APÊNDICE "A"

REQUISITOS MÍNIMOS DA SOLUÇÃO

1. ITEM 1 - SOLUÇÃO DE CONTROLE DE DADOS PARA APLICAÇÃO EM NUVEM

1.1. A solução deverá ser fornecida em ambiente de nuvem, sem necessidade de instalação de componentes físicos no ambiente da CONTRATADA;

1.2. O tráfego da solução deverá ser tratado em Data Centers dentro do território nacional, sem que seja necessário o redirecionamento dos dados para fora do Brasil;

1.2.1. Para alta disponibilidade a solução deverá possuir no mínimo dois Data Centers redundantes no território nacional;

1.2.1.1. Garantir disponibilidade de 99.999% das estruturas de Data Centers;

1.2.1.2. Deve permitir medir a experiencia dos usuários nos acessos destinados ao Microsoft Office 365 através da medição de latência da conexão;

1.2.1.3. Deve manter os metadados analisados pela solução por no mínimo 90 dias;

1.2.1.4. A solução deverá possuir mecanismo de monitoramento de telemetria para análise e identificação de performance através de painel específico para apresentar as latências entre o cliente e a unidade de processamento do fabricante e da unidade de processamento do fabricante até o serviço SaaS Microsoft Office 365;

1.2.1.5. Deve possuir dashboard específico para apresentar a volumetria de tráfego por unidade de processamento do fabricante (pop);

1.2.1.6. Deve possuir painel específico com dados relacionados ao cliente, garantindo visibilidade quanto a versões em uso, usuário ativos, Bytes baixados e carregados, quantidade de sessões diárias;

1.3. Deverá possuir peering com principais provedores de SaaS (Amazon, Microsoft, Google, Akamai, Cloudflare, Facebook e Oracle Cloud) para melhor conectividade;

1.4. A solução deverá ser capaz de inspecionar tráfego TLS, incluindo a versão 1.3;

1.4.1. Deve permitir configurar exceções para que a política de inspeção do túnel TLS não se aplique;

1.5. Deverá permitir instalação de agentes em sistemas operacionais Windows e MacOS;

1.6. Deverá possuir console única para gerenciamento e visualização, conforme descrito a seguir:

1.6.1. Possuir dashboard com resumo das atividades e incidentes;

1.6.2. Permitir a emissão de relatórios de usuários, sites e aplicações, IPs, e atividades dos usuários;

1.6.3. A solução deverá possuir painel específico com dados relacionados ao cliente, garantindo visibilidade quanto a versões em uso, usuário ativos, Bytes baixados e carregados, quantidade de sessões diárias;

1.7. A solução deverá permitir integração com Microsoft Active Directory e Microsoft Azure AD;

1.8. A solução deverá interceptar o tráfego web e o tráfego de aplicações SaaS em tempo real, realizando análise das atividades e executando ações conforme as políticas configuradas;

1.9. O entendimento de aplicações SaaS é subdividido conforme segue:

1.9.1. Gerenciada: toda e qualquer aplicação SaaS corporativa, a qual a ANTT mantém acordo comercial firmado e vigente para os usuários internos.

1.9.2. Não gerenciada: Conhecida como ShadowIT, ou seja, aplicações SaaS terceiras as quais não possuem nenhum acordo comercial junto a ANTT, sendo o usuário o responsável pela manutenção do ambiente.

1.10. A solução deverá suportar encaminhamento do tráfego para processamento de pelo menos os seguintes métodos:

1.10.1. Túnel IPSEC;

1.10.2. Túnel GRE;

1.10.3. Proxy Explicito;

1.10.4. Cliente do próprio fabricante;

1.10.5. Proxy Reverso para o Office 365;

1.11. A solução deve diferenciar e controlar o tráfego da instância corporativa do Microsoft Office 365 da ANTT frente ao Microsoft Live, cujo ambiente é pessoal;

1.12. Deve permitir visualizar e controlar o tráfego de aplicações não gerenciadas (Shadow IT);

1.13. Deve permitir a criação de listas com arquivos autorizados para as ações de Download e Upload;

1.14. Deverá possuir capacidade de categorização e classificação de URLs, conforme segue:

1.14.1. Deve possuir pelo menos 100 categorias de URL pré-definidas;

1.14.2. Deve permitir o isolamento do navegador por meio de tecnologia RBI, limitando as ações do usuário em acessos a URLs não categorizadas, controlando no mínimo download e upload de arquivos.

1.14.3. Deve permitir alertar ou bloquear os acessos à URLs maliciosas;

1.14.4. Permitir a configuração de políticas baseadas nas categorias e determinação do período de aplicação da política;

1.14.5. Deve pemitir o bloqueio de exploração de ataques Web que possam vitimizar os usuários da ANTT;

1.14.6. Deve possuir categorias especializadas em segurança, permitindo o bloqueio de sites maliciosos, de phishing, proxy anônimo, botnet, Command and Control, Fraude, DGA, Spam e Spyware.

1.15. A solução deve possuir capacidade de categorizar, no mínimo, 15 mil aplicações SaaS não gerenciadas:

1.15.1. Deve permitir a configuração de listas de exceção para categorias especificas, de modo que o tráfego destas categorias não passará pelo Data Center da solução;

1.15.2. Deve permitir a configuração de quais aplicações ou categorias passarão pelo processo de decriptografia para análise;

1.16. Deve fornecer controle para aplicações WEB2.0, permitindo, no mínimo o bloqueio e permissão de ações de POST, SHARE, DELETE, DOWNLOAD e UPLOAD;

1.17. A solução deverá possuir no mínimo as seguintes funcionalidades:

1.17.1. Visibilidade de tráfego não gerenciado (Shadow IT);

1.17.2. Proteção contra malwares;

1.17.3. Proteção contra perda de dados;

1.17.4. Análise comportamental dos usuários;

1.18. A solução deverá ser capaz impedir e controlar atividades em aplicações não gerenciadas, como Facebook, Linkedin, Youtube, dentre outras.

1.19. Deve permitir o controle de upload e download de arquivos e aúdio na aplicação SaaS Whatsapp.

1.20. A solução deve ser capaz de realizar análise das instancias corporativas e pessoais das aplicações SaaS gerenciadas;

1.20.1. Deverá permitir a criação de políticas para permitir o acesso e atividades (download, upload etc.) em instancias corporativas e bloquear em instancias pessoais (Ex: Outlook, Gmail);

1.20.2. Deve permitir o bloqueio de qualquer upload ou download de arquivos para aplicações na categoria Webmail não gerenciadas;

1.20.3. Deve possuir capacidade de aplicar políticas nas aplicações corporativas do Microsoft Office 365 (OneDrive, Sharepoint, Outlook e Teams);

1.20.4. A solução deverá prover proteção de dados através perfis de DLP pré-definidos e perfis customizáveis;

1.20.4.1. Os perfis pré-definidos devem se basear em normas regulatórias (LGPD e GDPR);

1.20.4.2. Deve possuir, expressões regulares, dicionários e palavras chaves;

1.20.4.3. Deve permitir executar as políticas configuradas em, no mínimo 100 tipos de arquivo;

1.20.4.4. Os perfis de DLP deverão ter disponibilidade de utilização em aplicações corporativas (OneDrive, Sharepoint, Teams, Outlook), aplicações categorizadas (Gmail, Google Drive, Dropbox etc.) e sites (Facebook etc.);

1.20.4.5. A política de LGPD deverá possuir informações de dados como CPF, CNH, RG e título de eleitor;

1.20.4.6. A solução deve possuir proteção de contra malware através de análise de assinaturas e heurística;

1.20.4.6.1. Deve prevenir o download de arquivos maliciosos em acessos a URLs e webmail;

1.20.4.6.2. Deve prevenir o download de arquivos maliciosos em aplicações SaaS;

1.20.4.6.3. Deve prevenir o upload de arquivos maliciosos na instância corporativa do Office 365;

1.20.4.7. A solução deve permitir a análise de comportamento do usuário através da detecção de atividades suspeitas baseado em regras comportamentais pré-definidas, dentre elas:

1.20.4.7.1. Análise de geolocalização;

1.20.4.7.2. Análise de execução de downloads e uploads massivos;

1.20.4.7.3. Análise de vazamento de credencias expostas na Internet;

1.20.4.8. A solução deve ser capaz de avaliar os seguintes critérios para determinar a postura do dispositivo dos usuários para acesso a aplicações SaaS:

1.20.4.8.1. Sistema operacional;

1.20.4.8.2. Processos executados;

1.20.4.8.3. Arquivos presentes no dispositivo;

1.20.4.8.4. Inserção em domínio de Active Directory;

1.20.4.8.5. Presença de certificado;

1.20.4.8.6. A solução deve permitir a criação de políticas de acordo com avaliação da postura do dispositivo;

1.20.4.8.7. A solução deve permitir envio de IOC’s para plataformas terceiras de EDR, SIEM e NGFW;

1.21. A solução deve permitir a integração com o ambiente corporativo do Office 365 (One Drive, Sharepoint, Teams e Outlook) através de API;

1.21.1. A integração deve ser feita de modo direto entre o provedor de segurança e a instancia do Office 365, sem necessidade de customização do back-end da solução ou via modalidade hibrida através do posicionamento de equipamentos físicos;

1.22. A solução deverá fazer escaneamento completo do ambiente das aplicações do Office 365;

1.22.1. Deve permitir a aplicação de políticas que realizam a identificação e classificação de dados para, no mínimo, os padrões de LGPD e Código fonte;

1.22.2. Deve permitir a aplicação de políticas customizadas via regex para identificação de máscaras de LGPD, incluindo Renavam e Placa de Carro, em documentos;

1.22.3. Deve permitir a criação de uma regex em busca de AWS Key dentro de documentos armazenados no OneDrive e Sharepoint corporativos;

1.23. A solução deverá possuir controle específicos para o ambiente AWS existente na ANTT, garantindo minimamente:

1.23.1. Controle de acesso a máquinas que possuam a conformidade conforme disposto no item 1.20.4.8.

1.23.2. Bloqueio de ações para usuários não autorizados – Exemplo: não permitir Shutdown, Terminate, Stop de instâncias EC2.

1.23.3. Controle de download dos buckets corporativos que contenham informações confidenciais.

1.24. Para a aplicação do OneDrive, a solução deve garantir controle e definições de acesso:

1.24.1. Deve permitir ações de alerta, criptografia, restrição de acesso e retenção legal;

1.24.2. Deve permitir o controle de compartilhamento dos arquivos em no mínimo privado, publico, compartilhamento interno e compartilhamento externo;

1.24.3. Deve definir os acessos por proprietário, usuário interno, domínio específico, somente visualização;

1.24.4. Deve permitir excluir um link compartilhado publicamente;

1.24.5. Deve permitir remover permissões de acesso;

1.25. Para a aplicação Sharepoint, a solução deve garantir controle e definições de acesso:

1.25.1. Deve permitir o bloqueio do compartilhamento de pasta com permissão de escrita para usuários internos e externos;

1.25.2. Deve permitir exclusão de links compartilhados publicamente;

1.25.3. Deve permitir a revogação de um link compartilhado com usuários externos;

1.25.4. Deve permitir o bloqueio de compartilhamento de pastas de arquivos com usuários externos;

1.26. Para a aplicação Outlook, a solução deve garantir controle e definições de acesso:

1.26.1. Deve analisar o corpo do e-mail e anexos conforme regras de perda de dados configuradas (pré-definidas e customizadas);

1.26.2. Deve permitir configurar regras especificas para domínios;

1.26.3. Deve permitir configuração de módulo de SMTP Proxy para integração com o a instância do Microsoft Exchange e aplicar políticas para controle de vazamento de dados;

1.27. Para a aplicação Teams, a solução deve garantir controle e definições de acesso:

1.27.1. Deve permitir o bloqueio de mensagens e documentos conforme regras de DLP configuradas (pré-definidas e customizadas);

1.27.2. Deve inventariar os usuários e times existentes na conta corporativa da ANTT;

1.28. A solução deverá prover módulo para acesso a aplicações internas, garantindo o acesso exclusivo e dedicado a aplicação desejada sem que seja necessário atribuir o acesso a um segmento de rede interno, para no mínimo 1000 usuários;

1.28.1. Será permitido a instalação de appliances físico ou virtual no ambiente da CONTRATADA para conexão segura entre a nuvem do fabricante e às aplicações internas;

1.28.2. O acesso deve ser baseado nos protocolos TCP e UDP para no mínimo, as conexões abaixo:

1.28.2.1. SSH – Porta TCP 22;

1.28.2.2. RDP – Porta TCP/UDP 3389;

1.28.2.3. FTP – TCP 21;

1.28.2.4. HTTP – TCP 80,443 e outras;

1.28.3. Deve ser capaz de avaliar constantemente a identidade do usuário;

1.28.4. Deve ser capaz de avaliar o dispositivo do usuário, determinando condições para que os dispositivos sejam permitidos ou bloqueados;

1.28.5. Deve permitir configurar a liberação ou bloqueio das aplicações através de usuários, grupo de usuários e OUs;

1.28.6. Deve permitir o bloqueio e notificação do usuário quando o acesso for negado;

1.28.7. Deverá permitir acesso às aplicações HTTP e HTTPS sem necessidade do agente instalado na máquina;

2. ITEM 2 - SERVIÇO DE OPERAÇÃO ASSISTIDA

2.1. A console de administração deve ser centralizada para gerenciar todos os dispositivos, independentemente da localização geográfica. Trata-se serviço de operação assistida da Contratada, na modalidade 8x5, pelo período de 8h às 18h de segunda a sexta feira;

2.2. O serviço de operação assistida a ser prestado pela CONTRATADA tem por objetivo a correção de falhas ou inconsistências detectadas, de forma a garantir o pleno e correto funcionamento da solução;

2.3.1. Para chamados classificados com criticidade baixa e média, o profissional deverá possuir certificação que comprove habilidade em administrar, integrar e/ou implantar solução no ambiente da CONTRATANTE;

2.3.2. Para chamados classificados com criticidade alta, o profissional deverá possuir certificação de nível especialista da solução;

2.3. O serviço compreende auxílio na configuração das funcionalidades contratadas, esclarecimento de dúvidas e restabelecimento do serviço;

2.4. Deverá ser gerado relatório mensal com resumo de utilização das funcionalidades habilitadas, exibindo vulnerabilidades e exposições de dados encontrados no escopo dos serviços em nuvem utilizados pela ANTT, para tratativa de remediação que deve ser realizada pela equipe técnica da CONTRATANTE;

2.5. A CONTRATANTE deverá realizar análise consultiva sobre as configurações do ambiente atual da solução contratada, a fim de orientar e fomentar alterações que visam as melhores práticas para a ANTT;

2.6. As solicitações deverão ocorrer através de abertura de chamado técnico, através de portal disponibilizado pela CONTRATADA ou através de telefone de plantão 0800;

2.7.1. A abertura de cada chamado deverá receber um identificador único;

2.7.2. A contratada poderá efetuar um número ilimitado de chamados técnicos, devendo a CONTRATANTE cumprir o SLA no prazo estipulado neste instrumento;

2.7.3. Após a abertura de cada chamado, deverá ser iniciado o tempo de resposta ao chamado, de acordo com a criticidade de cada solicitação, conforme abaixo:

Criticidade	Tempo de Resposta	Tempo de Conclusão
Alta	2h	4h
Média	4h	6h
Baixa	6h	8h

2.7.4. Os chamados classificados com criticidade Alta, são definidos pela situação emergencial ou indisponibilidade total dos serviços;

2.7.5. Os chamados classificados com criticidade Média, são definidos pela indisponibilidade parcial ou mal funcionamento de alguns serviços;

2.7.6. Os chamados classificados com criticidade Baixa, são definidos pela situação não emergencial, geração de dúvidas e validações de configurações ou manutenções de baixo impacto;

2.7. Os chamados serão considerados concluídos quando houver restabelecimento dos serviços contratados;

2.8. Os atendimentos deverão ocorrer preferencialmente de forma remota, sendo necessário o atendimento presencial em casos específicos, solicitados pela CONTRATANTE;

2.9. Deverá ser fornecido pela Contratada contato de gerente técnico responsável pelos atendimentos;

2.10. Deverá ser realizado repasse de conhecimento da solução implantada, com duração de até 40 horas, para turma de até 08 alunos;

2.11.1. O repasse de conhecimento deverá ser realizado por profissional certificado da CONTRATADA, além de disponibilizar material didático para consulta;

2.11.2. O repasse de conhecimento deverá cobrir todas as funcionalidades fornecidas com relação a implantação, configuração e administração da solução;

2.11.3. O repasse de conhecimento deverá ser realizado preferencialmente de forma remota ou dentro das dependências da CONTRADADA.

3. ITEM 3 - SOLUÇÃO DE DESCOBERTA E CORREÇÃO DE VULNERABILIDADE DE SEGURANÇA

3.1. Características gerais

3.1.1. Toda a solução deverá ser de mesma marca, sem qualquer tipo de customização não autorizada pelo mesmo;

3.1.2. Caso a solução ofertada não possua o framework de correção das vulnerabilidades, este poderá ser ofertado por agentes e visões separadas;

3.1.3. Deverá estar licenciado para, no mínimo, 2300 endereços IP;

3.1.4. O gerenciamento do serviço deve ser 100% em nuvem;

3.1.5. O Serviço deve prover no mínimo 99.95% de disponibilidade no nível de serviço;

3.1.6. O Serviço deve ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

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

3.1.8. Deve possibilitar, por meio da console, no mínimo 4 (três) métodos de escaneamento:

3.1.8.1. Scan ativo;

3.1.8.2. Scan com uso de agentes;

3.1.8.3. Scan passivo;

3.1.9. Scanner em nuvem já disponível para uso, sem a necessidade de instalação;

3.1.10. Deve ser capaz de identificar no mínimo 50.000 CVE´S;

3.1.11. O Serviço deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferente do padrão CVSS;

3.1.12. Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial (machine learning);

3.1.13. O Algoritmo de priorização deve considerar no mínimo 100.000 vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade;

3.1.14. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica do serviço de gestão de vulnerabilidades;

3.1.15. O Serviço deve ser capaz de aplicar algoritmos de inteligência artificial (Machine learning) para analisar mais de 130 fontes de dados relacionadas a vulnerabilidades;

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

3.1.16.1. CVSSv3 Impact Score;

3.1.16.2. Idade da Vulnerabilidade;

3.1.16.3. Se existe ameaça ou exploit que explore a vulnerabilidade;

3.1.16.4. Número de produtos afetados pela vulnerabilidade;

3.1.16.5. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;

3.1.16.6. Lista de todas as fontes (canais de mídia social, dark web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade;

3.1.17. O Serviço de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação);

3.1.18. Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras;

3.1.19. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura, incluindo feeds de inteligência de ameaças, tanto de fontes públicas como também de fontes não gratuitas;

3.1.20. O Serviço deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

3.1.21. O Serviço deve possuir conectores para a seguintes plataformas:

3.1.21.1. Amazon Web Service (AWS);

3.1.21.2. Microsoft Azure;

3.1.21.3. Google Cloud Platform;

3.1.22. O Serviço deve ser capaz de analisar vulnerabilidades em servidores na AWS utilizando somente o conector, sem a necessidade de instalação de agente ou uso de qualquer outro tipo de sensor de rede do serviço;

3.1.23. O Serviço deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;

3.1.24. O Serviço deve ser PCI ASV (Approved Scanning Vendor);

3.1.25. O Serviço deve ser capaz de identificar novos hosts no ambiente sem a necessidade de um scan;

3.1.26. O Serviço deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

3.1.27. O Serviço deve ser licenciada para no mínimo 50 scanners ativos;

3.1.28. O Serviço deve ser licenciada para o uso de no mínimo 20 sensores passivos de rede para realizar o monitoramento em tempo real do ambiente;

3.1.29. Deve ser possível determinar quais portas estão abertas em determinado ativo;

3.1.30. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo:

3.1.30.1. Endereço IPv4 e IPv6;

3.1.30.2. Sistema Operacional;

3.1.30.3. Nome NetBIOS:

3.1.30.4. FQDN;

3.1.31. O Serviço deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

3.1.31.1. Bancos de dados;

3.1.31.2. Hypervisors;

3.1.31.3. Dispositivos móveis;

3.1.31.4. Dispositivos de rede;

3.1.31.5. Endpoints;

3.1.31.6. Aplicações.

3.1.32. Deve realizar em tempo real a identificação de informações sensíveis no

tráfego de rede do ambiente;

3.1.33. O Serviço deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

3.1.34. Deve ter a capacidade de guardar em tempo real informações de GET, POST e Download que trafeguem na rede;

3.1.35. O Serviço deve ser capaz de em tempo real detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;

3.1.36. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real sem a necessidade de um agente;

3.1.37. O Serviço deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados;

3.1.38. O Serviço deve ser licenciada pra uso agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional, para o número total de ativos contratados.

3.1.39. O Serviço deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como Hypervisors e Dispositivos de Rede;

3.1.40. O Serviço deverá estar licenciada para varreduras em dispositivos móveis (Ex.: Smartphones, Tablets), sendo realizada através de integração com solução de MDM de mercado ou uso de agente próprio;

3.1.41. O Serviço deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

3.1.42. O Serviço deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento de configurações e vulnerabilidades;

3.1.43. O Serviço deve incluir a capacidade de programar períodos onde varreduras não podem ser executadas em determinados ativos, podendo selecionar no mínimo a frequência da agenda (diário, semanal, etc), hora de início e fim da janela, quais ativos serão excluídos e o fuso horário do agendamento;

3.1.44. O Serviço deve ser configurável para permitir a otimização das configurações de varredura, permitindo no mínimo definir o período de timeout, o número de conexões TCP concorrentes e reduzir a análise em execução caso detecte congestionamento de rede;

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

3.1.46. O Serviço deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

3.1.47. O Serviço deve ser capaz de realizar pesquisas de dados confidenciais;

3.1.48. Deve permitir executar uma análise de remediação, para verificar que uma solução foi aplicada corretamente. Essa análise de remediação será executada somente nos ativos impactados, analisando somente a vulnerabilidade remediada, sendo sua política criada especificamente para esta finalidade;

3.1.49. Deverá ser possível agrupar sensores em grupos. O Serviço deverá automaticamente distribuir uma atividade de análise entre os sensores pertencentes ao grupo, para aumentar a performance de um scan;

3.1.50. O Serviço deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é nova, persistente, corrigida ou reapareceu no ativo;

3.1.51. Deverá ser possível aceitar uma vulnerabilidade, onde a mesma não irá mais aparecer na console. Este processo poderá ser feito para um único ativo ou múltiplos ativos. Ainda, deverá ser possível definir uma data de expiração para a Aceitação.

3.1.52. Deverá ser possível modificar a severidade das vulnerabilidades, de um único ativo ou múltiplos ativos, podendo ainda definir uma data de expiração para esta modificação.

3.1.53. O Serviço deve suportar o uso de tags nos ativos, sendo estes aplicados de forma manual ou automaticamente;

3.1.54. No caso de Tags automáticas, deverá ser possível configurar regras para atender, no mínimo:

3.1.54.1. Ativo analisado ou não em relação a vulnerabilidades;

3.1.54.2. Informações de nuvem pública, como por exemplo região na AWS, Azure resource ID ou GCP Cloud Project ID;

3.1.54.3. Software instalado no ativo;

3.1.54.4. Sub rede;

3.1.54.5. Sistema Operacional.

3.1.55. Deverá ser possível configurar quais usuários, ou grupos de usuários, podem editar as Tags;

3.1.56. O Serviço deverá usar as Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada tag;

3.1.57. Ser possível fazer análise dos ativos através de Tags, como exemplo todos os Ativos que possuem a tag Linux.

3.2. Controle de usuários

3.2.1. O Serviço deve suportar RBAC (role based access control) com no mínimo 5 tipos de usuários pré-definidos;

3.2.2. Deve possuir no mínimo um perfil administrador e um perfil somente leitura

3.2.3. Deve permitir autenticação com SingleSign On suportando os padrões SAML 2.0 ou Shibboleth.

3.2.4. O Serviço deve possibilitar a criação de Grupos de Usuários;

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

3.2.6. Possuir duplo fato de autenticação nativo na própria console;

3.2.7. Deve possibilitar configurar permissões, por usuário e grupo de usuário, específicas para cada política de análise de vulnerabilidades. No mínimo deverá ser possível configurar permissões de Nenhum Acesso, Somente Ver Resultados,

Configuração ou Execução das políticas.

3.3. Relatórios e Dashboards

3.3.1. Deve ser capaz de exportar dashboards em modelo de relatórios, tanto de forma manual e periódico de acordo com a frequência estabelecida pelo administrador;

3.3.2. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

3.3.3. O Serviço deve suportar o envio automático de relatórios para destinatários específicos;

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

3.3.5. O Serviço deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;

3.3.6. Deve possuir ao menos 10 modelos de dashboards já criados, podendo ser customizados;

3.3.7. A solução deve permitir exportar dados do que está sendo apresentado na tela, no mínimo para:

3.3.7.1. Ativos gerenciados pelo Serviço;

3.3.7.2. Todas as vulnerabilidades existentes no ambiente e em quais ativos ela existe;

3.3.7.3. Vulnerabilidades por ativo gerenciado pelo serviço;

3.3.7.4. Vulnerabilidades de um único ativo;

3.3.7.5. Uma única vulnerabilidade e todos os ativos que possuem;

3.3.8. Deve ser possível exportar os dados em HTML, PDF ou CSV;

3.3.9. Em caso de exportação por CSV deve ser possível selecionar, via console de gerenciamento, quais campos deseja exportar;

3.3.10. Deve ser possível exportar somente os gráficos dos dashboards, através da console de gerenciamento, em PDF, PNG e JPG;

3.3.11. Deve ser possível criar um novo Dashboard e definir este como padrão de visualização do usuário, ou seja, o primeiro dashboard a aparecer na console no acesso

3.3.12. Deve ser possível configurar um filtro permanente no Dashboards para apresentar informações de todos os ativos, ou somente ativos específicos do ambiente

3.3.13. O Serviço deve permitir compartilhar Dashboards com um ou mais usuários, bem como com grupo de usuários da aplicação

3.3.14. Deve ser possível configurar SLAs em dias, representando a idade das vulnerabilidades no ambiente, sendo o período onde a mesma foi encontrada até a resolução. Está informação deverá ser apresentada no Dashboard do serviço.

3.4. Análise de Conformidade

3.4.1. O Serviço deve ser totalmente licenciada para realizar scans de auditoria e compliance;

3.4.2. O Serviço deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

3.4.3. O Serviço deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada;

3.4.4. Toda O Serviço deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL;

3.4.5. O Serviço deverá possuir modelos prontos de padrões de configuração, no mínimo para: CIS, DISA e MSCT (Microsoft Security Compliance Toolkit);

3.4.6. Deve suportar a verificação de compliance para no mínimo:

- **3.4.6.1.** Bluecoat ProxySG;
- **3.4.6.2.** Brocade Fabric OS;
- **3.4.6.3.** Checkpoint;
- **3.4.6.4.** Cisco IOS;
- **3.4.6.5.** Citrix Xenserver;
- **3.4.6.6.** Fireeye;
- **3.4.6.7.** Fortinet FortiOS;
- **3.4.6.8.** IBM iSeries;
- **3.4.6.9.** Netapp Data ONTAP;
- **3.4.6.10.** Palo Alto Firewall;
- **3.4.6.11.** Red Hat Enterprise Virtualization;
- **3.4.6.12.** Unix;

3.4.6.13. Windows;

3.4.6.14. Vmware.

3.4.7. O Serviço deve mostrar se o critério de compliance foi atendido ou não fornecendo no mínimo os seguintes status:

3.4.7.1. Passou;
3.4.7.2. Falhou;
3.4.7.3. Atenção.

3.5. Requisitos de Segurança

3.5.1. O Serviço deve criptografar todas as informações em trânsito;

3.5.2. Deve utilizar no mínimo chave AES-256 para criptografar os dados armazenados;

3.5.3. O Serviço deve ser capaz de gerar uma chave randômica com no mínimo 256 bits para cada scanner conectado na plataforma de gerência;

3.5.4. Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados no mínimo com protocolo TLS 1.2 com tamanho de chave de 4096 bits;

3.5.5. Dados indexados devem possuir no mínimo criptografia utilizando algoritmo AES-256;

3.5.6. A plataforma deve ser capaz de gerar uma chave randômica de no mínimo 128 bits para qualquer “Job” gerado;

3.5.7. A plataforma deve utilizar no mínimo chave AES-256 para Backups e dados Replicados

3.5.8. Todas as credenciais armazenadas na plataforma deverão ser criptografadas com algoritmo AES-256, no mínimo;

3.5.9. O Serviço deve possuir no mínimo as seguintes certificações de privacidade e segurança:

3.5.9.1. EU-U.S. Privacy Shield Framework;

3.5.9.2. Swiss-U.S. Privacy Shield Framework;

3.5.9.3. Cloud Security Alliance (CSA) STAR;

3.5.10. O Serviço deve possuir ferramentas e processos automatizados para monitorar: Uptime, Comportamentos anômalos e performance da plataforma;

3.5.11. Deve possuir retenção na nuvem de no mínimo 12 meses dos resultados dos scans realizados no ambiente;

3.5.12. Os dados de clientes deverão ser totalmente separados um dos outros, não possuindo compartilhamento de dados;

3.5.13. O Serviço deverá implementar controles de segurança, como Análise de Vulnerabilidade no mínimo semanal, Firewalls, segmentação de rede, e monitoramento de segurança 24/7/365, para garantir a segurança da aplicação;

3.5.14. O Serviço deverá seguir metodologias de Desenvolvimento Seguro;

3.5.15. O Serviço deverá possuir ISO 27001.

3.6. Análise de Risco do Ambiente

3.6.1. O Serviço deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

3.6.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

3.6.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

3.6.4. O Serviço deve ser capaz de realizar um benchmark no ambiente da CONTRATANTE comparando sua maturidade com outras organizações do mesmo setor;

3.6.5. O Serviço deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro.

3.6.6. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

3.6.7. O Serviço deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo).

3.6.8. O Serviço deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos.

3.6.9. O Serviço deve permitir um acompanhamento histórico do nível de exposição da organização;

3.6.10. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente.

3.6.11. O Serviço deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão.

3.6.12. O Serviço deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área.

3.6.13. O Serviço deve permitir a segregação lógica entre aplicações distintas da empresa afim de obter a pontuação referente exposição cibernética por aplicação.

3.7. Gestão de Vulnerabilidade em Aplicações Web

3.7.1. O Serviço de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

3.7.2. O Serviço deverá capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS);

3.7.3. A plataforma deverá avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

3.7.4. O Serviço deverá ser homologada como PCI ASV

3.7.5. Deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

3.7.6. Deve possui modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados;

3.7.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

3.7.7.1. Cookies, Headers, Formulários e Links;

3.7.7.2. Nomes e valores de parâmetros da aplicação;

3.7.7.3. Elementos JSON e XML;

3.7.7.4. Elementos DOM;

3.7.8. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

3.7.9. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

3.7.10. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

3.7.11. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

3.7.12. Deve ser capaz de instituir no mínimo os seguintes limites:

3.7.12.1. Número máximo de URLs para crawl e navegação;

3.7.12.2. Número máximo de diretórios para varreduras;

3.7.12.3. Número máximo de profundidade dos elementos DOM;

3.7.12.4. Tamanho máximo de respostas;

3.7.12.5. Limite de requisições de redirecionamentos;

3.7.12.6. Tempo máximo para a varredura;

3.7.12.7. Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

3.7.12.8. Número máximo de requisições HTTP por segundo.

3.7.13. O Serviço deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

3.7.13.1. Limite em segundos para timeout de requisições de rede;

3.7.13.2. Número máximo de timeouts antes que a varredura seja abortada;

3.7.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

3.7.15. Deve ser capaz de enviar notificações através de no mínimo E-mail;

3.7.16. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

3.7.17. Deverá avaliar sistemas web utilizando frameworks modernos, como AJAX, HTML5 e SPA;

3.7.18. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

3.7.19. Deverá ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger).

3.7.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:

3.7.20.1. Autenticação básica (digest);

3.7.20.2. NTLM;

3.7.20.3. Form de login;

3.7.20.4. Autenticação de Cookies;

3.7.20.5. Autenticação através de Selenium.

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

3.7.22. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

3.7.23. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise;

3.7.24. Deve ser capaz de exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

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

3.7.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

3.7.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

3.7.27.1. Payload injetado;

3.7.27.2. Evidência em forma de resposta da aplicação;

3.7.27.3. Detalhes da requisição HTTP;

3.7.27.4. Detalhes da resposta HTTP;

3.7.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

3.7.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

3.7.30. O Serviço deve possuir suporte a varreduras de componentes para no mínimo: WordpPess, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Tomcat JK connecto, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

3.7.31. O Serviço deverá possuir controle de permissão de usuários, com no mínimo menos 3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura;

3.7.32. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard do serviço;

3.7.33. O Serviço deverá possuir um Add-on para o browser que permite gravar uma macro de autenticação para criação do Selenium;

3.7.34. Deverá ser possível excluir a interação com elementos DOM durante o Scan. Está exclusão poderá ser configurada para cada elemento, sendo possível escolher o Conteúdo do texto ou do Atributo CSS.

3.7.35. O Serviço deverá possuir nativamente scanners pré-configurados em nuvem, para realização de scans externos. Estes scanners deverão obrigatoriamente possuir IP dedicado, com divulgação pública, para configuração de whitelist em Firewalls, WAFs, ou outros sistemas de proteção.

3.7.36. O Serviço deve possuir também sensores (scanner) on-premises. O Serviço deverá estar licenciada para o uso de no mínimo 10 sensores deste tipo.

3.7.37. Deverá ser possível exportar os gráficos do dashboard em PDF, PNG ou JPEG, nativamente pela console de gerência.

3.7.38. Deve ser possível alterar o user agent utilizado pelo serviço;

3.7.39. O Serviço deve suportar listas de exclusão globais;

3.7.40. Deve possuir um dicionário já criado com as principais páginas comuns e páginas de backup existentes.

3.7.41. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas;

3.7.42. Ser possível gerar relatório das vulnerabilidades, no mínimo em PDF, HTML e CSV.

3.8. Gestão de correção de vulnerabilidades de segurança

3.8.1. Deve prover visibilidade e cobertura em tempo real para os sistemas operacionais e aplicações utilizadas nos ativos da organização, ou seja, qualquer alteração no inventário (instalação / desinstalação / alteração de aplicativos e / ou ativos deve ser refletida instantaneamente na solução).

3.8.2. Deve ter a possibilidade de instalar um componente na rede interna para fazer o caching de patches, atendendo requisitos de ativos que não podem realizar download das atualizações diretamente da internet. Tal componente deve ser

executado em pelo menos um dos seguintes sistemas operacionais: Ubuntu ou Red Hat Linux.

3.8.3. Deve prover atualização de patches para servidores sem interrupção do serviço principal, sem forçar a reinicialização do mesmo.

3.8.4. Deve atualizar não apenas o Sistema operacional, mas também as aplicações instaladas nos ativos.

3.8.5. Deve trabalhar com reconhecimento automático de aplicações instaladas nos hosts, mantendo também o fluxo de atualizações disponível.

3.8.6. Deve fornecer gerenciamento de patches fim a fim para o sistema operacional Windows;

3.8.7. Deve fornecer gerenciamento de patches para aplicações de terceiros no Windows;

3.8.8. Deve fornecer gerenciamento de patch para o sistema operacional Linux;

3.8.9. Deve fornecer gerenciamento de patches para aplicativos de terceiros no Linux e não apenas na camada de SO.

3.8.10. Deve fornecer gerenciamento de patches para o sistema operacional Mac.

3.8.11. Para o sistema operacional Windows, minimamente, as seguintes aplicações devem poder ser atualizadas:

3.8.11.1. 7-zip;

3.8.11.2. Adobe Reader;

3.8.11.3. Acrobat Reader;

3.8.11.4. Adobe Photoshop;

3.8.11.5. Adobe Creative Cloud;

3.8.11.6. Adobe Flash Player;

3.8.11.7. Autocad;

3.8.11.8. Keepass;

3.8.11.9. Openssl;

3.8.11.10. Opera;

3.8.11.11. Python;

3.8.11.12. Google Chrome;

3.8.11.13. Google Earth;

3.8.11.14. Google Picasa;

3.8.11.15. Google Drive;

3.8.11.16. Mozilla Firefox;

3.8.11.17. Mozilla Thunderbird;

3.8.11.18. Sun Java;

3.8.11.19. Microsoft Office;

3.8.11.20. Microsoft Visual Studio;

3.8.11.21. Microsoft System Center;

3.8.11.22. Microsoft SQL Server;

3.8.11.23. Microsoft Exchange;

3.8.11.24. Microsoft Edge;

3.8.11.25. Microsoft Teams;

3.8.11.26. Microsoft OneDrive;

3.8.11.27. Microsoft Internet Explorer;

3.8.11.28. Microsoft Outlook;

3.8.11.29. Microsoft Visio;

3.8.11.30. Microsoft Windows Defender;

3.8.11.31. Notepad++;

3.8.11.32. PowerBI;

3.8.11.33. Microsoft IIS;

3.8.11.34. Tomcat;

3.8.11.35. PDF Reader;

3.8.11.36. Zoom;

3.8.11.37. Vmware Workstation;

3.8.11.38. Webex;

3.8.11.39. Whatsapp;

3.8.11.40. Telegram;

3.8.11.41. Signal.

3.8.12. Para os sistemas operacionais Linux, minimamente, as seguintes aplicações devem poder ser atualizadas:

3.8.12.1. Abrt;

3.8.12.2. Adduser;

3.8.12.3. Alsa-Lib

3.8.12.4. Alsa-Tools-Firmware;

3.8.12.5. Apparmor;

3.8.12.6. Apport;

3.8.12.7. Apt-Utils;

3.8.12.8. Base-Files;

3.8.12.9. Bash;

3.8.12.10. Binutils;

3.8.12.11. BZIP2;

3.8.12.12. Chrony;

3.8.12.13. Coreutils;

3.8.12.14. Crontabs;

3.8.12.15. Curl;

3.8.12.16. Dash;

3.8.12.17. Debianutils;

3.8.12.18. Device-Mapper;

3.8.12.19. Diffstat;

3.8.12.20. Diffutils;

3.8.12.21. Dirmngr;

3.8.12.22. Distro-Info;

3.8.12.23. Dnsutils;

3.8.12.24. Dpkg;

3.8.12.25. Elfutils;

3.8.12.26. Fdisk;

3.8.12.27. Findutils;

3.8.12.28. Firewalld;

3.8.12.29. FTP;

3.8.12.30. Gdisk;

3.8.12.31. Git;

3.8.12.32. GLIB2;

3.8.12.33. Glibc;

3.8.12.34. Glibc-Common;

3.8.12.35. GNUPG2;

3.8.12.36. Gnupg-Utils;

3.8.12.37. Grep;

3.8.12.38. Grub2-Tools;

3.8.12.39. Grub-Common;

3.8.12.40. Gzip;

3.8.12.41. Iproute;

3.8.12.42. Iprutils;

3.8.12.43. Iptables;

3.8.12.44. Iputils;

3.8.12.45. Kernel-Tools;

3.8.12.46. Kmod;

3.8.12.47. Libcap;

3.8.12.48. Mount;

3.8.12.49. Net-Tools;

3.8.12.50. Openssh;

3.8.12.51. Openssl;

3.8.12.52. Open-Vm-Tools;

3.8.12.53. PAM;

3.8.12.54. Passwd;

3.8.12.55. Patchutils;

3.8.12.56. Perl;

3.8.12.57. Postfix;

3.8.12.58. Python;

3.8.12.59. RPM;

3.8.12.60. Rsyslog;

3.8.12.61. Shadow-Utils;

3.8.12.62. Sqlite;

3.8.12.63. Sudo;

3.8.12.64. Tar;

3.8.12.65. Tcpdump;

3.8.12.66. Telnet;

3.8.12.67. Time;

3.8.12.68. Unzip;

3.8.12.69. Vim;

3.8.12.70. Wget;

3.8.12.71. Yum;

3.8.12.72. Zerofree;

3.8.12.73. Zip.

3.8.13. Para os sistemas operacionais MAC, minimamente, as seguintes aplicações devem poder ser atualizadas:

3.8.13.1. Microsoft Office;

3.8.13.2. Zoom;

3.8.13.3. 1password;

3.8.13.4. Acrobat Reader;

3.8.13.5. Mongodb;

3.8.13.6. Signal;

3.8.13.7. Google Chrome;

3.8.13.8. Whatsapp

3.8.13.9. Safari;

3.8.13.10. Microsoft Teams;

3.8.13.11. Microsoft OneDrive;

3.8.13.12. Mozilla Firefox.

3.8.14. Deve prover avaliação contínua de vulnerabilidades para identificação de quais atualizações devem ser instaladas em cada host.

3.8.15. Deve fornecer painel com priorização de ameaças com base nos ativos, aplicações ou sistemas operacionais.

3.8.16. A priorização de vulnerabilidade e correções a serem realizadas deve ser combinada com um motor inteligência interna a própria solução.

3.8.17. O processo de priorização e remediação de vulnerabilidades deve acompanhar todo o seu ciclo de vida, ou seja, descoberta/identificação, correção manual ou automatizada e contabilização nas visões para acompanhamento das ações que foram tomadas.

3.8.18. Deve permitir a execução de comandos de forma remota em todos os dispositivos que possuem os agentes instalados.

3.8.19. Deve permitir o agendamento de instalação das atualizações (Patches) ou execução de script de forma remota.

3.8.20. Deve possibilitar a execução de ações automáticas pré-configuradas e personalizadas (Ações Automáticas).

3.8.21. As ações automáticas devem possibilitar a instalação automática de patches baseado em critérios personalizáveis, como:

3.8.21.1. Atualizações de sistema operacional;

3.8.21.2. Atualizações de aplicações específicas;

3.8.21.3. Por grupo de dispositivo previamente definido;

3.8.21.4. Por severidade/criticidade do patch de correção.

3.8.22. Toda instalação de patch deve permitir a opção de reinicialização automática da estação/servidor, dando também a opção para que o usuário cancele o restart, se necessário.

3.8.23. Deve ser possível enviar “pop-ups” para os usuários, quando os mesmos estiverem pendentes de reinicialização.

3.8.24. Deve possibilitar a geração de scripts para Windows, Linux e Mac na mesma visão.

3.8.25. Deve possuir proteção contra vulnerabilidades de dia 0 (zero day).

3.8.26. Deve possuir mecanismos de "Ações recomendadas", de forma a guiar as correções a serem realizadas.

3.8.27. Deve suportar segregação de função por usuário, ou seja, permitir que usuários da mesma empresa tenham permissões diferentes dentro da plataforma.

3.8.28. Deve ser capaz de segregar diferentes ativos entre diferentes grupos de usuários com diferentes níveis de permissão.

3.8.29. A segregação de ativos por grupos, deve respeitar características dinâmicas, de forma a movimentar os ativos entre os grupos de forma automática. Tal característica deve suportar a configuração, minimamente, dos seguintes atributos (Para movimentação automática dos ativos):

3.8.29.1. Nome do ativo;

3.8.29.2. Tipo do ativo;

3.8.29.3. Nível de risco do ativo;

3.8.29.4. Status do ativo;

3.8.29.5. CVE's específicos detectados no mesmo;

3.8.29.6. Aplicações específicas instaladas nos ativos, assim como a versão detectada do mesmo;

3.8.29.7. Sistema operacional e versão do mesmo.

3.8.30. Deve fornecer proteção de virtual Patching para aplicações terceiras.

3.8.31. Deve funcionar de forma oculta no sistema operacional, não apresentando interface para o usuário final.

4. ITEM 4 – SOLUÇÃO DE CORRELAÇÃO DE EVENTOS DE SEGURANÇA E RESPOSTA A INCIDENTES

4.1. Arquitetura

4.1.1. Deve ser on-premise ou baseada em nuvem (Cloud), de forma a manter todos os eventos armazenados na nuvem do fabricante da solução.

4.1.2. Não serão aceitos serviços entregues por meio de software livre ou open-source.

4.1.3. A solução deve fornecer componentes já licenciados para coleta e envio de logs/tráfego até a plataforma central.

4.1.4. O componente para coleta de logs/tráfego deve fornecer a possibilidade de instalação em servidores Windows, Linux ou imagens prontas previamente fornecidas.

4.1.5. A solução deve suportar processamento de logs/eventos para, no mínimo os itens inseridos na tabela abaixo:

4.1.6. Deverá estar licenciada, em nome da CONTRATADA, de forma a manter o processamento em tempo real ou realizar o buffer dos eventos, mesmo que o tráfego de eventos ultrapasse o volume licenciado nas horas de pico.

4.1.7. Suportar um tráfego de logs de, no mínimo, 3000 eventos por segundo (EPS).

4.1.8. Deve possuir capacidade de recebimento e armazenamento, mínimo, de todos os logs de ativos de segurança, alertas de segurança, tráfego de pacotes, dentre outras informações relacionadas, em formado bruto (raw) e/ou metadados, necessárias para fins de correlacionamento e forense, conforme especificação abaixo:

Tráfego de Pacotes	**Logs, Eventos, Alertas, dentre outras informações**

Metadados	Armazenar por no mínimo 365 dias	Armazenar por no mínimo 365 dias
Dados brutos (raw)	Armazenar por no mínimo 365 dias	Armazenar por no mínimo 365 dias

4.1.9. Deve ter a capacidade de manter os itens coletados indexados para buscas rápidas por pelo menos 7 dias. Itens a serem buscados em datas superiores ao período de indexação devem respeitar o período de retenção do tópico anterior.

4.2. Requerimentos Gerais

4.2.1. Deverá ser capaz de gerenciar de forma eficiente incidentes de segurança. O software de gerenciamento de incidentes de segurança deve permitir a definição de um processo abrangente desde o registro e triagem inicial de um incidente até sua resolução e prevenção.

4.2.2. Deve permitir a automação de fluxos de forma gráfica, incluindo estágios, tarefas paralelas ou sequenciais, regras de decisão e aprovação, sem a necessidade de programação ou alteração de código fonte para as integrações já existentes.

4.2.3. Deve permitir automatização e orquestração de fluxos relacionados a resposta de incidentes de segurança, integrando e simplificando as operações.

4.2.4. Deve fornecer visibilidade, rastreabilidade e indexação dos eventos detectados, integrando as várias ferramentas de segurança que a entidade possui, aumentando a capacidade de detecção e maturidade da segurança cibernética.

4.2.5. Deve permitir acelerar a resposta às lacunas de segurança cibernética por meio de análise contextual, automação de processos e capacidade de articulação para investigação, utilizando fluxos de análise e inteligência associada às metodologias de ataque de grupos de cibercrime.

4.2.6. Deve identificar, registrar e indexar incidentes de segurança rapidamente, registrando os eventos relatados pelas soluções que a CONTRATADA atualmente possui.

4.2.7. Deve permitir integração e interoperabilidade com o ecossistema de segurança da entidade, independentemente da marca dos produtos de segurança utilizados.

4.2.8. Deve permitir a integração baseada em fluxos de trabalho através do cruzamento de dados das soluções de segurança como Firewalls, IPSs e sistemas de chamados.

4.2.9. Deve possuir controle granular de níveis de acesso a plataforma.

4.2.10. Deve funcionar, obrigatoriamente, com autenticação de dois fatores nativa, sendo eles: OTP, SMS ou voz.

4.2.11. Deve permitir que você configure políticas restritas de senha como período de redefinição, bloqueio por tentativas sem sucesso, histórico de senha e desativação de usuários por tempo de inatividade.

4.2.12. Deve registrar e listar todos os alertas ativos, permitindo filtros e pesquisas sob demanda em uma linguagem de queries.

4.2.13. Deve permitir a criação de listas a serem utilizadas durantes as pesquisas, com objetivo de poder facilmente utiliza-las para inclusão ou remoção de recursos na busca, evitando a repetição de comandos, tornando as ações de caça a ameaças (hunting) mais ágeis.

4.2.14. Deve possuir alertas indicando a gravidade do incidente, permitindo a detecção, validação e investigação, a fim de reconstruir toda a cadeia do ataque.

4.2.15. Deve suportar uma linha do tempo visual em relação aos eventos registrados.

4.2.16. Deve oferecer suporte à integração com soluções de segurança de terceiros. A integração deve ser baseada em syslog, ingestão/absorção de alertas e/ou análise de tráfego de rede.

4.2.17. Deve permitir a criação de painéis e dashboards com gráficos de gestão, de forma ágil e intuitiva, sem a necessidade de programação e alteração do código-fonte.

4.2.18. Deve permitir aos atendentes e solucionadores de incidentes a possibilidade de criação de seus próprios painéis e gráficos dentro da solução, compartilhando sempre que necessário com grupos ou usuários específicos, permitindo gerenciamento das permissões de compartilhamento de acordo com os perfis de cada usuário.

4.2.19. Deve permitir a criação de gráficos, utilizando como origem de dados, as informações de diferentes soluções de segurança da organização.

4.2.20. Deve permitir configurar o envio automático e agendado de relatórios e gráficos gerenciais para grupos de usuários ou usuários específicos.

4.2.21. Deve incluir painéis unificados, buscas e relatórios, para facilitar a transição da detecção para a investigação e a resposta subsequente ao incidente relatado.

4.2.22. O coletor da solução deverá ser capaz de coletar, aplicar parsing, normalizar e categorizar os eventos dos dispositivos monitorados em tempo próximo ao real.

4.2.23. Deve possuir parsing, para interpretação automática de logs, para pelo menos as seguintes marcas/soluções:

4.2.23.1. Aerohive;

4.2.23.2. Akamai;

4.2.23.3. AWS;

4.2.23.4. Apache;

4.2.23.5. Arbor;

4.2.23.6. ArcSight;

4.2.23.7. Aruba;

4.2.23.8. Barracuda;

4.2.23.9. BeyondTrust;

4.2.23.10. BlueCoat;

4.2.23.11. Broadcom;

4.2.23.12. Brocade;

4.2.23.13. Carbom Black;

4.2.23.14. CheckPoint;

4.2.23.15. Cisco;

4.2.23.16. Citrix;

4.2.23.17. Crowdstrike;

4.2.23.18. CyberArk.

4.2.23.19. Cylance;

4.2.23.20. Docker;

4.2.23.21. Eset;

4.2.23.22. F5;

4.2.23.23. FireEye;

4.2.23.24. Forcepoint;

4.2.23.25. Forescout;

4.2.23.26. Fortinet;

4.2.23.27. Graylog;

4.2.23.28. HP;

4.2.23.29. IBM;

4.2.23.30. Imperva;

4.2.23.31. Juniper;

4.2.23.32. Mandiant;

4.2.23.33. McAfee;

4.2.23.34. Microsoft;

4.2.23.35. Nagios;

4.2.23.36. Nginx;

4.2.23.37. Oracle;

4.2.23.38. Palo Alto;

4.2.23.39. Proofpoint;

4.2.23.40. Pulse Secure;

4.2.23.41. Riverbad;

4.2.23.42. RSA;

4.2.23.43. SonicWall;

4.2.23.44. Sophos;

4.2.23.45. Splunk;

4.2.23.46. Symantec;

4.2.23.47. Tenable;

4.2.23.48. Trend Micro;

4.2.23.49. Varonis;

4.2.23.50. Digital Guardian;

4.2.23.51. Vmware;

4.2.23.52. WatchGuard;

4.2.23.53. Zscaler.

4.2.24. Deve fornecer um módulo de UEBA ao qual possa ser utilizado para análise avançada do comportamento de entidades (computadores e usuários) aos quais podem estar envolvidos em atividades maliciosas. O módulo de UEBA deve utilizar técnicas avançadas para análise de comportamento sendo possível correlacionar eventos e extrair informações relevantes as quais devem ser utilizadas para definir o perfil de risco das entidades.

4.2.25. Deve analisar os tipos de log enviados e realizar sugestões de envio de importantes fontes de detecção de malware na qual ele não está recebendo logs. Exemplo: a organização não está enviando logs de firewall e DHCP, tais logs ampliam o poder de detecção da plataforma. Este recurso deve estar em execução automaticamente.

4.2.26. Deve possuir dashboards e relatórios que classifiquem os logs que foram devidamente classificados, permitindo também a rápida visualização dos que não foram, para que as ações de "parsing" possam ser planejadas.

4.2.27. Deve possuir dashboards prontos que são alimentados a partir da ingestão de logs para pelo menos, os seguintes fabricantes:

4.2.27.1. AWS;

4.2.27.2. Carbon Black;

4.2.27.3. Checkpoint;

4.2.27.4. Cisco;

4.2.27.5. Crowdstrike;

4.2.27.6. Druva;

4.2.27.7. FireEye;

4.2.27.8. Google Cloud Plataform;

4.2.27.9. iBoss;

4.2.27.10. Imperva;

4.2.27.11. McAfee;

4.2.27.12. Microsoft;

4.2.27.13. Microsoft Azure;

4.2.27.14. Okta;

4.2.27.15. Palo Alto;

4.2.27.16. Proofpoint;

4.2.27.17. Sophos;

4.2.27.18. Symantec;

4.2.27.19. Virtru.

4.2.28. Deve possuir meios de monitoramento de saúde de todos os sensores que enviam logs para a console central.

4.2.29. Caso alguma fonte pare de enviar logs, a plataforma deve informar automaticamente os administradores para verificação.

4.2.30. Deve possuir nativamente integrações para serviços de nuvem, considerando minimamente:

4.2.30.1. AWS CloudTrail;

4.2.30.2. AWS CloudWatch;

4.2.30.3. AWS GuardDuty;

4.2.30.4. AWS S3;

4.2.30.5. AWS Security Hub;

4.2.30.6. AWS VPC Flow Logs;

4.2.30.7. Azure;

4.2.30.8. Azure Active Directory (Para UEBA);

4.2.30.9. Bitglass;

4.2.30.10. Box.com;

4.2.30.11. Canary;

4.2.30.12. CipherCloud CASB+;

4.2.30.13. Cisco Umbrella;

4.2.30.14. Cisco Umbrella S3;

4.2.30.15. Corelight;

4.2.30.16. Crowdstrike Falcon;

4.2.30.17. CSC Global Domain Manager;

4.2.30.18. Digital Guardian;

4.2.30.19. Druva;

4.2.30.20. Duo Auth;

4.2.30.21. Entrust Intellitrust;

4.2.30.22. FireEye Detection on Demand for AWS S3;

4.2.30.23. FireEye Email Threat Prevention;

4.2.30.24. FireEye Message Security for Slack;

4.2.30.25. FireEye Messaging Security for Microsoft 365;

4.2.30.26. FireEye Network Security;

4.2.30.27. Google Cloud;

4.2.30.28. Google Cloud Audit Events;

4.2.30.29. Kentik;

4.2.30.30. McAfee MVision Mobile;

4.2.30.31. Microsoft CASB;

4.2.30.32. Microsoft Graph;

4.2.30.33. Microsoft Office 365;

4.2.30.34. Mimecast;

4.2.30.35. Netskope;

4.2.30.36. Okta;

4.2.30.37. Proofpoint CASB Integration;

4.2.30.38. Proofpoint SIEM Integration;

4.2.30.39. Qualys File Integrity Monitoring;

4.2.30.40. Security Onion;

4.2.30.41. Signal Sciences WAF;

4.2.30.42. Sophos Antivirus SIEM Integration;

4.2.30.43. Symantec Mobile Protection;

4.2.30.44. Symantec Web Security Service;

4.2.30.45. Windows Defender ATP;

4.2.30.46. Zimperium.

4.3. Inteligência de Ameaças

4.3.1. Deve incluir regras de correlação e inteligência de ameaças.

4.3.2. Deve incluir um pacote de regras para detecção. Elas devem ser alimentadas automaticamente, sem gerar impacto ou solicitar intervenção de um analista. Por sua vez, ela deve permitir a criação de regras personalizadas pela CONTRATADA, incluído a entrada manual de novos indicadores de comprometimento.

4.3.3. Deve fornecer uma boa variedade de regras de inteligência já criadas e disponíveis para detecção de ameaças e também permitir customização de novas para atender necessidades específicas.

4.3.4. Deve incluir inteligência de ameaças que revise, valide e compare as fontes que estão sendo utilizadas para detecção de ameaças.

4.3.5. Deve incluir a descrição das famílias de malware.

4.3.6. Deve fornecer atribuição automática de alertas a grupos de APTs.

4.3.7. O fabricante deve possuir especialistas em segurança que estejam monitorando as ameaças atuais ao redor do mundo, gerando a partir disso, novos pacotes de regras para aprimorar a solução em seu nível de detecção. Tal serviço não deve ocasionar custo adicional para a CONTRATANTE.

4.3.8. O fabricante deve rastrear grupos de crimes cibernéticos, a fim de aprimorar regras de detecção a partir de incidentes globais.

4.3.9. Deve utilizar uma rede de inteligência que processa diversas amostras de malware exclusivas por dia.

4.3.10. Deve injetar inteligência nos dados de log registrados.

4.3.11. Deve oferecer análises sobre "beaconing", permitindo no mínimo, a detecção de malwares que tentam estabelecer contato com “Command and Control”.

4.3.12. Deve incluir como fonte de inteligência as ameaças, plataformas de segurança contratadas e permitir identificar a telemetria e o perfil de proliferação de um ataque, além de ter informações sobre vítimas e táticas, técnicas e procedimentos geralmente utilizados pelo invasor.

4.3.13. Deve possibilitar consultas de segurança específicas (Buscando referências a malwares ou ataques conhecidos), incluindo análise, para no mínimo:

4.3.13.1. URLs;

4.3.13.2. Domínios;

4.3.13.3. Hashes MD5;

4.3.13.4. Endereços IP.

4.3.14. Deve permitir a criação de listas a serem utilizadas com escopo de inteligência, facilitando assim o uso das mesmas em regras ou mesmo para customizar detecções especificas do negócio.

4.3.15. Deve fornecer a possibilidade de análise de malwares, executando o mesmo de maneira controlada (sandbox), a fim de receber um relatório sobre os comportamentos encontrados com a execução.

4.3.16. Depois que uma ameaça for detectada, ela deve relacionar as informações registradas na plataforma central e as vincular fornecendo detalhes de inteligência.

4.3.17. Deve oferecer análises mínimas em:

4.3.17.1. Beaconing;

4.3.17.2. Beaconing Diferencial;

4.3.17.3. Geo-feasibility;

4.3.17.4. Uso indevido de credenciais;

4.3.17.5. Detecção de conexão não reconhecida;

4.3.17.6. Detecção de Fast-Flux DNS;

4.3.17.7. Entropia DNS;

4.3.17.8. Detecção de ataques via PowerShell;

4.3.17.9. Detecção de Exfiltração de Dados;

4.3.17.10. Detecção de conexões de entrada SSH, Telnet, SMB e RDP que sejam anômalas;

4.3.17.11. Detecção de contas comprometidas com VPN;

4.3.17.12. Detecção de movimento lateral.

4.3.18. Deve permitir que sejam realizadas pesquisas em seu ambiente para atividades de "caça" a malwares e atividades maliciosas.

4.3.19. Deve possuir capacidade analítica de eventos/tráfego, independente das regras, para detecção de no mínimo os seguintes comportamentos:

4.3.19.1. Uso suspeito de chave da API Amazon Web Services (AWS);

4.3.19.2. Login de autenticação multifator anormal do Duo com base no histórico de login anterior deste usuário;

4.3.19.3. Atividade anormal do Google Cloud Platform (GCP) por um usuário;

4.3.19.4. Logon anormal no Microsoft Office 365 com base no histórico de logon anterior deste usuário;

4.3.19.5. Login anormal do Okta com base no histórico de login anterior deste usuário;

4.3.19.6. Login anormal do protocolo RDP (Remote Desktop Protocol) com base no histórico de login anterior deste usuário;

4.3.19.7. Download ou upload anormal de arquivo do SharePoint com base no histórico anterior deste usuário;

4.3.19.8. Detecção de força bruta do Citrix NetScaler, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

4.3.19.9. Detecção de força bruta no Druva, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

4.3.19.10. Tráfego de rede para domínios semelhantes a (permutações) do domínio da organização descoberto. Isso pode indicar um ataque de phishing ou alguma outra atividade suspeita.

4.3.19.11. Detecção de força bruta no Linux, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

4.3.19.12. Detecção de força bruta do Office 365, realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

4.3.19.13. Okta detecção de força bruta. Isso realiza verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

4.3.19.14. Vários logins de RDP pelo mesmo usuário.

4.3.19.15. Vários logins de RDP no mesmo host.

4.3.19.16. Login de VPN anormal com base no histórico de login de VPN anterior do usuário.

4.3.19.17. Uma conta de usuário foi excluída dentro de 24 horas após sua criação.

4.3.19.18. Detecção de força bruta do Windows NT LAN Manager (NTLM), realizando verificações de pulverização de senha e logons bem-sucedidos da mesma fonte.

4.3.19.19. Vários erros de "usuários únicos não encontrados" de uma fonte. Isso pode indicar uma tentativa de enumeração do usuário.

4.3.19.20. Vários processos exclusivos de um usuário ou host dentro de um curto período de tempo. Isso pode indicar atividade de reconhecimento.

4.4. Capacidades de Investigação

4.4.1. Deve incluir recursos de workflow para resposta a incidentes de segurança.

4.4.2. Deve ser capaz de coordenar os processos de segurança atuais no nível de alertas de rede e alertas de outras soluções de segurança.

4.4.3. Deve fornecer recursos de busca e pesquisa nas estações de trabalho, de acordo com os seguintes exemplos:

4.4.3.1. Ampla pesquisa por comportamentos maliciosos conhecidos;

4.4.3.2. Caça proativa de atividades suspeitas;

4.4.3.3. Investigação completa nos endpoints comprometidos;

4.4.3.4. Procurar evidências de intrusões avançadas como ameaças sem arquivo (fileless).

4.4.4. Deve fornecer recursos de resposta em tempo real, para no mínimo:

4.4.4.1. Investigar todos as atividades em terminais suspeitos;

4.4.4.2. Reproduzir a linha do tempo completa de um ataque avançado;

4.4.4.3. Capturar detalhes da atividade que ocorreu durante intrusões;

4.4.4.4. Executar uma análise aprofundada no nível de: Acesso ao disco, análise de memória e detecção de rootkit.

4.4.5. Depois que a solução detectar um alerta, a mesma deve fornecer pelo menos as seguintes informações:

4.4.5.1. A inteligência em torno do alerta detectado;

4.4.5.2. Métodos de detecção da ameaça em questão;

4.4.5.3. Mostrar graficamente uma linha do tempo de eventos relacionados ao alerta detectado;

4.4.5.4. Dicas de pesquisa para orientar os analistas em todo o processo de resposta a incidentes. Essas dicas devem estar associadas à experiência que o fabricante tem em responder a incidentes críticos de segurança em empresas em todo o mundo;

4.4.5.5. Mostrar os eventos brutos (raw data) que geraram o alerta;

4.4.5.6. Histórico de eventos associados.

4.4.6. A visualização de um caso deve permitir pelo menos, as seguintes ações:

4.4.6.1. Controle do Nome, Status, Prioridade, Classificação e Descrição do caso;

4.4.6.2. Permitir que o caso seja assinado para algum usuário;

4.4.6.3. Permitir que qualquer log/evento relacionado possa ser adicionado e visualizado no mesmo;

4.4.6.4. Permitir a visualização de todos os alertas/incidentes envolvidos no caso;

4.4.6.5. Permitir que o caso seja exportado em formatos CSV e JSON;

4.4.6.6. Permitir a adição e visualização de comentários no caso.

4.4.7. Deve incluir dicas intuitivas de investigação, trazendo automaticamente no mínimo, os seguintes dados para consulta no alerta:

4.4.6.1. Existem outras regras alertadas para esse IP de origem?

4.4.6.2. Existem regras acionadas que foram baseadas em sensores de inteligência, relacionadas a algum desses índices de comprometimento?

4.4.6.3. Quais logs estão disponíveis para este dispositivo?

4.4.6.4. Quais logs estão disponíveis para este IP?

4.4.6.5. Em quais outros hosts esse malware foi encontrado?

4.4.6.6. Existem outros logs com esse hash?

4.4.6.7. Existem alertas relacionados usando o IP do agente?

4.4.6.8. Existem alertas relacionados usando o este dispositivo?

4.4.6.9. Existem alertas relacionados usando o hash envolvido no incidente?

4.4.8. No nível analista/operador, Deve fornecer:

4.4.8.1. Um painel de pesquisa, onde são registrados alertas e casos atribuídos aos analistas;

4.4.8.2. Detalhe de alertas como: nível de risco, nome do alerta, tipo de alerta, origem, data da primeira ocorrência, data da última ocorrência, número de

eventos, resumo, fontes e destino, status do alerta e opções de: exportação do alerta nos formatos CSV e JSON para excluir e\ou fechá-lo;

4.4.8.3. Cada alerta deve poder ser atribuído a um analista específico, para iniciar o processo de investigação, contenção, caça, etc.;

4.4.8.4. Deve haver um painel de casos, que permita a criação, gerenciamento e alocação de casos, a fim de rastrear as atividades e o tempo de resposta de cada analista;

4.4.8.5. Cada caso pode conter vários alertas, várias anotações, para validar o estado evolutivo na resposta a um incidente;

4.4.8.6. A ferramenta deve poder atribuir a cada caso níveis de: prioridade, gravidade e, como opção, outro tipo de classificação;

4.4.8.7. Cada caso deve ter: Descrição, Eventos, Alertas, Revisões e Notas, bem como o registro do qual o analista foi designado ou modificou o caso.

4.4.9. Deve ter a capacidade de realizar pesquisas para o processo de busca proativa e reativa nos eventos e metadados coletados de maneira automática.

4.4.10. Deve ter um módulo de pesquisa avançada ou indexação de pesquisa que contenha:

4.4.10.1. Um módulo de ajuda de sintaxe;

4.4.10.2. Um módulo de histórico de pesquisas;

4.4.10.3. Um módulo de pesquisa salva como favorita;

4.4.10.4. Capacidade de salvar a pesquisa.

4.4.11. As pesquisas devem ter uma sintaxe completa baseada em Query Language contemplando documentação completa e atualizada.

4.4.12. Deve incluir opções de pesquisa, com base em cada um dos campos de metadados, como: Domínio, porta de destino, método HTTP, metaclasses, porta de origem, useragent, IP de Origem, IP de destino, etc.

4.4.13. Deve possuir um módulo de UEBA ao qual poderá ser utilizado para melhor compreensão dos eventos, identificando possíveis entidades (equipamentos ou usuários) envolvidos anteriormente em outros eventos maliciosos ou suspeitos.

4.4.14. A visualização de um alerta/incidente deve permitir pelo menos, as seguintes ações:

4.4.14.1. Assinar o incidente para um analista;

4.4.14.2. Marcar como falso positivo;

4.4.14.3. Adicionar o alerta em um caso para um trabalho aprofundado envolvendo mais pessoas e artefatos de investigação;

4.4.14.4. Fechar ou suprimir o alerta;

4.4.14.5. Exportar o alerta para CSV ou JSON;

4.4.14.6. Fazer pesquisas de Índices de comprometimento diretamente em bases externas como VirusTotal e DomainTools;

4.4.14.7. Adicionar através de um clique, artefatos em listas para facilitar o trabalho de investigação e melhorar a assertividade das regras de detecção;

4.4.14.8. Visualizar a correlação de índices de comprometimento em outros incidentes abertos ou fechados;

4.4.14.9. Consultar análises realizadas automaticamente em bases de inteligência cibernética;

4.4.14.10. Analisar o histórico de modificações no incidente;

4.4.14.11. Adicionar comentários no incidente;

4.4.14.12. Quando realiza análise em sandbox para artefatos envolvidos em incidentes, permitir a visualização das modificações que o binário realizou.

4.4.15. Ao visualizar um tipo de evento, a plataforma deve permitir, a partir de cliques com o mouse (Sem necessidade de escrita de query), incrementar as buscas, para pelo menos as seguintes ações:

4.4.15.1. Realizar uma busca por qualquer campo daquela classe. Exemplo: Ip de origem/destino, hash md5, destinatário/remetente, ações aplicadas, etc;

4.4.15.2. No caso de uma busca já estar sendo realizada, deve ser possível adicionar qualquer campo listado na busca atual para seguimento das atividades de hunting;

4.4.15.3. Deve ser possível também realizar exclusões na busca a partir do valor de qualquer campo listado;

4.4.15.4. Dever ser possível realizar um agrupamento de qualquer valor listado, formando automaticamente um dashboard, estabelecendo as contagens e classificações de acordo com os valores dos campos;

4.4.15.5. Quando visualizado algum índice de comprometimento, deve ser possível realizar pesquisas em bases externas como VirusTotal e DomainTools;

4.4.15.6. Deve ser possível adicionar índices de comprometimento em listas para facilitar as buscas e criação de regras.

4.4.16. Deve permitir que as buscas mais realizadas sejam salvas para execução rápida sempre que necessário.

4.4.17. Toda busca realizada deve ter a possibilidade de ser transformada em uma regra para detecção de comportamentos desejados.

5. ITEM 5 - SOLUÇÃO DE SIMULAÇÃO AUTOMATIZADA DE ATAQUES CIBERNÉTICOS

5.1. Validação contínua de segurança

5.1.1. **Deve proporcionar simulação, avaliação e gestão estendida da postura de** segurança da organização, permitindo medir a efetividade através de testes e avaliações do nível de proteção do perímetro e de ambientes internos para que haja uma compreensão completa quanto a efetividade dos controles de segurança.

5.1.2. Deve permitir que os profissionais de segurança possam identificar, diagnosticar, gerenciar, controlar e validar sua postura de segurança cibernética de ponta a ponta.

5.1.3. Deve fornecer minimamente um caminho para validação de brechas e simulações de ataques (BAS), automatização de Red Teaming, gerenciamento da superfície de ataques (ASM) e cenários avançados para Purple Teaming.

5.1.4. Deve permitir recriar cenários reais de ataques à infraestrutura de segurança da organização sem gerar impactos ao ambiente.

5.1.5. Deve fornecer a possibilidade de executar os ataques baseados em táticas, técnicas e procedimentos que os atacantes e grupos de criminosos cibernéticos utilizam, sendo eles utilizados em pelo menos os seguintes cenários:

5.1.5.1. Reconhecimento – Validação de domínios e subdomínios a fim de identificar fraquezas e vulnerabilidades expostas na internet referente a organização. Nesta fase, a solução deverá utilizar de fontes de inteligência aberta (OSINT) para descoberta de credencias e outras informações as quais possam beneficiar um atacante.

5.1.5.2. Base Inicial – Ataques relacionados a fase de acesso inicial, execução, persistência e escalação de privilégio.

5.1.5.3. Execução & C2C – Técnicas de evasão de defesa, acesso de credenciais e descoberta do ambiente.

5.1.5.4. Propagação na rede – Movimentação lateral, coleção e comunicação externa C2C, permitindo que o atacante mova para seus objetivos finais.

5.1.5.5. Ações com objetivos – Comunicação externa para exfiltração de dados e geração de impacto.

5.1.6. Deve permitir simulações automáticas, orientadas a avaliar os ajustes e configurações de distintos controles de segurança.

5.1.7. Deve permitir a simulação de táticas, técnicas e procedimentos maliciosos de forma individual, assim como permitir a simulação de forma secundária respeitando o ciclo de vida de um ataque.

5.1.8. Deve identificar quais testes foram executados com êxito e quais falharam durante o processo de prevenção. Para os resultados, deve haver a possibilidade de criação de evidência da detecção e/ou bloqueio através de uma integração com um SIEM, e/ou no próprio dispositivo que detectou e/ou bloqueou a simulação.

5.1.9. As simulações serão executadas a partir de componentes da solução ou equipamento reservado exclusivamente para ela.

5.1.10. Deve ser implementada em modelo de nuvem SaaS, podendo ela permitir a implementação em regiões de nuvem disponíveis para o território brasileiro quando necessário.

5.1.11. Deve possuir suporte e licenciamento para realização de avaliações em diferentes vetores de ataque tais como, endpoint, rede, web e cloud.

5.1.12. Deve possuir um módulo capaz de fornecer através de sua rede de inteligência ameaças emergentes e relevantes para a plataforma, fornecendo informações detalhadas sobre tais ameaças e quais medidas de remediação recomendadas.

5.1.13. Deve permitir integração com soluções de gestão de vulnerabilidades, fornecendo apoio para priorização de riscos encontrados na organização, através do consumo dos relatórios fornecidos pela ferramenta de gestão de vulnerabilidades, deve ser possível apresentar de forma clara quais CVEs estão disponíveis na plataforma de ataques para simulação.

5.1.14. Deve permitir integração com diferentes serviços de SSO, tais como: ADFS, Azure AD, OKTA, JumpCloud entre outros.

5.1.15. Deve permitir a integração com diferentes plataformas de segurança via API.

5.1.16. Todos os componentes devem poder ser gerenciados por uma console central, permitindo a configuração, monitoração e atualização dos agentes de forma automática.

5.1.17. Toda a comunicação entre os componentes deve ser feita através de protocolos seguros como HTTPS com TLS 1.2 ou superior.

5.1.18. Deve suportar a comunicação dos componentes instalados por meio de um proxy web.

5.1.19. O processo de instalação dos agentes deve ser feito de forma manual, automatizada ou em lote.

5.1.20. Deve fornecer em cada um de seus vetores o nível de risco encontrado após cada simulação, devendo a plataforma comparar o resultado atual com o anterior para fornecer uma visão de avanço ou regresso dos testes, estes dados poderão ser utilizados para definição de baseline do ambiente.

5.1.21. Deve suportar regras SIGMA e fornecer para alguns cenários a opção de convertê-las em buscas (queries) as quais poderão ser utilizadas para buscas em plataformas de SIEM ou até mesmo criação de regras de correlação.

5.1.22. Deve ser capaz de poder trocar informações com outras tecnologias de segurança do ambiente para fornecer, melhor visibilidade na detecção, gestão de vulnerabilidades, automação de playbooks e validação de processos internos. Permitindo no mínimo as seguintes integrações:

- **5.1.22.1.** Azure Sentinel
- **5.1.22.2.** BlackBerry Cylance OPTICS
- **5.1.22.3.** BlackBerry Cylance PROTECT
- **5.1.22.4.** Carbon Black
- **5.1.22.5.** CrowdStrike Falcon
- **5.1.22.6.** Cynet
- **5.1.22.7.** IBM Qradar
- **5.1.22.8.** InsightVM
- **5.1.22.9.** LogRhythm
- **5.1.22.10.** McAfee ESM SIEM
- **5.1.22.11.** MicroFocus ArcSight
- **5.1.22.12.** Microsoft Defender ATP

5.1.22.13. Microsoft Defender TVM

5.1.22.14. Nexpose

5.1.22.15. Palo Alto Cortex XDR

5.1.22.16. Palo Alto Cortex XSOAR

5.1.22.17. Qualys VM

5.1.22.18. RSA Archer

5.1.22.19. RSA Netwitness

5.1.22.20. SentinelOne

5.1.22.21. Service Now

5.1.22.22. Splunk

5.1.22.23. Sumo logic SIEM

5.1.22.24. Tenable IO

5.1.22.25. Tenable SC

5.1.22.26. Trellix EDR

5.1.23. Todos os produtos de segurança que não possuírem integração direta, devem poder ser integrados por meio soluções de correlacionamento de eventos (SIEM), permitindo a integração com produtos não homologados.

5.1.24. Deve fornecer suporte a regras SIGMA e suportar através de uma interface amigável capacidade de conversão das regras para padrões que possam ser utilizados em diferentes plataformas através da geração de scripts ou queries, suportando conversão para minimamente as seguintes tecnologias:

5.1.24.1. Arcsight

5.1.24.2. Azure Sentinel

5.1.24.3. ElastAlert

5.1.24.4. Elastic Search

5.1.24.5. Humio

5.1.24.6. IBM Qradar

5.1.24.7. Kibana

5.1.24.8. Limacharlie

5.1.24.9. Logpoint

5.1.24.10. Netwitness

5.1.24.11. Splunk

5.1.24.12. Sumologic

5.1.25. Deve permitir a visualização do status de conexão e versão de software dos agentes, permitindo através da console realizar operações como reinicialização, deleção ou mesmo desinstalação do componente.

5.1.26. Deve permitir avaliar as capacidades de defesa da organização contra táticas, técnicas e procedimentos utilizados por grupos criminosos conhecidos.

5.1.27. Deve possuir uma biblioteca de ataques associada a criminosos cibernéticos e deve atualizá-la de forma automática quando novas ameaças emergentes surgirem.

5.1.28. Deve permitir a criação de perfis de adversários.

5.1.29. O portfólio de ataques deve ser baseado em frameworks e padrões de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS, Microsoft DRAPE e NIST.

5.1.30. As simulações de ataque devem corresponder, sempre que possível, a uma técnica descrita pelo MITRE e apresentar detalhes sobre os respectivos TTPs.

5.1.31. As simulações de ataque também devem possuir mapeamentos com NIST 800-53 facilitando assim a adequação de padrões e frameworks.

5.1.32. Deve incluir diversas simulações de ataque predefinidas, que incluem minimamente os seguintes tipos de ataques:

5.1.32.1. Para validação do vetor de endpoint a plataforma deve oferecer simulações de ataque para:

5.1.32.2. Ransomware: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de ransomwares, devendo estes buscar arquivos sensíveis no host e utilizar chaves geradas de forma segura e controlada para criptografia de arquivos.

5.1.32.3. Worm: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de worms, devendo estes realizar a descoberta de hosts vulneráveis e simular a ploriferação para eles através de técnicas utilizando protocolos tais como SMB.

5.1.32.4. Trojan: Validação da efetividade de recursos para detecção de anomalias (comportamento) durante a execução segura de trojans, estes deverão coletar informações gerais do host como nome de usuário, e-mail e

outras. Podendo também estabelecer comunicação utilizando diferentes métodos de reverse shell.

5.1.32.5. Antivírus: Validação da efetividade de inspeção e proteção de ameaças contra arquivos maliciosos, os malwares escritos em disco devem ser atualizados diariamente através de diversos feeds de segurança.

5.1.32.6. MITRE ATT&CK: Validação da efetividade dos recursos de anti-malware através da execução de comandos customizados que devem simular o comportamento de adversários mapeados no framework ATT&CK.

5.1.33. Para validação do vetor de web gateway a plataforma deve oferecer simulações de ataque para:

5.1.33.1. Phishing: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção de ataques de phishing, acessando IPs e URLs reais associados a ataques de phishing identificados recentemente.

5.1.33.2. Ransomware: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra ransomware, acessando IPs e URLs reais associados ao Ransomware, como servidores Botnet, C&C, sites de distribuição e pagamento.

5.1.33.3. C&C: Validação da efetividade dos recursos de filtragem dinâmica de URL e proteção contra malwares, acessando IPs e URLs reais associados a atividades de C&C como Botnet.

5.1.33.4. Política: Validação da efetividade da proteção de filtro de categorias do gateway da web. A validação é feita através do acesso a diferentes sites divididos por categorias, como pornografia, jogos de azar etc.

5.1.33.5. Arquivos: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade de malwares simulados que imitam o comportamento de worms, trojans e ransomware.

5.1.33.6. Exploits: Validação da efetividade dos recursos de inspeção de tráfego de entrada e eficácia da proteção contra arquivos maliciosos. A validação é realizada através da tentativa de baixar por HTTPS uma variedade

de malwares que simulam o comportamento de worms, trojans e ransomware.

5.1.34. Para validação do vetor de email gateway a plataforma deve oferecer simulações de ataque para:

5.1.34.1. Ransomware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por ransomwares, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

5.1.34.2. Worm: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por worms, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

5.1.34.3. Malware: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos utilizadas por diferentes códigos maliciosos (malwares), estas validações devem poder simular cenários interativos envolvendo técnicas de exploração de controles como UAC, roubo de credenciais e C&C. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente

5.1.34.4. Payload: Validação da efetividade dos recursos de proteção de e-mail através de técnicas de execução de códigos em payloads, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

5.1.34.5. Exploits: Validação da efetividade dos recursos de proteção de e-mail através da execução de diversos arquivos que exploram diferentes vulnerabilidades em programas, toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

5.1.34.6. Dummy: Validação da efetividade dos recursos de proteção de e-mail através da execução de diferentes técnicas de execução de códigos, isto deve incluir uso de recursos conhecidos como payloads do metasploit como exemplo MessageBox. Toda execução deve ser realizada de forma segura sem gerar impactos ao ambiente.

5.1.34.7. True File Type Detection: Validação da efetividade dos recursos de proteção de e-mail através do envio de arquivos com diferentes extensões não

pertencentes ao seu formato de arquivo original, este teste deve apoiar na identificação de possíveis brechas que podem ser utilizadas para comprometer o ambiente através da falsificação de formatos originais de arquivos.

5.1.35. Para validação do vetor de web application firewall (WAF) a plataforma deve oferecer simulações de ataque para minimamente:

5.1.35.1. SQL injection

5.1.35.2. Cross-site scripting (XSS)

5.1.35.3. File inclusion for remote code execution

5.1.35.4. Command injection

5.1.36. Para validação de vazamento de dados (DLP) a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

5.1.36.1. **HTTP & HTTPS:** Exfiltração de dados por HTTP/S, injetando dados confidenciais em cabeçalhos de solicitação HTTP/S enviados para um servidor remoto.

5.1.36.2. Browser HTTP & HTTPS: Exfiltração de dados através de navegadores como IE, Edge e/ou Chrome.

5.1.36.3. DNS: Exfiltração de dados pela porta 53.

5.1.36.4. Tunelamento DNS: Exfiltração de dados sobre o protocolo DNS (túnel através de servidores DNS públicos). Injetando dados confidenciais em uma solicitação de DNS enviada a servidores DNS públicos.

5.1.36.5. Tunelamento ICMP: Exfiltração de dados sobre cabeçalhos ICMP. Injetando dados confidenciais em um pacote de eco (ECHO) enviado para um servidor remoto.

5.1.36.6. Telnet: Exfiltração de dados pela porta de rede Telnet 23.

5.1.36.7. SFTP: Exfiltração de dados sobre o protocolo SFTP.

5.1.36.8. Outras Portas: Exfiltração através do upload de dados confidenciais para servidores de hospedagem de arquivos externos por meio de portas de rede abertas.

5.1.36.9. Email: Usando email corporativo no Outlook para transmitir dados confidenciais.

5.1.36.10. Serviços de nuvem: Exfiltração de dados confidenciais para ou por meio de serviços e aplicativos em nuvem.

5.1.36.11. Dispositivos Removíveis: Exfiltração de dados confidenciais através da cópia para dispositivos de mídia removíveis, como USB.

5.1.37. Para validação de movimentação lateral a plataforma deve oferecer simulações de ataque que permitam validação dos seguintes métodos:

5.1.37.1. Pass-the-Password

5.1.37.2. Pass-the-Ticket

5.1.37.3. Pass-the-Hash

5.1.37.4. Brute Force

5.1.37.5. LLMNR/NBT-NS Poisoning and Relay

5.1.37.6. Kerberoast

5.1.37.7. Password Spraying

5.1.37.8. Steal LAPS passwords

5.1.38. Deve fornecer a possibilidade de criar modelos customizados nos vetores de ataque sem causar impactos ao ambiente.

5.1.39. Para o cenário de movimentação lateral, o agente deve poder atuar exatamente como um atacante no ambiente, não devendo este depender da implementação de outros agentes para validação dos diferentes métodos. Deve possuir capacidade de realizar um “pivoting” na rede e fornecer um mapa de toda trilha percorrida e alvos alcançados, podendo os alvos serem considerados ou não joias da coroa (Crown Jewels).

5.1.40. Deve fornecer um caminho para validação completa da cadeia de ataque (Full Kill-chain), permitindo assim que seja avaliadas fases tais como pré-exploração, exploração e pós-exploração.

5.1.41. Deve permitir a criação de campanhas de phishing customizadas para avaliação da conscientização dos colaboradores em cenários reais, as campanhas devem minimamente permitir que sejam criados conteúdos através da plataforma em português.

5.1.42. Cada um dos testes ou ações hospedadas na base de conhecimento, deve ter uma descrição e o código da técnica ou das táticas de acordo com a nomenclatura do MITRE.

5.1.43. Deve ter a capacidade de repetir periodicamente os testes que o usuário deseja e comparar os resultados de cada execução com um resultado esperado, permitindo definir se o ataque foi detectado, bloqueado e que tipo de registro foi detectado no SIEM ou nas tecnologias de segurança testadas.

5.1.44. Os componentes de ataque devem poder ser instalados, minimamente, nos seguintes ambientes:

5.1.44.1. Windows 11 build 22000+, 10 build 1067, 8.1, 7 SP1

5.1.44.2. Server 2012 ou superior

5.1.44.3. Linux Alpine 3.12, Ubuntu 16.04, Debian 10, CentOS 7, RHEL 7, Fedora 33, openSUSE 15 e SUSE Enterprise 12 SP2 ou versões superiores

5.1.44.4. MacOS 10.15x ou superior

5.1.45. Deve realizar as simulações de ataque através de um agente único ao qual deverá ser capaz de executar ataques em diferentes vetores de forma individual ou simultânea.

5.1.46. Deve permitir através de um framework aberto a customização de diferentes cenários e cadeias de execução que sejam compatíveis minimamente com as seguintes plataformas:

5.1.46.1. Powershell

5.1.46.2. Python

5.1.46.3. Bash

5.1.46.4. Sh

5.1.46.5. CMD

5.1.47. Deve possuir uma console em nuvem a qual deverá ser utilizada para orquestração e envio dos ataques.

5.1.48. O painel principal (dashboard) deve apresentar de forma clara os vetores licenciados assim também como informações sobre controles de segurança, ameaças emergentes, integrações e outros detalhes importantes que possam ser utilizados para melhor compreensão dos testes realizados.

5.1.49. Deve permitir a criação de painéis dinâmicos aos quais permitam a customização e manipulação de dados a serem apresentados no novo painel (dashboard).

5.1.50. Deve possuir um dashboard que exiba todas as informações de vulnerabilidades baseadas em ataques, incluindo proteção geral de controles de segurança, principais vulnerabilidades encontradas em ativos de rede, principais ativos vulneráveis, principais CVEs e muito mais.

5.1.51. Deve possuir em seu painel principal a opção de rastreabilidade em tempo de execução dos testes.

5.1.52. Deve fornecer uma visão global dos itens que foram identificados.

5.1.53. Deve fornecer uma visão detalhada após integração com plataformas de gestão.

5.1.54. Deve possuir uma interface amigável em seu agente para facilitar o gerenciamento de ataques em andamento, visualização de logs e configurações pertinentes aos recursos envolvidos no ataque, proxy, e-mail etc.

5.1.55. Após conclusão dos ataques envolvendo de forma individual ou conjunta os vetores de ataque deverá ser fornecido um score de risco, este score deve prover uma clara visão sobre a maturidade atual e histórica do ambiente.

5.1.56. Deve permitir a geração de relatórios técnicos ou gerenciais aos quais devem conter minimamente:

5.1.56.1. Informações sobre o score de risco atual;

5.1.56.2. Descrição e recomendação para correção dos problemas encontrados;

5.1.57. Deve permitir em sua guia de relatórios a extração de dados completos contendo informações gerais de todos os ataques realizados em um determinado vetor, assim também como oferecer opções para download de relatórios em formato PDF, CSV ou TXT.

5.1.58. Deve permitir a geração de relatórios e download dos mesmos através de sua interface assim como permitir o envio dos mesmos através de e-mail.

5.1.59. Deve permitir a geração de relatórios e visão detalhada por ambientes.

5.1.60. A solução deverá prover uma visão clara do desempenho individual de cada vetor de ataque assim como também possuir um gráfico de comparação para benchmark.

5.1.61. Deve fornecer um caminho simples para minimamente:

5.1.61.1. Realizar a abertura de chamados;

5.1.61.2. Gerenciar usuários da plataforma;

5.1.61.3. Acessar documentações do produto;

5.1.61.4. Gerenciar logs e atividades em execução.

5.1.62. A console deve fornecer uma guia para download e gestão dos agentes implementados.

6. ITEM 6 – SOLUÇÃO DE DESCOBERTA E CORREÇÃO DE VULNERABILIDADE DE SEGURANÇA

6.1. Características gerais

6.1.1. Deve permitir fácil integração com tecnologias em nuvem como o Microsoft 365.

6.1.2. Deve possuir ao menos 2 diferentes métodos de implementação, sendo um deles menos evasivo, ou seja, não requerendo alterações de registros DNS como MX, possibilitando assim, a integração via API da Microsoft.

6.1.3. Deve operar em tempo real, analisando e retendo e-mails até que seja determinado se ele deve ser excluído, colocado em quarentena e\ou enviado para o servidor de correio eletrônico.

6.1.4. Deve implementar minimamente as seguintes funcionalidades de MTA:

6.1.4.1. Capacidade de filtrar as conexões recebidas pelo IP de origem, para limitar quem pode enviar e-mail para a solução;

6.1.4.2. Suportar o uso do Transport Layer Security (TLS) suportando pelo menos TLS 1.2. Além disso, você deve poder forçar o uso do TLS nos e-mails de entrada ou saída, bloqueando as sessões que não são criptografadas;

6.1.4.3. Deve verificar a identidade do MTA do próximo salto usando TLS e certificados digitais.

6.1.5. Deve oferecer suporte ao gerenciamento de congestionamentos para evitar o colapso das sessões de entrada. Suportando minimamente os seguintes modos:

6.1.5.1. Rejeitar conexões, para não receber mais e-mails;

6.1.5.2. Não analisar o tráfego e enviar diretamente;

6.1.5.3. Descartar o email.

6.1.6. Depois que o email for analisado e liberado, ele poderá ser enviado para o próximo salto utilizando, pelo menos uma das seguintes opções:

6.1.6.1. Reenviar para um único IP;

6.1.6.2. Envio para vários IPs, usando um sistema de prioridade para poder distribuir tráfego com diferentes taxas de carga;

6.1.6.3. Enviar usando os resultados de uma consulta DNS para o registro MX do domínio de cada destinatário.

6.1.7. Deve permitir visualização de estatísticas relacionadas ao número de correspondências vistas com os itens que constam nas listas negra ou branca.

6.1.8. Deve ser capaz de criar um e-mail de notificação para o administrador e, opcionalmente, para os destinatários das mensagens bloqueadas. O e-mail deve poder ser configurado para conter o texto definido pelo administrador.

6.1.9. Deve permitir a criação alertas de notificações a serem enviados por e-mail.

6.1.10. Deve oferecer suporte ao rastreio de mensagens através de no mínimo as opções abaixo:

6.1.10.1. Atributos da mensagem;

6.1.10.2. ID da fila;

6.1.10.3. ID original da mensagem.

6.1.10.4. Remetente;

6.1.10.5. Destinatário;

6.1.10.6. Assunto;

6.1.10.7. Status da mensagem;

6.1.10.8. Resultado de análise de ameaças avançadas;

6.1.10.9. Resultado de análise de spam;

6.1.10.10. Resultado de análise de malware;

6.1.10.11. Ações de políticas de conteúdo;

6.1.10.12. Tamanho da mensagem;

6.1.10.13. IP do remetente;

6.1.10.14. Mensagens que contenham anexo;

6.1.10.15. Domínios cadastrados na plataforma.

6.1.11. Durante a realização de filtros para rastreamento de mensagens, Deve permitir a utilização de expressões condicionais, permitindo negar atributos da mensagem na busca como:

6.1.11.1. Remetente;

6.1.11.2. Destinatário;

6.1.11.3. Assunto;

6.1.11.4. Status da mensagem;

6.1.11.5. Resultado de análise de ameaças avançadas;

6.1.11.6. Resultado de análise de spam;

6.1.11.7. Resultado de análise de malware;

6.1.11.8. Ações de políticas de conteúdo;

6.1.11.9. IP do remetente.

6.1.12. Deve permitir relatórios estatísticos baseados em:

6.1.12.1. Estatísticas de recebimento e entrega de mensagens;

6.1.12.2. Estatísticas de mensagens retidas pelos filtros da solução;

6.1.12.3. Número de mensagens retidas por conterem ameaças avançadas;

6.1.12.4. Número de mensagens retidas por tentativa de representação;

6.1.12.5. Número de mensagens retidas por conterem malwares;

6.1.12.6. Número de mensagens retidas por serem classificadas como SPAM;

6.1.12.7. Estatísticas de motivo de rejeição de mensagens;

6.1.12.8. Estatísticas contendo médias do tamanho das mensagens;

6.1.12.9. Estatísticas dos principais tipos de anexos recebidos/enviados;

6.1.12.10. Estatísticas de acionamento de regras de listas negras e brancas;

6.1.12.11. Estatísticas de acionamento de regras de conteúdo;

6.1.12.12. Estatísticas contendo os remetentes que mais enviaram mensagens para organização;

6.1.12.13. Estatísticas contendo o IP dos remetentes que mais enviaram mensagens para organização;

6.1.12.14. Estatísticas contendo os usuários internos que mais recebem/enviam e-mails.

6.1.13. Deve exibir um mapa de ameaças, organizando as detecções de ameaças avançadas recebidas por seus devidos países de origem.

6.1.14. Deve permitir integração com qualquer provedor de email.

6.1.15. Deve possuir auditoria de ações executadas no console administrativo para consulta.

6.1.16. Não deve limitar o número de domínios a serem protegidos.

6.1.17. Deve permitir a criação de grupos de domínio a serem cadastrados para organização dos mesmos.

6.1.18. Para mensagens de saída da organização, deve implementar uma chave de autenticação a ser verificada em todas as mensagens. Qualquer mensagem que não contenha a chave indicada, deverá ser rejeitada.

6.1.19. Deve permitir a criação de regras para detecção de, no mínimo:

6.1.19.1. Ataques de spoofing;

6.1.19.2. Validação de SPF;

6.1.19.3. Bloqueio de newsletter e marketing mail;

6.1.19.4. Bloqueio de mensagens com assunto em branco;

6.1.19.5. Bloqueio por palavra chave.

6.1.20. As regras customizadas devem permitir a utilização de, pelo menos, os seguintes atributos para condições de acionamento:

6.1.20.1. Envelope From;

6.1.20.2. Envelope From Domain;

6.1.20.3. Assunto;

6.1.20.4. Palavras chave;

6.1.20.5. HELO/EHLO Name;

6.1.20.6. Body;

6.1.20.7. Body Size;

6.1.20.8. Header exists;

6.1.20.9. Header value;

6.1.20.10. Recipient;

6.1.20.11. DMARC verdict;

6.1.20.12. DKIM result;

6.1.20.13. SPF result;

6.1.20.14. Reverse Domain;

6.1.20.15. Message size;

6.1.20.16. Sender IP;

6.1.20.17. Country;

6.1.20.18. Anexos.

6.1.21. As condições de acionamento de regras customizadas, devem permitir, pelo menos, os seguintes operadores lógicos:

6.1.21.1. Igual;

6.1.21.2. Contém;

6.1.21.3. Validação de expressão regular;

6.1.21.4. Campo vazio?

6.1.22. As regras customizadas devem permitir a utilização de, pelo menos, as seguintes ações:

6.1.22.1. Inserir Header;

6.1.22.2. Modificar o assunto;

6.1.22.3. Bypassar verificações de segurança;

6.1.22.4. Roteamento da mensagem;

6.1.22.5. Entrega normal;

6.1.22.6. Rejeição da conexão;

6.1.22.7. Movimentar mensagem para quarentena.

6.1.23. As regras customizadas devem permitir que os anexos sejam manipulados utilizando, pelo menos, os seguintes atributos:

6.1.23.1. Extensão do arquivo;

6.1.23.2. Nome do arquivo;

6.1.23.3. Hash do arquivo;

6.1.23.4. Tipo real do arquivo;

6.1.23.5. Tamanho do arquivo.

6.1.24. As regras customizadas devem permitir criação de exceções utilizando, pelo menos, os seguintes atributos:

6.1.24.1. Envelope From;

6.1.24.2. Envelope From Domain;

6.1.24.3. Assunto;

6.1.24.4. Palavras chave;

6.1.24.5. HELO/EHLO Name;

6.1.24.6. Body;

6.1.24.7. Body Size;

6.1.24.8. Header exists;

6.1.24.9. Header value;

6.1.24.10. Recipient;

6.1.24.11. DMARC verdict;

6.1.24.12. DKIM result;

6.1.24.13. SPF result;

6.1.24.14. Reverse Domain;

6.1.24.15. Message size;

6.1.24.16. Sender IP;

6.1.24.17. Country;

6.1.24.18. Anexos.

6.1.25. Deve permitir a configuração de, pelo menos, os seguintes limites de parâmetros de mensagens:

6.1.25.1. Número de mensagens por domínio de destinatário;

6.1.25.2. Número de mensagens por IP do remetente;

6.1.25.3. Número de Mensagens por Endereço do Remetente;

6.1.25.4. Volume de mensagens por domínio de destinatário;

6.1.25.5. Volume de mensagens por IP do remetente;

6.1.25.6. Volume de mensagens por endereço do remetente.

6.1.26. Deve funcionar, obrigatoriamente, com autenticação de dois fatores nativa, sendo eles: OTP, SMS ou voz.

6.2. Antivirus & AntiSpam

6.2.1. Deve fornecer no mínimo capacidade para lidar com ameaças conhecidas e possuir recursos para detectar e bloquear ameaças modernas e desconhecidas.

6.2.2. Deve suportar a análise de URLs "reduzidos", como Tiny URL, bit.ly ou outros.

6.2.3. Os URLs detectados como maliciosos devem incluir uma captura de tela do site malicioso.

6.2.4. Deve poder adicionar um cabeçalho de email indicando o resultado da análise realizada, para que o MTA a seguir possa definir regras de processamento condicional para esse cabeçalho, identificando minimamente os seguintes resultados:

6.2.4.1. Email limpo;

6.2.4.2. Anexo malicioso;

6.2.4.3. URL maliciosa;

6.2.4.4. Estrutura de email suspeita;

6.2.4.5. Email não analisado;

6.2.4.6. Erro na análise.

6.2.5. O texto do cabeçalho deve ser modificável pelo administrador.

6.2.6. Deve analisar arquivos compactados.

6.2.7. Deve analisar os arquivos que estão ofuscados.

6.2.8. Deve poder analisar os URIs protegidos com base64.

6.2.9. Deve detectar, analisar e bloquear ataques de rootkit.

6.2.10. Deve detectar, analisar e bloquear ataques de injeção de DLL que tentam modificar aplicativos instalados no sistema operacional, como as ferramentas do MS Office.

6.2.11. Deve permitir remediação automática para Office 365 em e-mails que se tornaram maliciosos depois da entrega.

6.2.12. O processo de remediação para o Microsoft 365 deve permitir a execução de pelo menos, as seguintes ações na caixa do usuário:

6.2.12.1. Remediação automática, para e-mails que se tornaram maliciosos depois da entrega;

6.2.12.2. Movimentação de mensagens da caixa de entrada do usuário para qualquer outra pasta definida;

6.2.12.3. Remover a mensagem da caixa de entrada do usuário e armazenar a mesma na quarentena da solução;

6.2.12.4. Deletar a mensagem permanentemente, mesmo que a mensagem já tenha sido recebida pelo usuário.

6.2.13. Deve fornecer detecção e proteção em tempo real contra ataques de coleta de credenciais, representação e spear-phishing.

6.2.14. Deve possuir ferramentas avançadas contra táticas de representação que se tornam cada vez mais comuns em ataques virtuais.

6.2.15. Contra ataques de representação deve considerar em suas análises no mínimo:

6.2.15.1. Frequência que um usuário recebe e-mails de um remetente específico (Consultando também bases globais de inteligência pra correlacionamento);

6.2.15.2. Indicadores de domínios e endereços IP que normalmente se comunicam com cada cliente e o serviço de email como um todo;

6.2.15.3. Idade do domínio em questão;

6.2.15.4. Domínios conectados pela primeira vez com a plataforma.

6.2.16. Deve possuir ferramentas para detectar a idade de domínios e tratar automaticamente domínios registrados recentemente como suspeitos.

6.2.17. Deve suportar a definição de um tamanho máximo de e-mail, para evitar riscos de ataques de saturação.

6.2.18. Deve permitir a criação de listas brancas para poder enviar diretamente os e-mails recebidos sem serem analisados. Essas listas devem poder ser definidas de acordo com:

6.2.18.1. Endereço de email do remetente;

6.2.18.2. Domínio remetente;

6.2.18.3. IP de origem;

6.2.18.4. País de origem da qual a mensagem é recebida.

6.2.19. Deve permitir a criação de listas negras para bloquear diretamente os e-mails recebidos sem serem verificados. Essas listas devem poder ser definidas de acordo com:

6.2.19.1. Endereço de email do remetente;

6.2.19.2. Domínio remetente;

6.2.19.3. IP de origem;

6.2.19.4. País de origem da qual a mensagem é recebida.

6.2.20. Deve permitir a instalação de soluções de antivírus, para consulta de inteligência de detecção de outros fabricantes. Deve permitir a utilização das bases de pelo menos, os seguintes fabricantes:

6.2.20.1. Ad-Aware;

6.2.20.2. AegisLab;

6.2.20.3. Agnitum;

6.2.20.4. Avast;

6.2.20.5. AVG;

6.2.20.6. Bitdefender;

6.2.20.7. ClamAV;

6.2.20.8. Comodo;

6.2.20.9. eSafe;

6.2.20.10. ESET-NOD32;

6.2.20.11. F-secure;

6.2.20.12. Fortinet;

6.2.20.13. Karpersky;

6.2.20.14. MalwareBytes;

6.2.20.15. McAfee;

6.2.20.16. Microsoft;

6.2.20.17. Panda;

6.2.20.18. Sophos;

6.2.20.19. Symantec;

6.2.20.20. TrendMicro.

6.3. Proteção de ameaças avançadas (ATP)

6.3.1. Deve ser capaz de analisar os URLs incluídos no email para acessar os objetos de risco para os quais eles apontam, permitindo que eles sejam analisados em Sandbox.

6.3.2. Deve poder analisar URLs de FTP que não possuem o protocolo especificado (http:// ou https://).

6.3.3. Deve ser capaz de extrair senhas do corpo do email para tentar desbloquear arquivos criptografados ou protegidos por senha.

6.3.4. Deve incluir uma lista de domínios a serem bloqueados associados aos ataques de Typosquatting, nos quais o usuário é redirecionado para um site mal-intencionado por ter cometido um erro de digitação ao escrever o domínio.

6.3.5. Deve ser capaz de detectar alertas retroativos, ou seja, alertas sobre URLs ou anexos que não foram detectados como maliciosos antes, mas que após uma atualização são listados como maliciosos.

6.3.6. Os alertas retroativos devem ser claramente identificados como tal entre os outros alertas.

6.3.7. As mensagens que se enquadram nas detecções retroativas devem ser removidas de forma automática da caixa dos usuários após assertividade da análise.

6.3.8. Deve detectar código malicioso em documentos e arquivos como:

6.3.8.1. Microsoft Office em todas versões com suporte atualizado;

6.3.8.2. Documentos PDF;

6.3.8.3. Arquivos compactados.

6.3.9. Deve ser capaz de detectar e analisar URLs incorporados em arquivos PDF.

6.3.10. Deve ser capaz de detectar URLs ocultas em que a URL exibida não corresponde a URL que está realmente incorporada na mensagem. A diferença deve ser detectada no texto ou no protocolo.

6.3.11. Deve suportar a criação de regras no formato YARA, versão 3.4 ou superior.

6.3.12. Deve ser capaz de detectar, interromper e conter ataques de dia zero, ameaças persistentes (APT) e Spear Phishing.

6.3.13. No caso de e-mails, se um administrador confirmar que o e-mail analisado não é potencialmente malicioso, ele poderá ser liberado.

6.3.14. Se um ato malicioso for detectado em um e-mail, deve ser possível enviar um aviso ao administrador e ao destinatário. Essa detecção deve poder ser feita em ataques desconhecidos de dia zero e / ou ameaças persistentes.

6.3.15. Deve apresentar o risco associado a cada uma das ameaças, indicando se é baixo, médio ou alto risco.

6.3.16. Deve registrar toda a atividade que um objeto malicioso tenta executar, registrando as modificações do sistema operacional/aplicativo que ele consegue modificar, como:

6.3.8.1. Registro do Windows;

6.3.8.2. Registro da aplicação;

6.3.8.3. Registro de processos;

6.3.8.4. Registro de arquivos;

6.3.8.5. Registro de comportamento;

6.3.8.6. Registro de comunicações.

6.3.17. Deve analisar os anexos de email, compactados, ofuscados e /ou criptografados.

6.3.18. Deve fornecer conhecimento profundo sobre ataques e agressores de investigações da linha de frente e observações de adversários.

6.3.19. A busca de ameaças avançadas deve percorrer minimamente as extensões abaixo:

6.3.19.1. EXE;

6.3.19.2. DLL;

6.3.19.3. PDF;

6.3.19.4. SWF;

6.3.19.5. DOC/DOCX;

6.3.19.6. XLS/XLSX;

6.3.19.7. PPT/PPTX;

6.3.19.8. JPG;

6.3.19.9. PNG;

6.3.19.10. MP3;

6.3.19.11. MP4;

6.3.19.12. ZIP/RAR/TNEF.

6.3.20. A proteção para e-mail deve permitir a possibilidade de atuação em caso de ameaças de ransonware iniciados por e-mail antes que a comunicação com o centro de comando seja efetivada.

6.3.21. Deve possuir dados analíticos e machine learning para detecção de ameaças que tentam evadir as tradicionais detecções por assinatura.

6.3.22. Todos os alertas gerados em detecções de ameaças avançadas, devem ter a possibilidade de serem enviados para soluções de SIEM.

6.3.23. Deve permitir que URLs suspeitas sejam reescritas para links seguros, evitando que usuários tenham acesso direto a links suspeitos, gerando um alerta (Que pode ser customizado) avisando que a URL é suspeita ou até mesmo impedindo o acesso se a mesma for considerada maliciosa.

6.4. Quarentena

6.4.1. Deve fornecer um ambiente de quarentena para e-mails identificados como maliciosos. O administrador deve poder gerenciar esses e-mails, liberando ou excluindo-os conforme considerar.

6.4.2. A quarentena deve permitir armazenamento de pelo menos 14 dias para todas as mensagens armazenadas.

6.4.3. Os e-mails em quarentena devem poder ser baixados em sua forma original.

6.4.4. Deve ser possível realizar uma pré visualização da mensagem em quarentena, em formato texto e HTML.

6.4.5. O sistema de quarentena deve permitir pesquisas e listagens filtradas com base minimamente nos seguintes atributos:

6.4.5.1. Data;

6.4.5.2. Razão do bloqueio;

6.4.5.3. Domínios cadastrados na plataforma;

6.4.5.4. Remetente;

6.4.5.5. Destinatário;

6.4.5.6. Assunto;

6.4.5.7. Domínio do remetente.

6.4.6. Deve implementar a funcionalidade de quarentena do usuário, permitindo que os próprios usuários finais façam liberação de suas mensagens.

6.4.7. Deve permitir ou não que usuários façam gerenciamento de listas negras e brancas particulares em sua visualização da quarentena.

6.4.8. Deve permitir quais categorias de ameaças devem ser apresentadas na quarentena do usuário, ou seja, mesmo que algumas mensagens sejam movidas para a quarentena, deve ser possível controlar se a mesma deve aparecer ou não na quarentena do usuário. O controle de quais mensagens devem ir ou não para a visualização do usuário final deve ser controlado para, pelo menos, as seguintes categorias de detecção:

6.4.8.1. Ameaças avançadas;

6.4.8.2. Malware/vírus;

6.4.8.3. Detecção de regras customizadas;

6.4.8.4. Mensagens classificadas como SPAM.

6.4.9. Deve realizar o envio de uma notificação para usuários finais, contendo as mensagens movidas para quarentena, permitindo que as mesmas sejam visualizadas pelo link da quarentena, ou liberadas diretamente pela notificação recebida.

6.4.10. Deve ser possível escolher usuários que não devem receber a notificação de quarentena.

6.4.11. O modelo da notificação da quarentena deve ser criado pela console de gerenciamento, permitindo a customização das características via HTML. Deve ser possível realizar a visualização de uma prévia da notificação antes que a mesma seja habilitada.

7. ITEM 7 – SERVIÇOS TÉCNICOS ESPECIALIZADOS EM RESPOSTA A INCIDENTES DE SEGURANÇA

7.1. Os serviços especializados listados deverão conter as seguintes frentes de atuação:

I. Serviços de operação e sustentação de segurança;

II. Serviço de Gestão de Incidentes de Segurança;

III. Serviço de descoberta e gestão de vulnerabilidades de segurança;

IV. Serviço de validação de segurança.

7.2. Requisitos Gerais

7.2.1. Os serviços deverão ser prestados em horário comercial corrente do CONTRATANTE, de segunda-feira a sexta-feira, presencialmente, nas dependências do CONTRATANTE (sede da CONTRATANTE);

7.2.2. As horas do serviço técnico especializado serão utilizadas sob demanda, a critério da ANTT para realização da manutenção preventiva e corretiva e das atividades relacionadas à solução;

7.2.3. O serviço técnico especializado inclui no mínimo as seguintes atividades:

7.2.4. A CONTRATADA será responsável pela implementação, suporte, administração diária e sustentação de todos os serviços envolvidos neste certame, contemplando qualquer envolvimento em qualquer demanda que tenha relação com as soluções envolvidas;

7.2.5. Entende-se por implementação, todos os passos necessários para completa instalação dos serviços, seguindo as melhores práticas para cada tema envolvido, de modo que os mesmos fiquem completamente operacionais para utilização no ambiente;

7.2.6. Entende-se por suporte, o acompanhamento contínuo de saúde dos serviços, assim como aplicação de correções para qualquer comportamento anômalo

identificado, assim como a instalação de novas versões e patches de correção;

7.2.7. Entende-se por administração diária, que a CONTRATADA será responsável pela administração de todos os passos técnicos e processos que envolvem os serviços contratados, de forma que as mesmas sejam 100% integradas ao ambiente da CONTRATANTE, porém utilizando a mão de obra da CONTRATADA;

7.2.8. Entende-se por sustentação, que a CONTRATADA será responsável pela tratativa de todas as saídas técnicas que envolvem os serviços contratados, sendo responsáveis pela implementação de cada processo, integração ou interação técnica de qualquer natureza envolvendo os serviços contratados;

7.2.9. Fica fora do escopo da CONTRATADA, apenas atividades que envolvam interação com as ferramentas de rede e infraestrutura da CONTRATANTE, porém a CONTRATADA ainda fica responsável pela indicação de todas as necessidades de atuação para que os times responsáveis possam desenvolver suas tarefas e atender a novas demandas técnicas elencados pelos serviços contratados.

7.2.10. A CONTRATADA deverá seguir o processo de mudança estabelecido pelo CONTRATANTE.

7.2.11. A CONTRATADA deverá implementar conceitos de Threat Hunting, monitorando de forma contínua todos eventos correlacionados;

7.2.12. As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas fora do horário regular, salvo quando expressamente autorizado;

7.2.13. As manutenções programadas, que impliquem em extensiva parada do ambiente serão realizadas durante um final de semana. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos;

7.2.14. Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção;

7.2.15. A contrata deverá de forma proativa, analisar políticas e processos de

segurança da CONTRATANTE e realizar sugestões de melhoria a serem implementadas em conjunto com todas as equipes envolvidas.

7.2.16. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ ou certificações oficiais dos serviços envolvidos neste Certame;

7.2.17. A CONTRATADA deverá elaborar e manter atualizados os Planos de Capacidade, de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres para os serviços objeto deste Termo;

7.2.18. Os serviços devem ser executados de acordo com normas, procedimentos e técnicas adotadas pela CONTRATANTE;

7.2.19. Deverá ser fornecido ao CONTRATANTE acesso à console dos serviços fornecidos para que seja possível o acompanhamento, auditoria e direcionamento de ações no ambiente;

7.2.20. A CONTRATADA deverá comunicar a CONTRATANTE quanto ocorrência de qualquer incidente de segurança, seguido de todas as ações de remediação realizadas.

7.2.21. Os contatos para notificação de incidentes críticos ou fluxos para aprovação de ações serão documentados durante o período de implementação.

7.2.22. A CONTRATADA deverá assumir atividades de customização de interpretação de logs/eventos que possam não ser interpretados nativamente pelo SIEM. Tais atividades não deverão ter nenhum custo adicional.

7.2.23. A CONTRATADA deverá customizar e disponibilizar dashboards/relatórios solicitados pela CONTRATANTE. Essas visões serão armazenadas na console do SIEM e poderão ser consultadas a qualquer momento. Tais atividades não deverão ter nenhum custo adicional e serão realizadas dentro do horário comercial.

7.2.24. Sempre que necessário, a CONTRATADA deverá customizar regras de detecção no SIEM, atendendo boas práticas de segurança da informação e também a demandas específicas da CONTRATANTE.

7.2.25. Qualquer atividade realizada fora do horário comercial não deverá atribuir nenhum custo adicional para a CONTRATANTE.

7.2.26. Qualquer atualização de plataformas envolvidas na contratação não deverá ter nenhum custo adicional para a CONTRATANTE.

7.2.27. A CONTRATADA deverá realizar ações referentes a resposta a incidentes de segurança, envolvendo sempre que necessário responsáveis por soluções administradas por time terceiros, com o objetivo de manter a disponibilidade e qualidade de todos os serviços tecnológicos.

7.2.28. Sempre que necessário envolvimento de times terceiros que administram outras soluções da CONTRATANTE, a CONTRATADA deverá enviar os incidentes preenchidos, analisados e contextualizados, apenas para tomada de decisão e/ou execução de ações pontuais.

7.2.29. Toda interação com times terceiros deverão ser realizadas por e-mail ou através da ferramenta de chamados da CONTRATANTE, ficando a cargo da CONTRATANTE definir qual meio será adotado.

7.2.30. A CONTRATADA deverá ter fluxos de resposta a incidentes bem definidos para os mais variados tipos de incidentes existentes.

7.2.31. A CONTRATADA deverá criar relatórios gerenciais a serem apresentados e entregues para a CONTRATANTE mensalmente, em dia a ser definido no período de implementação. Os dados deste relatório poderão ser customizados a pedido da CONTRATANTE, de modo a atender necessidades específicas de negócio. Adicionalmente, os relatórios devem conter índices de resposta a incidentes, indicadores e efetividade de todas os serviços contratados.

7.2.32. Todas as ações de resposta a incidentes executadas pela CONTRATADA deverão ser armazenadas em procedimentos operacionais, para consultas sempre que necessário.

7.2.33. A contratada deverá detectar e reportar qualquer tipo de incidentes que tenham características de reincidência.

7.2.34. Serão considerados incidentes de segurança, minimamente, as seguintes ações:

7.2.33.1. Aplicações maliciosas detectadas em estações de trabalho e servidores;

7.2.33.2. Exploração de vulnerabilidades;

7.2.33.3. Uso indevido de credenciais;

7.2.33.4. Phishing ou spam;

7.2.33.5. Ataques de Força Bruta;

7.2.33.6. Execução de códigos ou scripts maliciosos;

7.2.33.7. Ataques de saturação;

7.2.33.8. Comunicações com IPs ou domínios maliciosos;

7.2.33.9. Atividades que tenham o intuito de comprometer a integridade de ativos e entidades da CONTRATANTE;

7.2.33.10. Atividades que tenham o intuito de comprometer a confidencialidade de informações da CONTRATANTE;

7.2.33.11. Atividades que tenham o intuito de comprometer a disponibilidade dos serviços tecnológicos oferecidos pela CONTRATANTE.

7.2.35. A CONTRATADA deverá disponibilizar um canal, por e-mail, possibilitando que a CONTRATANTE comunique qualquer incidente de segurança não detectado por soluções de segurança existentes, para que as devidas investigações sejam realizadas.

7.2.36. A CONTRATADA deverá operar todas as plataformas contidas nesta contratação, de forma a realizar todas as atividades pertinentes as mesmas (Exceto ações de infraestrutura específicas administradas pela CONTRATANTE), seguindo melhores práticas recomendadas pelos fabricantes e potencializando ao máximo a capacidade de entrega de cada plataforma.

7.2.37. A CONTRATADA deverá entregar um relatório de implementação das soluções (as-built) contidas neste certame, contendo todos os passos realizados para implementação e configuração das soluções.

7.2.38. Para o faturamento mensal dos itens, a contratada deverá emitir e apresentar o “Relatório Mensal de Acompanhamento do Contrato”, que deverá conter, minimamente:

7.2.38.1. Registro de todas as atividades realizadas para cada solução de proteção envolvida neste certame;

7.2.38.2. Registro de indicadores referentes a cada camada de proteção envolvida;

7.2.38.3. Sumários de quantidade de logs ingeridos para cada fonte integrada ao SIEM;

7.2.38.4. Sumário de todos os incidentes de segurança registrados seguido de quais ações foram tomadas pelo time de resposta;

7.2.38.5. Sumário de injeções de inteligência cibernéticas aplicadas nos eventos de segurança registrados;

7.2.38.6. Sumário de toda as vulnerabilidades de segurança encontradas no período do relatório;

7.2.38.7. Sumário de todos os e-mails retidos, organizando por camada de proteção;

7.2.38.8. Estatísticas de todas as vulnerabilidades que foram corrigidas no período;

7.2.38.9. Resultados completos de testes de segurança direcionados a técnicas de movimentação lateral na rede;

7.2.38.10. Resultados completos de testes de segurança direcionados política de navegação Web e firewall;

7.2.38.11. Resultados completos de testes de segurança direcionados a solução de proteção de e-mail corporativo;

7.2.38.12. Resultados dos testes de campanhas de phishing realizadas com os usuários da ANTT;

7.2.38.13. Resultados completos de testes de segurança direcionados a solução de WAF em uso pela ANTT;

7.2.38.14. Resultados completos referentes ao nível de maturidade de segurança da ANTT baseado nos testes de segurança realizados.

7.3. Serviços de Operação e sustentação de segurança

7.3.1. Tem por objetivo sustentar e operar todas as soluções e serviços de segurança envolvidos neste processo de contratação, trabalhando em conjunto com times de sustentação da CONTRATANTE para agregar inteligência e eficiência.

7.3.2. Principais atividades a serem executadas de forma contínua pela CONTRATADA:

7.3.2.1. Acompanhar a execução dos serviços para o cumprimento dos níveis de serviço estabelecidos;

7.3.2.2. Priorizar os atendimentos críticos, conforme definição do CONTRATANTE;

7.3.2.3. Monitorar de forma permanente e realizar avaliações críticas sobre os

produtos e serviços de segurança do CONTRATANTE;

7.3.2.4. Traçar curvas de comportamento, definir a volumetria média de acessos e identificar comportamentos não usuais, visando antecipar a identificação de incidentes de segurança, antes mesmo de impacto nos serviços;

7.3.2.5. Atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;

7.3.2.6. Reagir aos eventos de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes nos sistemas ou serviços de TI do CONTRATANTE;

7.3.2.7. Atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer os sistemas e serviços de TI;

7.3.2.8. Prover os fiscais do contrato com os relatórios técnicos e gerenciais suficientes para a comprovação dos serviços realizados;

7.3.2.9. Supervisionar sua equipe na execução dos serviços executados;

7.3.2.10. Orientar a atuação da equipe técnica em situações críticas de trabalho, bem como interagir com os usuários quando a situação requerer;

7.3.2.11. Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da CONTRATANTE, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;

7.3.2.12. Consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;

7.3.2.13. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE através das aberturas de chamados no sistema de gestão de serviços de TI;

7.3.2.14. Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;

7.3.2.15. Manter atualizado o Configuration Management Database (CMDB) na ferramenta de Gerenciamento de Serviços de TI utilizada pelo CONTRATANTE;

7.3.2.16. Administrar todas as soluções envolvidas na contratação em questão;

7.3.2.17. Abrir chamados técnicos para os serviços de suporte técnico remoto das

soluções de hardware e software relacionados à Segurança da Informação no ambiente tecnológico do CONTRATANTE;

7.3.2.18. Realizar as atividades em estrita observância na Política de Segurança da Informação (PSI) e demais normas estipuladas pelo CONTRATANTE;

7.3.2.19. Implantar as melhorias solicitadas pelos servidores do CONTRATANTE;

7.3.2.20. Participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;

7.3.2.21. Realizar de forma contínua análise de vulnerabilidades, apontando todas as correções que precisam ser realizadas. Tal serviço deve também priorizar aquilo que representa maior criticidade ao ambiente da CONTRATANTE;

7.3.2.22. A CONTRATADA deverá realizar a gestão de privilégios de todas as aplicações executadas nas estações de trabalho e servidores Windows, de forma a permitir que apenas aplicações válidas tenham poder de execução;

7.3.2.23. A CONTRATADA deverá fazer a gestão do controle de acesso a rede de forma contínua, interagindo com o time de redes da CONTRATANTE, de forma a manter processos eficazes de descoberta, classificação e avaliação de postura de dispositivos que acessam a rede, contribuindo também para criação de processos que venham permitir o fácil controle/isolamento de dispositivos que venham a fornecer riscos para o ambiente.

7.3.3. Execução de mudanças de configuração nos ativos sob sua administração;

7.3.4. Execução das atividades relativas aos normativos e governança do CONTRATANTE naquilo que for relativo à sua área de atuação.

7.3.5. As atividades abaixo deverão ser realizadas de forma contínua, a fim de manter o processo de melhoria contínua no que tange segurança da informação:

7.3.5.1. Implementação, sustentação e administração da solução de SIEM;

7.3.5.2. Configuração de repositórios e processamento de logs/eventos;

7.3.5.3. Criação/envio de procedimentos para envio de logs para soluções administradas por equipes terceiras;

7.3.5.4. Customização da interpretação dos logs sempre que necessário;

7.3.5.5. Criação/configuração de alertas para cada tipo de log processado;

7.3.5.6. Monitoramento de saúde de recebimento de logs de todas as fontes configuradas para envio;

7.3.5.7. Configuração e disponibilização dos agentes de privilégios;

7.3.5.8. Criação/Manutenção de regras de detecção;

7.3.5.9. Implementação, sustentação e administração da solução de gestão de vulnerabilidades;

7.3.5.10. Implementação, sustentação e administração da solução de controle de acesso à rede;

7.3.5.11. Configurar políticas para análise e correção de posturas indesejadas;

7.3.5.12. Apontar vulnerabilidades por ordem de criticidade e acompanhar o processo de remediação das mesmas.

7.3.6. A CONTRATADA deverá acionar o fabricante das ferramentas sempre que necessário, sem nenhum custo adicional para o CONTRATANTE.

7.3.7. Qualquer atividade técnica, referente aos serviços contratados neste certame que eventualmente não tenham sido listados, também serão de responsabilidade da CONTRATADA.

7.3.8. Fica fora do escopo da CONTRATADA apenas atividades referentes a interações referente as ferramentas de rede e infraestrutura da CONTRADA, onde os times de sustentação local deverão ser acionados para qualquer tratativa necessária.

7.4. Serviço de descoberta e gestão de vulnerabilidades de Segurança

7.4.1. A CONTRATADA deverá implementar camadas de gerenciamento completo de vulnerabilidades no ambiente da CONTRATANTE, desde a descoberta até a resolução das vulnerabilidades.

7.4.2. Para a correção de cada vulnerabilidade, a CONTRATADA deverá interagir com o time da CONTRATANTE para acompanhar todas as trilhas de resolução da vulnerabilidade.

7.4.3. No caso de vulnerabilidades envolvidas em sistemas o Windows, a CONTRATADA deverá interagir com o time que administra a solução de correção de atualizações já utilizada pela CONTRATANTE para revisar todas as ações já em prática, de forma a estabelecer um fluxo saudável de atualizações de segurança recorrentes no ambiente.

7.4.4. No caso de correções de vulnerabilidades em softwares não cobertos pelo software de gestão de patches já em uso pela CONTRATANTE, a CONTRATADA deverá sugerir opções disponíveis para resolução definitiva do problema.

7.4.5. Para vulnerabilidades encontradas em sistemas WEB e servidores sustentados pela CONTRATADA, o time técnico da CONTRATANTE deverá interagir com o time responsável já atuante no ambiente para apresentar a vulnerabilidade, apontar os caminhos de resolução, aplicar a correção em conjunto e acompanhar o processo de validação do serviço hospedado no ativo em questão.

7.4.6. A CONTRATANTE será responsável pela sustentação de todos os scanners de vulnerabilidades necessários para cobertura completa e contínua do ambiente da CONTRATADA. No caso de utilização de máquinas virtuais, o time de virtualização da CONTRATADA deverá ser envolvido em toda as atividades onde se faça necessário intervenções diretamente no console do componente.

7.4.7. A CONTRATADA deverá realizar scans de vulnerabilidade contínuos no ambiente da CONTRATANTE, de forma a manter conhecimento a qualquer vulnerabilidade encontrada.

7.4.8. A CONTRATADA deverá gerir os relatórios e planejar as ações de correção de forma a zelar para que o ambiente da CONTRATANTE tenha sempre o menor nível de risco possível, quanto a vulnerabilidades existentes que tenham sido encontradas durante os scans.

7.4.9. Os scans de vulnerabilidade deverão ser executados em todo o ambiente de forma a manter o ambiente cobertos quanto ao conhecimento de possíveis brechas de segurança existentes. No caso de ambientes onde a segregação de rede não permita comunicação direta com o servidor que realiza o scan, a CONTRATADA deverá implementar agentes que façam os scans com periodicidade a ser definida.

7.4.10. Deverá automatizar processos para remediação automática de vulnerabilidades de segurança em sistemas operacionais e aplicações instaladas nas estações/servidores;

7.4.11. Deverá impor um fluxo de atualizações passando pela fase de homologação antes de produção;

7.4.12. O fluxo deve ser automatizado e sem interrupção de forma a manter o ambiente sempre seguro frente a novas vulnerabilidades descobertas;

7.4.13. No caso de sistemas que não possam ser atualizados, a CONTRATADA deverá indicar melhores práticas de segurança para proteção do ativo e diminuição da superfície de ataque que permeia aquele ativo.

7.5. Serviço de Gestão de Incidentes de Segurança

7.5.1. Tem por objetivo analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado obedecendo os frameworks NIST e SANS de resposta a incidente de segurança da informação e boas práticas de mercado.

7.5.2. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

7.5.3. O início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for detectado pelas plataformas responsáveis ou através do serviço de monitoramento, porém não se limitando a estes. Poderá o corpo técnico de segurança do CONTRATANTE a qualquer tempo, abrir um incidente de segurança.

7.5.4. Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança da CONTRATADA, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

7.5.5. Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança da CONTRATADA, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

7.5.6. Como próximo passo o grupo de resposta a incidente de segurança da CONTRATADA, deverá comunicar ao time de segurança da informação do CONTRATANTE as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.

7.5.7. Juntamente com o CONTRATANTE o grupo de resposta a incidente de segurança da CONTRATADA, deverá definir a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de

criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente.

7.5.8. Após análises iniciais do incidente, caberá ao o grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

7.5.9. Todo o processo de análise e resultados obtidos devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que o CONTRATANTE acompanhe todos os passos para a solução do incidente.

7.5.10. Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança da CONTRATADA deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional do CONTRATANTE, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do CONTRATANTE.

7.5.11. Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA através do grupo de resposta a incidente de segurança, inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

7.5.12. Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão.

7.5.13. O grupo de resposta a incidente de segurança da CONTRATADA, deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

7.5.14. O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano) ;

7.5.15. A contratada deverá prover serviços de resposta aos incidentes de segurança da informação diante os eventos registrados no monitoramento;

7.5.16. A CONTRATADA deverá prover inteligência de proteção contra ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra ataques cibernéticos, sendo responsável por:

7.5.16.1. Pesquisar novos tipos de ataques, vírus, malwares, Botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

7.5.16.2. Criar, em colaboração com a CONTRATANTE, casos de uso (regras) que devem ser implementados no SIEM fornecido;

7.5.16.3. Revisar periodicamente as regras do SIEM, realizando as adaptações e evoluções necessárias;

7.5.16.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para resposta a incidentes, correspondentes às regras do SIEM;

7.5.17. O serviço deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

7.5.17.1. Relatórios de ameaças e segurança;

7.5.17.2. Relatórios de Botnets e centros de Comando e Controle;

7.5.17.3. Identificação de exploit kits;

7.5.17.4. Indicadores de ataques “ZeroDays” ;

7.5.17.5. Indicadores de comprometimento, suspeitas e avisos informativos;

7.5.17.6. Inteligência de tendências;

7.5.17.7. Proxies anônimos;

7.5.17.8. Classificação de sites;

7.5.17.9. Endereços de rede TOR.

7.6. Serviço de validação de segurança

7.6.1. Os profissionais alocados deverão realizar testes, a partir da solução de validação de segurança para verificar se os ativos de segurança estão respondendo a ameaças cibernéticas existentes;

7.6.2. O serviço deve ser capaz de testar a eficiência dos ativos de segurança em ambiente de produção, executando simulações de ataque entre seus componentes de software distribuídos, sem causar danos ou degradação do ambiente;

7.6.3. Tais testes devem ser contínuos a fim de criar um baseline de possíveis modificações nos resultados durante o período contratual.

7.6.4. Os ativos de segurança a serem validados contemplam, no mínimo, IDS/IPS, Firewall, Endpoint Security e WAF;

7.6.5. Deve avaliar o nível de segurança fornecido por um grupo de endpoints e ativos de segurança de rede independentemente de fabricante e tecnologia;

7.6.6. Deve executar simulações de ataque entre seus componentes sem iniciar conexões com nenhum servidor, aplicativo ou sistema em produção, a fim de fornecer uma avaliação livre de riscos;

7.6.7. Deve simular ataques, relatar ameaças não bloqueadas e propor medidas de mitigação às ameaças de forma contínua, além de permitir a visualização para cada cenário de ataque;

7.6.8. Para a execução de exploração de vulnerabilidades, Malwares e ataques às aplicações web, devem ser usados “payloads” reais de ataques maliciosos;

7.6.9. Durante a verificação dos controles de segurança de endpoint, devem ser reproduzidos métodos maliciosos usados por APTs (Advanced Persistent Threats) sem que o sistema operacional seja infectado;

7.6.10. Deverão ser realizados testes contínuos de movimentação lateral, de modo a identificar e prevenir possibilidades para atacantes navegarem pela rede corporativa.

7.6.11. Deverão ser realizados testes quanto a efetividades de ataque do tipo command and control, onde o atacante consegue fechar conexão com o centro de controle para efetivação da ação maliciosa.

7.6.12. Deve executar ataques em aplicações Web sobre os protocolos HTTP e HTTPS;

7.6.13. Deve executar ataques de URLs usando protocolo HTTP e HTTPS a partir da Internet ou internamente;

7.6.14. Deverão ser executados testes de acessos a URLs por categorização, de forma a validar a política de acesso web já em implementada pela CONTRATANTE.

7.6.15. Deve realizar testes de SMTP, tanto a partir da Internet para o domínio corporativo quanto entre contas de domínios corporativos;

7.6.16. Os testes via SMTP deverão compor campanhas de phishing, de forma a testar a capacidade de resposta dos usuários a ameaças deste gênero.

7.6.17. Deve utilizar técnicas, táticas e procedimentos contidos no MITRE ATT&CK.

7.6.18. Deve gerar relatórios de todos os ataques realizados, estabelecendo um benchmark de proteção a ser comparado a cada teste., de forma a fornecer relatórios de progresso ou declínio na efetividade das demais tecnologias de proteção em uso.

---------- **FIM DO APÊNDICE “A”** ----------