ANA
AGÊNCIA NACIONAL DE ÁGUAS
E SANEAMENTO BÁSICO

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA (DOD)
Documento nº 02500.049501/2022-01

DEMANDA	Contratação de solução de segurança
DATA	

INTRODUÇÃO
O Documento de Oficialização da Demanda institui a Equipe de Planejamento da Contratação e deve conter a aprovação do Superintendente de Tecnologia da Informação.

1. Descrição Detalhada da Demanda

Contratação de empresa especializada em segurança cibernética para prestação dos seguintes serviços:

1. **Serviços de Gestão de Vulnerabilidades,** o objetivo desse serviço é identificar as possíveis vulnerabilidades de segurança da informação no ambiente da **ANA** (infraestrutura e aplicações), que seriam vetores de ataques e fixar uma blindagem contra a exploração dessas vulnerabilidades, evitando que ataques cibernéticos obtenham sucesso. Espera-se também as orientações, o acompanhamento e a verificação das aplicações das correções de vulnerabilidade.
2. **Serviços de Gestão de Segurança para Infraestrutura e Sistemas Críticos**, esse serviço visa avaliar continuamente e ininterruptamente os acessos aos sistemas críticos por meio de credenciais administrativas. Os eventos gerados serão analisados, sendo em caso positivo, transformados em um incidente de segurança da informação, obedecendo um processo rigoroso de gestão de eventos.
3. **Serviços de Monitoramento de Ataques Cibernéticos,** o objetivo desse serviço é monitorar todo e qualquer tipo de ataque cibernético direcionado à **ANA**, através da análise de correlações de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, e em casos positivos, transformados em um incidente de segurança da informação, obedecendo um processo rigoroso de gestão de eventos.
4. **Serviços de Resposta a Incidentes de Segurança Cibernética,** o objetivo desse serviço é analisar, remediar, conter e documentar os eventos de segurança da informação, e caso descubra um ataque iminente, deve transformar em um incidente de segurança da informação. Esse serviço é executado por um **SOC** do inglês *Security Operation Center*, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas.

5. **Serviços de Governança e Conformidade de Segurança Cibernética,** tem por objetivo conscientizar, acompanhar, averiguar e garantir, que todas as regras de segurança da informação estabelecida para a instituição, estão sendo cumpridas e seguidas pelos seus colaboradores.
6. **Serviços de Testes de Invasão (Pentest)** terá como objetivo identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas especificas para tentar obter acesso não autorizado e privilegiado aos ativos e informações da Instituição.
7. **Serviços de Conscientização da Segurança da Informação,** para conscientização de todos os usuários do parque tecnológico da **ANA**, sobre a importância de seguir as políticas de segurança da informação estabelecidas. Identificando proativamente os usuários que seriam vetores de ataques, e tornando-os elegíveis para um programa de capacitação interna, sobre boas práticas de segurança da informação no ambiente corporativo da**ANA**.
8. **Serviços de Proteção de Endpoints e Servidores de Rede**, seu objetivo é proteger as estações de trabalho e os equipamentos servidores de rede corporativos, de forma eficiente, bloqueando a entrada e saída de informações críticas ou sensíveis, bem como examinar todo o conteúdo em busca de vírus, malwares, botnets ou outras ameaças avançadas.
9. **Serviços de Proteção de Mensageria**, seu objetivo é proteger o serviço de mensageria utilizado pelos usuários internos, de forma eficiente, bloqueando a entrada e saída de e-mails indesejáveis, bem como examinar todo o conteúdo em busca de vírus, spams, phishing, botnets, ameaças avançadas, vazamento de informações, entre outros.
10. **Serviços de Inteligência Aplicada a Segurança Cibernética**, tem por objetivo o monitoramento e a eliminação das informações, de qualquer tipo, relativa a **ANA**, suas autoridades e demais servidores que estejam trafegando ou sendo negociadas nas redes web consideradas perigosas ou seja nas **Dark Web e Deep Web**.

Observação: os serviços ora apresentados precisam ser prestados com apoio de ferramentas adequadas, os quais devem ser providos sob responsabilidade exclusiva da empresa contratada, cujos requisitos mínimos são apresentados no Anexo I deste Documento de Oficialização de Demanda.

2. Identificação e Ciência do Integrante Administrativo

NOME	REBECA CRIVELARO CAMPOS	**MATRÍCULA**	1556533
Declaro ter ciência das competências do INTEGRANTE ADMINISTRATIVO definidas na IN SGD/ME nº 1/2019, bem como minha indicação para exercer esse papel na equipe que irá realizar o Planejamento da Contratação descrita nesse documento.			

(assinado eletronicamente)
REBECA CRIVELARO CAMPOS
Analista Administrativa
Integrante Administrativa

3. Equipe de Planejamento da Contratação

Integrante Requisitante	FABIANO COSTA DE ALMEIDA	Matrícula	1830348
Integrante Técnico	CLÁUDIO PEREIRA	Matrícula	1438137
Integrante Administrativo	REBECA CRIVELARO CAMPOS	Matrícula	1556533

4. Aprovação

Aprovo o prosseguimento da contratação, considerando sua relevância e oportunidade em relação aos objetivos estratégicos e as necessidades da Área Requisitante.

Desta forma, institua-se a Equipe de Planejamento da Contratação, de acordo com o Guia de Contratação de Soluções de TIC da ANA. Conforme o art. 29, § 8º da IN SGD/ME nº 01/2019, a Equipe de Planejamento da Contratação será automaticamente destituída quando da assinatura do contrato.

Encaminhe-se à Superintendência de Administração, Finanças e Gestão de Pessoas - SAF para instituição da Equipe de Planejamento da Contratação por meio de Portaria.

(assinado eletronicamente)
MAYARA NASCIMENTO DE FARIAS DUTRA DE ANDRADE
Superintendente Adjunta de Tecnologia da Informação

ANEXO I

REQUISITOS MÍNIMOS DE FERRAMENTAS PARA APOIAR OS SERVIÇOS DE:

1. **Serviços de Gestão de Vulnerabilidades.**
2. **Serviços de Gestão de Segurança para Infraestrutura e Sistemas Críticos.**
3. **Serviços de Monitoramento de Ataques Cibernéticos.**
4. **Serviços de Resposta a Incidentes de Segurança Cibernética.**
5. **Serviços de Governança e Conformidade.**
6. **Serviços de Testes de Invasão (Pentest).**
7. **Serviços de Conscientização da Segurança da Informação.**
8. **Serviços de Proteção de Endpoints e Servidores de Rede..**
9. **Serviços de Proteção de Mensageria.**
10. **Serviços de Inteligência Aplicada a Segurança Cibernética.**

1. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE GESTÃO DE VULNERABILIDADES

1.1. REQUISITOS DA FERRAMENTA PARA AMBIENTES CRÍTICO

1.1.1. Deve possibilitar, por meio da console, no mínimo 01 (um) método de escaneamento:

1.1.1.1. Scan ativo;

1.1.1.2. Scan com uso de agentes;

1.1.1.3. Scan passivo;

1.1.2. A solução deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferentes do padrão CVSS;

1.1.3. Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial;

1.1.4. O Algoritmo de priorização deve considerar vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade;

1.1.5. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades;

1.1.6. A solução deve ser capaz de aplicar algoritmos de inteligência artificial (Machine learning) para analisar fontes de dados relacionadas a vulnerabilidades;

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

1.1.7.1. CVSSv3 Impact Score;

1.1.7.2. Idade da Vulnerabilidade;

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

1.1.7.4. Número de produtos afetados pela vulnerabilidade;

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

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

1.1.8. A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação);

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

1.1.10. Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo;

1.1.11. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

1.1.12. A solução deve possuir conectores para a seguintes plataformas:

1.1.12.1. Amazon Web Service (AWS);

1.1.12.2. Microsoft Azure;

1.1.12.3. Google Cloud Platform;

1.1.12.4. Qualys Assets;

1.1.13. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;

1.1.14. A solução deve ser capaz de identificar novos hosts no ambiente, sem a necessidade de um scan;

1.1.15. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

1.1.16. A solução deve possibilitar, no mínimo 50 (cinquenta) scanners ativos;

1.1.17. A solução deve possibilitar, no mínimo, 20 (vinte) sensores passivos de rede para realizar o monitoramento em tempo real do ambiente;

1.1.18. Deve ser possível determinar em tempo real, quais portas estão abertas em determinado ativo;

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

1.1.19.1. BIOS UUID;

1.1.19.2. MAC Address;

1.1.19.3. Nome NetBIOS:

1.1.19.4. FQDN;

1.1.20. A solução deve ser capaz de realizar - em tempo real - a descoberta de novos ativos para, no mínimo:

1.1.20.1. Bancos de dados;

1.1.20.2. Hypervisors;

1.1.20.3. Dispositivos móveis;

1.1.20.4. Dispositivos de rede;

1.1.20.5. Endpoints;

1.1.20.6. Aplicações;

1.1.21. Deve realizar - em tempo real - a identificação de informações sensíveis no tráfego de rede do ambiente;

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

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

1.1.24. A solução deve ser capaz de - em tempo real - detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;

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

1.1.26. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo, no mínimo, Windows, Linux e Mac OS, bem como appliances virtuais;

1.1.27. A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões, e gerenciar todos por uma console central;

1.1.28. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de configurações e vulnerabilidades;

1.1.29. A solução deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como, por exemplo, em determinados dias do mês ou determinados horários do dia;

1.1.30. No caso em que uma atividade de varredura for interrompida por invadir o período não permitido, a mesma deve ser capaz de ser reiniciada de onde parou;

1.1.31. A solução deve ser configurável para permitir a otimização das configurações de varredura;

1.1.32. A solução 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;

1.1.33. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até o acesso de sistema ou administrativo;

1.1.34. A solução deve ser capaz de realizar pesquisas de dados confidenciais;

1.1.35. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

1.1.36. 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 nos servidores;

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

1.1.38. A solução deve ser capaz de realizar um benchmark no ambiente da **ANA**, comparando sua maturidade com outras organizações do mesmo setor;

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

1.1.40. A solução 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).

1.1.41. A solução deve gerar uma pontuação global referente a exposição cibernética da organização, baseada nas pontuações de cada um dos ativos.

1.1.42. A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria, assim como outras empresas do mercado.

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

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

1.1.45. A solução deve permitir a segregação lógica entre áreas distintas da empresa, a fim de obter a pontuação referente a exposição cibernética por área.

1.1.46. Deve ser capaz de executar relatórios manuais e periódicos de acordo com a frequência estabelecida pelo administrador;

1.1.47. A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

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

1.1.49. A solução deve suportar o envio automático de relatórios para destinatários específicos;

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

1.1.51. Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

1.1.52. A solução deve possuir relatórios pré-configurados com as seguintes informações:

1.1.52.1. Hosts verificados sem credenciais;

1.1.52.2. Top 100 Vulnerabilidades mais críticas;

1.1.52.3. Top 10 Hosts infectados por Malwares;

1.1.52.4. Hosts exploráveis por Malwares;

1.1.52.5. Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

1.1.52.6. Vulnerabilidades críticas e exploráveis;

1.1.52.7. Máquinas com vulnerabilidades que podem ser exploradas;

1.1.52.8. Relatórios contendo scans credenciados que tiveram erro ou falha;

1.1.53. A solução deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;

1.1.54. Deve possuir dashboard apresentando visão das vulnerabilidades discriminadas por sua criticidade e idade;

1.1.55. A solução deve criptografar todas as informações em trânsito;

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

1.1.57. A solução deve ser capaz de gerar uma chave randômica com no mínimo 256 bits para cada scanner conectado na plataforma de gerência;

1.1.58. Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados - no mínimo - com protocolo TLS 1.3, com tamanho de chave de 4096 bits;

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

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

1.1.61. A solução deve possuir no mínimo as seguintes certificações de privacidade e segurança:

1.1.61.1. EU-U.S. Privacy Shield Framework.

1.1.62. A solução deve possuir ferramentas e processos automatizados para monitorar: Uptime, Comportamentos anômalos e performance da plataforma;

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

1.1.64. A solução deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo, no mínimo, mas não se limitando, a base de ameaças apontadas pelo OWASP Top 10;

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

1.1.66. A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

1.1.67. Deverá avaliar - no mínimo - os padrões de segurança OWASP Top 10;

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

1.1.68.1. Cookies, Headers, Formularios e Links;

1.1.68.2. Nomes e valores de parâmetros da aplicação;

1.1.68.3. Elementos JSON e XML;

1.1.68.4. Elementos DOM;

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

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

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

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

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

1.1.73.1. Número máximo de URLs para crawl e navegação;

1.1.73.2. Número máximo de diretórios para varreduras;

1.1.73.3. Número máximo de elementos DOM;

1.1.73.4. Tamanho máximo de respostas;

1.1.73.5. Tempo máximo para a varredura;

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

1.1.73.7. Número máximo de requisições HTTP por segundo;

1.1.73.8. Autenticação Básica (Digest);

1.1.73.9. NTLM;

1.1.73.10. Autenticação de Cookies;

1.1.73.11. Autenticação através de Selenium;

1.1.74. Deve ser capaz de importar scripts de autenticação Selenium previamente configurados pelo usuário;

1.1.75. 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;

1.1.76. A solução deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

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

1.1.78. Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;

1.1.79. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;

1.1.80. A solução deve ser capaz de realizar varreduras nos seguintes componentes:

1.1.80.1. Red Hat JBoss, AngularJS, Apache, Apache Tomcat;

1.1.80.2. Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin, Nodejs, Javascript, Java e YUI

1.1.81. O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da **ANA**;

1.2. REQUISITOS DA FERRAMENTA PARA AMBIENTES NÃO CRÍTICO

1.1.82. Deve possuir personalização de relatórios classificados por vulnerabilidade ou host;

1.1.83. Os relatórios devem ser exportados pelo menos em HTML, CSV ou PDF;

1.1.84. Deve ser capaz de enviar notificações de resultados de varredura por e-mail;

1.1.85. A solução deve prover a descoberta e varredura de ativos:

1.1.85.1. Varreduras incluindo redes IPv4 / IPv6 / FQDN;

1.1.85.2. Varreduras em busca de vulnerabilidades sem utilização de credenciais;

1.1.85.3. Varreduras utilizando credenciais e verificação de patches;

1.1.85.4. Varreduras de sistemas operacionais, dispositivos de rede, hypervisors, base dados, servidores web;

1.1.86. Deve possuir trilha de auditoria;

1.1.87. Suportar hypervisors pelo menos, Red Hat Enterprise Virtualization (RHEV), VMware, além de outros;

1.1.88. Deve ser compatível com os sistemas Operacionais: Windows 7 SP1, 8.1 e 10, Windows Server 2003/2008 R2 ou superior, Linux Debian 9 e 10 Red Hat ES 6,7 e 8, no mínimo;

1.1.89. A varredura por credenciais deve ser suportada nas seguintes bases de dados: Oracle, SQL Server, MySQL, PostgreSQL;

1.1.90. Deve possuir varredura de conformidade personalizada para Windows e Unix,

1.1.91. Possuir suporte a detecção de vírus, malwares botnets, processos conhecidos e desconhecidos;

1.1.92. A solução deve auditar o agente do antivírus instalados, informando se está mal configurado e estão com regras desatualizadas;

1.1.93. Auditoria de configuração baseada no mínimo em critérios do CIS, mas não limitada a outros entes como: CERT, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI;

1.1.94. Possui suporte a configuração de políticas e templates;

1.1.95. A solução deve conter pontuação de risco: ranking de vulnerabilidade baseado em CVSS, cinco níveis (crítico, alto, médio, baixo, informações), níveis de gravidade personalizáveis para reformulação de riscos;

1.1.96. Possuir escaneamento de quantidade de IPs de destino/dispositivos alvo ilimitados;

1.1.97. O Gerenciamento deverá ser realizado por interface web;

1.1.98. A solução deve possuir agendamento de escaneamento possibilitando definir subnets ou IP's alvo específicos;

1.1.99. A solução deve apresentar formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e configurações necessárias para eliminar ou, não sendo possível, para reduzir a exposição ao risco;

1.1.100. Deve fornecer o acesso a templates (modelos de configuração pré-determinados) de escaneamento para identificação de vulnerabilidades específicas (por exemplo, o ransomware WannaCry e suas variantes);

1.1.101. Identificadores CVE (Common Vulnerabilities and Exposures) associados as vulnerabilidades identificadas para geração de relatórios, gerenciamento de riscos e mitigação de ameaças;

1.1.102. Identificação de vulnerabilidades de aplicação, tais como: Cross-SiteScripting, SQL Injection e outros;

1.1.103. Manutenção do histórico de escaneamentos anteriores.

2. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE GESTÃO DE SEGURANÇA PARA INFRAESTRUTURA E SISTEMAS CRÍTICOS

2.1. REQUISITOS DA FERRAMENTA DE GESTÂO DE DISPOSITIVOS E AMBIENTES

2.1.1. Gerenciar em dispositivos-alvo baseados, em no mínimo, as seguintes tecnologias:

2.1.1.1. Sistemas operacionais Linux/Unix, Red Hat, Microsoft Windows;

2.1.1.2. Hypervisors: VMWare, RedHat KVM e Microsoft Hyper-V;

2.1.1.3. Contas de usuários de sistemas;

2.1.1.4. Contas de usuários de serviço;

2.1.1.5. Credenciais do Microsoft COM+;

2.1.1.6. Credenciais do Microsoft Internet Information Service – IIS;

2.1.1.7. Credenciais do Apache TomCat;

2.1.1.8. Credenciais do RedHat JBoss;

2.1.1.9. Objetos do Microsoft Active Directory (usuários, grupos e computadores);

2.1.1.10. Objetos do Lightweight Directory Access Protocol – LDAP (usuários, grupos e computadores);

2.1.1.11. Contas de usuários e administradores de bancos de dados Microsoft SQL Server, MySQL, Oracle, PostgreSQL;

2.1.1.12. Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi;

2.1.1.13. Contas de equipamentos ativos de conectividade de redes SAN (Storage Area Network) e NAS (Network Attached Storage);

2.1.1.14. Contas de usuários e administradores de consoles de gerenciamento de computadores servidores;

2.1.1.15. Contas de usuários e administradores de consoles de gerenciamento de solução de segurança para endpoints e servidores.

2.1.1.16. Contas de usuários e administradores de estações de trabalho;

2.1.1.17. Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo;

2.1.1.18. Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas etc.;

2.1.1.19. Credenciais de nuvem em VMWare ESXi, Azure, Office 365 ou outras.

2.1.2. A solução deve possuir função de monitoramento e análise de comportamento, que toma por base os eventos gerados por todos os itens desta especificação técnica (repositório digital seguro, gravador e monitor de sessões, funcionalidades para proteção local de servidores, controladores de domínio e estações de trabalho);

2.1.3. Deve montar perfis de comportamento dos usuários acessando todos os dispositivos-alvo através da solução, por meio dos eventos coletados;

2.1.4. Deve alertar abusos e comportamentos fora dos padrões aprendidos/mapeados;

2.1.5. Exibir de forma gráfica o resumo dos eventos recebidos pela plataforma, classificados por origem, tais como LDAP, SIEM e a própria solução;

2.1.6. Deve detectar os seguintes comportamentos anormais:

2.1.6.1. Acesso privilegiado à solução durante horários irregulares. Detectado quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental;

2.1.6.2. Acesso privilegiado à solução durante dias irregulares. Detectado quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental;

2.1.6.3. Acesso excessivo a contas privilegiadas. Detectado quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental;

2.1.6.4. Acesso privilegiado à solução através de IP irregular ou desconhecido. Detectado quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental;

2.1.6.5. Acesso privilegiado não gerenciado. Detectado quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução;

2.1.6.6. Máquina acessada a partir de endereços IP incomuns;

2.1.6.7. Máquina acessada durante horários irregulares. Detectado quando uma máquina é acessada em um horário irregular, de acordo com seu padrão de utilização;

2.1.6.8. Acessos excessivos a uma máquina;

2.1.6.9. Acesso anômalo a várias máquinas. Detectado quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto;

2.1.6.10. Máquina incomum originando acesso;

2.1.6.11. Usuário incomum fazendo login de uma máquina de origem conhecida;

2.1.6.12. Suspeita de roubo de credenciais. Detectado quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução;

2.1.6.13. Alteração de senha suspeita. Detectado quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução;

2.1.6.14. Acesso privilegiado realizado fora da solução, diretamente no dispositivo alvo;

2.1.6.15. Usuário inativo da solução. Detectado quando ocorrem indicações de atividade de um usuário inativo;

2.1.6.16. Delegação não restrita. Detectado através da análise das contas de domínio. Contas com delegação irrestrita são contas que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco;

2.1.6.17. Contas SPN vulneráveis. Detectado quando as contas privilegiadas com configuração de SPN (nome principal de serviço) podem estar vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da conta;

2.1.6.18. Atividades suspeitas detectadas durante uma sessão privilegiada. Detectado quando é identificada uma sessão privilegiada com atividades (comandos e anomalias na solução) definidas como suspeitas;

2.1.6.19. Conta de serviço conectada interativamente. Detectado quando a solução identifica um logon interativo realizado por uma conta de serviço;

2.1.7. Realizar a identificação e o correlaciona mento de todos os eventos citados combinando as ações mencionadas que caracterizam comportamentos anormais como, por exemplo, usuário acessando a solução em horário e máquina incomuns, com acesso originado de IP incomum, utilizando conta não anteriormente utilizada (suspeita de roubo de credencial);

2.1.8. Permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos;

2.1.9. Possibilitar colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador;

2.1.10. Permitir o encerramento automatizado da sessão em caso de detecção de atividade suspeita de alta criticidade.

2.1.11. Fornecer por meio de integração para que soluções de terceiros também possam encerrar sessões suspeitas (ex: SIEM executa terminação de sessão);

2.1.12. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em Comandos Linux, Comandos, janelas e aplicações Windows, Expressões regulares para comandos em geral e Eventos configurados manualmente, permitindo a atribuição de nível de risco customizado.

2.1.13. Monitorar e avaliar as atividades de contas ou grupos privilegiados que não são administrados pela solução;

2.1.14. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade de senha que incluem, no mínimo, o comprimento da senha (quantidade de caracteres), a frequência de troca da senha, a especificação de caracteres permitidos ou proibidos na composição da senha e o gerenciamento do histórico das senhas geridas;

2.1.15. Mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;

2.1.16. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;

2.1.17. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos;

2.1.18. Garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;

2.1.19. Garantir a quantidade de acessos à sua interface conforme a necessidade da ANA, podendo inclusive serem ilimitados. Não é aceita a limitação do número de contas que podem ser gerenciadas em um alvo licenciado;

2.1.20. Deve utilizar banco de dados, para armazenamento de credenciais, com as melhores práticas de segurança, com mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução.

2.1.20.1. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software que o compatibilize com a solução;

2.1.20.2. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação;

2.1.21. Utilizar banco de dados para armazenamento de credenciais que permita alta disponibilidade e mecanismos para a recuperação de desastres, e que também seja compatível com soluções de backup e arquivamento disponíveis no mercado;

2.1.22. Permitir o Backup e Recovery de seu Banco de Dados, bem como das Configurações de Software estabelecidas, permitindo a execução de Backups automatizados, com a programação/agendamento de horários;

2.1.23. Suportar a implementação em parque computacional Windows Server 2008 R2 e versões superiores ou em parque computacional Red Hat;

2.1.24. Suportar instalação em VMWare, Red Hat KVM ou Hyper-V;

2.1.24.1. Caso não seja compatível, a solução deverá ser entregue com licenças de software (ex: hypervisor diverso ao do item acima ou sistema operacional específico) que a compatibilize com as ferramentas de infraestrutura da ANA;

2.1.24.2. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação;

2.1.25. Prover, sem custos adicionais para a ANA, alta disponibilidade dos elementos críticos da solução (Cofres Digitais e Gateways de Acessos Privilegiados) com funcionamento em modo ativo-ativo ou ativo-stand-by em cada uma das localidades (site principal e site redundante adicional), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação;

2.1.26. Caso seja necessário, a ANA proverá a infraestrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego etc.) para implantação e uso da solução em alta disponibilidade;

2.1.27. Prover, no mínimo, um ambiente adicional externo da solução para testes e homologação, replicando todo o ambiente de produção, em número de licenças e funcionalidades;

2.1.28. Caso a solução fornecida faça uso das funcionalidades disponibilizadas pelas CALs (Client Access License) do serviço Microsoft Remote Desktop Services (RDS) para acessos através da mesma, a ANA irá disponibilizar tal Infraestrutura, para que não seja afetada a experiência dos usuários.

2.1.29. Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas e domínios, independentemente de sua quantidade;

2.1.30. Permitir a opção de implementar o gerenciamento de troca de senhas em redes segregadas e remotas a fim de acomodar links de alta latência, redes isoladas (DMZ) e outras restrições semelhantes;

2.1.31. Possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma. Deve ainda ser compatível com os seguintes métodos e padrões de criptografia:

2.1.31.1. AES com chaves de 256 bits;

2.1.31.2. FIPS 140-2;

2.1.31.3. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo(s) fabricante(s) da solução ofertados;

2.1.32. Incorporar medidas de segurança, incluindo:

2.1.32.1. Criptografia, a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações web dos usuários finais;

2.1.33. Ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (repositório seguro), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso a todas as senhas de identidades privilegiadas gerenciadas pela solução;

2.1.34. Integrar-se com soluções de autenticação de duplo fator, incluindo tokens físicos, tokens em software, tokens de evento, tokens de tempo e outras que possuam suporte para envio de tokens via SMS e e-mail;

2.1.35. Prover uma interface gráfica para que os administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem necessidade de serviços profissionais de terceiros;

2.1.36. Prover arquitetura para que os administradores possam configurar as integrações que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros;

2.1.36.1. A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, WMI, SSH e HTTP/HTTPS;

2.1.37. Integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações:

2.1.37.1. Atividades administrativas de delegação e revogação de acesso as credenciais privilegiadas;

2.1.37.2. Atividades de recuperação, liberação e alterações de senhas;

2.1.37.3. Atividades executadas pelos usuários na aplicação web;

2.1.37.4. Eventos agendados.

2.1.38. Descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;

2.1.39. Descobrir e alterar credenciais privilegiadas em ambientes Linux e Unix;

2.1.40. Gerenciar credenciais em interfaces de gerenciamento de servidores “out-of-band”, tais como Dell iDrac, IBM IMM ou compatíveis com o padrão IPMI – Intelligent Platform Management Interface;

2.1.41. Descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com Open LDAP;

2.1.42. Descobrir e alterar contas privilegiadas usadas em serviços web em, no mínimo, aplicações baseadas em Microsoft IIS);

2.1.43. Descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados;

2.1.44. Permitir o agrupamento lógico de credenciais, obedecendo uma hierarquia, a fim de simplificar a configuração e aplicação de políticas apropriadas para diferentes tipos de sistemas alvo, além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas;

2.1.45. Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e realizar verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino correspondam às mesmas senhas armazenadas no banco de dados da solução. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento;

2.1.46. Proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas e arquivos em texto claro;

2.1.47. Conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso, devendo conceder acesso a:

2.1.47.1. Sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no sistema operacional do servidor de destino, possibilitando habilitar gravação da sessão caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

2.1.47.2. Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução;

2.1.47.3. As sessões acessadas podem ser monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os vídeos gerados possam ser armazenados de modo seguro em drivers locais de rede, pastas compartilhadas, etc.;

2.1.47.4. Caso tenha formato proprietário, a solução deverá conter meios de acessar os vídeos.

2.1.47.5. Filtrar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado.

2.1.47.6. A função de gravação de sessões deve realizar o isolamento de sessões de acesso, atuando como um proxy/servidor de salto entre a máquina do usuário e o ativo a ser acessado.

2.1.47.7. A função de gravação de sessões deve ser provida em alta disponibilidade, no modelo ativo-ativo ou ativo-stand-by, tanto no site principal quanto no site adicional previsto para a função DR.

2.1.47.8. Quando em ambiente distribuído entre dois Data Centers, a solução deverá permitir que cada equipamento armazene suas gravações de maneira segura em storage local, evitando a transmissão desnecessária de dados entre diferentes Data Centers.

2.1.47.9. Ainda que as gravações estejam armazenadas em locais diferentes, a solução deve permitir que essas evidências sejam consultadas a partir de qualquer console web instalada, de maneira centralizada.

2.1.48. Permitir que os usuários solicitem acesso aos gestores através de interface web intuitiva;

2.1.49. Realizar automaticamente a descoberta, detecção, importação e armazenamento no repositório seguro de chaves SSH em sistemas Linux, implementando:

2.1.49.1. Suporte a chaves nos tamanhos 1024, 2048, 4096 e 8192 bits;

2.1.49.2. Análise da relação de confiança das chaves detectadas com outras máquinas na rede;

2.1.49.3. Auditoria e controle dos acessos às chaves por sistema de aprovações;

2.1.49.4. Renovação periódica ou sob demanda das chaves;

2.1.49.5. Verificação da validade e sincronia das chaves com o destino;

2.1.49.6. Reconciliação de chaves, renovando-as e armazenando-as novamente;

2.1.49.7. Conexão transparente a ativos da rede, utilizando as chaves armazenadas;

2.1.49.8. Gerenciamento em grupos, permitindo que múltiplas máquinas herdem a mesma chave SSH.

2.1.50. Permitir que os comandos executados em sistemas Linux monitorados sejam gravados em modo texto;

2.1.51. Possuir funcionalidade de "AD Bridge" para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD;

2.1.52. Fornecer aplicação web para acesso às funcionalidades básicas da solução que seja compatível com ao menos dois dos principais navegadores do mercado (Internet Explorer, Google Chrome e Firefox);

2.1.53. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário;

2.1.54. Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;

2.1.55. Permitir o envio automático de logs para servidores SYSLOG, de forma aderente ao disposto em RFC 5424 – The Syslog Protocol (IETF);

2.1.56. Ser configurável para enviar alertas disparados pelo sistema e eventos de usuário baseados nos arquivos de log, valores de registro, e-mail, logs de evento do Windows, Syslog, enfileiramento de mensagens Microsoft e executando aplicações específicas;

2.1.57. Controlar o acesso aos relatórios se baseando nas permissões configuradas na solução;

2.1.58. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas;

2.1.59. Caso os componentes da solução sejam segregados uns dos outros, a sua intercomunicação não deverá conter senhas em texto claro;

2.1.60. Criar relatórios que podem ser exportados em pelo menos um dos formatos editáveis: HTML, CSV, XLSX ou XLS;

2.1.61. A solução deverá disponibilizar:

2.1.61.1. Mecanismo de retirada e devolução de contas e senhas compartilhadas;

2.1.61.2. Definição de tempo de validade: permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

2.1.61.3. Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;

2.1.61.4. Troca de senhas por demanda: permitir a troca de senhas nos sistemas gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (grupo de todos os sistemas operacionais UNIX, por exemplo);

2.1.62. Ser capaz de, durante o processo de definição da política de composição de senha:

2.1.62.1. Gerar senhas aleatórias com extensão de 127 (cento e vinte e sete) caracteres ou mais;

2.1.62.2. Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos;

2.1.62.3. Especificar qual o tipo de caractere na composição das senhas a serem geradas;

2.1.62.4. Implementar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada. Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses grupos, onde esses privilégios de acesso

possam ser atribuídos por critérios como tipo de dispositivo, sistemas operacionais, banco de dados e aplicativos de virtualização;

2.1.62.5. Garantir que a senha gerada seja diferente do nome da conta correspondente. Exemplo: se a credencial ou conta tem o nome “Administrador” a senha gerada jamais pode ser composta da mesma forma;

2.1.62.6. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha;

2.1.62.7. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;

2.1.62.8. Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo;

2.1.63. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características:

2.1.63.1. Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável;

2.1.63.2. Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos;

2.1.63.3. No que diz respeito à descoberta automatizada de identidades privilegiadas, a solução deve ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução;

2.1.63.4. Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas;

2.1.63.5. A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;

2.1.64. Suportar, através da interface Web para acesso e recuperação das senhas, de forma nativa, a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução;

2.1.65. A interface web e de administração deverão ser compatíveis com os seguintes métodos de autenticação de duplo fator: certificados digitais, smart cards, tokens RSA, Oauth ou Google Authentication, para todos os usuários da solução;

2.1.66. A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução;

2.1.67. A solução deve apresentar relatórios com visibilidade hierárquica, contendo listas e filtros de ordenação, de tal forma que os usuários possam detalhar as informações e os recursos que desejam acessar;

2.1.68. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

2.1.68.1. Lista de sistemas gerenciados;

2.1.68.2. Senhas armazenadas;

2.1.68.3. Eventos de alteração de senha;

2.1.68.4. Permissões de acesso web;

2.1.68.5. Auditoria de contas, sistemas e usuários;

2.1.68.6. Alerta em tempo real.

2.1.69. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das interações dos usuários com a solução, tais como:

2.1.69.1. Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;

2.1.69.2. Alterações nas funções de delegação;

2.1.69.3. Adições, deleções e alterações de senhas gerenciadas pela solução;

2.1.69.4. Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas;

2.1.69.5. Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;

2.1.70. Possuir funcionalidade para monitoramento de saúde da solução, com a capacidade de chaveamento entre nós no caso de falhas;

2.1.71. Visando a garantia do funcionamento da solução como um todo, este item deve ser entregue com total integração com os demais itens desta especificação.

2.1.72. Deve proteger o Controlador de Domínio contra roubo de identidade e acesso não autorizado.

2.1.73. Deve monitorar atividades internas no controlador de domínio e tráfego de segmento de rede que este esteja instalado, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário.

2.1.74. Deve detectar em tempo real atividades anômalas, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios;

2.1.75. Deve detectar a recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash);

2.1.76. Deve detectar a obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro (Golden Ticket);

2.1.77. Deve detectar a recuperação maliciosa de credenciais do controlador de domínio (DCSync).

3. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICO

3.1. REQUISITOS DAS FERRAMENTAS DE APOIO AO MONITORAMENTO

3.1.1. Permitir integração com qualquer sistema de correlação de eventos (SIEM) para recebimento de alertas e abertura automática de incidentes para tratamento via fluxo de trabalho. A plataforma contratada deverá suportar o recebimento de alertas em formato Syslog;

3.1.2. Permitir o acesso a distintos painéis de controle, totalmente customizáveis sem a necessidade do uso de programação, através da utilização de perfis diferenciados;

3.1.3. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática;

3.1.4. Permitir o recebimento de Alertas de Segurança;

3.1.5. Permitir a criação de Investigações de Incidentes que não sejam necessariamente relacionados à Segurança da Informação;

3.1.6. Possibilitar o registro de Análise Forense, tanto para rede quanto para host.

3.2. REQUISITOS DA FERRAMENTA DE GESTÂO DE LOGS E OPERACÃO DE INCIDENTES (SIEM)

3.2.1. Deve possuir arquitetura de forma distribuída, possuindo no mínimo os seguintes módulos ou componentes: módulo de coleta de pacotes e logs e geração de metadados, módulo de indexação, agregação e enriquecimento dos metadados dos coletores, módulo de correlaciona mento avançado de alertas e tratamento de incidentes e módulo de gerencia centralizada de todos os outros módulos envolvidos;

3.2.2. Permitir a correlação de eventos provenientes de logs e pacotes do tráfego de rede, devidamente estruturados em metadados;

3.2.3. A solução deve ser capaz de processar, correlacionar e armazenar 8000 (oito mil) eventos por segundo (EPS), de forma sustentada;

3.2.4. Deverá ter capacidade e ser licenciada para processar no mínimo todos os eventos gerados pelos ativos de segurança do ambiente tecnológico listados anteriormente;

3.2.5. Ser capaz de integrar em uma única console de visualização, dados e metadados de logs e pacotes do tráfego de rede;

3.2.6. Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;

3.2.7. Possuir compatibilidade e integração nativa com pelo menos uma solução de forense comportamental de endpoints (EDR), com intuito de complementar a visibilidade entregue e capacidade de análise de atividade maliciosa;

3.2.8. Prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;

3.2.9. Possuir a capacidade de navegação continua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;

3.2.10. Prover uma interface extremamente intuitiva, permitindo que em até três cliques seja possível chegar a uma ação suspeita ou ataque, sem prévio conhecimento da mesma;

3.2.11. Integrar-se nativamente com uma solução de análise forense de estações, sendo capaz de utilizar dados e indicadores de comprometimento gerados pela mesma;

3.2.12. Permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

3.2.13. Deve possuir pelo menos 150 regras pré-definidas;

3.2.14. A solução deve possuir a funcionalidade de UEBA (User and Entity Behavior Analytics).

3.2.15. Deve permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por e-mail;

3.2.16. O fabricante da solução deve possuir ampla experiência em malwares, assim como possuir seu próprio centro de pesquisa e desenvolvimento e inteligência às novas ameaças;

3.2.17. Deve ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros;

3.2.18. Deve permitir o desenvolvimento e customização de interpretadores (parsers) utilizando linguagens XML e LUA, através de ferramenta gráfica do mesmo fabricante;

3.2.19. Deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

3.2.19.1. relatórios de ameaças e segurança;

3.2.19.2. relatórios de botnets e centros de Comando e Controle;

3.2.19.3. identificação de exploit kits;

3.2.19.4. indicadores de ataques “zero-day”;

3.2.19.5. indicadores de comprometimento, suspeitas e avisos Informativos;

3.2.19.6. inteligência de tendências;

3.2.19.7. proxies anônimos;

3.2.19.8. classificação de sites;

3.2.19.9. endereços de rede TOR.

3.2.20. Deve possuir integração nativa com módulo de análise de malware de mesmo fabricante;

3.2.21. O módulo de análise de malware deve permitir o uso de regras YARA;

3.2.22. Deve possuir integração nativa com soluções de gestão de centro de operações de segurança (Security Operations Center - SOC);

3.2.23. Deve permitir a criação de perfis de visualização do metadados derivados dos dados capturados;

3.2.24. Deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;

3.2.25. Deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;

3.2.26. Deve permitir a captura de dados de forma distribuída e toda a análise centralizada;

3.2.27. Deve possuir controle de acesso baseado em papéis e perfis de usuários;

3.2.28. Deve permitir gerar relatórios em formatos HTML, PDF e CSV;

3.2.29. Deve possuir um módulo para construção de relatórios customizados pelo usuário, com funcionalidade do tipo arrastar-e- colar para definição dos campos e elementos deles;

3.2.30. Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolos SYSLOG e SNMP;

3.2.31. Permitir integração nativa com módulo opcional para detecção e análise de comportamento de malware do tipo “0- day” em endpoints (EDR), de forma aprimorar as investigações da solução;

3.2.32. Permitir a definição e customização de alertas, relatórios e gráficos;

3.2.33. Possuir integração com serviço de diretório (Active Directory) e Pluggable Authentication Module (PAM);

3.2.34. Disponibilizar uma API ou SDK permitindo a integração e customização com a solução;

3.2.35. Suportar a comunicação criptografada entre os componentes envolvidos;

3.2.36. Fazer uso de protocolo proprietário entre os componentes, para garantir máximo desempenho;

3.2.37. Deve ser projetada para possuir escalabilidade infinita;

3.2.38. Possuir um módulo de monitoração de desempenho e saúde dos equipamentos envolvidos;

3.2.39. Suportar o gerenciamento dos componentes através de uma interface de gerência central;

3.2.40. Possuir métricas de saúde dos equipamentos como: utilização de CPU, temperatura da CPU, utilização de memória, disco rígido, status do serviço, status das conexões;

3.2.41. O hardware para implementação da solução será fornecido pela infraestrutura da ANA, contudo todo e qualquer software, inclusive do hipervisor caso a solução seja virtual, deverá ser fornecido e licenciado pela CONTRATADA.

3.2.42. Possuir relatórios de conformidade e regulamentações pré-definidos (out-of-the-box) como BASEL II, FERPA, FFIEC, FISMA, GLBA, HIPPA, ISO27002, NERC-CIP, NISPOM, PCI e SOX;

3.2.43. Utilizar sistema operacional baseado em Linux;

3.2.44. Deverá segregar a visualização de relatórios apenas para usuários com a devida permissão;

3.2.45. Possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;

3.2.46. Suportar a integração nativa com sistemas de GRC (Governance, Risk e Compliance), possibilitando a integração de dashboards entre as soluções e provendo contexto de governança a um incidente gerado pela solução proposta;

3.2.47. Possuir a funcionalidade para resolução de endereços IP, como localização da cidade, pais e organização das conexões;

3.2.48. Possuir a capacidade de exportar e importar arquivos no formato packet capture (pcap);

3.2.49. Permitir a visualização das sessões nos seguintes formatos: metadado, texto, hexadecimal, pacotes, reconstrução Web (HTTP), reconstrução e-mail (SMTP) e arquivos (binários);

3.2.50. Suportar a análise de dados na camada de aplicação (modelo OSI) a partir de entidades como usuários, e-mail, endereço, arquivos e ações;

3.2.51. Suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;

3.2.52. A solução deve suportar a decriptação de tráfego SSL, por meio do uso de appliances físicos dedicados a este propósito;

3.2.53. Suportar a geração de hash (MD5 e SHA1) para verificação de integridade dos arquivos extraídos a partir do tráfego de rede capturado;

3.2.54. Deve possuir a capacidade de extração de metadados do tráfego de dados capturado, com reconhecimento nativo de no mínimo os seguintes protocolos e aplicações: FTP, SCP, HTTP, HTTPS, IMAP, IRC, MAIL (RFC822), NETBIOS, POP3, RDP, SIP, SMB, SMIME, SMTP, SNMP, SSH, TELNET, TNS, DNS, TORRENT.

3.2.55. Possuir a capacidade de criação de interpretadores (parsers) para protocolos e aplicações proprietárias e/ou não conhecidas;

3.2.56. Possuir a capacidade de identificação de protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação;

3.2.57. Permitir isolar sessões de tráfegos, com identificação de conteúdo (payload) de origem e destino, para os protocolos ICMP, TCP e UDP;

3.2.58. Permitir a extração dos arquivos presentes no tráfego de rede capturado no formato compactado .zip;

3.2.59. Alertar em tempo real sobre tráfego coincidente com assinaturas pré-definidas e permitir a visualização da sessão em que a assinatura ocorreu, assim como a exportação da sessão para o formato .pcap;

3.2.60. Possuir ferramenta para administração centralizada dos módulos de captura do tráfego de rede, permitindo a replicação de parâmetros de configuração entre os dispositivos a partir de uma única fonte;

3.2.61. Deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;

3.2.62. Ser capaz de analisar tráfego IPv4 e IPv6;

3.2.63. Permitir a customização de um interpretador de busca, cuja função é analisar todas as sessões de rede em busca de palavras chaves ou sentenças;

3.2.64. Funcionar somente em modo passivo sem adicionar latência à rede durante a monitoração passiva;

3.2.65. Armazenar todos os pacotes de forma segura;

3.2.66. Permitir nativamente, a análise automatizada e ampla de malwares e suas atividades de rede;

3.2.67. Permitir a captura e análise de características suspeitas em arquivos de conteúdo executável na rede em tempo real; A solução deve possuir um mecanismo de pontuação de risco no momento da análise de malwares;

3.2.68. Possuir painel (dashboard) configurável que permita a rápida visualização do status da segurança e acesso granular a sessão reconstruída equivalente ao tráfego que gerou o alerta;

3.2.69. Possuir a capacidade de exibir visualmente os objetos trafegados pela rede sem a necessidade de manipular os dados diretamente na console ou banco de dados;

3.2.70. Permitir que a partir de uma informação existente em um relatório, se verifique o tráfego de rede que a gerou através de recurso de "drill-down";

3.2.71. Ser capaz de identificar a troca de extensão de arquivos (arquivo .exe enviado como .jpg);

3.2.72. Possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;

3.2.73. Permitir o processamento de eventos/logs, apenas com a adição de componentes para tal finalidade, mantendo a taxonomia dos metadados;

3.2.74. Ser capaz coletar e armazenar todos os logs de ativos de rede e dispositivos que são recebidos em sua interface de rede, gravando-os em formato original para posterior uso em fins forenses;

3.2.75. Ser capaz de coletar os logs dos ativos de rede e dispositivos de forma não intrusiva, sem a instalação de agentes;

3.2.76. Suportar a criação de interpretadores (parsers) para os logs não suportados nativamente através de linguagem XML e LUA;

3.2.77. Suportar a criação de interpretadores (parsers) customizados para no mínimo 20 sistemas proprietários das proponentes;

3.2.78. Suportar de forma nativa os logs de pelo menos 300 dispositivos diferentes de diversos fabricantes;

3.2.79. Possuir a capacidade de geração de alertas sobre qualquer dado ou comportamento desejado e permitir o envio deste alerta a plataformas externas como SIEM ou SYSLOG;

3.2.80. Possuir capacidade de coletar logs de sistemas operacionais Windows, Linux, Unix e FreeBSD;

3.2.81. Ser capaz de coletar logs de firewalls, antivírus, IDSs, proxies, servidores DNS, load balancers e demais dispositivos de segurança;

3.2.82. Ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SYSLOG-NG, SNMP, Microsoft Windows Event Logging API, Microsoft Windows Remote Management, CheckPoint LEA, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC, CISCO e CISCO Security Device Event Exchange (SDEE);

3.2.83. Utilizar formatos de logs/eventos através de formatos nativos de cada fabricante do dispositivo, sem utilizar um tipo de formato comum definido pelo proponente da solução;

3.2.84. Deve exigir a adição de agentes ou software nos dispositivos monitorados, exceto caso o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;

3.2.85. Deve coletar e armazenar logs/eventos dos dispositivos sem realizar normalização no momento da coleta;

3.2.86. Deve fazer uso de sistema de bancos de dados relacional por questão de desempenho, normalização e DBAs requeridos por esses sistemas;

3.2.87. Permitir que os logs/eventos dos dispositivos da CONTRATANTE sejam enriquecidos com informações de classificação de risco;

3.2.88. Permitir o correlacionamento de logs/eventos próximo ao tempo real;

3.2.89. Possuir um painel de controle (Dashboard), onde através de simples "drill-down" possa ver o log/evento coletado; A solução deve fornecer painel de controle (Dashboard) que constantemente mostre o status do ambiente de correlação de eventos; A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;

3.2.90. Permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;

3.2.91. Oferecer uma plataforma unificada, acessível via browser WEB para realizar investigações, gestão de incidentes, gestão de alertas, gestão de relatórios, administração dos componentes e gestão de inteligência externa;

3.2.92. Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;

3.2.93. Possuir a capacidade de análise avançada de eventos em tempo real através de regras de correlacionamento e eventos complexos em dados correlacionados através da linguagem EPL (Event Processing Language), com mecanismo de versão igual superior à 5.3;

3.2.94. Suportar nativamente a coleta de NetFlow, sendo capaz de capturar, analisar e correlacionar de forma contínua até 25000 fluxos por segundo na versão 5 e 15000 fluxos por segundo na versão 9;

3.2.95. Deve detectar de forma nativa ataques do tipo NetFlow Synflood na coleta de Netflows;

3.2.96. Ter a habilidade de receber logs/eventos oriundos de um relay de syslogs;

3.2.97. Suportar o recebimento de eventos no formato Common Event Format (CEF);

3.2.98. Possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;

3.2.99. Possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.

3.2.100. Suportar de forma nativa e automática o armazenamento em camadas, com as seguintes funcionalidades: HOT (dados presentes em sistemas como DACs e SANs), WARM (dados presentes em sistemas como NAS para pesquisa, execução de relatórios, exportação de dados) e COLD (dados presentes em sistemas de armazenamento off-line para possível restauração em WARM);

3.2.101. Suportar nos sistemas de armazenamento de longo prazo, pelo menos 3 algoritmos de compressão: gzip, bzip2 e lzma;

3.2.102. Permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;

3.2.103. Permitir a exportação de logs/eventos armazenados nos formatos texto, XML, JSON, CSV;

3.2.104. Possuir um módulo específico para tratar dados arquivados e/ou recuperados;

3.2.105. Ser baseada em plataforma WEB, com acesso via browser padrão de mercado, sem a necessidade de instalação de aplicações cliente nas estações dos analistas responsáveis pela resposta aos incidentes;

3.2.106. Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:

3.2.106.1. Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;

3.2.106.2. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

3.2.106.3. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos etc.;

3.2.106.4. Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;

3.2.106.5. Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;

3.2.106.6. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise; Permitir inserir análise forense de host e rede como um complemento da análise do incidente;

3.2.106.7. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;

3.2.106.8. Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2);

3.2.106.9. Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux; A solução deve possuir tecnologia de análise comportamental (UBA), baseado em técnicas de "machine learning" e analises estatísticas para a monitoração de segurança, gerando índices de riscos para eventos e entidades mapeadas;

3.2.107. Exibir a data e hora do último login no rodapé da interface, de forma garantir que a credencial não esteja sendo compartilhada;

3.2.108. Permitir o processamento de informações estruturadas de ameaças STIXTM ("Structured Threat Information eXpression");

3.2.109. Possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando à redução de erros de lógica e sintaxe;

3.2.110. Permitir o ajuste de sessões concorrentes na interface de gerência;

3.2.111. Permitir a customização de perfis de visualização de metadados de acordo com o objetivo da investigação (ex.: Analise Web, Analise e-mail, Analise de Arquivos, etc.);

3.2.112. Possuir um menu de contexto na interface de investigações, de forma visualizar instantaneamente se endereços foram encontrados em Alertas, Incidentes ou Listas.

3.3. **REQUISITOS DA FERRAMENTA DE GESTÂO DE DISPOSITIVOS DE REDE (NDR)**

3.3.1. A solução deve permitir análise comportamental da rede e seus componentes, dispositivos e usuários na detecção de anomalia(s), através de tecnologia baseada em Inteligência Artificial e Machine Learning.

3.3.2. A solução deve realizar as inspeções, processamento, análise e detecção de anormalidades, sem a necessidade do envio de dados para fora da rede ou envio de logs (característica de SIEM) ou utilizando inteligência externa.

3.3.3. Solução deve realizar a inspeção de todo trafego das redes do CONTRATANTE, de forma off-line, não dependendo da instalação de agentes nos dispositivos ou de envio de dados (syslog)

3.3.4. Solução deve realizar a inspeção de todo trafego das redes da CONTRATANTE, também a nível de camada de aplicação (Layer 7), de forma off-line, não dependendo da instalação de agentes em computadores

3.3.5. A coleta e análise do comportamento do tráfego deverão ser realizadas obrigatoriamente por equipamento (hardware) dedicado a esta função instalados nas dependências da CONTRATANTE.

3.3.6. A responsabilidade de integração e suporte dos componentes de software e hardware da solução deve ser unificada sob um mesmo fornecedor, ainda que a solução tenha componentes de diferentes fabricantes.

3.3.7. A solução deve ser inteiramente funcional, não sendo aceita solução parcial e/ou solução com necessidade de aquisição de componentes adicionais para o correto funcionamento da mesma. Para caso de componentes adicionais os mesmos (licenciamento) devem estar comtemplados na proposta comercial.

3.3.8. Todos os componentes de software, hardware da solução devem estar em suas últimas versões estáveis.

3.3.9. O hardware permite expansão de armazenamento sem a necessidade de substituição de equipamento ou reconfiguração de software,

3.3.10. A solução deverá armazenar os registros dos eventos de anomalias no mínimo por 30 dias a fim de prover qualquer consulta.

3.3.11. A solução deverá suportar análise de no mínimo 2000 ativos

3.3.12. A solução deve realizar as inspeções por meio de espelhamento de portas através de interface Ethernet de 1Gbps e ou fibra ótica (10baseSR) de 10Gbps com no mínimo duas portas.

3.3.13. A solução de deve permitir Threat Hunting, análise comportamental da rede e seus componentes, detecção de anomalia(s) o e visibilidade de rede.

3.3.14. Deve utilizar no mínimo os seguintes métodos de inteligência artificial para criação de perfis de uso e identificação de desvios comportamentais na rede:

3.3.14.1. Machine learning não supervisionado

3.3.14.2. Machine learning supervisionado

3.3.14.3. Deep Learning

3.3.14.4. Redes Neurais

3.3.15. A solução não deve depender de pré-configurações baseadas na rede da organização para que identifique associações entre múltiplos elementos da rede para que consiga identificar anomalias de comportamento.

3.3.16. A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e contínua se adaptando a variações de comportamento destes durante o tempo.

3.3.17. A solução deve possuir mecanismos de DPI (Deep Packet Inspection).

3.3.18. Solução deve realizar a inspeção do tráfego de forma off-line através de tráfego espelhado nos switches, ou seja, não dependendo de qualquer alteração de roteamento e fluxo de dados da rede.

3.3.19. A ferramenta deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede.

3.3.20. A solução deve inspecionar e analisar os dados brutos da rede através de espelhamento de porta (SPAN/Port MIrror) ou através do uso de TAP – Terminal Access Point.

3.3.21. A ferramenta deve suportar a ingestão de dados através de mecanismos de tunelamento de tráfego na camada 2 (enlace) do modelo OSI como VXLAN e ERSPAN.

3.3.22. A ferramenta deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra ataques cibernéticos.

3.3.23. A ferramenta deve permitir a inspeção de plataformas como:

3.3.23.1. Amazon AWS

3.3.23.2. Microsoft Azure

3.3.23.3. Google G-Suite

3.3.23.4. Office 365

3.3.23.5. SalesForce

3.3.23.6. Dropbox enterprise

3.3.23.7. Componentes virtuais (máquinas virtuais)

3.3.23.8. Endpoint para Sistemas Operacionais.

3.3.23.9. Docker, Kubernetes e AWS Fargate.

3.3.23.10. Box

3.3.23.11. Slack

3.3.23.12. Zoom

3.3.24. A solução deve identificar de forma autônoma, os dispositivos conectados na rede no mínimo com as seguintes informações.

3.3.24.1. Classificação do tipo de dispositivo (desktop, servidor, Impressora, camera, iot, etc);

3.3.24.2. IP do dispositivo;

3.3.24.3. Mac Address;

3.3.24.4. Nome DNS do dispositivo;

3.3.24.5. Primeira vez que o dispositivo/IP foi visto na rede;

3.3.24.6. Última vez que o dispositivo foi visto na rede;

3.3.24.7. Associação com usuários (login Active Directory) quando cabível."

3.3.25. A ferramenta deve criar métricas, de forma autônoma, de raridade de Ips, Domínios DNS, Dispositivos, etc. baseado na frequência que estes são acessados através da rede.

3.3.26. A ferramenta deve criar métricas, de forma autônoma, de anormalidades comparando a ação atual de um dispositivo, usuário, IP, domínio, etc. contra as ações de mesmo escopo realizadas no passado.

3.3.27. A métrica de anormalidade deve apresentar o percentual de desvio do comportamento atual de um dispositivo comparado com o comportamento passado aprendido.

3.3.28. A ferramenta deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:

3.3.29. A solução deverá informar sobre conexões a destinos raros na internet, não frequentemente visitados por dispositivos da rede interna e/ou usuários.

3.3.30. Possui informações de Whois e Geolocalização para os endereços IP e URL classificadas como ameaças.

3.3.31. Dispositivo realizando conexões para destinos raros na internet não frequentemente visitados com por dispositivos da rede interna.

3.3.32. Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.

3.3.33. Dispositivo se comunicando com um servidor usando um certificado expirado.

3.3.34. Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.

3.3.35. Detectar dispositivo com conexões para um IP externo raro de maneira regular. (Beaconing)

3.3.36. Detectar grande número de solicitações para servidores Webs, os quais estão retornando códigos de erro HTTP.

3.3.37. Detectar atividade de penetração ou escaneamento de portas na rede.

3.3.38. Detectar dispositivos internos realizando movimentação lateral.

3.3.39. Detectar vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.

3.3.40. Detectar dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS)

3.3.41. Detectar dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.

3.3.42. Detectar dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico

3.3.43. Detectar dispositivo fazendo alto volume de requisições de DNS repetidas.

3.3.44. Detectar dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.

3.3.45. Detectar o servidor DNS interno agindo como um resolvedor de DNS aberto (OpenDns).

3.3.46. Detectar dispositivo se comunicando com o serviço de anonimização da rede TOR.

3.3.47. Detectar dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.

3.3.48. Detectar atividade anormal de PowerShell e o Windown Romote Mamagement, seguido por uma conexão a um destino externo raro seguido de download de arquivo suspeito.

3.3.49. Detectar dispositivo executando comandos PsExec ou Telnet em uma máquina remota.

3.3.50. Detectar dispositivos transferindo volume de dados para fora da rede (IP público) e/ou internamente.

3.3.51. Detectar dispositivos trocando um volume de dados anormal com outro dispositivo na rede interna.

3.3.52. Detectar dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.

3.3.53. Detectar dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.

3.3.54. Detectar dispositivo fazendo conexões com hostnames raros associados a uma botnet.

3.3.55. Detectar dispositivo solicitando um domínio conhecido por hospedar malwares.

3.3.56. Detectar dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de arquivos da rede SMB.

3.3.57. Detectar dispositivo transferindo um volume de moderado a grande de dados para fora da rede durante um período de 24 horas ou mais por meio de um grande volume de conexões.

3.3.58. Detectar dispositivo fazendo download dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.

3.3.59. Detectar dispositivos se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de transferência de arquivos na rede interna.

3.3.60. Detectar dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.

3.3.61. Detectar dispositivo não conseguiu estabelecer uma sessão SMB2 seguida de uma configuração bem-sucedida da sessão SMB1 usando credenciais administrativas.

3.3.62. Detectar dispositivo lendo e gravando volumes de dados semelhantes para compartilhamentos de arquivos remotos.

3.3.63. Detectar dispositivo acessando arquivos que possuem de senhas não criptografadas.

3.3.64. Detectar dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.

3.3.65. Detectar dispositivo fazendo conexões web externas sem usar um proxy web.

3.3.66. 5.20.3.39. Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.

3.3.67. 5.20.3.40. Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.

3.3.68. Detectar dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.

3.3.69. Detectar dispositivos causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.

3.3.70. Detectar dispositivos fazendo download de arquivo executável (exe e/ou msi) vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

3.3.71. Detectar dispositivos fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

3.3.72. Detectar dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.

3.3.73. Detectar dispositivo informando no cabeçalho User-Agent que possui um sistema operacional o qual é diferente do SO que realmente está utilizando.

3.3.74. Detectar dispositivo fazendo download de um arquivo que não corresponde ao seu 'File Type' de uma fonte externa que a rede normalmente não acessa.

3.3.75. Detectar dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros, exemplo: GoogleDrive, DropBox, Wetransfer, OneDrive etc.

3.3.76. Detectar dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

3.3.77. Detectar dispositivo fazendo download de um arquivo suspeito e em seguida fez uma conexão para um destino externo com o qual a rede normalmente não se comunica.

3.3.78. Detectar dispositivo enviando dados para o Pastebin, Zerobin.net, ghostbin.com, rentry.co, controlc.com, hastebin.com.

3.3.79. Detectar dispositivos usando um sistema terceiro de mensageria (Whatsapp, telegram, Hangout ou similares).

3.3.80. Detectar dispositivo acessando rede social (Facebook ou similares).

3.3.81. Detectar dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.

3.3.82. Detectar dispositivo fazendo conexões peer-to-peer BitTorrent.

3.3.83. Detectar dispositivos fazendo conexões SQL para IPs externos a rede.

3.3.84. Detectar dispositivo que recebeu um número anormalmente grande de conexões de entrada de IP externos raros.

3.3.85. Detectar dispositivo enviando uma quantidade anormal alta de dados para destinos fora da rede.

3.3.86. Detectar dispositivo trocando um volume de dados anormal com outro dispositivo na rede interna.

3.3.87. Detectar dispositivo enviando uma quantidade anormalmente alta de dados externamente para um local para o qual a rede não enviou dados anteriormente.

3.3.88. Detectar dispositivo explorado vulnerabilidade Heartbleed na rede interna.

3.3.89. Detectar dispositivo se conectando a um DNS SinkHole conhecido.

3.3.90. Detectar dispositivo realizando grandes volumes de pequenas conexões SSH e/ou RDP.

3.3.91. Detectar dispositivo iniciando um grande número de conexões RDP e/ou SSH e conexões não realizadas anteriormente.

3.3.92. Detectar dispositivo recebendo um grande número de conexões RDP ou SSH de entrada de IPs externos raros.

3.3.93. Alteração de bloco CIDR de uma subrede.

3.3.94. Alteração no comportamento de tráfego DHCP.

3.3.95. Detectar novo servidores de DNS e DHCP na rede.

3.3.96. Detectar servidores de proxy web na rede.

3.3.97. Detectar a adição ou remoção de domínios DNS na rede

3.3.98. Detectar perdas de pacotes e retransmissões superior a um percentual parametrizável na ferramenta ou anormal.

3.3.99. Detectar credenciais de alto privilégio sendo utilizada para acessar servidores (podendo ser parametrizadas ou visualizada pelo AD).

3.3.100. Detectar uma credencial efetuando login de uma origem incomum.

3.3.101. Detectar credenciais usadas em múltiplos dispositivos internos.

3.3.102. Possuir funcionalidade integrada para reconstrução completa de arquivos, a partir dos PCAPs capturados, inclusive de arquivos anexos a e-mails, trafegados na web ou compartilhados entre usuários;

3.3.103. Realizar inspeção em pacotes https (https inspection).

3.3.104. Permitir recebimento de logs externos para a realização da análise, tais como Microsoft Active Directory, Checkpoint e McAffe.

3.3.105. Possuir interface gráfica de gerenciamento, independente de plataforma, preferencialmente em Web via protocolo HTTPS, uso de criptografia TLS 1.2, funcionando nos navegadores Google Chrome, Microsoft New Edge e Firefox,

3.3.106. A solução deve se integrar com serviço OpenLDAP e/ou AD a fim de possibilitar a autenticação na interface, autorização de usuários e para consultas com objetivos de enriquecer os dados inspecionados.

3.3.107. A solução deve permitir a utilização de segundo fator de autenticação nativa para logins na interface web.

3.3.108. A interface deve permitir a procura e navegação a qualquer dispositivo, usuário, Ips, portas, tipos de ataques etc. que tenham sido inspecionados em qualquer horário/data armazenada pela solução.

3.3.109. Possuir alertas de detecção de anomalias contendo no mínimo os seguintes dados:

3.3.109.1. Data e horário.

3.3.109.2. Dispositivo e/ou usuários que originou a ação.

3.3.109.3. Descrição técnica do evento.

3.3.109.4. Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco.

3.3.109.5. Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta."

3.3.110. Permitir que os alertas de anomalias sejam enviadas por e-mail e/ou sistema de mensageria (WhatsApp, Telegram, SMS etc.)

3.3.111. Permitir a visibilidade dos logins dos usuários aos dispositivos da rede (Desktops e notebooks)

3.3.112. Deve permitir o recebimento de logs de sistemas externos utilizando padrões de mercado, como CEF, LEEF, JSON e Syslog.

3.3.113. Deve permitir a integração nativa com plataforma de gerenciamento de chamados como HPSM, Atlassian, JIRA e ServiceNow.

3.3.114. Deve permitir a integração com plataformas de Threat Inteligence utilizando os protocolos STIX/TAXII.

3.3.115. A plataforma deve possuir OPEN API para suportar integração com sistemas terceiros.

3.3.116. Deve possuir ferramenta para a criação e customização de relatório e envio.

3.3.117. Possuir relatório gerencial indicando a quantidade total de dispositivos, quantidade total de sub redes e throghput (máximo e média).

3.3.118. Deve indicar a quantidade total de dispositivos, quantidade total de sub redes e banda média processada.

3.3.119. Possuir sumário das violações por fase do ataque.

3.3.120. Possuir sumário dos dispositivos com maior nível de brechas não usuais.

3.3.121. Possuir sumario dos top dispositivos que mais violaram comportamentos anômalos.

3.3.122. Mostrar as violações mais frequentes a principais itens de compliance como: uso de USB no dispositivo, google drive, tráfego RDP saindo da rede, acesso a servidor SQL através da internet, dentre outros.

3.3.123. Possuir sumário dos dispositivos que mais violaram os itens de compliance gerando risco a organização.

3.3.124. Deve permitir que o relatório seja exportado para documento padrão .PDF e/ou .csv.

3.3.125. Deve possuir mecanismo para busca de dados diretamente na base de dados da ferramenta.

3.3.126. Possuir sumário das tops violações e/ou comportamentos anômalos

4. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

A mesmas do Item 3. Assim sendo é necessário que esteja em execução demanda do serviço apoiado pelo item 3 para a prestação deste tipo de serviço.

5. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE GOVERNANÇA E CONFORMIDADE

5.1. REQUISITOS DA FERRAMENTA PARA TODOS OS GRUPOS DA ARQUITETURA

5.1.1. A solução deve oferecer a possibilidade de integração via API nos seus diversos módulos;

5.1.2. A solução deve permitir a criação de permissões de utilização a nível de usuário Role Based Access Control (RBAC);

5.1.3. A solução deve ter a capacidade de carregar/alterar usuários em massa bem como seus tipos de funções;

5.1.4. A solução deve possuir recursos de registros de auditoria para que possamos monitorar quando e onde nossos usuários finais fizeram o login no aplicativo;

5.1.5. A solução e seus módulos deverão estar licenciadas para número ilimitado de usuários e administradores.

5.2. REQUISITOS DA FERRAMENTA DE GESTÃO DE PREFERÊNCIAS E CONSENTIMENTO UNIVERSAL

5.2.1. A solução deve possuir a capacidade de registrar e reunir o status de consentimento do titular de dados;

5.2.2. A solução deve possuir a capacidade de rastrear o consentimento do titular dos dados por finalidade de processamento e assunto;

5.2.3. A solução deve possuir a capacidade rastrear todas as alterações de consentimento por data e identificação;

5.2.4. A solução deve suportar uma variedade de opções de desativação;

5.2.5. A solução deve possuir a capacidade de fornecer informações de apoio ao Encarregado dos dados e funções de responsabilidade empresarial relacionadas;

5.2.6. A solução deve possuir a capacidade se integrar, via API, com outras ferramentas de marketing (SFDC, Marketo, Pardot e Eloqua);

5.2.7. A solução deve oferecer um portal de consentimento onde o titular pode alterar e revogar os seus consentimentos a qualquer momento;

5.2.8. A solução deve permitir a vinculação de diferentes identificadores a um mesmo titular (e-mail, telefone, matrícula, código etc.);

5.2.9. A solução deve permitir a criação de elementos de dados e vinculá-los aos consentimentos;

5.2.10. A solução deve permitir a vinculação de política de privacidade aos consentimentos;

5.2.11. A solução deverá versionar as alterações nos atributos dos consentimentos.

5.3. **GESTÃO DE INCIDENTES E VIOLAÇÕES**

5.3.1. Possuir capacidade de gerenciar incidentes e possíveis violações;

5.3.2. Promover trilha de auditoria detalhada que evidencie todas as ações tomadas para minimização / correção do incidente;

5.3.3. Suportar notificações automáticas por e-mail e fluxos de trabalho ao longo do ciclo de vida do incidente;

5.3.4. Possuir fluxos de trabalho automatizados e customizáveis com possibilidade de atribuição de tarefas a outras áreas para cada incidente documentado;

5.3.5. Possuir recursos de relatórios para gestão de riscos e incidentes;

5.3.6. Permitir que tanto o público interno quanto o externo possam relatar um incidente em página específica no Portal (intranet e internet);

5.3.7. Verificar e atender às regras de notificação de violações nos regulamentos locais e globais;

5.3.8. Permitir a criação de fluxos de trabalhos específicos para cada tipo de incidente;

5.3.9. Prover recomendações de notificações baseadas nos tipos de dados envolvidos no incidente;

5.3.10. A solução deverá permitir a criação de formulários para registro de incidentes;

5.3.11. A solução deverá permitir a criação de avaliações para análise do incidente.

5.4. **REQUISITOS DA FERRAMENTA DE GESTÃO DE AVISO E POLÍTICAS**

5.4.1. A solução deve possuir a capacidade de gerenciar o processo de criação, gestão e publicação de políticas e avisos em sites e aplicativos;

5.4.2. A solução deve possuir a capacidade de se integrar com sistemas de gestão de conteúdo já existentes;

5.4.3. A solução deve possuir um histórico de versões e fornecer notificações quando são feitas alterações nas políticas;

5.4.4. A solução deve possuir a capacidade de importar e manter políticas existentes diretamente na sua solução.

5.5. **REQUISITOS DA FERRAMENTA DE GESTÃO DE POLÍTICAS CORPORATIVAS**

5.5.1. A solução deverá permitir a criação de políticas, procedimentos e normas corporativas;

5.5.2. A solução deverá permitir a vinculação de controles às políticas corporativas;

5.5.3. A solução deverá permitir o versionamento das políticas, procedimentos e normas corporativas;

5.5.4. A solução deverá registrar o aceite dos funcionários as políticas corporativas;

5.5.5. A solução deverá permitir a criação de fluxos de criação/revisão/aprovação das políticas corporativas;

5.5.6. A solução deverá permitir a vinculação das políticas aos itens do mapeamento de dados (ativos, processos, entidades e fornecedores);

5.5.7. A solução deverá permitir a definição da vigência da política corporativa.

6. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE TESTES DE INVASÃO (Pentest)

As ferramentas de apoio serão aquelas que habilitem a execução dos serviços de pentest.

7. FERRAMENTA(S) DE APOIO PARA SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

7.1. REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADE DE SOLUÇÃO EDUCACIONAL CONTRA-ATAQUE DE PHISHING

7.1.1. A solução deve possuir sua própria estrutura de envio de e-mails (Servidores SMTP), não onerado os recursos do CONTRATANTE para o envio dos e-mails de simulação;

7.1.2. A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos;

7.1.3. A solução educacional contra-ataque de Phishing deve ser capaz de criar templates educacionais exclusivos para o CONTRATANTE, em português com a logo marca do CONTRATANTE;

7.1.4. A solução educacional contra-ataque de Phishing deve possibilitar na visão do usuário atacado a inserção de dados, no entanto, sejam eles quais forem os dados não devem ser armazenados de nenhuma forma, em nenhuma área de armazenamento, sejam internas a solução quanto externa;

7.1.5. A solução educacional contra-ataque de Phishing deve ser capaz de, durante a criação do e-mail template customizado para o CONTRATANTE, conter no mínimo as parametrizações abaixo:

7.1.5.1. Seleção de usuário e de grupo de usuários que farão parte da simulação;

7.1.5.2. Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, especifica por grupo a ser atingido;

7.1.5.3. Definição de assunto do e-mail de simulação do ataque Phishing;

7.1.5.4. Definição do nome do remetente que enviará o e-mail de simulação do ataque Phishing; Definição do endereço (usuário e domínio) do e-mail de simulação do ataque Phishing.

7.1.6. A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:

7.1.6.1. Nome do usuário;

7.1.6.2. Sobrenome;

7.1.6.3. Endereço de e-mail;

7.1.7. A solução educacional contra-ataque de Phishing deve ser capaz de criar relatórios executivos e mostrar de forma gráfica no console do produto no mínimo:

7.1.7.1. Verificação de quantas simulações foram enviadas para o CONTRATANTE;

7.1.7.2. Verificação de quantos usuários acessaram o e-mail de simulação de ataque Phishing;

7.1.7.3. Verificação de quantos usuários abriram o arquivo anexo do e-mail de simulação de ataque Phishing;

7.1.7.4. Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque Phishing; Verificação de quantos usuários reportaram para a área de TI a existência de um ataque Phishing;

7.1.7.5. Verificação de quantos usuários executaram os módulos de conscientização educacional Anti-Phishing;

7.1.8. A solução educacional contra-ataque de Phishing deve ser capaz de construir uma mensagem de conscientização, informando que usuário foi pego em uma simulação de ataque Phishing, a qual deve ser mostrada no momento que seja caracterizado como se o usuário estivesse realmente sofrido um ataque;

7.1.9. A solução educacional contra-ataque de Phishing deve ser capaz de indicar a necessidade de o usuário participar de uma campanha para conscientização, a partir da mensagem de conscientização (item anterior) na qual deverá existir um link direcionando para a campanha indicada para o usuário e grupos de usuários;

7.1.10. A solução educacional contra-ataque de Phishing deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização do CONTRATANTE.

8. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE PROTEÇÃO DE ENDPOINTS E SERVIDORES DE REDE

8.1. REQUISITOS DA FERRAMENTA EM TERMOS GERAIS

8.1.1. A solução deve oferecer a possibilidade de integração via API nos seus diversos módulos;

8.1.2. A solução deve permitir a criação de permissões de utilização a nível de usuário Role Based Access Control (RBAC);

8.1.3. A solução deve ter a capacidade de carregar/alterar usuários em massa bem como seus tipos de funções;

8.1.4. A solução deve possuir recursos de registros de auditoria para que possamos monitorar quando e onde nossos usuários finais fizeram o login no aplicativo;

8.1.5. A solução e seus módulos deverão estar licenciadas para número ilimitado de usuários e administradores.

8.2. REQUISITOS DA FERRAMENTA PARA CONSOLE DE GERÊNCIA

8.2.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa;

8.2.2. Deve possibilitar instalação "silenciosa", podendo utilizar de scripts, ou soluções para deploy e upgrade de software, sem a interação do usuário final;

8.2.3. "A solução deve possibilitar limitar ou bloquear a execução de aplicativos por hash, nome do arquivo, nome do aplicativo ou versão do aplicativo ou outra forma, ainda que em armazenamento externo e removível."

8.2.4. Deve permitir o rastreamento e bloqueio de infecções;

8.2.5. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

8.2.6. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

8.2.7. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente, desde que seja suportado pela solução atual;

8.2.8. Deve permitir a desinstalação através do console de gerenciamento da solução;

8.2.9. Deve ter a possibilidade de exportar/importar configurações da solução através do console de gerenciamento;

8.2.10. A solução deve permitir a geração de backup ou snapshots da base de dados de forma periódica e dos demais componentes (configurações, chaves criptográficas e/ou certificados) através do console de gerenciamento ou em momento de implementação da solução;

8.2.11. Deve ter a possibilidade de determinar a capacidade ou prazo de armazenamento da área de quarentena;

8.2.12. Deve permitir a deleção dos arquivos quarentemados;

8.2.13. Deve permitir remoção automática de clientes inativos por determinado período;

8.2.14. Identificar através da integração com o Active Directory ou LDAP, a partir da solução de segurança, quais máquinas estão sem a solução de antivírus instalada;

8.2.15. Deve permitir que a solução utilize consulta externa a base de reputação (sites ou arquivos) integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão ou protegendo contra execução de forma automática baseado na resposta à consulta da base do fabricante;

8.2.16. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

8.2.17. Deve permitir agrupamento automático de estações de trabalho e notebooks do console de gerenciamento baseando-se no escopo do Active Directory ou IP;

8.2.18. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

8.2.19. Deve possuir solução de reputação de sites ou arquivos, de forma local, para ameaças já conhecidas, integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão ou protegendo contra execução de forma automática, baseado na resposta à consulta da base do fabricante;

8.2.20. Deve registrar no sistema de monitoração de eventos do console de antivírus informações relativas ao usuário autenticado no sistema operacional quando detectada infecção;

8.2.21. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento do console de antivírus;

8.2.22. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento do console de antivírus, que não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

8.2.23. Deve prover segurança através de SSL para as comunicações entre o servidor e o console de gerenciamento web ou console MMC;

8.2.24. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

8.2.25. Deve permitir a criação de usuários locais de administração do console de antivírus;

8.2.26. Deve possuir a integração com o Active Directory ou LDAP para utilização de seus usuários para administração do console de antivírus;

8.2.27. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes do console de gerenciamento;

8.2.28. Deve bloquear acessos indevidos à área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

8.2.29. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

8.2.30. Deve permitir a gerência de domínios separados para usuários previamente definidos;

8.2.31. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido no console de administração, caso haja falha na limpeza de arquivos maliciosos;

8.2.32. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto, ou categorizar com metodologia similar de reputação determinada pelo fabricante;

8.2.33. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou implementar níveis de permissionamento granular possibilitando acesso somente ao conteúdo devido;

8.2.34. Os blocos de informações pertencentes aos painéis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos ou implementar níveis de permissionamento granular possibilitando acesso somente ao conteúdo devido;

8.2.35. A seleção de uma informação específica sobre um evento malicioso, através de um clique, deve redirecionar às informações mais detalhadas, tais como: qual foi a ameaça, como ela é detectada e mitigada, e a possível solução de contorno.

8.3. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO AVANÇADA PARA SERVIDORES WINDOWS / LINUX**

8.3.1. Permitir a implantação dos módulos de segurança citados, no mínimo para os seguintes sistemas operacionais: Windows Server 2012 ou superior e Sistemas Operacionais Linux, no mínimo para as distribuições: Red Hat, Suse, CentOs, Debian e Ubuntu.

8.3.2. Possuir a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais a partir de uma console única e centralizada do mesmo fabricante;

8.3.3. Executar rastreamento nas máquinas virtuais e fornecer lista de todas as recomendações de segurança para os softwares que estiverem instalados nessas máquinas virtuais, bem como do sistema operacional;

8.3.4. Proteger de forma automática e transparente contra brechas de segurança descobertas, interrompendo somente o tráfego de rede malicioso;

8.4. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE FIREWALL**

8.4.1. Operar como firewall de host stateful bidirecional, monitorando as comunicações nos servidores protegidos;

8.4.2. Possuir a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

8.4.3. Possuir a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

8.4.4. Permitir que regras de Firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

8.4.5. Permitir que as regras de Firewall executem as seguintes ações, ou equivalentes: Allow, Log Only, bypass, force allow, deny;

8.4.6. Permitir realizar pseudo stateful em tráfego UDP;

8.4.7. Permitir limitar o número de conexões entrantes e de saída de um determinado IP de origem;

8.4.8. Permitir a criação de novas regras utilizando templates padrão;

8.4.9. Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para monitoração e alertas.

8.5. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE INSPEÇÃO DE PACOTES**

8.5.1. Possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

8.5.2. Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do SO e demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações;

8.5.3. Permitir execução de varreduras sob demanda ou agendada;

8.5.4. Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão.

8.5.5. Permitir que a opção de detecção e bloqueio seja implementada de forma global (todas as regras) ou apenas para uma regra ou grupos de regras;

8.5.6. Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais:

8.5.7. Windows 2012 ou superior;

8.5.8. Red Hat, Suse, CentOs, Debian e Ubuntu;

8.5.9. Aplicações padrão de mercado, tais como: Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.

8.5.10. Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque;

8.5.11. Possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

8.5.12. Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting;

8.5.13. Implementar a customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

8.5.14. Permitir configuração de regras de IDS/IPS diferenciadas de acordo com horário ou dia da semana;

8.5.15. Deverá ser capaz de proteger tráfego incoming SSL;

8.5.16. Apresentar informações detalhadas das regras de blindagem contra vulnerabilidades, contendo links com referências externas, quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

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

8.5.18. Permitir habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

8.5.19. Permitir que as regras de IPS atuem detectando ou bloqueando os eventos que as violem, de modo que o administrador possa decidir qual ação deva ser tomada;

8.5.20. Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para monitoração e alertas;

8.5.21. Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host.

8.6. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE MONITORAMENTO DE INTEGRIDADE**

8.6.1. Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

8.6.2. Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais Linux;

8.6.3. Possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;

8.6.4. Possuir a capacidade de monitorar mudanças efetuadas no registro do Windows;

8.6.5. Possuir a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e, customização para criação de regras avançadas;

8.6.6. Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura;

8.6.7. Permitir execução de varreduras sob demanda ou agendada;

8.6.8. Rastrear arquivos por criação, última modificação, último acesso, permissões, proprietário, grupo, tamanho, SHA1, SHA256 e Flags;

8.6.9. Gerar alertas toda vez que uma modificação ocorrer, em tempo real para ambiente Windows e, pseudo tempo real para ambiente Linux utilizando agente;

8.6.10. Registrar em relatório todas as modificações que ocorram nos objetos monitorados;

8.6.11. Classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

8.6.12. Possibilitar a escolha do diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

8.7. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE INSPEÇÃO DE LOG'S**

8.7.1. Possuir capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

8.7.2. Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura;

8.7.3. Permitir execução de varreduras sob demanda ou agendada;

8.7.4. Permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

8.7.5. Permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

8.7.6. Implementar inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor;

8.7.7. Permitir modificar as regras por severidade de ocorrência de eventos;

8.8. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE ANTI-MALWARE E REPUTAÇÃO WEB**

8.8.1. Permitir a proteção em tempo real contra códigos maliciosos, possibilitando a tomada de ações distintas para cada tipo de ameaça;

8.8.2. Permitir execução de varreduras sob demanda ou agendada;

8.8.3. Possibilitar a criação de listas de exclusão para processos, diretórios ou arquivos do SO;

8.8.4. Possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

8.8.5. Implementar a proteção contra acesso a websites ou URLs consideradas maliciosas, de baixa reputação ou não categorizadas;

8.8.6. Permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema.

8.9. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE CONTROLE DE APLICAÇÃO**

8.9.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

8.9.2. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256

8.9.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash é por máquina;

8.9.4. A console deverá exibir eventos de no mínimo 30 dias;

8.9.5. A solução deverá possuir funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente;

8.10. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADES DE GERENCIAMENTO**

8.10.1. Permitir o envio de notificações via SMTP;

8.10.2. Permitir o envio de registros de logs a um servidor remoto;

8.10.3. Implementar gravação de eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;

8.10.4. Permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;

8.10.5. Permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

8.10.6. Permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;

8.10.7. Armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados Oracle e MS SQL;

8.10.8. Permitir opções de permissionamento, no mínimo, para modos de visualização e edição de políticas;

8.10.9. Permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários;

8.10.10. Possuir dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

8.10.11. Possuir a capacidade de criar políticas de forma global para todas as máquinas virtuais, por perfis e individualmente para cada host;

8.10.12. Prover perfis padrões pré-definidos e aptos a funcionar de acordo com sua denominação;

8.10.13. Permitir o envio de eventos da console via SNMP;

8.10.14. Permitir o rollback de atualização de regras pela console de gerenciamento;

8.10.15. Gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

8.10.16. Possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;

8.10.17. Possuir a capacidade de classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.

8.11. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO ANTI-MALWARE WINDOWS ESTAÇÕES DE TRABALHO E NOTEBOOKS**

8.11.1. Deve ser capaz de realizar a proteção contra a execução de códigos maliciosos nos seguintes sistemas operacionais: Windows 7 SP1 (x86/x64), Windows 8 e 8.1 (x86/x64), Windows 10 (x86/x64);

8.11.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

8.11.3. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, ransomware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

8.11.4. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

8.11.4.1. Processos em execução em memória principal (RAM);

8.11.4.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

8.11.4.3. Arquivos compactados automaticamente em, pelo menos, os seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

8.11.4.4. Aprendizado de máquina (Machine Learning) e análise comportamental (Behavioral Analysis);

8.11.4.5. Arquivos recebidos por meio de programas de comunicação instantânea (skype, yahoo messenger, google talk, icq, dentre outros).

8.11.5. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens, tais como javascript, vbscript/Activex;

8.11.6. Deve possuir detecção heurística de vírus desconhecidos;

8.11.7. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

8.11.8. Deve permitir diferentes modos de detecção (varredura ou rastreamento):

8.11.9. Em tempo real de arquivos acessados pelo usuário;

8.11.10. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

8.11.11. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

8.11.12. Por linha-de-comando, parametrizável;

8.11.13. A solução deve permitir rastreamento automático do sistema com as seguintes opções:

8.11.13.1. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

8.11.13.2. Ação: somente alertas via smtp e snmp, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena). Deverá ser possível configurar a aplicação de duas ações ao mesmo tempo;

8.11.13.3. Frequência: horária, diária, semanal e mensal;

8.11.13.4. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

8.11.14. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

8.11.15. Deve permitir alteração/modificação do tempo de assinatura do cache pelo administrador;

8.11.16. Deve permitir a utilização de Centro de Inteligência de reputação para análise granular de arquivos ou URL's maliciosas, de modo a prover rápida detecção de novas ameaças;

8.11.17. Em caso de problemas com a conectividade com a rede deverá ser possível manter uma base local para consulta de no mínimo hash de arquivos ou URL's maliciosas;

8.11.18. Deve ser capaz de aferir a reputação das URL's ou arquivos acessados pelas estações de trabalho e notebooks, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

8.11.19. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

8.11.20. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante ou implementar a proteção apenas a parte maliciosa do site, possibilitando acesso somente a conteúdo confiável;

8.11.21. Deve permitir a restauração de maneira granular de arquivos quarentemados sob suspeita de representarem risco de segurança;

8.11.22. Deve ser capaz de criar White List / Blacklist dos sites acessados.

8.11.23. Deve permitir a adição às listas de exclusão/arquivos conhecidos de modo a evitar novas detecções dos arquivos no ambiente de gestão da solução de endpoint;

8.12. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO ANTI-MALWARE ESTAÇÕES DE TRABALHO MAC OS X**

8.12.1. Compatibilidade com Mac OS 10.13 ou superior.

8.12.2. Suporte ao Apple Remote Desktop para instalação remota da solução;

8.12.3. Gerenciamento integrado à console de gerência central da solução;

8.12.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, ransomware, adwares e outros tipos de códigos maliciosos;

8.12.5. Permitir a verificação das ameaças da maneira manual e agendada;

8.12.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

8.12.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infecções a arquivos;

8.12.8. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

8.12.9. Deve possuir no mecanismo de autoproteção as seguintes proteções:

8.12.9.1. Proteção e verificação dos arquivos de assinatura;

8.12.9.2. Proteção dos processos do agente de segurança;

8.12.9.3. Proteção do diretório de instalação do agente de segurança.

8.13. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO PARA SMARTPHONES E TABLETS**

8.13.1. Compatibilidade:

8.13.1.1. Apple iOS 6.x ou superior.

8.13.1.2. Android OS 4.x, 5.x ou superior.

8.13.1.3. Deverá prover para Android proteção em tempo real do sistema de arquivos do dispositivo, interceptação e verificação de todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.

8.13.1.4. Arquivos abertos no smartphone Android.

8.13.1.5. Programas instalados usando a interface do smartphone.

8.13.2. Deverá prover proteção por meio da verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

8.13.3. Deverá isolar em área de quarentena os arquivos infectados.

8.13.4. Deverá atualizar as bases de vacinas de modo agendado.

8.13.5. Deverá bloquear spam de SMS por meio de Black Lists.

8.13.6. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

8.13.7. Deverá ter a funcionalidade de instalação remota através de MDM.

8.13.8. Capacidade de detectar Jailbreak em dispositivos iOS.

8.13.9. Capacidade de bloquear no Android o acesso a site por reputação em dispositivos.

8.13.10. Capacidade de bloquear no Android o acesso a sites phishing ou malicioso.

8.13.11. Capacidade de configurar no Android White e Black Lists de aplicativos.

8.13.12. Capacidade de ajustar as configurações de:

8.13.12.1. Uso de aplicativos;

8.13.12.2. Senha do usuário;

8.13.12.3. Conexão de mídia removível;

8.13.13. Capacidade de instalar certificados digitais em dispositivos móveis;

8.13.14. Capacidade de reinicializar a senha de dispositivos iOS;

8.13.15. Capacidade de bloquear um dispositivo iOS;

8.14. **REQUISITOS DA FERRAMENTA PARA SOLUÇÃO DE ANTIVÍRUS – CRIPTOGRAFIA**

8.14.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais Windows: Windows Windows 7 (x86/x64), Windows 8 e 8.1 (x86/x64) e Windows 10 (x86/x64) e superior;

8.14.2. Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para: disco completo (FDE – full disk encryption), pastas e arquivos, mídias removíveis, anexos de e-mails e automática de disco;

8.14.3. Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

8.14.4. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

8.14.5. Possuir suporte ao algoritmo de criptografia AES-256;

8.14.6. Possuir a capacidade de exceções para criptografia automática;

8.14.7. Possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

8.14.8. Possuir certificação FIPS 140-2;

8.14.9. Possuir funcionalidade de criptografia por software ou hardware;

8.14.10. Ser compatível com os padrões SED (self-encrypting drive), Opal e Opal2;

8.14.11. Possuir compatibilidade com autenticação por múltiplos fatores;

8.14.12. Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

8.14.13. Possuir a possibilidade de configurar senha de administração local na estação de trabalho para desinstalação do módulo;

8.14.14. Possuir políticas por usuários, grupos e dispositivos;

8.14.15. Possuir no mínimo 02 métodos de autenticação seguintes para desbloquear um disco:

8.14.16. Autenticação com Active Directory, single sign-on com Active Directory, senha pré-definida, número pin e smart card;

8.14.17. Possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas ou procedimento com objetivo similar;

8.14.18. O ambiente de autenticação pré-inicialização deve permitir a mudança do leiaute do teclado;

8.14.19. Prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

8.14.20. Permitir a gerência ou a integração com as seguintes soluções terceiras de criptografia: Microsoft Bitlocker e Apple Filevault;

8.14.21. A partir do console de administração centralizada ou através de procedimentos de administração deve ser possível:

8.14.21.1. Permitir a visualização das estações de trabalho que tenham aplicação de política pendente;

8.14.21.2. Permitir a visualização do autor de determinada política;

8.14.21.3. Permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir do console de administração;

8.14.21.4. Permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

8.14.21.5. Permitir a exibição de aviso legal quando a estação é inicializada;

8.14.21.6. Permitir, em nível de política, a indicação de pastas a serem criptografadas;

8.14.21.7. Possibilitar que cada política ou usuário tenha uma chave de criptografia única;

8.14.21.8. Permitir, em nível de política ou usuário, a escolha da chave de criptografia a ser utilizada;

8.14.21.9. Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

8.14.21.10. Possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho.

8.15. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO E CONTROLE DE DISPOSITIVOS**

8.15.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções:

8.15.1.1. Acesso total;

8.15.1.2. Leitura e escrita;

8.15.1.3. Leitura e execução;

8.15.1.4. Apenas leitura;

8.15.1.5. Bloqueio total;

8.15.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como CDROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

8.15.3. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

8.15.4. Capacidade de bloquear modens nas entradas USB;

8.15.5. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

8.15.6. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CDROM) mesmo com a política de bloqueio total ativa.

8.16. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO HOST IPS E HOST FIREWALL**

8.16.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais Windows e Linux;

8.16.2. Possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS;

8.16.3. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

8.16.4. Permitir ativar e desativar o produto sem a necessidade de remoção;

8.16.5. Permitir proteção em real-time ou varredura de portas lógicas do sistema operacional para identificar quais estejam abertas e possibilitando tráfego de entrada ou saída;

8.16.6. A funcionalidade de host IPS ou host firewall deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

8.16.7. Prover proteção contra as vulnerabilidades dos sistemas operacionais Windows e Linux por meio de regras de host IPS;

8.16.8. Deve ser capaz de listar as vulnerabilidades dos sistemas operacionais Windows e Linux;

8.16.9. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura contra-ataques dia zero;

8.16.10. Deve ser capaz de identificar e bloquear ataques conhecidos através de assinaturas;

8.16.11. A atualização de assinaturas não deve exigir reinício do sistema operacional;

8.16.12. Deve executar proteção em real-time ou efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host IPS para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

8.16.13. A varredura de segurança deve ser capaz de identificar as regras de host IPS que não são mais necessárias e desativá-las. Na proteção em real-time as proteções devem estar sempre ativas;

8.16.14. Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host IPS, tais como Oracle Java, Adobe Reader, Adobe Flash Player, Realnetworks Real Player, Microsoft Office, Apple iTunes, Apple Quick Time, Apple Safari, Google Chrome, Mozilla Firefox, Opera Browser, Microsoft Internet Explorer, entre outras;

8.16.15. Deve fornecer proteção contra vulnerabilidades existentes nas estações de trabalho;

8.16.16. Deve proteger contra-ataques locais iniciados por CD's ou dispositivos USB;

8.16.17. Deve proteger contra-ataques que trafegam por fluxos criptografados;

8.16.18. Deve proteger contra-ataque de negação de serviço;

8.16.19. Deve proteger contra tentativas de invasão;

8.16.20. Deve possuir proteção contra BOTs;

8.16.21. Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

8.16.22. Deve permitir a criação de políticas de segurança personalizadas;

8.16.23. Deve permitir bloquear conexões ou limitar o número de conexões simultâneas no sistema operacional;

8.16.24. A solução deve permitir a emissão de alertas via SMTP e SNMP;

8.16.25. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

8.16.26. Deve permitir criar regras com base nos seguintes parâmetros:

8.16.26.1. Descrição;

8.16.26.2. Ação;

8.16.26.3. Direção;

8.16.26.4. Protocolo de Rede;

8.16.26.5. Aplicação e Executáveis;

8.16.26.6. Tempo de aplicação da regra.

8.16.27. Deve possuir integração com o Centro de Inteligência do fabricante para verificar a reputação do endereço IP e informar quatro níveis ou categorizar com metodologia similar de reputação determinada pelo fabricante:

8.16.27.1. Mínimo;

8.16.27.2. Não verificado;

8.16.27.3. Médio;

8.16.27.4. Alto.

8.16.28. Para evitar consumo de banda, a solução deve manter um cache para este tipo de consulta;

8.16.29. Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;

8.16.30. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

8.16.31. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

8.16.32. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou implementar níveis de permissionamento granular possibilitando acesso somente ao conteúdo devido;

8.16.33. Os blocos de informações pertencentes aos painéis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos ou implementar níveis de permissionamento granular possibilitando acesso somente ao conteúdo devido;

8.16.34. A seleção de uma informação específica sobre um evento malicioso, através de um clique, deve redirecionar as informações mais detalhadas tais como qual foi a ameaça, como ela é detectada e mitigada (se for o caso) e a possível solução de contorno;

8.17. **REQUISITOS DA FERRAMENTA PARA CONTROLE DE APLICAÇÕES**

8.17.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos sistemas operacionais Windows;

8.17.2. Deve permitir a criação de políticas de segurança personalizadas;

8.17.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

8.17.3.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

8.17.3.2. Range de endereços IPs;

8.17.3.3. Sistema operacional;

8.17.3.4. Usuários, máquinas ou grupos do Active Directory/OpenLDAP.

8.17.4. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

8.17.5. A solução deve permitir a verificação dos logs que serão analisados de acordo com os seguintes critérios:

8.17.5.1. Nenhum;

8.17.5.2. Somente bloqueios;

8.17.5.3. Somente regras específicas;

8.17.5.4. Todas as aplicações executadas.

8.17.6. A solução de segurança deve permitir o controle do intervalo de envio dos logs;

8.17.7. A solução de segurança deve permitir o controle do intervalo para envio de atualização de cada política;

8.17.8. A solução de segurança deve permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

8.17.9. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;

8.17.10. A solução de segurança deve permitir o controle do intervalo de quando os inventários de aplicações são executados ou implementar o controle de aplicações e dispositivos em real-time;

8.17.11. As políticas de segurança devem permitir o controle através de regras de aplicação;

8.17.12. As regras de controle de aplicação devem permitir as seguintes ações:

8.17.12.1. Permissão de execução;

8.17.12.2. Bloqueio de execução;

8.17.12.3. Bloqueio de novas instalações.

8.17.13. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

8.17.14. As funcionalidades de controle de aplicação ou reputação devem permitir os seguintes métodos para identificação das aplicações:

8.17.14.1. Hash do executável;

8.17.14.2. Atributos do certificado utilizado para assinatura digital do executável;

8.17.14.3. Caminho lógico do executável;

8.17.14.4. Base de assinaturas de certificados digitais válidos e seguros.

8.17.15. As regras de controle de aplicação devem possuir categorias de aplicações;

8.17.16. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

8.17.17. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou implementar níveis de permissionamento granular possibilitando acesso somente ao conteúdo devido;

8.17.17.1. Os blocos de informações pertencentes aos painéis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos ou implementar níveis de permissionamento granular possibilitando acesso somente ao conteúdo devido;

8.17.17.2. A seleção de uma informação específica sobre um evento malicioso, através de um clique, deve redirecionar as informações mais detalhadas tais como qual foi a ameaça, como ela é detectada e mitigada (se for o caso) e a possível solução de contorno.

8.18. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO CONTRA VAZAMENTO DE INFORMAÇÕES (DLP)**

8.18.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:Windows Server 2012 (32/64-bit) ou superior, Windows 7 SP1 (x86/x64), Windows 8 e 8.1 (x86/x64), Windows 10 (x86/x64) e superior.

8.18.2. Deve possuir, nativamente, templates para atender as seguintes regulamentações: PCI/DSS, HIPA, Glba, SB-1386, US PII.

8.18.3. Deve ser capaz de detectar informações, em documentos nos formatos:

8.18.3.1. Microsoft Office (doc, docx, xls, xlsx, ppt, pptx)

8.18.3.2. OpenOffice;

8.18.3.3. rtf, wordpad, text; xml, html;

8.18.3.4. Gráficos: visio, postscript, pdf, tiff,

8.18.3.5. Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2,

8.18.3.6. unix/linux zip, lzh;

8.18.3.7. Códigos: C/C++, Java, Verilog, Autocad, .js, .vbs e demais arquivos de Script;

8.18.4. Deve ser capaz de detectar informações, com base em:

8.18.4.1. Dados estruturados, dados pessoais, endereços de e-mail, CPF, entre outros;

8.18.4.2. Palavras ou frases configuráveis;

8.18.4.3. Expressões regulares;

8.18.4.4. Extensão dos arquivos.

8.18.5. Deve ser capaz de detectar em arquivos compactados;

8.18.6. Deve permitir a criação de modelos personalizados para identificação de informações;

8.18.7. Deve permitir a criação de políticas personalizadas;

8.18.8. Deve permitir a criação de políticas baseadas em múltiplos modelos;

8.18.9. Deve permitir mais de uma ação para cada política, como:

8.18.9.1. Apenas registrar o evento da violação;

8.18.9.2. Bloquear a transmissão;

8.18.9.3. Gerar alertar para o usuário;

8.18.9.4. Gerar alertar na central de gerenciamento;

8.18.9.5. Capturar informação para uma possível investigação da violação.

8.18.10. Deve permitir criar regras distintas com base se a estação está fora ou dentro do ambiente físico da **ANA**;

8.18.11. Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

8.18.11.1. Cliente de e-mail;

8.18.11.2. Protocolos HTTP, HTTPS, FTP;

8.18.11.3. Mídias removíveis;

8.18.11.4. Discos óticos CD/DVD;

8.18.11.5. Gravação CD/DVD;

8.18.11.6. Aplicações de mensagens instantâneas;

8.18.11.7. Tecla de print screen;

8.18.11.8. Aplicações P2P;

8.18.11.9. Área de transferência do Windows;

8.18.11.10. Webmail;

8.18.11.11. Armazenamento na nuvem (cloud);

8.18.11.12. Impressoras;

8.18.11.13. Scanners;

8.18.11.14. Compartilhamentos de arquivos;

8.18.11.15. Activesync;

8.18.11.16. Criptografia PGP;

8.18.12. Deve permitir a criação de exceções nas restrições dos meios de transmissão.

8.19. **REQUISITOS DA FERRAMENTA PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADOS**

8.19.1. A solução deve possuir funcionalidades para detecção avançada de ameaças.

8.19.2. Deve possuir proteção contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow).

8.19.3. Deve oferecer proteção proativa contra-ataques de dia zero (zero-day attacks).

8.19.4. Deve possuir tecnologia de análise de comportamentos suspeitos para detecção e eliminação de ameaças desconhecidas.

8.19.5. A solução deverá prover as funcionalidades de proteção inbound (tráfego de entrada) de malware com filtro de ameaças avançadas e análise de execução em tempo real, bem como proteção outbound (tráfego de saída).

8.19.6. Implementar modo de configuração totalmente transparente para o usuário final, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego na estação de trabalho;

8.19.7. Capacidade de detecção malware, keyloggers, trojans, spyware, worms e assemelhados por comportamento dos processos em memória.

8.19.8. Implementar engine específica para cada malware e/ou códigos maliciosos;

8.19.9. Implementar mecanismo de detecção heurística, detecção por fingerprints ou semelhante para verificação de ameaça direcionada, com possibilidade de ação imediata de eliminação e possível restauração de dados.

8.20. **REQUISITOS DA FERRAMENTA PARA GERENCIAMENTO CENTRALIZADO**

8.20.1. Suportar o gerenciamento a partir de um ponto de acesso único para todos os componentes da soluçã ou múltiplas consoles para gerenciamento;

8.20.2. Gerenciar, sem perda de desempenho, logs de grande volume das atividades e eventos gerados pela solução;

8.20.3. Suportar base de dados SQL;

8.20.4. Integrar-se com o LDAP e Active Directory;

8.20.5. Permitir níveis de administração por usuários, máquinas ou grupos;

8.20.6. Permitir o gerenciamento do servidor a partir de console instalada em outra máquina;

8.20.7. Permitir a constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis à grupos de usuários;

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

8.20.9. Permitir criação de templates de relatórios customizados;

8.20.10. Gerar relatórios e gráficos com o detalhamento da conformidade dos patches aplicados;

8.20.11. Geração de relatórios e gráficos pré-formatados e parametrizáveis, com saídas em html ou pdf;

8.20.12. Permitir exportação dos relatórios e gráficos para os seguintes formatos: html, pdf (relatórios);

8.20.13. Deve prover painéis de gerenciamento e exibam continuamente métricas-chave, tais como tempo de permanência sem incidentes de segurança, vulnerabilidades pendentes, tempo de contenção, infecções remediadas, grupos de usuários que mais oferecem riscos de segurança etc.;

8.20.14. Deve permitir a criação de painéis e relatórios customizados;

8.20.15. Deve permitir a exportação dos dados de painéis e relatórios, no mínimo, nos formatos PDF e CSV;

8.20.16. Deve possibilitar o agendamento de relatórios cujo conteúdo seja encaminhado por e-mail ou para um servidor de arquivos, para um destino definido pelo administrador;

8.20.17. Permitir o gerenciamento do servidor através do protocolo TCP/IP, em modo cliente servidor, ou múltiplas camadas com uso de HTTP/HTTPS;

8.20.18. Permitir o gerenciamento das ferramentas nos clientes a partir de um único servidor;

8.20.19. Permitir a alteração das configurações das ferramentas nos clientes e servidores, remotamente;

8.20.20. Permitir a atualização dinâmica de listas de assinaturas e regras (de vírus, filtros de IDS etc.) com frequência, no mínimo, diária e horária definida pelo usuário;

8.20.21. Permitir a atualização incremental da lista de definições de vírus nos clientes a partir da rede local;

8.20.22. Permitir atualização, verificação de vírus e upgrades em períodos pré-determinados, na inicialização do sistema operacional ou no logon na rede;

8.20.23. Permitir o armazenamento das informações coletadas nos clientes em uma base de dados centralizada;

8.20.24. Permitir diferentes níveis de administração do servidor, independentemente do login da rede;

8.20.25. Possibilitar a criação de grupos de máquinas baseadas em regras definidas em função do endereço IP do cliente;

8.21. **REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADE DE ATUALIZAÇÃO**

8.21.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

8.21.2. Deve permitir atualização incremental da lista de definições de vírus para as seguintes situações:

8.21.2.1. Servidor baixar diretamente da internet;

8.21.2.2. Servidor atualizando de outro servidor;

8.21.2.3. Cliente atualizando de um servidor;

8.21.2.4. Cliente atualizando de outro cliente.

8.21.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

8.21.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

8.21.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, independentemente da versão do sistema operacional Windows, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações;

8.21.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, hotfix;

8.21.7. O servidor da solução de antivírus deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

8.21.8. Deve possibilitar que o administrador verifique nos registros de atualizações dos endpoints, se as mesmas foram realizadas através da console de gerenciamento central ou do agente replicador;

8.21.9. O agente replicador de atualizações e configurações deve ser capaz de gerar localmente versões incrementais das vacinas a serem distribuídas para os demais endpoints de proteção, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

8.21.10. A atualização de hotfix, service packs, versão do produto entre servidores e clientes deverá permitir ser realizada tanto de forma automática quanto de forma manual.

9. FERRAMENTA(S) DE APOIO A GESTÃO DE MENSAGERIA PROATIVA

9.1. REQUISITOS DA FERRAMENTA PARA GESTÃO DE MENSAGERIA PROATIVA

9.1.1. O produto deve oferecer sistema de reputação de IP em tempo real para detectar e bloquear mensagens de SPAMs;

9.1.2. Deve suportar organização de fila por prioridade de acordo com a reputação;

9.1.3. Deve suportar as seguintes tecnologias para detectar e filtrar a entrada de e-mails indesejados em nível de transmissão:

9.1.3.1. A verificação de DNS reverso (RDNS);

9.1.3.2. SPF (Sender Policy Framework);

9.1.3.3. Lista de autorizados/lista negra;

9.1.3.4. Ataque de captura de diretório (harvest attack);

9.1.3.5. Verificação de remetente/destinatário.

9.1.4. Deve oferecer o recurso de controle de conexão e controle de frequências de mensagens recebidas e enviadas, respectivamente;

9.1.5. Deve suportar lista de autorizados e lista negra (Nível corporativo e nível de usuário) baseados em IP/endereço/domínio;

9.1.6. O banco de dados de assinaturas do antispam deve ser atualizado por padrão a cada hora ou em uma frequência configurável;

9.1.7. Deve suportar classificação de URL dos links embutidos para uma melhor detecção de SPAM;

9.1.8. Deve oferecer recurso de detecção de spam baseado em imagem como, por exemplo, imagens pornográficas dentro do e-mail. Com este recurso, deve ser possível ajustar o nível de sensibilidade;

9.1.9. Deve oferecer um recurso de varredura de anexos (com um amplo espectro de tipos de anexos que podem ser varridos) para detectar mensagens de spam baseado em arquivo;

9.1.10. Deve suportar varredura de dicionários dos tipos Adulto, Procura de Emprego, Jogos de Azar, Drogas, Conteúdo Ofensivo, Armas e Violência, e possibilitar a criação de dicionários customizados;

9.1.11. Para as mensagens detectadas como spam, deve possuir a possibilidade de entregar ou enviar para a quarentena;

9.1.12. As mensagens detectadas como SPAM posicionadas na fila de quarentena devem possuir os seguintes controles:

9.1.12.1. Entregar;

9.1.12.2. Excluir;

9.1.12.3. Reprocessar;

9.1.12.4. Continuar processando;

9.1.12.5. Encaminhar;

9.1.12.6. Download;

9.1.12.7. Adicionar para a lista bloquear sempre;

9.1.12.8. Adicionar para a lista permitir sempre.

9.1.13. Deve possuir perfil de administrador específico para acesso a quarentena, de modo que apenas o administrador designado possa buscar e manipular a mensagem na fila;

9.1.14. Deve possuir a possibilidade de reportar os e-mails falso positivos. Deve haver um botão na fila de quarentena em que permita a obtenção de um relatório;

9.1.15. Deve possuir a configuração de análise Léxica para detecção de SPAM permitindo customização;

9.1.16. Deve possuir a configuração de análise Heurística para detecção de SPAM permitindo customização;

9.1.17. Deve contar com engine de Antivírus;

9.1.18. Deve possuir as opções de permitir e mover para quarentena os e-mails com um vírus detectado;

9.1.19. Deve oferecer métodos proativos de detecção dos novos vírus (Zero Day) presentes nos e-mails;

9.1.20. O mecanismo de antivírus deve ser capaz de remover os anexos infectados;

9.1.21. Deve detectar URLs com risco de segurança, conhecidos ou suspeitos, embutidos no e-mail que sejam indicadores de ataques de spyware, malware ou phishing;

9.1.22. Deve permitir o gerenciamento da quarentena de vírus, sendo possível acessar e manipular e-mails com vírus em quarentena;

9.1.23. O mecanismo de detecção de vírus deve suportar varredura para as direções inbound, outbound e interno.

9.1.24. Deve permitir a configuração de mensagem de saudação de SMTP, tempo de retardo e FQDN (Full Qualified Domain Name) para estabelecimento da sessão SMTP;

9.1.25. Deve possuir os seguintes controles de conexão e de mensagens:

9.1.25.1. Limite de conexões simultâneas por IP e o tempo ocioso permitido;

9.1.25.2. Limite de tamanho da mensagem, volume ou os destinatários por conexão.

9.1.26. Deve oferecer prevenção de captura de diretórios (harverst attack);

9.1.27. Deve ser possível a configuração do tempo da nova tentativa em caso de falha na entrega;

9.1.28. Deve suportar autenticação interna do remetente;

9.1.29. Deve suportar grupos de usuários (OpenLDAP/Samba 3 ou AD);

9.1.30. Deve suportar roteamento/entrega baseados em domínio;

9.1.31. Deve suportar entrega em TLS baseada na política;

9.1.32. Deve possuir funcionalidade de consulta a serviço de Blacklist em tempo real;

9.1.33. Deve possuir integração com serviço de blacklist da Spamhaus nativamente ou permitir a customização de até 3 serviços de blacklist;

9.1.34. Deve suportar as seguintes tecnologias de filtragem de conteúdo:

9.1.34.1. Varredura por palavras-chave;

9.1.34.2. Varredura por expressões regulares;

9.1.34.3. Varredura por padrões avançados;

9.1.34.4. Varredura por padrões regulatórios PII, PHI e PCI DSS;

9.1.34.5. Varredura por impressões digitais (fingerprints).

9.1.35. Deve possuir recurso de gerenciamento de incidentes;

9.1.36. Deve possuir recurso de auto remediação para usuário final;

9.1.37. Deve suportar as seguintes possibilidades para notificação de eventos:

9.1.37.1. E-mail;

9.1.37.2. Pop-up;

9.1.37.3. SNMP.

9.1.38. Deve suportar gerenciamento granular de incidentes baseados em função e acesso a dados;

9.1.39. Deve suportar canal seguro TLS de servidor para servidor baseado em políticas;

9.1.40. Deve suportar criptografia de e-mail sem instalação de softwares clientes;

9.1.41. Deve suportar criptografia de e-mails baseada em nuvem;

9.1.42. Deve ter a possibilidade de integração com soluções de criptografia de terceiros;

9.1.43. Deve suportar interface (UI) web de descriptografia de e-mails;

9.1.44. Deve suportar gerenciamento centralizado, incluindo configuração de políticas, quarentenas e logs/relatórios;

9.1.45. Deve suportar interface (UI) de gerenciamento baseado na web;

9.1.46. Deve oferecer contas de administradores granulares baseadas em funções;

9.1.47. Deve oferecer recursos de alerta, incluindo e-mail e SNMP;

9.1.48. Deve suportar políticas/varredura para direções inbound, outbound e interna;

9.1.49. Deve possuir funcionalidade de backup do sistema para armazenamento local e remoto;

9.1.50. Deve possuir modelos pré-definidos de filtros, ações e políticas de tráfego;

9.1.51. Deve possuir trilha de auditoria das ações dos usuários administradores;

9.1.52. Deve suportar o painel com gráfico em tempo real e dashboard gráfico para o resumo de atividades de filtragem de e-mails;

9.1.53. Deve possuir os seguintes grupos de relatórios para escolha:

9.1.53.1. Resumo geral de mensagens;

9.1.53.2. Resumo de mensagens de recebidas;

9.1.53.3. Resumo de mensagens enviadas;

9.1.53.4. Resumo de segurança de dados;

9.1.53.5. Resumo de spam e vírus;

9.1.53.6. Resumo de transferência de mensagem;

9.1.53.7. Capacidade do sistema.

9.1.54. Deve suportar a criação de relatórios customizados nos formatos HTML, XLS e PDF, para depois salvá-los e agendar a distribuição;

9.1.55. Deve possuir a capacidade de agendamento de relatórios;

9.1.56. Deve suportar relatórios consolidados de múltiplos appliances;

9.1.57. Deve possuir gerenciamento de logs de mensagens com informações detalhadas oferecidas nos logs de acompanhamento das mensagens;

9.1.58. Deve possuir uma interface de busca de logs;

9.1.59. Os logs devem poder ser exportados para arquivos nos formatos PDF, CSV e HTML;

9.1.60. Deve possuir painel de monitoramento de fluxo de mensagens e conexões em tempo real;

9.1.61. Deve possuir as seguintes filas pré-definidas:

9.1.61.1. Vírus;

9.1.61.2. Spam;

9.1.61.3. Exceções;

9.1.61.4. Falha de criptografia;

9.1.61.5. Falha de descriptografia;

9.1.61.6. Arquivados.

9.1.62. Deve suportar a possibilidade de criação de filas customizadas;

9.1.63. Deve possuir as seguintes ações para as mensagens das filas:

9.1.63.1. Entregar;

9.1.63.2. Excluir;

9.1.63.3. Reprocessar;

9.1.63.4. Continuar processando;

9.1.63.5. Encaminhar;

9.1.63.6. Download;

9.1.63.7. Adicionar para a lista bloquear sempre;

9.1.63.8. Adicionar para a lista permitir sempre.

9.1.64. Deve suportar a função de administrador de quarenta, para usuários que devam ter permissões para acessar mensagens de filas especificas;

9.1.65. Deve possuir a possibilidade de relatar Falsos Positivos da fila;

9.1.66. Deve possuir mecanismo de busca de mensagens na fila;

9.1.67. A interface de gerenciamento pessoal de e-mails deve possuir suporte as linguagens:

9.1.67.1. Inglês;

9.1.67.2. Português.

9.1.68. Deve possuir mensagem de notificação para quando o usuário tiver um e-mail (enviado ou recebido) bloqueado;

9.1.69. A mensagem de notificação deve possuir a possibilidade de customização;

9.1.70. A mensagem de notificação deve possuir os seguintes controles para o usuário:

9.1.70.1. Não é Spam;

9.1.70.2. Entregar;

9.1.70.3. Excluir;

9.1.70.4. Adicionar para a lista bloquear sempre;

9.1.70.5. Adicionar para a lista permitir sempre.

9.1.71. O portal de gerenciamento pessoal deve possuir uma interface (UI) baseada na web.

9.1.72. Deve possuir a possibilidade de autorizar ou bloquear e-mails dentro do portal de gerenciamento pessoal;

9.1.73. O administrador deve poder especificar quais das seguintes filas podem ser acessadas pelo usuário final:

9.1.73.1. Vírus;

9.1.73.2. Spam;

9.1.73.3. Exceções.

9.1.74. Deve suportar a autenticação de usuários baseada em OpenLDAP/Samba 3 ou AD para login no portal de gerenciamento pessoal de e-mails;

9.1.75. O produto deve suportar modo híbrido (integração com solução na nuvem) para inspeção de mensagens nas direções inbound e outbound;

9.1.76. Deve suportar para configuração para redundância, balanceamento de carga e HA (High Availability, ou alta disponibilidade);

9.1.77. Deve possuir a capacidade de configurar cluster de Appliances físicos ou virtuais nativamente;

9.1.78. Deve utilizar o banco de dados Oracle ou MySQL ou Microsoft SQL Server;

9.1.79. Deve poder ser integrado com aplicativos de segurança Web e de Dados e gerenciados por uma interface (UI) centralizada;

9.1.80. Deve suportar a instalação de appliances físicos e/ou virtuais;

9.1.81. Os Appliances Virtuais devem suportar instalação em ambiente VMWare ESX/ESXi;

9.1.82. A solução deve permitir o crescimento escalável de unidades de appliances virtuais sem a necessidade de licenciamento adicional.

.

10. FERRAMENTA(S) DE APOIO A SERVIÇO DE INTELIGÊNCIA APLICADA A SEGURANÇA

10.1. REQUISITOS DA FERRAMENTA PARA FUNCIONALIDADE DE SOLUÇÃO EDUCACIONAL CONTRA-ATAQUE DE PHISHING

10.1.1. Deverá identificar, reconhecer, coletar, analisar, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis;

10.1.2. Coletar diariamente informações de pelo menos 44 fontes relevantes de inteligência sobre ameaças disponíveis pelo mundo, de categorias como phishing, código, propriedade intelectual, chaves/senhas, botnets, internet profunda (deep web), spam, aplicativos falsos e documentos confidenciais;

10.1.3. Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças;

10.1.4. Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente da ANA em questão, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança;

10.1.5. Deverá permitir o gerenciamento, configuração e utilização centralizada de todos os recursos disponibilizados;

10.1.6. Deverá possuir painel de visualização de fácil utilização e configuração, permitindo a seleção da(s) funcionalidade(s) que será(ão) utilizada(s);

10.1.7. Deverá possuir modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas;

10.1.8. Deverá ser possível, de forma simples e rápida, a alteração dos critérios de busca de informações de acordo com as necessidades da ANA;

10.1.9. Deverá fornecer análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo:

a) Visualização de perfis relacionados a palavras-chaves;

b) Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;

c) Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas;

d) Apresentação dos dados filtrados em painéis com as principais fontes identificadas na busca.

10.1.10. Possibilitar a exportação das informações identificadas nos formatos CSV, JSON, bem como a geração de relatórios em PDF;

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

10.1.12. A integração deve ser realizada por meio de API Rest;

10.1.13. Deverá identificar a emissão de certificados para domínios monitorados e de nomes similares a termos ligados à ANA;

10.1.14. Deverá identificar a criação de domínios monitorados e de nomes similares a termos pré-definidos e configuráveis;

10.1.15. Realizar o monitoramento de marcas, por palavras-chave definidas, na internet;

10.1.16. A solução deverá ser capaz de analisar imagens para identificar abuso de marca, a partir de modelos fornecidos pela ANA;

10.1.17. As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas;

10.1.18. O serviço deverá realizar a detecção de domínios registrados que possam oferecer, no mínimo:

a) Riscos de serem utilizados de forma maliciosa, variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares);

b) Descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual e seu conglomerado;

c) Capacidade de detecção de páginas de phishing por quaisquer meios disponíveis;

d) Validar domínios suspeitos em repositórios de phishing.

10.1.19. Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, IRC, Pastebin, Scribd, ReclameAQUI, Apple Store, 4Shared, Google Play, Vimeo e Github;

10.1.20. Deverá, previamente à contratação, possuir métodos de coleta de redes sociais, páginas, portais e fóruns na internet superficial, profunda e oculta ("clear web", "deep web" e "dark web");

10.1.21. Informar anomalias nos registros de nomes dos domínios monitorados ("whois", registros DNS, etc.);

10.1.22. Monitorar as BINs de cartões de crédito da ANA, mediante lista que será enviada pós contratação;

10.1.23. Realizar a análise de áudio de no mínimo 1 plataforma de mensagens, caso identifique correspondência com os critérios pesquisados, fazer a transcrição de áudio;

10.1.24. Na transcrição dos áudios analisados nos vídeos, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pela ANA;

10.1.25. O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise;

10.1.26. Realizar análise de conteúdo de imagens (OCR);

10.1.27. Identificar, disponibilizar e possibilitar a análise de trechos anteriores e posteriores dos textos capturados, sendo possível identificar a origem e o desdobramento do(s) assunto(s) pesquisado(s), de acordo com as necessidades da ANA;

10.1.28. Atuar de forma efetiva, no mínimo, com os aplicativos WhatsApp, Telegram, Discord e IRC;

10.1.29. Possuir foco no Brasil com fontes relevantes relacionadas a grupos de fraudadores do sistema financeiro brasileiro;

10.1.30. Permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria;

10.1.31. Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta;

10.1.32. Atuar de forma efetiva, no mínimo, com Twitter, Instagram, Youtube e Facebook;

10.1.33. Monitorar, no mínimo, a rede de compartilhamento de textos Pastebin e a plataforma de compartilhamento de códigos Github e Bitbucket;

10.1.34. A CONTRATADA deverá manter total sigilo e confidencialidade dos serviços prestados à ANA no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados;

10.1.35. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes da CONTRATADA;

10.1.36. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (Executivos) e da própria empresa em redes sociais;

10.1.37. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso da ANA ou que permitam burlar os meios de proteção desses direitos;

10.1.38. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque a reputação da instituição ou ainda a tentativa de captura de credenciais da ANA;

10.1.39. Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twittter, Linkedin, Instagram, YouTube etc. que tenham relação com a ANA e não seja autorizado por essa instituição;

10.1.40. Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas;

10.1.41. Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas da ANA, divulgações relacionadas a clientes e empregados da ANA, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial;

10.1.42. A plataforma disponibilizada pela CONTRATADA deve oferecer conexão segura através do protocolo HTTPS;

10.1.43. A plataforma deve permitir realizar a abertura de chamados a partir de um evento;

10.1.44. A CONTRATADA deve possuir mecanismos próprios que realizem a monitoração das principais Redes Sociais (Facebook, Twitter, Linkedin, Instagram, YouTube, etc.) e lojas de aplicativos para Smartphones (Google Play Store e Apple Store);

10.1.45. A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo TLDs e gTLDs, que verifique a utilização do uso indevido da marca da ANA no nome do domínio ou na URL cadastrada, contendo o domínio/URL cadastrado, a empresa que administra o registro do domínio, e os dados proprietário do domínio;

10.1.46. A CONTRATADA deverá acatar novas palavras-chave, listas de palavras, desde que estejam no contexto da mesma área de negócio da ANA sempre que demandados pela ANA para elaboração dos parâmetros de busca a serem executados;

10.1.47. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência;

10.1.48. A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências;