ou em modo passivo (modo de escuta), monitorando as comunicações nos servidores.

12.2.2.97.14 As regras de firewall de host da solução devem permitir, no mínimo, as seguintes ações ou ações equivalentes: Liberar, Somente Registar o Log e Negar.

12.2.2.97.15 A solução deve ser capaz de controlar o tráfego baseado no Tipos de Protocolos, Endereços IP e intervalo de portas.

12.2.2.97.16 A solução deve ser capaz de analisar o servidor detectando o tipo e versão do sistema operacional e demais aplicações, recomendando ações para blindagem ou patching de vulnerabilidades existentes no sistema operacional e nas aplicações.

12.2.2.97.17 A solução deve permitir que a opção de detecção e bloqueio seja implementada de forma global, apenas para um ativo ou grupos de ativos.

12.2.2.97.18 Ações de blindagem e aplicação de patching de correção deverão ocorrer independente da camada de virtualização, seja ela conteinirizada, virtualizada ou hiperconvergente Nutanix..

12.2.2.97.19 A solução deve possuir um módulo de Proteção Web para verificação de sites, inclusive tráfego HTTPS, e downloads a fim de impedir o acesso e mitigar o risco de infecção por pragas virtuais.

12.2.2.97.20 A solução deve ser capaz de bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede.

12.2.2.97.21 A solução deve permitir que as regras de IPS ou anti-exploit atuem detectando ou bloqueando os eventos que as violem, de modo que o administrador possa decidir qual ação deva ser tomada.

12.2.2.98 Características da Solução de Antimalware com XDR e Atualização Continuada para Contêiners

12.2.2.98.1 A solução deve ser capaz de identificar e bloquear ataques entre contêineres.

12.2.2.98.2 A solução deverá utilizar sensores para escanear imagens de container localizadas no datacenter on-premises e em nuvem.

12.2.2.98.3 A solução deverá analisar as imagens e os containers durante a fase de desenvolvimento, no processo deploy, após o deploy e em tempo de execução.

12.2.2.98.4 Durante a fase de desenvolvimento a solução deve ter a capacidade de identificar vulnerabilidades, códigos maliciosos, chaves privadas e segredos, além de violação de conformidade, antes da imagem ir para a produção.

12.2.2.98.5 Na fase de deployment a solução deverá ter a capacidade de controle de admissão baseado em políticas, o qual deverá bloquear imagens que estejam fora do padrão definido pela organização.

12.2.2.98.6 Durante a execução em produção, a solução deverá ser capaz de fazer uma verificação contínua da conformidade e das regras aplicadas na fase de homologação.

12.2.2.98.7 As políticas da solução devem ser segmentadas de acordo com as fases do pipeline.

12.2.2.98.8 A solução deve detectar tanto ameaças instaladas via gerenciador de pacote quanto aplicações instaladas diretamente.

12.2.2.98.9 As análises realizadas pelos sensores devem ser enviadas para a console de gerenciamento para fins de reporte e correlação.

12.2.2.98.10 A solução deve monitorar, quando em execução, os containers em busca de ações que violem as regras pré-definidas e mapeadas na matriz do MITRE ATT&CK.

12.2.2.98.11 A solução ao identificar vulnerabilidades deverá apresentar, no mínimo: detalhamento do CVE relacionado, índice de exposição do risco e ações a serem tomadas.

12.2.2.98.12 Durante a fase de implantação, a solução deve permitir apenas monitorar as atividades dos containers e, caso o administrador deseje, a solução deve permitir realizar bloqueio da ação, isolamento e restauração do pod, de acordo com a fase.

12.2.2.98.13 A solução deve ser compatível com soluções de cluster Kubernetes em nuvem, incluindo: Amazon Kubernetes Service (EKS), Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS) e outras tecnologias de contêiners do mercado.

12.2.2.98.14 A solução deve exibir os eventos que ocorreram nos containers, contemplando ao menos: ação, data/hora, cluster, política e regra que gerou o evento, severidade, nome da imagem do container, nome do pod.

12.2.2.98.15 A solução deve ser capaz de criar regras de proteção e compliance baseadas nas propriedades do pod, da imagem e do container, baseadas resultados do escaneamento da imagem e acesso ao kubectl.

12.2.2.98.16 A solução deve permitir criar regras e exceções, incluindo, no mínimo:

12.2.2.98.17 Containers que executam com permissão de root.

12.2.2.98.18 Containers com permissão para escalar privilégios.

12.2.2.98.19 Containers que podem escrever em sistemas de arquivos root.

12.2.2.98.20 Imagens de container com malware.

12.2.2.98.21 Imagens de container com vulnerabilidades.

12.2.2.98.22 O sensor da solução deve ser compatível com a arquitetura de microsserviços.

12.2.2.98.23 A solução deve ser integrada à esteira de desenvolvimento da organização para analisar imagens de containers antes que elas possam ir para a produção.

12.2.2.98.24 A solução deve possuir API's que possam ser utilizadas para a integração da solução com softwares de terceiros.

12.2.2.98.25 A solução deve realizar análise de maneira automática no momento da build da imagem ou sob demanda.

12.2.2.98.26 Os resultados das análises realizadas pelos sensores devem ser enviados para console para serem utilizados como objetos para as políticas e regras.

12.2.2.98.27 A solução deve contemplar proteção contra-ataques: direcionados e suas variantes, 0Day (dia zero), ransomware, malwares, backdoors, vulnerabilidades desconhecidas ou novas, tais como as que possam causar estouro de buffer (overflow), ataques iniciados a partir de mídias removíveis, proteção contra BOTs e variantes, e ainda ter tecnologia de análise de comportamentos suspeitos para detecção e eliminação de ameaças desconhecidas, entre outras formas de ataque.

12.2.2.98.28 A solução deve detectar segredos e chaves incorporados nas imagens.

12.2.2.98.29 A solução deve realizar consultas de verificação personalizadas para encontrar arquivos suspeitos ou indesejados.

12.2.2.98.30 A solução deve analisar o conteúdo da imagem baseado em uma lista de verificação de conformidade que inclua itens do documento público NIST 800-190, Appendix B—NIST SP 800-53 and NIST Cybersecurity Framework Security Controls Related to Container Technologies.

12.2.2.98.31 A solução deve fornecer os níveis de criticidade das vulnerabilidades encontradas em cada análise.

12.2.2.98.32 A solução deve ter a capacidade de criar regras manuais, além das regras automáticas fornecidas pela solução, incluindo o formato YARA.

12.2.2.99 Características da Solução de Antimalware com XDR e Atualização Continuada para Ambiente de Colaboração

12.2.2.99.1 A solução deve permitir a identificação e proteção contra ameaças no Microsoft Office 365 e Google GSuite.

12.2.2.99.2 A solução deve identificar e bloquear ações realizadas pelos usuários, quanto a tentativas de carregar arquivos maliciosos para o Microsoft Office 365 e Google GSuite.

12.2.2.99.3 A solução deve ser capaz de analisar ameaças em tempo real nos serviços integrados, identificando componentes maliciosos e tomando as ações necessárias para conter ameaças.

12.2.2.99.4 A solução deve ser capaz de analisar ameaças mesmo que os arquivos estejam armazenados nas caixas de email dos usuários ou em diretórios do Microsoft Office 365 e Google GSuite.

12.2.2.99.5 A solução deverá integrar nuvem-a-nuvem, através de API da Microsoft e Google.

12.2.2.99.6 As políticas da solução deverão ser aplicáveis por usuário ou grupo sincronizado da estrutura de serviço online (Microsoft ou Google).

12.2.2.99.7 A solução deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em sandbox com a gerência centralizada do fabricante.

12.2.2.99.8 A solução deve ter a capacidade de integração com serviços de autenticação de single sign-on com, pelo menos, ADFS e Azure AD.

12.2.2.99.9 A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente ou evento.

12.2.2.99.10 A solução deve ser capaz de apresentar informações relacionadas à matriz do MITRE para cada um dos eventos detectados no ambiente, caso possuam.

12.2.2.99.11 A solução deve utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente.

12.2.2.99.12 A solução deverá possuir integração nativa com a plataforma de XDR via API, não sendo aceito integrações que necessitem agentes adicionais ou plug-ins.

12.2.2.100 Especificações Técnicas da Console de Gerenciamento - Solução de Antimalware com XDR

12.2.2.100.1 A solução deve ser capaz de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status da solução, etc.)

12.2.2.100.2 A solução deve ser capaz de identificar os ativos de informação com agentes desatualizados.

12.2.2.100.3 A solução deve registrar tentativas e impedir limpeza ou manipulação dos logs do sistema operacional.

12.2.2.100.4 Os logs registrados por meio do agente devem ser acessíveis por SSH, SCP ou HTTPS, sempre com controle de acesso.

12.2.2.100.5 A solução deve possibilitar a listagem dos computadores infectados usando como parâmetros as informações enviadas pelos agentes com base na rede de inteligência (threat inteligence) do fabricante.

12.2.2.100.6 A solução deverá permitir acessar as configurações via HTTPS para autenticação dos administradores, bem como, permitir o uso do múltiplo fator de autenticação (MFA) e permitir configurar senha para acessar as configurações do cliente para os ativos de informação.

12.2.2.100.7 A solução deve ser capaz de exibir a lista dos ativos de informação que possuam o antimalware instalado, contendo, no mínimo, informações como: nome da máquina, usuário logado, versão do antivírus, versão do agente, data da vacina, data da última verificação, status da solução, data da última comunicação com a console, dentre outras).

12.2.2.100.8 No gerenciamento de licenças da solução, deve ser informada a quantidade contratada e quantidade em utilização de clientes.

12.2.2.100.9 A solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras.

12.2.2.100.10 A solução deve permitir realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.

12.2.2.100.11 A solução deve ser capaz de gerar relatórios dos e-mails suspeitos identificados nos ativos de informação.

12.2.2.100.12 A solução deve possuir a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas a partir de uma console para gestão e configuração de seus módulos.

12.2.2.100.13 A solução deve ser capaz de distribuir pacotes de instalação dos agentes, de atualizações, tanto do agente quanto de vacinas, bem como as configurações dos seus módulos para quaisquer ativos de informação ou grupod e ativos a partir da console, por meio de compartilhamento administrativo, script de logon, GPO de Active Directory ou outra solução homologada pelo Ministério.

12.2.2.100.14 A solução deve ter a capacidade de implementar integração entre a gerência e plataformas de terceiros (ferramentas para BI, por exemplo).

12.2.2.100.15 A solução deve possibilitar a monitoração e geração de relatórios a partir da console de administração.

12.2.2.100.16 A solução deve possibilitar a criação de dashboards personalizados que apresente componentes gráficos para monitoração e visualização de informações de agentes (ativos), versões de agentes, linha do tempo de eventos, status de proteção, eventos listados por: ativo de informação, nome do processo/ameaça, regras, usuários e grupos e informações atualizadas diariamente sobre principais riscos de cibersegurança e permitir a exportação para, no mínimo, dois formatos distintos.

12.2.2.100.17 O gerenciamento da solução deve estabelecer uma correlação de eventos entre os módulos gerenciados possibilitando priorização nas ações a serem tomadas, possibilitar ainda uma análise inteligente dos eventos relacionados, identificação das tentativas de exploração e identificação de toda a cadeia de ataque ou da tentativa de exploração de uma vulnerabilidade permitindo analisar, no mínimo: sua origem, identificar as ameaças relacionadas, linha de tempo dos logs, os ativos de informação relacionados e comprometidos, os metadados relevantes à análise dos incidentes, e que gere informação para proteção efetiva do ambiente e para análise sólida das ações.

12.2.2.100.18 A solução deve fornecer ferramenta de pesquisa de ativos de informação que não possuem o agente instalado, com opção de instalação preferencialmente de forma remota ou atraves de scripts ou GPO.

12.2.2.100.19 A solução deve permitir atualizar os agentes a partir de um ponto centralizado, ou seja, sem a necessidade de intervenção local. Em caso de falha durante a atualização, a solução deve ser capaz de abortar a instalação de forma automática ou manual e manter a versão atual.

12.2.2.100.20 A solução deve ser capaz de fazer integrações por meio de API REST via serviço Web utilizando o protocolo HTTPS com autenticação.

12.2.2.100.21 A solução deve permitir ao administrador configurar para cada tipo de ameaça, no mínimo, as ações:

12.2.2.100.21.1Quarentenar

12.2.2.100.21.2Limpar.

12.2.2.100.21.3Excluir, nesse caso deve permitir análise sandbox

12.2.2.100.22 A console deve possuir integração com LDAPs e com o serviço de diretório Microsoft Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

12.2.2.100.23 A solução deve permitir a divisão lógica dos computadores ou da rede, dentro da estrutura de gerenciamento em domínios, grupos ou através de endereçamento IP com administração individualizada por grupo e máquina.

12.2.2.100.24 A solução deve possuir um Controle de Aplicações (Application Control) ou similar, com capacidade de criação de regras e políticas personalizadas definindo quais aplicativos ou sistemas podem ou não ser executados pelos usuários.

12.2.2.100.25 A solução deve permitir a configuração de ações diferenciadas para cada tipo de ativo de informação (Servidor de arquivos, web, banco de dados, entre outros).

12.2.2.100.26 A solução deve permitir a criação de listas de exclusões ou exceções na qual as pastas, arquivos e aplicativos não serão verificados pela solução.

12.2.2.100.27 A solução deve possuir backups da base de dados da solução, para atendimento a auditorias internas e recuperação de desastres.

12.2.2.100.28 A solução deve permitir selecionar quais módulos serão instalados ou ativados, tanto na instalação local quanto na instalação remota, possibilitando a instalação ou ativação posterior.

12.2.2.100.29 A solução deverá suportar o tráfego de trabalho, garantindo a alta disponibilidade, o balanceamento de carga e tolerância a falhas, mesmo que esteja em serviço na nuvem.

12.2.2.100.30 A solução deve possibilitar a indicação de ativos para efetuar a função de replicador de atualizações e configurações. para ambiente interno, inclusive para aqueles que não possuem conectividade com a internet.

12.2.2.100.31 A solução deve descobrir automaticamente os endpoints que não possuem o cliente instalado e executar a instalação remota, atraves de scrpits ou GPO.

12.2.2.100.32 A solução deve possibilitar notificar os administradores por e-mail caso a solução não receba atualizações por um determinado período.

12.2.2.100.33 A console de gerenciamento deve permitir somente ao administrador desabilitar as configurações nos ativos de informação, desinstalar ou parar o serviço da solução.

12.2.2.100.34 A console de gerenciamento deve permitir somente ao administrador desabilitar separadamente os itens e cada um dos subitens de acesso as configurações dos ativos, bem como distinguir diferentes sub-redes e grupos para ativar ou desativar funcionalidades.

12.2.2.100.35 A solução dever ser capaz de criar contas de usuário com diferentes níveis de acesso de administração e operação.

12.2.2.100.36 A console da solução deverá fornecer acesso gráfico aos eventos e alertas detectados, com opção de salvaguardar dos logs ou direcioná-los para um servidor syslog ou através de API, além de oferecer mecanismos de emissão de alarmes via comunicação eletrônica (e-mail, teams) e syslog ou SNMP.

12.2.2.100.37 Todos os eventos gerados pela solução devem ser armazenados por um período mínimo de 6 (seis) meses.

12.2.2.100.38 A console deverá possibilitar a criação, edição, habilitação, desativação e deleção de alertas customizados, com emissão via SNMP ou integração via API, para integração com outros sistemas de gerenciamento.

12.2.2.100.39 A solução deverá possuir integração com sistemas SIEM, para possibilitar coleta de logs de gerenciamento e correlação em tempo real.

12.2.2.100.40 A solução deve possuir capacidade para respostas de forma autônoma ou automatizada, visando remediar ou bloquear as detecções\intrusões, permitindo minimamente: atualizar listas de bloqueios e exceções (IOCs), compartilhar dados de inteligência, e ainda possuir a capacidade de reverter qualquer configuração realizada a fim de conter um problema.

12.2.2.100.41 A solução deve possuir capacidade agnóstica para emissão de respostas de forma autônoma ou automatizada, visando remediar as detecções\intrusões em diferentes tecnologias, permitindo minimamente: atualizar listas de bloqueios e exceções, compartilhar dados de inteligência, executar validações em soluções externas, encerrar processos, isolar e restaurar ativos de informação, fazer varreduras ou análises e aplicar atualizações de forma automatizada, ou reverter qualquer configuração realizada a fim de conter um incidente ou problema

12.2.2.100.42 A solução deve possibilitar notificar eventos e enviar alertas de forma proativa para os administradores.

12.2.2.100.43 A solução deve apresentar alertas ou informações na console, caso os dados de telemetria gerados tenham relação com algum tipo de campanha de ameaças globais.

12.2.2.100.44 A solução quando enviar arquivo à quarentena, deve possibilitar remover manualmente e através da console esses arquivos.

12.2.2.100.45 A solução deve permitir que a estação de trabalho seja atualizada via internet como forma alternativa ao ser desconectada da rede corporativa.

12.2.2.100.46 A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade.

12.2.2.100.47 A solução de gerência em nuvem, do próprio fabricante, deverá suportar o tráfego de trabalho, garantindo a alta disponibilidade, o balanceamento de carga e tolerância a falhas.

12.2.2.100.48 Caso necessário, a console de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais utilizados pelo Ministério.

12.2.2.100.49 A solução deve registrar e armazenar, no mínimo, as informações sobre o comportamento malicioso dos sistemas e aplicações, dos ativos de informação e dos usuários.

12.2.2.100.50 A solução deve possibilitar pesquisas em parâmetros, mínimos, como: comunicações específicas, malware específico ou hash, chave de registro, atividade da conta, processos em execução e IOCs.

12.2.2.100.51 A solução deve permitir a visualização e diagnóstico de eventos de segurança com base no histórico dos eventos registrados.

12.2.2.100.52 A solução deve possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base, no mínimo, sistemas e aplicações, dos ativos de informação e dos usuários.

12.2.2.100.53 A solução deve ser capaz configurar a verificação contra ameaças para ser executada de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do Sistema Operacional, processo em execução na memória principal, arquivos recebidos por meio de programas de comunicação instantânea e arquivos executáveis, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS, Shell e Terminal).

12.2.2.100.54 A solução deve permitir configurar agendamento e segregar ativos para início de análises de forma a otimizar e reduzir impactos no ambiente do Ministério.

12.2.2.100.55 A solução deve permitir configurar o consumo dos recursos dos ativos de informação que será consumido durante uma análise.

12.2.2.100.56 A solução deve possuir a capacidade de implementação de regras, incluindo regras de IDS/IPS, e regras diferenciadas por função do ativo de informação em determinados horários e que possam ser customizados pelo administrador.

12.2.2.100.57 A solução deve apresentar informações detalhadas das regras de blindagem contra vulnerabilidades, contendo links com referências externas, quando aplicável, explicando a vulnerabilidade do fabricante e CVE relacionado.

12.2.2.100.58 A solução deve possuir recurso de auditoria de alteração das configurações e de acesso à ferramenta de administração, incluindo, no mínimo, usuários, data e horário dos acessos e ações realizadas.

12.2.2.100.59 A solução deve permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários.

12.2.2.100.60 A solução deve permitir o uso de base de conhecimento do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações.

12.2.2.100.61 A solução deverá permitir a parametrização pelo administrador de, no mínimo, os seguintes itens:

12.2.2.100.62 A solução deve permitir a sincronização com servidores NTP e configuração de fuso horários, para fins de auditoria e atendimento ao PPSI.

12.2.2.100.63 Disponibilizados para acesso externo (SFTP ou outro método).

12.2.2.100.64 A solução deve possibilitar o envio, via protocolo seguro, de arquivos da área de isolamento ou capturados em uma análise de incidente, para o fabricante da solução, sob responsabilidade e supervisão da Contratada, desde que não infrinja a Lei Geral de Proteção de Dados (LGPD).

12.2.2.100.65 A solução deverá suportar integração com os principais sistemas de monitoramento, tais como: Zabbix, Nagios ou outros.

12.2.2.101 Características Gerais da Solução de Inspeção de Rede Contra Ameaças Avançadas com Detecção e Resposta (NDR)

12.2.2.101.1 A solução deverá ser instalada de modo a detectar ameaças avançadas e persistentes (APT) no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados.

12.2.2.101.2 A solução de análise de rede deve ser licenciada a fim de inspecionar o Throughput e as infraestruturas das redes da CONTRATANTE.

12.2.2.101.3 A solução deve atuar com a inspeção de rede da CONTRATANTE, estendendo visibilidade sob tráfego das redes.

12.2.2.101.4 A solução deve aplicar técnicas de análise de tráfego avançadas baseadas, no mínimo, em aprendizagem de máquina, em inteligência artificial ou comportamental.

12.2.2.101.5 A solução deve atuar com técnicas de detecção e resposta específicos para modelos de detecção focados em rede, de forma a identificar comportamentos maliciosos.

12.2.2.101.6 A solução deve permitir que as vulnerabilidades descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso.

12.2.2.101.7 A solução deve permitir que seja implantado em linha com o tráfego de rede e em modo de espelhamento.

12.2.2.101.8 Caso a solução seja implementada em linha, o sensor deve permitir a criação de regras de by-pass para casos de falhas.

12.2.2.101.9 A solução deve suportar o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança.

12.2.2.101.10 A solução, durante a inspeção do tráfego de rede em tempo real, deverá ser capaz de identificar anomalias na rede e gerar alertas em casos de tráfego suspeito.

12.2.2.101.11 A solução deve ter a capacidade de analisar tráfego criptografado, sem necessidade de licenciamento adicional.

12.2.2.101.12 A solução deve analisar, preferencialmente de forma automática, as fases de um ataque direcionado, persistente e avançado, identificando, no mínimo, tentativas de coletas de informação, movimentação lateral, exfiltração de dados, descoberta de dispositivos e comunicações de comando e controle (C&C), e ainda ser capaz de apresentar em seus logs,

visibilidade de acordo com a matriz ATT&CK MITRE, pontuando características de táticas e técnicas de acordo com a ameaça detectada pela solução.

12.2.2.101.13 A solução deve identificar e mapear possíveis pontos de entrada nas redes que possam ser exploradas por atacantes.

12.2.2.101.14 A solução deve ser capaz de detectar ameaças web derivadas de vulnerabilidades e downloads de conteúdo malicioso.

12.2.2.101.15 A solução deve analisar, no mínimo, os protocolos, portas e serviços: HTTP, HTTPS, LDAP, FTP, Telnet, WebSocket, SMTP, POP3, DNS, SMB, RDP, Kerberos, IRC, SGBDs e ARP, incluindo ainda os protocolos mascarados ou tunelados.

12.2.2.101.16 A solução deve permitir analisar arquivos e arquivos binários em sandbox, permitindo identificar, no mínimo, ataques avançados (APT), Zero Days, códigos de exploração (exploits) embutidos, comportamentos maliciosos, vulnerabilidades conhecidas e desconhecidas e arquivos maliciosos no tráfego de rede, de forma automática quando aplicável e com capacidade de operar vários ambientes simultâneos e integrados.

12.2.2.101.17 A solução deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo, no mínimo, arquivos executáveis, scripts, PDF´s, PPTX, DOCX, XLSX, LNK, ELF, CHM, RTF, ODP, DLLs, JAR, ZIP e RAR.

12.2.2.101.18 Os módulos que compõem a solução devem atuar de forma integrada.

12.2.2.101.19 A solução deve possuir atualização automática de regras, políticas, patchs enginers.

12.2.2.101.20 Não serão aceitos appliances de Unified Threat Management (UTM) e Next-Generation Firewall (NGFW) para monitoramento do tráfego, ainda que possua recurso e licenciamento específico para análise de ameaças em rede.

12.2.2.101.21 A solução deve possuir funcionalidades de rastrear malwares, baseadas em, no mínimo: Detectar ameaças utilizando técnicas comportamentais e estatísticas (heurísticas, comportamental ou preditiva); verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção; analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar somente a partir da extensão do arquivo.

12.2.2.101.22 A solução deve permitir verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. A solução deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar somente a partir da extensão do arquivo e arquivos comprimidos em múltiplas camadas de empacotamento.

12.2.2.101.23 A solução deve suportar o monitoramento de múltiplas interfaces de rede conectadas a diferentes VLANs e Switches.

12.2.2.101.24 A solução deve permitir a análise de eventos de segurança de ativos de informação suspeitos de atividade maliciosa.

12.2.2.101.25 A solução deve possibilitar que modelos de detecção a nível de rede sejam customizados de acordo com as necessidades da CONTRATANTE.

12.2.2.101.26 A solução deve possuir regras que identifiquem comunicações, no mínimo, dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e análise de tráfego na porta.

12.2.2.101.27 A solução deve possuir regras que identifiquem comunicações dos ativos de informação com serviços não autorizados, tais como: consultas DNS, utilização de Servidor SMTP, streaming de mídia, peer-to-peer, instant messengers, API, Servidor DHCP, ARP e Servidor Proxy.

12.2.2.101.28 A solução deve permitir o upgrade e downgrade de versão de firmware.

12.2.2.101.29 A solução deve ser capaz de identificar, no tráfego de rede (Wifi) ameaças de dispositivos móveis.

12.2.2.101.30 A solução deve ser capaz de detectar nas redes, no mínimo: tentativas de escaneamento, propagação de malwares, tentativas de ataques de força bruta, movimentação lateral, tentativas de roubo de informação, ameaças que se replicam e exploits.

12.2.2.101.31 A solução deve ser capaz de identificar ameaças evasivas em tempo real atuando com análise profunda e inteligência para identificar e prevenir ataques.

12.2.2.101.32 A solução dever ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque e possibilitar a visualização de toda a cadeia de ataque ou da tentativa de exploração de uma vulnerabilidade permitindo analisar, no mínimo: sua origem, identificar as ameaças relacionadas, linha de tempo dos logs, os ativos de informação relacionados e comprometidos, os metadados relevantes à análise dos incidentes, e que gere informação para proteção efetiva do ambiente e para análise sólida das ações.

12.2.2.101.33 A solução deve mapear os métodos HTTP/HTTPS de requisições detectados ao longo de uma comunicação inspecionada.

12.2.2.101.34 A solução deve inspecionar os domínios e subdomínios trazendo informações sobre possíveis comprometimentos que possam subsidiar as ações de contenções.

12.2.2.101.35 A partir dos alertas gerados, a solução deve correlacionar os ativos de informação, contendo, no mínimo: IPs, hashs envolvidos, nome do ativo, data e hora, apontando possíveis indicadores de comprometimento (IOCs) nos ambientes.

12.2.2.102 Especificações Técnicas da Console de Gerenciamento - Solução de NDR

12.2.2.102.1 A solução deve fornecer uma console integrada com a console do XDR.

12.2.2.102.2 A solução deve replicar a comunicação captada por interface gráfica interativa ou Dashboards, a fim de facilitar a compreensão dos alertas gerados.

12.2.2.102.3 A solução deve possuir interface gráfica que apresente em tempo real estatísticas de ameaças detectadas, arquivos analisados, ativos de informação afetados, URL's maliciosas acessadas, dentre outros.

12.2.2.102.4 A solução deve trabalhar com geolocalização para identificar a origem geográfica de um ataque.

12.2.2.102.5 A solução deve apresentar panorama de detecções de comunicações suspeitas e maliciosas baseado em geolocalização, onde são marcadas origens geográficas de ataques e eventos de segurança monitorados pela solução, por meio de dashboards.

12.2.2.102.6 A solução deve ser capaz de identificar, filtrar e exibir em interface gráfica, atualizando dinamicamente os hosts com alto nível de risco e classificando os tipos de eventos detectados.

12.2.2.102.7 A console da solução deverá fornecer acesso gráfico aos eventos e alertas detectados, com opção de salvaguardar dos logs ou direcioná-los para um servidor syslog ou através de API, além de oferecer mecanismos de emissão de alarmes via comunicação eletrônica (e-mail, teams) e syslog ou SNMP.

12.2.2.102.8 A solução deve ter capacidade de agregação e correlação de logs de eventos de segurança de maneira evidente possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças conhecidas e desconhecidas, correlacionando com a solução de XDR.

12.2.2.102.9 A solução deve permitir exportar os logs, no mínimo, para dois formatos distintos.

12.2.2.102.10 A solução deverá possuir integração com sistemas SIEM, para possibilitar coleta de logs de gerenciamento e correlação em tempo real.

12.2.2.102.11 Todos os eventos gerados pela solução devem ser armazenados por um período mínimo de 6 (seis) meses.

12.2.2.102.12 A solução deve permitir busca por informações de destino e origem de comunicações, incluindo, no mínimo: endereço IP e grupo de IPs, endereço MAC, domínio, protocolo e redes.

12.2.2.102.13 A solução deve ser capaz de salvar os dados e eventos maliciosos de uma análise, possibilitando restaurar a mesma para continuá-la, consultá-la ou encerrá-la.

12.2.2.102.14 A solução deve ser capaz de gerar relatórios baseados nas análises.

12.2.2.102.15 A solução deve ser integrada com a console de gerência, com objetivo de correlacionar os eventos com as demais tecnologias de segurança.

12.2.2.102.16 A solução deve possuir interface web para busca e análise de incidentes.

12.2.2.102.17 A console deverá possibilitar a criação, edição, habilitação, desativação e deleção de alertas customizados, com emissão via SNMP ou integração via API, para integração com outros sistemas de gerenciamento.

12.2.2.102.18 A solução deve permitir a notificação de eventos e envio de alertas de forma proativa para os administradores.

12.2.2.102.19 O gerenciamento da solução deve estabelecer uma correlação de eventos com o módulo de XDR possibilitando uma análise inteligente dos eventos relacionados para uma análise sólida das ações.

12.2.2.102.20 A solução deve permitir a configuração de alarmes personalizados.

12.2.2.102.21 A solução deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa análise, para agilizar a obtenção do resultado

12.2.2.102.22 A solução deve possuir detalhes técnicos dos incidentes detectados, das estatísticas do tráfego analisado e dos indicadores de risco do ambiente.

12.2.2.102.23 A solução deverá possibilitar a criação, edição, habilitação, desativação e deleção de alertas customizados, com emissão via SNMP, via SMTP ou via API, para integração com outros sistemas de gerenciamento.

12.2.2.102.24 Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria.

12.2.2.102.25 A solução deve relacionar e organizar os ataques baseados na matriz do MITRE ATT&CK, identificando técnicas e táticas.

12.2.2.102.26 A solução deve prover pontuação de risco para o ambiente de redes da CONTRATANTE e deve ser possível analisar seu comportamento ao longo do tempo.

12.2.2.102.27 A solução deverá ser integrada ao LDAP, Active Directory, e EntraID do O365.

12.2.2.102.28 A solução deve possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque

12.2.2.102.29 A solução deve suportar a atribuição de papéis funcionais, para implantação de política de controle de acesso baseada em papéis (RBAC - Role-based access control).

12.2.3 A solução deve apresentar as vulnerabilidades que estão sofrendo algum tipo de exploração, elencando quanto as CVEs relacionadas com seu grau de risco.

12.2.3.1.1 A solução deve apresentar os alertas de ameaças direcionadas, suspeitas, e de dia zero, a fim de identificar possíveis ações maliciosas no ambiente das redes. Tais alertas devem apresentar, no mínimo:

12.2.3.1.1.1 A relação entre host name e IPs.

12.2.3.1.1.2 Requisições de rede.

12.2.3.1.1.3 URLs e Hashs.

12.2.3.1.1.4 Usuários e domínios.

12.2.4 A solução deve possibilitar customizar regras, exceções e configurações.

12.2.4.1.1 A solução deve ser baseada em inteligência artificial e aprendizagem de máquina, e possuir uma rede global de inteligência de ameaças a fim de potencializar os níveis de detecção de comportamentos anômalos.

12.2.4.1.2 A solução deve apresentar alertas caso os dados de telemetria gerados tenham relação com algum tipo de campanha de ameaças globais.

12.2.4.1.3 A solução deve enumerar a superfície de ataque, dependendo das fontes de dados conectadas, compreendendo, no mínimo:

12.2.4.1.4 Os ativos de informação, inclusive em nuvem.

12.2.4.1.5 Os usuários, apontando inclusive aqueles que detêm poderes administrativos.

12.2.4.1.6 As aplicações acessadas por usuários e dispositivos, apontando inclusive aquelas que passaram por recente vazamento de dados.

12.2.4.1.7 Os domínios, subdomínios e IPs públicos.

12.2.4.1.8 As portas de comunicação e serviços abertos em cada host público.

12.2.4.1.9 A solução deve mapear via rede os ativos de informação existentes e apontar aqueles que não são gerenciados pelos agentes da solução.

12.2.4.1.10 A solução deve apresentar a relação dos ativos de informação que o usuário acessou.

12.2.4.1.11 A solução deve informar o escopo, o impacto e os componentes afetados nos ativos de informação envolvidos em um incidente.

12.2.4.1.12 A solução deve ainda possibilitar, no mínimo:

12.2.4.1.13 Configurações que correlacione alertas em um incidente.

12.2.4.1.14 Que o administrador atribua o alerta a outro usuário/administrador.

12.2.4.1.15 Inserir informações adicionais.

12.2.4.1.16 Classificar status dos alertas.

12.2.4.1.17 Customizar indicadores de comprometimento (IOCs).

12.2.4.1.18 Incluir e remover arquivos, inclusive criptografados, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos.

12.2.4.1.19 A solução deve possuir capacidade de geração de relatórios por período contendo, no mínimo:

12.2.4.1.20 Sumário das detecções e do tráfego de rede inspecionado.

12.2.4.1.21 Visão Geral dos Incidentes de Segurança.

12.2.4.1.22 Discriminação dos Tipos de Incidentes.

12.2.4.1.23 Ameaças Analisadas e principais ameaças encontradas.

12.2.4.1.24 Vulnerabilidades identificadas.

12.2.4.1.25 Hosts Infectados.

12.2.4.1.26 Usuários em risco

12.2.4.1.27 Recomendações de Segurança.

12.2.4.1.28 A solução deve possibilitar a monitoração e geração de relatórios a partir da console de administração nos formatos PDF, HTML, CSV ou TXT, com a possibilidade de envio por e-mail e exportação.

12.2.4.1.29 O fornecimento do serviço será por demanda e através de solicitação da contratada como a seguir:

12.2.4.2 - **1 Gbps**: - O modelo de 1 Gbps atende ambientes com tráfego de rede moderado, processando até 1 Gigabit por segundo de dados da rede. Essa opção garante a detecção de ameaças, visibilidade de rede, alertas em tempo real, ferramentas de investigação e resposta a incidentes, integração com outras ferramentas de segurança e relatórios personalizados, dentro da capacidade de processamento contratada.

12.2.4.3 **- 2 Gbps:** O modelo de 2 Gbps atende ambientes com tráfego de rede significativo, processando até 2 Gigabits por segundo de dados da rede. Ele oferece as mesmas funcionalidades do NDR que o modelo de 1 Gbps - detecção de ameaças, visibilidade da rede, alertas, ferramentas de investigação, integração e dashboards - porém com capacidade de processamento superior para lidar com o aumento do tráfego.

12.2.4.4 **- 4 Gbps:** O modelo de 4 Gbps atende ambientes com alto tráfego de rede e necessidade de alta capacidade de processamento, suportando até 4 Gigabits por segundo de dados da rede. Ele oferece o mesmo conjunto completo de funcionalidades do NDR presente nos modelos anteriores, incluindo detecção avançada de ameaças, visibilidade detalhada da rede, alertas em tempo real, ferramentas robustas para investigação e resposta a incidentes, integração com outras ferramentas de segurança e dashboards personalizados, dentro da capacidade de processamento contratada.

12.2.4.5 Deverá ser possível realizar composição utilizando um ou mais itens dos modelos acima mencionados, de tal forma a suprir as necessidades de throughput da contratante;

12.2.4.6 Deverá ser possível alteração do volume de throughput solicitado durante a vigência do contrato.

12.2.5 SERVIÇO BÁSICO E ESPECIALIZADO (SOFTWARE/EQUIPAMENTO), ON-SITE OU REMOTAMENTE 24X7 - XDR

12.2.5.1 Os serviços de suporte técnico especializado configuram-se igualmente indispensáveis para a continuidade e integridade do sistema, para manter sua estabilidade operacional e, principalmente, para manter sua constante evolução e adequação aos cenários futuros advindos de aspectos externos ou internos da organização.

12.2.5.2 O Serviço Básico e Especializado escrito no presente item é relacionado à sustentação das operações da solução instalada nos endpoints do CONTRATANTE e na plataforma de administração das soluções. Os requisitos de desempenho para o processo de resposta a incidentes de segurança estão descritos no Requisitos técnicos de operação e gestão da solução.

12.2.5.3 Deverá a CONTRATADA viabilizar suporte técnico especializado nos termos a seguir:

12.2.6 Possuir portal de suporte para abertura de chamados e acesso à base de conhecimento, sendo possível o uso de ITSM (GSTI – Gerenciamento dos Serviços de TI) que a contratante indique;

12.2.6.1 O suporte deverá atender em escala 24x7x365;

12.2.7 Deve ser possível extrair através do portal de serviços relatórios por período selecionado, sendo obrigatório a extração mensal para fins de fiscalização, sobre incidentes e casos relevantes ao MGI;

12.2.8 O Serviço Básico e Especializado deverá prover, além do portal web, ou ferramenta ITSM (GSTI – Gerenciamento dos Serviços de TI) próprio ou que a contratante indique, meios de comunicação de incidentes número de telefone com tarifário local do Distrito Federal para abertura de chamado e/ou comunicadores em geral, para acionamentos em escala 24x7x365;

12.2.8.1 A CONTRATADA deverá prover documentação para uso do suporte técnico contemplando minimamente os seguintes tópicos:

12.2.8.2 Processo de abertura de chamado;

12.2.8.3 Processo de atualização de chamado;

12.2.8.4 Recomendações e melhores práticas específicas para o ambiente;

12.2.8.5 Manter uma base de conhecimento atualizada;

12.2.8.6 Informações técnicas a respeito das atualizações aplicadas.

12.2.8.7 Outras ferramentas além das descritas na especificação técnica da presente contratação que sejam necessárias à execução desses serviços serão de responsabilidade da CONTRATADA, sem custos adicionais para o MGI.

12.2.8.8 O suporte técnico a ser prestado pela CONTRATADA tem por objetivo a instalação, configuração, atualização, correção de falhas ou inconsistências detectadas sejam elas na gerência ou na solução dos ativos de informação, para garantir o pleno, correto e seguro funcionamento da solução de TI contratada.

12.2.8.9 O suporte técnico compreende, ainda, o auxílio na configuração dos componentes da solução para o correto funcionamento, além do esclarecimento de dúvidas dos servidores e prestadores de serviços do MGI, para garantir a melhor utilização e maximização dos recursos contratados.

12.2.9 As solicitações de atendimento técnico deverão ser realizadas através de abertura de chamados e partirão do MGI, por intermédio do Fiscal do Contrato, ou de outro servidor oficialmente designado, ou área do MGI designada para tal finalidade, e deverão ser protocoladas em registro próprio da CONTRATADA.

12.2.9.1 Para cada solicitação de atendimento técnico, deverá ser gerado um identificador único (protocolo) para fins de controle e acompanhamento. A CONTRATADA deverá informar esse identificador ao MGI, bem como manter o histórico de ações e atividades nos chamados realizados durante toda a vigência contratual.

12.2.10 Nas solicitações de atendimento, os colaboradores informarão no mínimo:

12.2.10.1 Nome do solicitante;

12.2.10.2 Número de série do equipamento atendido;

12.2.10.3 Local de atendimento;

12.2.10.4 Relato do problema e seu nível de criticidade;

12.2.10.5 Data e hora do chamado técnico;

12.2.10.6 Outras informações que julgar pertinentes para resolução do problema.

12.2.10.7 A contratante poderá efetuar um número ilimitado de chamados de suporte durante a vigência contratual para suprir suas necessidades de utilização dos objetos contratados.

12.2.10.8 O serviço de suporte será prestado em idioma português do Brasil.

12.2.10.9 Os serviços de suporte técnico/manutenção da solução deverão ser fornecidos diretamente pela CONTRATADA com expressa autorização do fabricante ~~da solução XDR~~ para os serviços de prevenção e resposta ~~fornecer serviço de MDR (Managed Detection and Response),~~ além de certificação que comprove a habilitação para execução do serviço;

12.2.10.10 Os serviços de suporte técnico/manutenção da solução deverão ser prestados por técnicos devidamente certificados pelo fabricante na solução ofertada e com experiência de, no mínimo, 12 (doze) meses em suporte/manutenção da solução, devendo a experiência ser comprovada por meio de registros em carteira de trabalho, contratos de prestação de serviços ou outros meios considerados idôneos pelo CONTRATANTE, excluindo-se desse rol a simples informação em currículo e meras declarações. A exigência de experiência mínima de 12 (doze) meses justifica-se pela especificidade e complexidade dos serviços a serem prestados, que envolvem a necessidade de sólidas e testadas competências em segurança cibernética e na própria solução.

12.2.10.11 Os Níveis Mínimos de Serviço compreendem seguirão o que estabelecido no corpo do TR (Termo de Referência).

12.2.10.12 A CONTRATADA deverá notificar o MGI sempre que houver novas atualizações da ferramenta de TI contratada e que requeiram ação por parte do time do CONTRATANTE.

12.2.10.13 Forma de Auditoria: A CONTRATADA deverá disponibilizar relação dos chamados contendo as seguintes informações:

12.2.10.14 Descrição da atualização

12.2.10.15 Versão

12.2.10.16 Data de disponibilização

12.2.10.17 Data de aplicação da versão

12.2.10.18 A disponibilização dos dados deverá ser feita via e-mail ou acesso à base de dados da ferramenta de chamados da CONTRATADA.

12.2.11 REQUISITOS TÉCNICOS DE OPERAÇÃO E GESTÃO DA SOLUÇÃO DE NDR

12.2.11.1 Os serviços de operação e gestão da solução NDR deverão ser fornecidos diretamente pela CONTRATADA com expressa autorização do fabricante da solução para fornecer serviço de MDR (Managed Detection and Response), além de certificação que comprove a habilitação para execução do serviço.

12.2.11.2 Os serviços de operação e gestão da solução deverão ser prestados por técnicos devidamente certificados pelo fabricante na ferramenta de NDR ofertada e com experiência de, no mínimo, 12 (doze) meses em operação e gestão de soluções similares, devendo a experiência ser comprovada por meio de registros em carteira de trabalho, contratos de prestação de serviços ou outros meios considerados idôneos pelo CONTRATANTE, excluindo-se desse rol a simples informação em currículo e meras declarações. A exigência de experiência mínima de 12 (doze) meses justifica-se pela especificidade e complexidade dos serviços a serem prestados, que envolvem a necessidade de sólidas e testadas competências em segurança de redes e na própria solução.

12.2.11.3 Mesmo se a prestação do serviço envolver recursos técnicos do fabricante, caberá à CONTRATADA o cumprimento de todas as condicionantes contratuais, bem como a manutenção dos níveis contratados, e, em caso de descumprimentos, a responsabilidade recairá integralmente sobre a CONTRATADA;

12.2.11.4 O serviço de monitoramento, operação e gestão, incluindo caça a ameaças na rede, será realizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o ano;

12.2.11.5 Caça contínua de ameaças na rede, analisando o tráfego de rede, logs de dispositivos de rede e outros dados relevantes, visando identificar e responder a atividades maliciosas na rede do CONTRATANTE.

12.2.11.6 O serviço deve analisar campanhas de malwares e incidentes gerados na gerência de administração da solução, com foco em vetores de ataque e exploração de vulnerabilidades na rede;

12.2.11.7 O serviço deve ser realizado através de análise humana e automatizada, contínua, 24x7, em busca de anomalias e potenciais atividades maliciosas na rede que fogem do escopo de detecção das ferramentas de segurança tradicionais.

12.2.11.8 O serviço deve ser fornecido utilizando a plataforma NDR ofertada. A CONTRATADA deverá apresentar e justificar a necessidade de qualquer integração externa para aprovação prévia do CONTRATANTE.

12.2.11.9 O serviço de caça a ameaças na rede deverá atuar de forma proativa em busca de descobrir a presença e prevenir um atacante mesmo sem a existência de uma detecção ferramental, ou seja,

o time de caça a ameaças não deverá restringir o início de suas atividades com base em uma detecção proveniente unicamente de alertas automatizados.

12.2.11.10 Relatórios de ameaças, incluindo vetores de ataque, indicadores de comprometimento (IOCs) e tendências de segurança na rede, fornecidos pela CONTRATADA, e relatórios de impacto entregues por e-mail ou outro meio de comunicação definido pela Contratada homologado pela Contratante e alertas no console de gerenciamento da solução;

12.2.11.11 Capacidade de recepcionar, priorizar e fazer a triagem de alertas de segurança relevantes para a rede provenientes da solução NDR e de outras ferramentas de segurança que compõem o ambiente do CONTRATANTE, previamente informadas por ela;

12.2.12 Visibilidade em fontes de dados de rede que incluem, mas não se limitam a: tráfego de rede (Netflow, sFlow, IPFIX), logs de firewall, logs de dispositivos de rede (switches, roteadores, VPNs) e outros dados relevantes para a detecção de ameaças na rede;

12.2.12.1 Monitoramento e detecção de anomalias no tráfego de rede, incluindo, mas não se limitando a: varreduras de portas, conexões suspeitas, tentativas de acesso não autorizado, tráfego de comando e controle (C2), exfiltração de dados e outros comportamentos indicativos de atividades maliciosas;

12.2.12.2 Monitoramento e detecção de anomalias comportamentais para usuários, com foco em atividades suspeitas relacionadas à rede, como acessos incomuns, alto volume de dados trafegados e acessos a partir de localizações incomuns;

12.2.12.3 Ajuste da solução NDR para o ambiente de rede do CONTRATANTE, incluindo regras de detecção personalizadas, políticas de segurança, exceções e integrações com outras ferramentas de segurança, conforme a necessidade e aprovação prévia do CONTRATANTE;

12.2.12.4 Apresentar ao CONTRATANTE a lista de “casos de uso” do serviço de NDR, com as técnicas de ataque, vetores de exploração e atividades maliciosas passíveis de detecção pela solução e respectivas prioridades acordadas;

12.2.12.5 Reportar os incidentes de segurança na rede do CONTRATANTE dentro da classificação do incidente e considerando o SLA estabelecido;

12.2.12.6 Fornecer ao CONTRATANTE recomendações para a resolução dos incidentes de segurança na rede, incluindo ações de contenção, remediação e hardening da infraestrutura de rede;

12.2.12.7 Receber a confirmação da equipe técnica do CONTRATANTE de que as recomendações para incidentes na rede foram aplicadas e os incidentes foram remediados;

12.2.12.8 Atuação das equipes ~~de engenharia~~ de segurança da CONTRATADA no aprimoramento das regras de detecção, correlação de dados e dashboards da solução NDR, em conjunto com a equipe do CONTRATANTE;

12.2.12.9 Acordar os canais de comunicação, visando rápida atuação entre as equipes para resolução de incidentes de segurança na rede;

12.2.12.10 Comunicação com as equipes do CONTRATANTE, disponibilizando o detalhamento dos eventos de segurança na rede identificados e ações de contenção recomendadas para o tratamento pelo CONTRATANTE;

12.2.13 A fim de manter o nível de segurança, e como forma de demonstrar regularmente a eficácia dos controles aplicados, a CONTRATADA realizará ou apoiará simulações controladas de intrusão na rede, com objetivo de identificar possíveis pontos fracos na implementação da solução e na postura de segurança da rede. As simulações devem ser executadas de forma automatizada e contínua, com a aprovação prévia do CONTRATANTE;

12.2.13.1 Analisar as tendências ao longo do tempo para identificar mudanças em padrões de tráfego e comportamento da rede que possam indicar atividades suspeitas;

12.2.14 A CONTRATADA fará a monitoração contínua e ininterrupta dos eventos e alertas de segurança na rede oferecidos pela solução NDR, com a finalidade de detectar ameaças em tempo real e encaminhar as informações a área de segurança do CONTRATANTE, auxiliando processos de investigação com a finalidade de acelerar o processo de detecção e resposta;

12.2.14.1 Deve utilizar tecnologias de detecção de ameaças em tempo real para identificar ameaças emergentes na rede, incluindo intrusões, movimentos laterais, e ataques cibernéticos, encaminhando-os ao serviço de SOC do CONTRATANTE;

12.2.14.2 O trabalho de caça a ameaças (hunting) na rede deve ser contínuo, avaliando-se sistematicamente todos os logs, alertas, fluxos de tráfego e telemetria produzida pela solução NDR e utilizando-se de técnicas e táticas modernas a fim de identificar ameaças zero-day, novas portas e protocolos utilizados por atacantes, e vulnerabilidades não identificadas na rede;

12.2.14.3 A partir da ocorrência de um incidente de segurança na rede, realizar as seguintes atividades de resposta aos incidentes, incluindo:

12.2.14.4 Detecção: identificar o evento na rede, realizar abertura do chamado e comunicação do incidente;

12.2.14.5 Triagem: realizar a análise inicial do incidente na rede (revisão de logs de rede, confirmação de origem, avaliação de falso positivo, complexidade e confirmação da criticidade dos ativos de rede envolvidos);

12.2.14.6 Análise: realizar análise do evento ocorrido na rede para mensurar impacto real do incidente, linha do tempo e eventual encerramento do incidente, assim como melhorias necessárias na segurança da rede;

12.2.14.7 Contenção: direcionar procedimentos de resposta a incidentes na rede conforme a categoria do incidente para que os analistas de resposta do CONTRATANTE possam executar as efetivas

adequações como resposta ao incidente, incluindo bloqueio de IPs e domínios maliciosos, quarentena de dispositivos infectados e aplicação de políticas de segurança mais restritivas;

12.2.14.8 Recuperação: assessorar com o envio de procedimentos de segurança que devem ser adotados pelo CONTRATANTE para retornar os serviços e sistemas de rede à produção;

12.2.14.9 Revisão: documentar o incidente e realizar sugestões de melhorias para a segurança da rede;

12.2.14.10 Todas as atividades do processo de resposta a incidentes de segurança na rede serão registradas pelos especialistas da CONTRATADA em ferramenta especialista do órgão contratante, conforme diretrizes e orientações fornecidas para inclusão de dados e acesso;

12.2.14.11 Para cada incidente de segurança na rede aberto e registrado, deverão ser documentadas no ticket as conclusões e lições aprendidas, além de sugestões de melhorias para mitigação das brechas identificadas na rede;

12.2.14.12 A CONTRATADA ficará responsável por elaborar de forma contínua as compilações de operação e procedimentos (Runbooks) com os procedimentos que descrevem o tratamento dos incidentes de segurança na rede detectados;

12.2.14.13 Mensalmente, deverão ser elaborados, no mínimo, os seguintes relatórios sobre o ambiente de rede do CONTRATANTE:

12.2.14.14 Visão baseada na matriz ATT&CK do instituto de pesquisa MITRE, com foco em táticas e técnicas de ataque à redes;

12.2.14.15 TOP 10 endereços IP de origem de atividades maliciosas;

12.2.14.16 TOP 10 endereços IP de destino de atividades maliciosas;

12.2.14.17 TOP 10 portas e protocolos utilizados em atividades maliciosas;

12.2.14.18 TOP 10 vulnerabilidades exploradas em ataques à rede;

12.2.14.19 TOP 10 ações dos atores de ameaça na rede;

12.2.14.20 Demonstração das análises de tráfego de rede realizadas (huntings de destaque);

12.2.14.21 Demonstração do cruzamento de incidentes e ameaças na rede capturadas pela equipe de inteligência (ex: CVEs de campanhas de ransomware que exploram vulnerabilidades em redes);

12.2.14.22 Runbooks de segurança de rede criados no período.

12.2.15 REQUISITOS TÉCNICOS DE OPERAÇÃO E GESTÃO DA SOLUÇÃO DE ANTISPAM

12.2.15.1 Os serviços de operação e gestão da solução ANTISPAM deverão ser fornecidos diretamente pela CONTRATADA com expressa autorização do fabricante da solução, além de certificação que comprove a habilitação para execução do serviço.

12.2.15.2 Os serviços de operação e gestão da solução deverão ser prestados por técnicos devidamente certificados pelo fabricante na ferramenta de ANTISPAM ofertada e com experiência de, no mínimo, 12 (doze) meses em operação e gestão de soluções similares, devendo a experiência ser

comprovada por meio de registros em carteira de trabalho, contratos de prestação de serviços ou outros meios considerados idôneos pelo CONTRATANTE, excluindo-se desse rol a simples informação em currículo e meras declarações. A exigência de experiência mínima de 12 (doze) meses justifica-se pela especificidade e complexidade dos serviços a serem prestados, que envolvem a necessidade de sólidas e testadas competências em segurança da informação na própria solução.

12.2.15.3 Mesmo se a prestação do serviço envolver recursos técnicos do fabricante, caberá à CONTRATADA o cumprimento de todas as condicionantes contratuais, bem como a manutenção dos níveis contratados, e, em caso de descumprimentos, a responsabilidade recairá integralmente sobre a CONTRATADA;

12.2.15.4 O serviço de monitoramento, operação e gestão, será realizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o ano;

12.2.15.5 O serviço deve analisar mudanças significativas no fluxo de e-mails, bem como os alertas de conteúdo e anexos;

12.2.15.6 O serviço deve ser realizado através de análise humana e/ou automatizada, contínua, 24x7, em busca de anomalias e potenciais atividades maliciosas na tramitação de mensagens.

12.2.15.7 Monitoramento e detecção de anomalias comportamentais para caixas de e-mail, com foco em envios e recebimentos suspeitos buscando movimentação lateral, envios incomuns, alto volume de dados trafegados e envios a partir de localizações incomuns;

12.2.15.8 Reportar os incidentes de movimentação suspeita no tráfego de e-mails na rede do CONTRATANTE dentro da classificação do incidente e considerando o SLA estabelecido;

12.2.15.9 Fornecer ao CONTRATANTE recomendações para a resolução dos incidentes de segurança no fluxo de e-mails, incluindo ações de contenção e remediação;

12.2.15.10 Receber a confirmação da equipe técnica do CONTRATANTE de que as recomendações para incidentes na rede foram aplicadas e os incidentes foram remediados;

12.2.15.11 Atuação das equipes de ~~engenharia~~ de segurança da informação da CONTRATADA no aprimoramento das regras de detecção, correlação de dados e dashboards da solução ANTISPAM, em conjunto com a equipe do CONTRATANTE;

12.2.15.12 Acordar os canais de comunicação, visando rápida atuação entre as equipes para resolução de incidentes de segurança de e-mail;

12.2.15.13 Comunicação com as equipes do CONTRATANTE, disponibilizando o detalhamento dos eventos de segurança identificados e ações de contenção recomendadas para o tratamento pelo CONTRATANTE;

12.2.15.14 A fim de manter o nível de segurança, e como forma de demonstrar regularmente a eficácia dos controles aplicados, a CONTRATADA realizará simulações controladas de intrusão na rede, com

objetivo de identificar possíveis pontos fracos na implementação da solução e na postura de segurança da rede. As simulações devem ser executadas de forma automatizada e contínua, com a aprovação prévia do CONTRATANTE;

12.2.15.15 Analisar as tendências ao longo do tempo para identificar mudanças em padrões de tráfego e comportamento de e-mail que possam indicar atividades suspeitas;

12.2.16 Deve utilizar tecnologias de detecção de ameaças em tempo real para identificar ameaças emergentes, incluindo intrusões, movimentos laterais, e tentativas de ataques cibernéticos, a partir das caixas de correio eletrônico, encaminhando-os a área de segurança do CONTRATANTE;

12.2.17 Para cada incidente de segurança aberto e registrado, deverão ser documentadas no ticket as conclusões e lições aprendidas, além de sugestões de melhorias para mitigação das brechas identificadas nas caixas de correio eletrônico;

12.2.17.1 A contratada deverá prestar suporte as caixas

12.2.17.2 ABUSE, podendo ser automatizado a abertura de chamados para os e-mails recebidos por esses canais de abertura de incidente.