



MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
POLÍCIA RODOVIÁRIA FEDERAL
DIRETORIA DE ADMINISTRAÇÃO E LOGÍSTICA

ANEXO I-B

ESPECIFICAÇÕES TÉCNICAS / CATÁLOGO DE SERVIÇOS

LOTE ÚNICO - FORNECIMENTO DE SOLUÇÃO AVANÇADA DE SEGURANÇA, COMPOSTA DE: MÓDULO DE PROTEÇÃO DE ENDPOINT (EPP e XDR) COM DETECÇÃO E RESPOSTAS A AMEAÇAS, MÓDULO CONTRA APT (PROTEÇÃO CONTRA AMEAÇAS PERSISTENTES AVANÇADAS), MÓDULO PARA PROTEÇÃO DE APLICAÇÕES, SERVIDORES FÍSICOS, VIRTUAIS, CONTAINER, MÓDULO DE GERENCIAMENTO DE RISCOS DE SUPERFÍCIE DE ATAQUE PARA A NUVEM COM GARANTIA E ATUALIZAÇÃO UPGRADE/UPDATE POR 12 (DOZE) MESES.

1. SOLUÇÃO DE SEGURANÇA - ESPECIFICAÇÕES TÉCNICAS

1.1. **Módulo de EPP e XDR** (Plataforma de proteção de *endpoint*): solução implantada em dispositivos *endpoint* para evitar ataques de *malware* baseados em arquivos, detectar atividades maliciosas e fornecer os recursos de investigação e correção necessários para responder a incidentes e alertas de segurança dinâmicos, incluindo *software*, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual; com monitoramento e resposta contínuos a ameaças avançadas de segurança cibernética, incluindo *software*, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.

1.2. **Módulo contra APT** (Proteção Contra Ameaças Persistentes Avançadas): solução de monitoramento contínuo que oferece visibilidade em tempo real, contra ameaças avançadas, como *exploits* de *zero-day* e *malwares* personalizados, que se caracterizam por serem desconhecidas, direcionadas e evasivas, tornando ineficientes as ferramentas de antivírus baseadas apenas em assinaturas para detecção de conteúdo malicioso, incluindo *software*, gerenciamento centralizado, licenciamento, suporte técnico e garantia pelo período contratual.

1.3. **Módulo de Proteção de aplicações, servidores físicos, virtuais, container:** Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes Vmware e OracleVM. A solução deverá permitir gerenciar políticas de segurança em múltiplas plataformas e sistemas operacionais, para hosts físicos, virtuais ou em nuvem (AWS - Amazon Web Services, Microsoft Azure, Google Cloud Platform - GCP, Huawei Cloud, IBM Cloud, Oracle Cloud).

1.4. **Módulo de Gerenciamento de riscos de superfície de ataque para a nuvem:** Ferramenta de gerenciamento de risco que permite descobrir, identificar, avaliar e priorizar continuamente os riscos organizacionais, enfatiza a identificação, avaliação e mitigação proativa de riscos;

1.5. Os módulos deverão ser gerenciados através de uma única console centralizada e do mesmo fabricante;

1.5.1. As soluções poderão ser ofertadas no modelo SaaS com disponibilidade mínima de 99,8% para todas as funcionalidades, em cada mês civil;

1.5.1.1. A console de gerenciamento deve ser acessível em qualquer ponto da rede da contratante sem a necessidade de uma conexão VPN;

1.5.1.3. A console de gerenciamento deverá permanecer acessível por pelo menos 90 (noventa) dias após o prazo contratual.

- 1.5.2. Os *softwares* que compõem a solução (ou *appliances*, se for o caso) devem ser oferecidos na última versão disponibilizada pelo fabricante.
- 1.5.4. Na data da proposta, nenhum dos *softwares* ou *appliances* ofertados poderão estar listados pelo fabricante com data definida para fim de suporte (“*end of support*”) ou fim de vendas (“*end of sale*”).
- 1.6. Deverá ser apresentado diagrama detalhado com as soluções ofertadas, abrangendo todo o conjunto de *softwares*, aplicação e gerenciamento unificado;
- 1.7. Suporte e atualizações: 12 (doze) meses;
- 1.8. **Módulo de EPP e XDR (Plataforma de proteção de *endpoint*, *detecção* e *resposta*):**
- 1.8.1. Solução de proteção de *endpoint* com capacidade de proteção para sistema operacional Windows 7/10, Mac, servidores Windows Server e servidores Linux (Redhat/CentOS);
- 1.8.2. Compatibilidade de instalação com os seguintes sistemas operacionais:
- 1.8.2.1. Microsoft Windows 10 Home / Pro / Education / Enterprise x86 / x64;
 - 1.8.2.2. Microsoft Windows 7 Home / Professional / Enterprise x86 / x64 SP1 e superior;
 - 1.8.2.3. Windows Server 2008 R2 todas edições;
 - 1.8.2.4. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
 - 1.8.2.5. Microsoft Windows Server 2016 todas edições;
 - 1.8.2.6. Microsoft Windows Server 2019 todas edições;
 - 1.8.2.7. Red Hat Enterprise Linux 6.7 e superior;
 - 1.8.2.8. Red Hat Enterprise Linux 7.2 e superior;
 - 1.8.2.9. CentOS-6.7 e superior;
 - 1.8.2.10. CentOS-7.2 e superior;
 - 1.8.2.11. Debian GNU / Linux 8.6 e superior;
 - 1.8.2.12. Debian GNU / Linux 9.4 e superior;
 - 1.8.2.13. macOS Mojave 10.14;
 - 1.8.2.14. macOS High Sierra 10.13;
 - 1.8.2.15. macOS Sierra 10.12;
 - 1.8.2.16. Suportar as seguintes plataformas virtuais:
 - 1.8.2.17. VMware vSphere 6 ou superiores
 - 1.8.2.18. VMware Workstation 14 Pro ou superiores
 - 1.8.2.19. Oracle - Virtual Server 3 ou superiores
 - 1.8.2.20. Possuir Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android.
- 1.8.3. **Console de Gerenciamento**
- 1.8.3.1. Características da console de gerenciamento da solução:
 - I - A console deve ser acessada via WEB, com utilização do protocolo HTTPS;
 - II - Console deve ser baseada no modelo cliente/servidor;
 - III - Compatibilidade com *Windows Failover Clustering* ou outra solução de alta disponibilidade;
 - IV - Deve permitir incluir usuários do *Active Directory* ou LDAP para acessarem a

console de administração;

V - Deve permitir o uso de *multi-factor authentication* seja via *e-mail* ou aplicativo (*token*);

VI - Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias, tais como: Criptografia, Gerenciamento de *Patches* e Módulo de Gerenciamento *Mobile*;

VII - As licenças de software deverão ser fornecidas na modalidade SaaS, *Software as a Service*, com pagamento único pelo período de 12 (doze) meses de utilização e deverão garantir o pleno funcionamento da solução durante todo o período de vigência contratual, incluindo atualizações, suporte e garantia do fabricante.

VIII - Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

IX - Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, *login script* e/ou GPO de *Active Directory*;

X - Deve registrar em arquivo de *log* todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

XI - Deve armazenar histórico das alterações feitas em políticas;

XII - A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

XIII - A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e visualizar painéis de controle;

XIV - Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

XV - Capacidade de instalar atualizações em computadores de testes antes de instalar nos demais computadores da rede;

XVI - Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

XVII - Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

XVIII - A comunicação entre o cliente e o servidor de administração deve ser criptografada;

XIX - Deve permitir a localização de máquinas novas na rede sem ter um agente ou *endpoint* instalado utilizando no mínimo dois dos seguintes parâmetros:

a) Nome do Computador;

c) Nome do Domínio;

e) *Range* de IP;

g) Sistema Operacional;

i) Máquina Virtual.

1.8.3.2. Capacidade de executar a regra do item anterior das seguintes formas:

I - Regra funcionar permanentemente;

II - Deve encontrar computadores na rede através de no mínimo três formas: Domínio, *Active Directory* e Sub-Redes;

III - Capacidade de monitorar diferentes *subnets* de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

IV - Capacidade de monitorar grupos de trabalhos ou *range de ip* a fim de encontrar máquinas novas para serem adicionadas a proteção;

V - Capacidade de, assim que detectar máquinas novas no *Active Directory*, *subnets* ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve permitir a instalação do agente ou do antivírus;

VI - Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias;

VII - Listar em um único local, todos os computadores não gerenciados na rede;

VIII - Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

1.8.4. Deve fornecer as seguintes informações dos computadores:

I - Se o antivírus está instalado;

II - Se o antivírus está iniciado;

III - Se o antivírus está atualizado;

IV - Minutos/horas desde a última conexão da máquina com a console;

V - Minutos/horas desde a última atualização de vacinas;

VI - Data e horário da última verificação executada na máquina;

VII - Versão do antivírus instalado na máquina;

VIII - Se é necessário reiniciar o computador para aplicar mudanças;

IX - Data e horário de quando a máquina foi ligada;

X - Quantidade de vírus encontrados (contador) na máquina;

XI - Nome do computador;

XII - Domínio ou grupo de trabalho do computador;

XIII - Data e horário da última atualização de vacinas;

XIV - Sistema operacional com *Service Pack*;

XV - Usuário(s) logado(s) naquele momento; e

XVI - Endereço IP.

1.8.5. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

1.8.6. Deve permitir a visualização de múltiplos painéis (*dashboards*) personalizáveis, visualizados através de gráficos/tabelas baseado nos módulos da plataforma;

1.8.7. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.8.8. Capacidade de fazer deste repositório de vacinas um *gateway* para conexão com o Servidor de Administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este *gateway* para receber e enviar informações ao servidor administrativo;

1.8.9. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.8.10. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;

1.8.11. Deve permitir adicionar senha para controle da interface do *endpoint* e impedir a

desinstalação por usuários;

1.8.12. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

1.8.13. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- I - Nome do vírus;
- II - Nome do arquivo infectado;
- III - Data e hora da detecção;
- IV - Nome da máquina ou endereço IP;
- V - Ação realizada.

1.8.13.1. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

1.8.13.2. Deve permitir níveis de administração por usuários ou grupos de usuários;

1.8.13.3. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador;

1.8.13.4. Deve criar um *backup* de todos arquivos deletados ou quarentenados em computadores para que possam ser restaurados através de comando na Console de Administração;

1.8.13.5. Capacidade de diferenciar máquinas virtuais ou VDI de máquinas físicas;

1.8.13.6. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

1.8.13.7. Capacidade de enviar *e-mails* para contas específicas em caso de algum evento;

1.8.13.8. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações via *e-mail*;

1.8.13.9. Capacidade de gerar e exportar relatórios pré-definidos, pelo menos, nos seguintes tipos de arquivos: PDF ou HTML ou XML;

1.8.13.10. Capacidade de customizar relatórios;

1.8.13.11. Deve conter relatórios com informações de efetividade de detecção, *ransomware*, canais de infecção, principais usuários que receberam ameaças, vírus e *spyware*;

1.8.13.12. Possuir informações estatísticas na console de gerenciamento com, no mínimo, as seguintes informações:

- I - Status da Proteção;
- II - Informações de Implementação;
- III - Atualizações;
- IV - Ameaças;
- V - Informação Geral;
- VI - Atualizações das Aplicações;

1.8.13.13. Solução deverá permitir a integração com *syslog*;

1.8.13.14. Capacidade de gerar *traps* SNMP para monitoramento de eventos.

1.8.14. **Proteção para Sistema Operacional Windows**

1.8.15. Características da solução de proteção para Sistema Operacional Windows:

- I - A proteção para estações de trabalho deverá prover Controle de Aplicações, *Anti-Malware*, *Machine Learning*, *Firewall* (HIPS), Controle de dispositivos, *Data Loss Prevention*, deverá ser em um único agente;
- II - Detectar, analisar e eliminar programas maliciosos, tais como vírus, *spyware*, *worms*, cavalos de tróia, *key loggers*, programas de propaganda, *rootkits*, *ransomware* e ataques do tipo *fileless*;
- III - A solução de antivírus deverá possuir funcionalidades específicas para prevenção contra a ação de *ransomwares*, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos com a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.
- IV - Antivírus de Arquivos residente (*anti-spyware*, *anti-trojan*, *anti-malware*) que verifique qualquer arquivo criado, acessado ou modificado;
- V - Antivírus de *Web* (módulo para verificação de sites e *downloads* contra vírus);
- VI - Antivírus de *E-mail* (módulo para verificação de *e-mails* recebidos e enviados, assim como seus anexos);
- VII - Proteção contra Ameaças de Rede (módulo de verificação de atividades suspeitas na rede);
- VIII - *Firewall* com IDS (sistema de detecção de intrusão);
- IX - Possuir controle de dispositivos externos;
- X - Capacidade de customização de acesso a sites com, no mínimo, as seguintes maneiras:
- XI - Algum tipo de controle de acesso a sites;
- XII - Possuir controle de execução de aplicativos.
- XIII - Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- XIV - Possuir Autodefesa contra os ataques aos serviços e processos do antivírus no *endpoint*;
- XV - Capacidade de escolher quais módulos serão instalados tanto localmente quanto remotamente ou via política;
- XVI - Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- XVII - Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- XVIII - O *Endpoint* deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- XIX - Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, por exemplo: “*Win32.Trojan.banker*”, para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- XX - Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- XXI - Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- XXII - Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento, ou capacidade de definir quantidade de consumo de *hardware*;
- XXIII - Capacidade de verificar somente arquivos novos e alterados;

- XXIV - Capacidade de verificar objetos usando heurística;
- XXV - Capacidade de agendar uma pausa na verificação;
- XXVI - As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- XXVII - Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
- XXVIII
- Deve permitir a filtragem de conteúdos maliciosos conforme categorização pré-definida pelo fabricante.
- XXIX - O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- XXX - Bloquear acesso ao objeto;
- XXXI - Apagar o objeto;
- XXXII - Tentar desinfetar o objeto.
- XXXIII
- Em caso positivo de limpeza deve restaurar o objeto para uso;
- XXXIV
- Em caso negativo de limpeza deve mover para quarentena ou apagar;
- XXXV - Anteriormente a qualquer tentativa de limpeza ou exclusão permanente, o antivírus deve realizar um *backup* do objeto;
- XXXVI
- Deve inspecionar o canal de *e-mail* contra atividades maliciosas ou deve possuir proteção dos protocolos IMAP, SMTP e POP3;
- XXXVII
- Capacidade de verificar tráfego nos *browsers*: Microsoft Edge, Firefox, Google Chrome e Safari;
- XXXVIII
- Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários);
- XXXIX
- Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurística;
- XL - Na verificação de tráfego *web*, caso encontrado código malicioso o programa deve:
- XLI - Perguntar o que fazer;
- XLII - Bloquear o acesso e informar sobre a ação com uma mensagem;
- XLIII - Permitir o acesso ao objeto;
- XLIV - Deve ter suporte total ao protocolo IPV6;
- XLV - O antivírus de *web* deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
- XLVI - Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo real;
- XLVII - Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;
- XLVIII
- Possibilidade de adicionar sites da *web* em uma lista de exclusão, onde não serão

verificados pelo antivírus de *web*;

XLIX - Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

L - Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra ameaças e explorações de rede. A base de dados de análise deve ser atualizada juntamente com as vacinas;

LI - O módulo de *Firewall* deve conter conjunto de regras de filtragem de pacotes, onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

LII - Todas as regras das funcionalidades de *firewall* e *ips de host* devem permitir apenas detecção (*log*) ou prevenção (bloqueio);

LIII - Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

LIV - Discos de armazenamento locais;

LV - Armazenamento removível;

LVI - Impressoras;

LVII - CD/DVD;

LVIII - Modems;

LIX - Wi-Fi;

LX - Adaptadores de rede externos;

LXI - Dispositivos *Bluetooth*;

LXII - Câmeras e *Scanners*;

LXIII - Deve possuir módulo que habilite ou não o funcionamento das conexões USB.

LXIV - Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário, este podendo ser vinculado há um usuário do *Active Directory*;

LXV - Capacidade de habilitar “*logging*” em dispositivos removíveis tais como *Pendrive*, Discos Externos, entre outros;

LXVI - Capacidade de configurar novos dispositivos por pelo uma das seguintes formas: Class ID/Hardware, ID/Vendor/Serial ID , IP/Hostname;

LXVII -Capacidade de limitar a execução de aplicativos por assinatura do executável (*hash MD5*), nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria, por exemplo: navegadores, gerenciador de *download*, jogos, aplicação de acesso remoto;

LXVIII

- Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

LXIX - Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de *firewall* até controle de aplicativos, dispositivos e acesso à *web*;

LXX - Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de *firewall* até controle de aplicativos, dispositivos e acesso à *web*;

LXXI - O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

LXXII -*Black list*: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

LXXIII

- *White list*: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

LXXIV

- Capacidade de recuperar chaves de registro, reparar sistemas de arquivo e deletar arquivos baixados por cavalos de troia.

LXXV -Bloquear atividade de *malware* explorando vulnerabilidades em *softwares* de terceiros.

LXXVI

- Capacidade de detectar anomalias no comportamento de um *software*, usando análise heurística e aprendizado de máquina (*machine learning*).

LXXVII

- Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e *Machine Learning*.

LXXVIII

- O módulo deve ser capaz de agir nos seguintes estados:

LXXIX

- Aprendizado: coleta informações sobre as atividades executadas pelo usuário.

LXXX -Bloqueio: bloqueia as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

LXXXI

- Notificação: notifica sobre as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

LXXXII

- Ter a capacidade de integração com *sandbox*, pelo qual deve ser entregue como produto que componha a solução, sendo do mesmo fabricante.

LXXXIII

- Deve ter suporte à arquivos de terceiros para gerenciamento através de REST API;

LXXXIV

- Módulo de proteção de *ransomware*, específico para a linha de servidores, com a capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um *malware* em um dispositivo que possua o mapeamento da pasta;

LXXXV

- Bloquear *malwares* tais como *Cryptlockers* mesmo quando o ataque vier de um computador sem antivírus na rede;

LXXXVI

- Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

1.8.16. **Proteção para Estações de Trabalho Mac**

1.8.16.1. Características da solução de proteção para estação de trabalho Mac:

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

II - Deve prover proteção residente para arquivos (*anti-spyware*, *anti-trojan*, *anti-malware* etc) que verifique qualquer arquivo criado, acessado ou modificado;

III - Possuir módulo de Antivírus *Web* para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços HTTP/HTTPS;

IV - Possuir módulo de bloqueio à ataques na rede;

V - Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

- VI - Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
- VII - Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- VIII - A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
- IX - Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- X - Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação;
- XI - Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- XII - Capacidade de verificar somente arquivos novos e alterados;
- XIII - Capacidade de verificar objetos usando heurística;
- XIV - Capacidade de agendar uma pausa na verificação;
- XV - O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- XVI - Bloquear o objeto;
- XVII - Deletar o objeto;
- XVIII - Realizar a limpeza do objeto;
- XIX - Em caso positivo de limpeza deve restaurar o objeto;
- XX - Em caso negativo de limpeza deve mover para quarentena ou apagar;
- XXI - Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um *backup* do objeto;
- XXII - Caso o *e-mail* possua códigos ou anexos maliciosos, a ferramenta deverá tomar uma ação de quarentena ou realizar a remoção do artefato.
- XXIII - As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- XXIV - Capacidade de voltar para a base de dados de vacina anterior;

1.8.17. **Proteção para Sistema Operacional Linux**

1.8.17.1. Características da solução de proteção para Sistema Operacional Linux:

- I - Antivírus de arquivos residente (*anti-spyware*, *anti-trojan*, *anti-malware*) que verifique qualquer arquivo criado, acessado ou modificado;
- II - As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- III - Capacidade de configurar a permissão de acesso às funções do antivírus com opção de gerenciamento de *backup*, permitindo a criação de cópias dos objetos infectados em um reservatório de *backup* antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
- IV - Detectar aplicações que possam ser utilizadas como vetor de ataque por *hackers*;
- V - Fazer detecções através de heurística;
- VI - Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos,

salvando tais arquivos em uma pasta de quarentena;

VII - Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

VIII - Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros *softwares*;

IX - Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

X - Capacidade de verificar objetos usando heurística;

XI - Possibilidade de escolha da pasta onde serão guardados os *backups* e arquivos em quarentena;

XII - Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

XIII - Deve possuir proteção anti-*cryptor*, com a função de proteger arquivos contra criptografia remota, que atinge diretórios locais com acesso à rede pelos protocolos SMB / NFS;

XIV - Permitir a criação de uma tarefa que faça o monitoramento de integridade de arquivos, pelo qual permite o rastreamento das ações executadas com os arquivos e diretórios nos escopos de monitoramento especificados na mesma;

XV - Deve possuir módulo de administração remoto através de ferramenta nativa ou *Webmin* (ferramenta nativa GNU-Linux);

1.8.18. **Criptografia**

1.8.18.1. O módulo deve ser entregue com a solução do *Endpoint* e ser gerenciado pela mesma console, sem que haja custo de licença adicional;

1.8.18.2. Compatibilidade de instalação nos seguintes Sistemas Operacionais Windows já elencados:

1.8.18.3. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

1.8.18.4. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

1.8.18.5. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de *pré-boot* para autenticação do usuário;

1.8.18.6. Capacidade de utilizar *Single Sign-On* para a autenticação de *pré-boot*;

1.8.18.7. Permitir criar vários usuários de autenticação *pré-boot*;

1.8.18.8. Capacidade de criar um usuário de autenticação *pré-boot* comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

1.8.18.9. Capacidade de criptografar *drives* removíveis de acordo com regra criada pelo administrador, com as opções:

I - Criptografar todos os arquivos individualmente;

II - Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

III - Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

IV - Verifica compatibilidade de *hardware* antes de aplicar a criptografia;

V - Possibilita estabelecer parâmetros para a senha de criptografia;

VI - Bloqueia a senha após um número de tentativas pré-estabelecidas;

1.8.18.10. Capacidade de permitir que o usuário solicite ao administrador as credenciais para decifragem de determinado arquivo criptografado;

1.8.18.11. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

1.8.18.12. Capacidade de criptografar arquivos por pastas, discos ou unidades externas.

1.8.18.13. Capacidade de deletar arquivos de forma segura após a criptografia;

1.8.18.14. Capacidade de criptografar somente o espaço em disco utilizado;

1.8.18.15. Deve ter a opção de criptografar arquivos selecionados pelo administrador. Deve fazer a detecção através do comportamento;

1.8.18.16. Deve fazer a correlação de eventos entre computadores na rede (*IoC Scanning*);

1.8.18.17. Deve detectar elevação de privilégio;

1.8.18.18. Deve enviar objetos para verificação no *Sandbox* de forma automática quando necessário utilizando a inteligência global da fabricante;

1.8.18.19. Deve enviar objetos para verificação em *Sandbox*;

1.8.18.20. Deve permitir coletar informações forenses do *endpoint* tais como:

I - Dados;

II - Estado do sistema operacional;

III - Processos iniciados;

IV - Conexões estabelecidas;

V - Arquivos criados;

VI - Registro modificado;

VII - Tentativas de conexão com um *host* remoto;

1.8.18.21. A segurança entre a comunicação da solução e o Console de Gerenciamento deverá ser realizada utilizando um certificado;

1.8.18.22. A solução deve ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo no mínimo as capacidades abaixo:

I - Parar um processo;

II - Deletar um objeto;

III - Quarentenar um arquivo;

IV - Recuperar um arquivo;

V - Prevenir a execução de um arquivo;

VI - Ou executar um *script* ou investigar ameaças em memória;

VII - Isolar o *host*.

1.8.19. **Módulo de Proteção contra APT (Ameaças Persistentes Avançadas)**

1.8.19.1. A PRF atualmente possui dois *appliances* físicos com capacidade individual de 4Gbps de volume de dados, desta forma os 8Gbps previstos para a sede contemplam as licenças e, as implementações para as demais regionais poderão ser ofertadas no modelo de *virtual appliance* - SaaS com disponibilidade mínima de 99,8% para todas as funcionalidades, em cada mês civil;

1.8.19.2. Ser dimensionado para a análise de tráfego de rede de toda a PRF

(*throughput* mínimo de 6.000 Mbps);

1.8.19.3. Possuir console de gerenciamento com *dashboard* customizável através de *widgets* ou similar;

1.8.19.4. Deverá apresentar a saúde do sistema, informando quais componentes estão atualizados ou não;

1.8.19.5. Deverá mostrar em tempo real o tráfego sendo processado pelos sensores;

1.8.19.6. Deverá apresentar em tempo real gráfico de pacotes descartados caso não suporte o tráfego gerado;

1.8.19.7. Deverá mostrar pelo menos as seguintes informações atualizadas sobre a ferramenta:

I - Saúde do sistema;

II - Tráfego em tempo real;

III - *Top* 10 domínios mais acessados;

IV - Mostrar alertas por importância;

V - *Top* 10 Ips mais acessados;

VI - Alertas por tecnologias de detecção;

VII - Alertas por vetor de ataques;

1.8.19.8. Deverá permitir criar novos usuários para acesso à console com pelo menos 3 (três) níveis de acesso;

1.8.19.9. Deverá permitir integração com o Console de Gerenciamento da ferramenta de antivírus caso seja necessário a implementação de EDR;

1.8.19.10. Os alertas deverão ser exibidos permitindo visualizar quantos são novos, quantos estão em processo e quantos já foram processados;

1.8.19.11. Deverá mostrar quantidades de eventos pela criticidade; alto, médio ou baixo;

1.8.19.12. Deverá suportar arquivos no formato CEF para integração com SIEM;

1.8.19.13. Possibilidade de marcar evento como processado para informar que o incidente já foi analisado e resolvido;

1.8.19.14. As seguintes informações devem ser mostradas nos alertas de eventos:

I - *Host* onde ocorreu o incidente;

II - Origem do ataque;

III - Destino do ataque;

IV - Dia e horário de quando ocorreu o ataque;

V - Nome do objeto considerado malicioso;

VI - Tamanho do objeto;

VII - *Hash* do objeto em pelo menos MD5 e SHA256;

VIII - URL do ataque;

IX - Nome da tecnologia responsável por identificar o ataque;

X - Informar se o ataque possui características baseado no YARA (ferramenta *open source*);

1.8.19.15. O Console de Gerenciamento deverá permitir que o administrador procure por eventos similares na rede baseado no tipo de arquivo, no *hash* do arquivo, tipo de evento e nome do arquivo;

- 1.8.19.16. Deverá permitir a instalação do sensor de *endpoint* de forma remota;
- 1.8.19.17. Possibilidade de mostrar a sequência de atividades executadas pelo *malware* quando executada no *sandbox*;
- 1.8.19.18. Deverá permitir fazer uma busca no sistema por eventos baseados em regras;
- 1.8.19.19. Fazer buscas de IoCs (indicadores de Comprometimento) no banco de dados através de informações recebidas pelos agentes;
- 1.8.19.20. Deverá permitir buscar no sistema eventos baseados nas seguintes categorias:
- I - Texto completo;
 - II - Por *host*;
 - III - Por tipo de evento;
 - IV - Por arquivos;
 - V - Pelo *hash* MD5 e SHA256;
 - VI - Pela conexão de rede;
 - VII - Chave de registro;
 - VIII - Eventos do Windows;
 - IX - Alteração de nome do *host*;
- 1.8.19.21. Deverá permitir importar IOCs (índices de Comprometimento) visando encontrar ataques de acordo com informações contidas no IoC;
- 1.8.19.22. Capacidade de finalizar processos remotamente nos *endpoints* que possuem a solução instalada;
- 1.8.19.23. Deverá possuir funcionalidade que permita prevenir um arquivo de ser executado em qualquer *host* com a solução instalada através de *hash* MD5/SHA256;
- 1.8.19.24. Deverá possuir capacidade de disponibilizar as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;
- 1.8.19.25. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;
- 1.8.19.26. Possibilidade de selecionar quais dispositivos serão afetados pela tarefa de prevenção de execução de arquivos;
- 1.8.19.27. Capacidade de baixar arquivos quarentenados diretamente pela console de administração da solução;
- 1.8.19.28. Capacidade de visualizar quantos *endpoints* possuem a solução instalada através de integração com o Console de Gerenciamento do antivírus;
- 1.8.19.29. Possuir relatórios customizáveis possibilitando adicionar ou remover colunas de identificação e status de eventos;
- 1.8.19.30. Deve permitir criar relatórios baseados na tecnologia de proteção utilizada;
- 1.8.19.31. Deverá permitir criar relatórios de eventos organizados pelas seguintes severidades: baixa, média e alta;
- 1.8.19.32. Permitir criar listas brancas baseadas nos seguintes filtros:
- I - Por *hash* MD5;
 - II - Por URL;

III - Por sub-rede.

1.8.19.33. Deverá permitir criar regras de notificações para envio por *e-mail* quando novos eventos são identificados pela ferramenta;

1.8.19.34. Deverá permitir configurar o *status* do *endpoint* de acordo com a quantidade de dias de inatividade;

1.8.19.35. Deverá permitir integrar a solução com pelo menos as seguintes ferramentas de SIEM: *ArchSight*, *Splunk* e *IBM Qradar*;

1.8.20. Características para o *Sandbox*

1.8.20.1. Suportar atualização da base de dados da Rede de Inteligência de forma automática e sem causar nenhum tipo de indisponibilidade da solução;

1.8.20.2. A análise inicial deve ser realizada de forma local no ambiente de detecção. O envio de artefatos para verificação no *sandbox* deve ocorrer de forma automática, ou seja, caso a inteligência do produto identifique a necessidade de encaminhar o objeto para análise no *sandbox*, este processo deve ocorrer sem a intervenção de qualquer usuário;

1.8.20.3. A solução deve ser capaz de prover dados forense detalhados, via interface gráfica, relacionados à infecção, demonstrando o ciclo de vida completo do ataque. Estes dados forenses devem incluir a cronologia completa do ataque e não apenas uma porção do ataque, além de:

I - URLs/sites web relacionados ao ataque;

II - Hashes MD5/SHA256;

III - Binários maliciosos anexados.

1.8.20.4. Deverá analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF's, executáveis, extensões do Microsoft Office, arquivos de mídia, *scripts*, ZIP, RAR, JAR, bat, vbs, vbe, ps1, dmg e pkg;

1.8.20.6. Deverá prover um método de disponibilizar *updates* das *sandboxes* sem requerer um completo *update* do sistema operacional ou *upgrade* da solução e sem indisponibilidade de sua detecção;

1.8.20.7. Toda análise básica de *malwares*, incluindo *malwares* desconhecidos, deve ser realizada de forma automatizada através da detecção do *exploit*, sem a necessidade de criação de regras específicas ou interação de um operador;

1.8.20.8. Toda a análise do comportamento do *malware* deve ser registrada em tempo de execução;

1.8.20.9. Deverá suportar importação de regras YARA personalizadas, para permitir flexibilidade na criação de regras para análise de ameaças;

1.8.20.10. Suportar mecanismo de *whitelist* pelos seguintes métodos:

I - Hash MD5 do arquivo;

II - Formato do arquivo;

1.8.20.11. Deverá permitir o envio de alertas por *e-mail*;

1.8.20.12. Deverá possuir a capacidade de detectar ameaças direcionadas, realizando inspeção de tráfego até a camada 7 (sete) de forma a prevenir ataques do dia zero e executar análise profunda de documentos que contenham conteúdo malicioso ou redirecionamentos para outras URL's maliciosas;

1.8.20.13. O *sandbox* da solução deve possuir mecanismos para prevenção de evasão.

1.8.21. Sensores de Detecção

- 1.8.21.1. Deverá permitir que o sensor monitore tráfego *WEB*, *Mail* e Rede;
- 1.8.21.2. Deverá permitir integração com solução de *proxy* utilizando o protocolo ICAP permitindo analisar protocolos seguros (ex: HTTPS);
- 1.8.21.3. Deverá verificar mensagens de *e-mail* através do protocolo POP3 e SMTP;
- 1.8.21.4. Deverá processar tráfego espelhado e extrair objetos e metadados do DNS;
- 1.8.21.5. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou *Switches*;
- 1.8.21.6. A solução deve suportar um *throughput* de análise de no **mínimo** 6.000 Mbps;
- 1.8.21.7. A solução deverá ser gerenciada por console *Web* suportando no mínimo os *browsers* Microsoft Edge, Firefox, Google Chrome e Safari;
- 1.8.21.8. Deverá permitir configurar mais de um sensor de rede caso o ambiente corporativo tenha mais de um ponto para análise;
- 1.8.21.9. Deverá possuir a capacidade de atualizar as vacinas, *engines*, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;
- 1.8.21.10. O Sensor de Rede deverá suportar SPAN Port ou TAP para análise do tráfego;
- 1.8.21.11. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
- 1.8.21.12. Deverá apresentar relatórios customizados de todas as suas funcionalidades.
- 1.8.21.13. O sensor deverá encaminhar automaticamente para a *sandbox* um artefato potencialmente perigoso identificado no tráfego de rede;
- 1.8.21.14. O sensor deverá alertar qualquer artefato malicioso identificado já conhecido sem a necessidade de intervenção manual;
- 1.8.21.15. Deverá detectar incidentes de segurança motivados por conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos além da detecção de *malwares* conhecidos e desconhecidos, *ransomware*, *Exploits*, *Botnets*, *Cross Site Script*, *SQL Injection*, comunicações p2p, *instant messengers*; *streaming*, tentativas de *scan* de rede, tentativas de *brute-force*, situações de evasão e roubo de informação etc;
- 1.8.21.16. Deverá ter capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;
- 1.8.21.17. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística.
- 1.8.21.18. Deverá atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;
- 1.8.21.19. Deverá permitir utilizar um sensor de rede como *proxy*, ou seja, deve permitir que o sensor receba informações do *Endpoint* para enviar ao Console de Gerenciamento;
- 1.8.21.20. O sensor deverá ter acesso a rede global de inteligência da fabricante;
- 1.8.21.21. Deverá integrar com a infraestrutura extraíndo objetos do tráfego de rede e efetuando uma análise inicial;
- 1.8.21.22. Deverá receber objetos para serem verificados dos *switches*, servidores de *proxy* e servidores de *e-mail*;

1.8.21.23. Deverá atuar como IDS na rede detectando anomalias no tráfego de rede e alertando o Console de Gerenciamento sobre os eventuais incidentes;

1.8.21.24. Caso necessário, deve suportar uma arquitetura única atuando como sensor de rede e console de gerenciamento em uma mesma máquina virtual;

1.8.21.25. Através de consulta na base global da fabricante, deverá detectar os seguintes itens:

I - Endereços envolvidos em campanhas de ataques persistentes;

II - Servidores de “*Command & Control*”;

III - Sites maliciosos;

IV - Sites de *phishing*;

1.8.21.26. Deverá possuir tecnologia de *cache* para evitar envio de solicitações duplicadas;

1.8.21.28. Deverá possuir capacidade de verificar *links* ativos em documentos do MS Office;

1.8.21.30. Deverá permitir a customização de regras para submissão de arquivos para o *Sandbox*;

1.8.21.32. Deverá ilustrar o ataque ou potenciais ameaças mostrando informações do que foi atacado e onde começou;

1.8.21.34. O Sensor de Rede deverá possuir a capacidade de analisar e verificar o histórico de acesso à internet afim de identificar chamadas de C&C;

1.8.21.36. O Sensor deverá listar por fase de Ataque Avançado Persistente (Ponto de Entrada, Comunicação Maliciosa, Movimentação Lateral e Exfiltração de dados) as máquinas afetadas;

1.8.21.38. Deverá permitir a geração de *logs* e integração com *SYSLOG Servers* e deverá conter no mínimo:

I - Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, *Exploits*, *Grayware* e detecções realizadas via Analisador Virtual;

II - Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

1.8.21.40. O sensor de *endpoint* deve ser compatível com fabricantes terceiras, permitindo que colete e envie informações ao Console de Gerenciamento sem causar conflito com a atual solução de antivírus;

1.8.21.42. Deverá ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou tunelamento de protocolo.

1.9. **Módulo de Proteção de aplicações, servidores físicos, virtuais, container**

1.9.1. Conter os seguintes módulos para a proteção de Servidores físicos, virtuais ou em nuvem:

1.9.1.1. Reputação Web;

1.9.1.2. Inspeção de Pacotes com virtual Patching (IDS/IPS);

1.9.1.3. Monitoramento de Integridade;

1.9.1.4. Inspeção de Logs;

1.9.1.5. Controle de Aplicações;

1.9.2. Para hosts gerenciados de Docker container deverá permitir a aplicação de regras de IPS/IDS e proteção contra artefatos maliciosos.

1.9.3. Permitir a implantação dos módulos de segurança supracitados, no mínimo para

os seguintes sistemas operacionais:

- 1.9.3.1. Windows Server 2003, 2008, 2012 e Windows 2016;
- 1.9.3.2. Sistemas Operacionais Linux, no mínimo para as distribuições: Red Hat, Suse, CentOS, Ubuntu e Debian.
- 1.9.4. A solução deverá permitir agrupar os hosts gerenciados em pastas, possibilitando para a aplicação de políticas.
- 1.9.5. Deverá possuir gerenciamento de todos os eventos relativos aos hosts gerenciados possibilitando, além do armazenamento dos eventos na própria solução, o seu encaminhamento para uma solução de SIEM.
- 1.9.6. A solução deverá ter a capacidade de se integrar com os principais softwares de SIEMs de mercado, no mínimo com: IBMQradar, Splunk e ArcSight de modo a permitir enviar os seus logs para essas soluções.
- 1.9.7. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers.
- 1.9.8. A solução deverá suportar o uso de REST API's para permitir a integração com outras aplicações.
- 1.9.9. O uso das REST API's deve suportar no mínimo as seguintes funcionalidades:
 - 1.9.9.1. Autenticação – Log in e Log out;
 - 1.9.9.2. Administração de Contas - Criação, edição e exclusão de contas de acesso;
 - 1.9.9.3. Eventos – Acesso à lista de eventos do módulo de Reputação Web;
 - 1.9.9.4. Monitoração de Status- Visualização do status dos hosts gerenciados.
- 1.9.10. Deverá permitir a criação de maneira personalizada de termos de compromisso para usuários de administração, via console de gerenciamento apresentando a mensagem personalizada ao usuário no momento de login.
- 1.9.11. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: no mínimo para Microsoft System Center Configuration Manager e Puppet.
- 1.9.12. A solução deverá efetuar a proteção contra códigos maliciosos através da instalação ou não de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça.
- 1.9.13. A solução deverá suportar a análise de comportamento (Behavior Monitoring) para a detecção avançada de ameaças.
 - 1.9.13.1. A funcionalidade de análise de comportamento deverá permitir o bloqueio de atividades suspeita de criptografia de arquivos visando impedir a propagação de ameaças do tipo ransomware.
 - 1.9.13.2. A funcionalidade de análise de comportamento deverá permitir o backup de arquivos que estiverem sendo criptografados, fazendo a restauração dos mesmos em caso de bloqueio do processo de criptografia.
- 1.9.14. A solução deverá incluir técnicas de Inteligência artificial baseada em algoritmo de Machine Learning para análise preditiva de ameaças.
- 1.9.15. Deve ser capaz de executar rastreamento nos hosts e fornecer lista de todas as recomendações de segurança para os softwares que estiverem instalados nesse host, bem como do sistema operacional.
- 1.9.16. Proteger de forma automática e transparente contra brechas de segurança descobertas, interrompendo somente o tráfego de rede malicioso.
- 1.9.17. Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para

monitoração e alertas.

- 1.9.18. Possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e demais aplicações.
- 1.9.19. Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do sistema operacional e as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no sistema operacional e aplicações (patch virtual).
- 1.9.20. Permitir execução de varreduras sob demanda ou agendada.
- 1.9.21. Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão.
- 1.9.22. 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.
- 1.9.23. Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais e aplicações:
 - 1.9.23.1. Windows 2003, 2008 e 2012;
 - 1.9.23.2. Linux Red Hat, Suse, CentOS e Debian;
 - 1.9.23.3. Aplicações padrão de mercado, tais como: Microsoft IIS, SQL Server, Microsoft Exchange, Microsoft Office, Red hat Oracle Database, PostgreSQL, Adobe Acrobat, Mozilla Firefox, Microsoft Edge, Google Chrome, Edge e Web Server Apache, Jboss, Wordpress, PHP, Joomla, Safari, Jenkins entre outros.
- 1.9.24. Possuir a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- 1.9.25. Possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- 1.9.26. Possuir a capacidade de detectar e bloquear ataques em aplicações web tais como: SQL Injection e Cross-Site Scripting;
- 1.9.27. 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;
- 1.9.28. Implementar a inspeção de tráfego incoming SSL;
- 1.9.29. Apresentar informações detalhadas das regras de blindagem contra vulnerabilidades, contendo links com referências externas, quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
- 1.9.30. 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;
- 1.9.31. 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;
- 1.9.32. Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
- 1.9.33. Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações terceiras;
- 1.9.34. Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais Linux;
- 1.9.35. Possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;
- 1.9.36. Possuir a capacidade de criação de regras de monitoramento em chaves de

- registro, diretórios e subdiretórios e, customização de XML para criação de regras avançadas;
- 1.9.37. Possuir a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de IPS/IDS, monitoramento de integridade e inspeção de logs de acordo com o resultado desta varredura;
- 1.9.38. Permitir execução destas varreduras sob demanda ou agendada;
- 1.9.39. Rastrear arquivos por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256 e Flags;
- 1.9.40. Gerar alertas toda vez que uma modificação ocorrer, em tempo real para ambiente Windows e, pseudo tempo real para ambiente Linux utilizando agente;
- 1.9.41. Registrar em relatório todas as modificações que ocorram nos objetos monitorados;
- 1.9.42. Classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- 1.9.43. Possibilitar a escolha do diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- 1.9.44. 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;
- 1.9.45. Permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
- 1.9.46. Permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
- 1.9.47. Implementar inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor;
- 1.9.48. Permitir modificar as regras por severidade de ocorrência de eventos;
- 1.9.49. Possibilitar a criação de listas de exclusão para processos, diretórios ou arquivos do sistema operacional;
- 1.9.50. Possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
- 1.9.51. Implementar a proteção contra acesso a websites ou URL's consideradas maliciosas, de baixa reputação ou não categorizadas;
- 1.9.52. Deve permitir a proteção contra acesso a websites ou url consideradas maliciosas ou de baixa reputação;
- 1.9.53. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
- 1.9.54. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;
- 1.9.55. A solução deverá permitir a implantação do módulo de controle de aplicações nas plataformas Linux e Microsoft Windows anteriormente descritas;
- 1.9.56. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
- 1.9.57. A solução deverá permitir o escaneamento de um host gerando uma imagem de baseline, a partir da qual qualquer mudança ou aplicação nova deverá ser bloqueada;
- 1.9.58. O agrupamento dos eventos deverá ser realizado pelo menos por hash ou por máquina;

- 1.9.59. Deverá possuir funcionalidade de janela de manutenção desabilitando a funcionalidade de controle de aplicação por um tempo pré-determinado reativando a sua funcionalidade após o termino da janela;
- 1.9.60. A solução deverá possuir no mínimo as funcionalidades de bloquear tudo o que não for permitido explicitamente (whitelist) e permitir tudo o que não for bloqueado explicitamente (blacklist).
- 1.9.61. Funcionalidades de Gerenciamento:
- 1.9.61.1. Permitir o envio de notificações via SMTP;
 - 1.9.61.2. Permitir o envio de registros de logs a um servidor remoto;
 - 1.9.61.3. Implementar gravação de eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;
 - 1.9.61.4. Permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;
 - 1.9.61.5. Permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;
 - 1.9.61.6. Permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;
 - 1.9.61.7. Armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados: PostgreSQL e MySQL;
 - 1.9.61.8. Permitir a definição de permissionamento, no mínimo, para os modos de visualização e edição de políticas;
 - 1.9.61.9. 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;
 - 1.9.61.10. Possuir dashboards para facilidade de monitoração, as quais poderão ser customizados pelo usuário;
 - 1.9.61.11. Possuir a capacidade de criar políticas de forma global para todas as máquinas virtuais, por perfis e individualmente para cada host;
 - 1.9.61.12. Permitir a criação/utilização de tags pré-definidas para o agrupamento e aplicação de políticas aos hosts segundo características comuns;
 - 1.9.61.13. Permitir o envio de eventos da console via SNMP;
 - 1.9.61.14. Permitir o rollback de atualização de regras pela console de gerenciamento;
 - 1.9.61.15. Gerar pacote de auto-diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
 - 1.9.61.16. Possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;
 - 1.9.61.17. Possuir a capacidade de classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.

1.10. **Módulo de Gerenciamento de riscos de superfície de ataque para a nuvem**

- 1.10.1. Descoberta Contínua e Automatizada: Identificação em tempo real de ativos em ambientes on-premises, cloud e híbridos
- 1.10.2. Inventário Abrangente: Catalogação de dispositivos, domínios voltados para internet, endereços IP (IPv4 e IPv6), aplicações cloud, storage em nuvem, containers e workloads
- 1.10.3. Ativos Não Gerenciados: Detecção de recursos desconhecidos, não gerenciados

e de terceiros

- 1.10.4. Suporte Multi-Cloud: Compatibilidade com AWS, Microsoft Azure e Google Cloud Platform
- 1.10.5. APIs e Microserviços: Identificação e avaliação de riscos em APIs e arquiteturas baseadas em containers
- 1.10.6. Avaliação Contínua de Configuração: Monitoramento em tempo real de configurações de segurança em nuvem
- 1.10.7. Detecção de Configurações Incorretas: Identificação automática de misconfigurations em recursos cloud
- 1.10.8. Conformidade Regulatória: Suporte a frameworks como SOC 2, PCI DSS, CIS Benchmarks, AWS Well-Architected Framework
- 1.10.9. Gerenciamento de Políticas: Aplicação uniforme de melhores práticas de segurança em ambientes multi-cloud
- 1.10.10. Remediação Guiada: Recomendações automatizadas para correção de problemas identificados
- 1.10.11. Pontuação de Risco Contextual: Sistema de scoring inteligente baseado em criticidade do ativo, atividade de ameaças e impacto nos negócios
- 1.10.12. Análise de Caminhos de Ataque: Visualização de potenciais vetores de ataque e exposições
- 1.10.13. Priorização Baseada em IA: Algoritmos de machine learning para priorizar riscos com base no contexto organizacional
- 1.10.14. Métricas de Exposição: Índices de risco, ataque e exposição para tracking de pressão de ataques
- 1.10.15. Detecção de Ameaças: Identificação proativa de atividades maliciosas em ambientes cloud
- 1.10.16. Correlação de Sinais: Análise integrada de telemetria de múltiplas camadas de segurança
- 1.10.17. Resposta Automatizada: Playbooks de segurança orientados por IA para contenção e remediação
- 1.10.18. Investigação Avançada: Ferramentas de threat hunting com visualizações interativas e mapeamento MITRE ATT&CK
- 1.10.19. Gerenciamento de Entitlements: Visibilidade centralizada de permissões e direitos de acesso em nuvem
- 1.10.20. Detecção de Privilégios Excessivos: Identificação de identidades com permissões além do necessário
- 1.10.21. Análise de Riscos de Identidade: Avaliação de riscos associados a contas de usuário e service accounts
- 1.10.22. Controle de Acesso Zero Trust: Implementação de princípios de menor privilégio
- 1.10.23. Inteligência Artificial e Machine Learning
 - 1.10.23.1. Motor de IA proativo integrado para detecção preditiva de ameaças
 - 1.10.23.2. Detecção de anomalias baseada em padrões de comportamento
 - 1.10.23.3. Threat Intelligence: Insights contextuais da rede global de pesquisa
 - 1.10.23.4. Previsão de Ameaças: Capacidade de antecipar movimentos de adversários
- 1.10.24. Integração e Orquestração

- 1.10.24.1. APIs RESTful: Interfaces de programação para integração com ferramentas de terceiros
- 1.10.24.2. Automation Center: Plataforma para automação de workflows de segurança
- 1.10.24.3. SIEM Integration: Conectividade nativa com soluções SIEM existentes
- 1.10.24.4. DevSecOps Integration: Integração com pipelines de CI/CD e ferramentas DevOps
- 1.10.24.5. Third-Party Connectors: Integração com ferramentas de segurança e TI existentes
- 1.10.25. Relatórios e Dashboards
 - 1.10.25.1. Dashboards Executivos: Visões customizáveis para diferentes stakeholders (CISO, CIO, SecOps)
 - 1.10.25.2. Relatórios de Conformidade: Documentação automática de compliance com padrões regulatórios
 - 1.10.25.3. Métricas de Negócio: KPIs alinhados com objetivos organizacionais
 - 1.10.25.4. Visualizações Interativas: Gráficos e mapas para análise visual de dados
- 1.10.26. Métodos de Coleta de Dados
 - 1.10.26.1. Agentless Scanning: Coleta de dados sem necessidade de instalação de agentes
 - 1.10.26.2. Native Telemetry: Integração direta com APIs dos provedores de nuvem
 - 1.10.26.3. Network Scanning: Varredura de rede para descoberta de ativos
 - 1.10.26.4. Cloud Connectors: Conectores especializados para cada provedor de nuvem
- 1.10.27. Segurança da Plataforma
 - 1.10.27.1. Criptografia: Dados em trânsito e em repouso protegidos com criptografia avançada
 - 1.10.27.2. Autenticação: Suporte a SSO, MFA e integração com provedores de identidade
 - 1.10.27.3. Controle de Acesso: RBAC (Role-Based Access Control) granular
 - 1.10.27.4. Auditoria: Logs detalhados de todas as atividades da plataforma
- 1.10.28. Plataformas Cloud Suportadas
 - 1.10.28.1. Amazon Web Services (AWS): Integração completa com serviços AWS
 - 1.10.28.2. Microsoft Azure: Conectividade nativa com recursos Azure
 - 1.10.28.3. Google Cloud Platform (GCP) - Suporte abrangente;
 - 1.10.28.4. Huawei Cloud - Suporte abrangente;
 - 1.10.28.5. IBM Cloud - Suporte abrangente;
 - 1.10.28.6. Oracle Cloud - Suporte abrangente.

2. SOLUÇÃO DE SEGURANÇA - REQUISITOS DE SEGURANÇA

- 2.1. Observar as diretrizes e procedimentos de Segurança da PRF, bem como o disposto em suas Normas Complementares;
- 2.2. Obedecer a todas as normas e procedimentos de segurança implementados no ambiente de TI da PRF;
- 2.3. As pessoas envolvidas na execução das atividades terão acesso às instalações da PRF por

meio de credenciais emitidas pela Administração e deverão executar as atividades em ambiente definido pela DISC, estando sujeitos, além do uso de crachás, a todas as formas de controles de acesso às dependências da instituição, tais como atendimento aos horários de expediente, vistoria de objetos que estejam portando, etc.; e

2.4. O acesso a áreas restritas por técnicos da contratada, obedecerá ao previsto nas normativas da PRF.

3. SOLUÇÃO DE SEGURANÇA - REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

3.1. As pessoas envolvidas na execução das atividades deverão, durante sua permanência dentro das instalações da PRF, se adequar às regras, costumes e normas internas que definem a conduta profissional e pessoal de servidores, colaboradores e visitantes da instituição.

3.2. Toda a documentação (manuais, etc.), bem como o sistema operacional dos equipamentos deverão estar em português.

3.3. O atendimento aos chamados de assistência técnica, por qualquer meio de comunicação, deverá ser efetuado em língua portuguesa.

3.4. A empresa CONTRATADA deverá observar o disposto na IN nº 01/2010-SLTI/MPOG referente a sustentabilidade ambiental.

3.5. O descumprimento de normas ambientais constatadas durante a execução do Contrato será comunicado pela PRF ao órgão de fiscalização do Distrito Federal ou da União.

4. SOLUÇÃO DE SEGURANÇA - METODOLOGIA DE TRABALHO

4.1. Serviços de Garantia e atualização (update/upgrade) da solução de segurança

4.1.1. A implantação e configuração deverão ser realizadas conforme disposto no Termo de Referência.

4.1.2. As rotinas de recebimento provisório e definitivo do objeto deverão observar as disposições do Termo de Referência.

4.1.3. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

4.1.4. Os requisitos de garantia para a solução estão no descritos no item 5.1 deste Anexo.

5. SOLUÇÃO DE SEGURANÇA - ESTIMATIVA DE VOLUME DE BENS / SERVIÇO

5.1. Garantia / atualização (update/upgrade) da solução de segurança por 12 (doze) meses, prorrogáveis em consonância com o contrato.

5.2. Suporte Técnico Local ou Remoto 24x7, por 12 meses. Estimativa: 12 (doze) meses, prorrogáveis em consonância com o contrato.

5.2.1. Os serviços de suporte técnico e manutenção deverão ser prestados a partir do início do fornecimento da subscrição da solução sendo que os prazos para atendimento dos chamados de suporte servirão como referência para medição de seus níveis de serviço.

5.2.2. A Contratada deverá enviar, sempre que disponibilizado pelo fabricante, as atualizações de versão, corretivas ou evolutivas, do software e/ou das bibliotecas para identificação de vulnerabilidades utilizadas nas análises e testes de segurança.

5.2.3. Para fins de medição dos serviços, a Contratada deverá entregar até o 5º (quinto) dia do mês subsequente ao da prestação dos serviços, o Relatório de Suporte Técnico e Manutenção Tecnológica apresentando:

5.2.3.1. Atualizações disponibilizadas no período;

5.2.3.2. Atualizações instaladas no período;

5.2.3.3. Relação dos chamados de suporte técnico;

5.2.3.4. Nome do requisitante;

- 5.2.3.5. Data de abertura do chamado;
- 5.2.3.6. Histórico do atendimento;
- 5.2.3.7. Data de encerramento;
- 5.2.3.8. Demais informações que sejam pertinentes à PRF

5.2.4. Deverá ser disponibilizado ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.

6. SOLUÇÃO DE SEGURANÇA - PRAZOS E CONDIÇÕES

6.1. Conforme disposto no e Termo de e no Anexo I-I Nível Mínimo de serviço.

7. SOLUÇÃO DE SEGURANÇA - VISTORIA, ENTREGA, ACEITE, ALTERAÇÃO E CANCELAMENTO

7.1. Vistoria

7.1.1. As licitantes poderão realizar vistoria técnica para fins de verificação do ambiente.

7.1.2. A vistoria deverá ser previamente agendada pelo telefone (0xx61) 2025-6823 com a DISC, no horário de 9:00 às 12:00 e de 14:00 às 17:00 horas, de segunda-feira a sexta-feira, no Edifício Sede da PRF em SPO, Quadra 03, Lote 05 - Complexo Sede da PRF - Brasília – DF.

7.2. Condições de Entrega

7.2.1. O objeto do contrato deverá ser entregue na DISC no Complexo da Sede da PRF em SPO, Quadra 03, Lote 5 - Brasília - DF, no horário de 08:00 às 17:00 horas.

7.3. Condições de Aceite

7.3.1. A Contratada deverá fornecer as informações necessárias para acesso à área de suporte no endereço eletrônico (website) do fabricante que contenha a documentação técnica (guias de instalação/configuração atualizados, FAQ's, etc.) e atualizações;

PRF

Documento assinado eletronicamente por **FABIO COVA MARTINS, Policial Rodoviário(a) Federal**, em 05/03/2026, às 16:18, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.

PRF

Documento assinado eletronicamente por **GISELE LIMA CARVALHO, Policial Rodoviário(a) Federal**, em 05/03/2026, às 16:20, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.

PRF

Documento assinado eletronicamente por **ANDRE LUIZ DE SOUZA ARRUDA, Policial Rodoviário(a) Federal**, em 05/03/2026, às 16:26, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.

PRF

Documento assinado eletronicamente por **GIOVANI AUGUSTO TAGLIAPIETRA, Policial Rodoviário(a) Federal**, em 05/03/2026, às 16:33, horário oficial de Brasília, com fundamento no art. 10, § 2º, da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020, e no art. 42 da Instrução Normativa nº 116/DG/PRF, de 16 de fevereiro de 2018.



A autenticidade deste documento pode ser conferida no site <https://sei.prf.gov.br/verificar>, informando o código verificador **71499944** e o código CRC **1336CF36**.



Referência: Processo nº 08650.032146/2025-38



SEI nº 71499944